



ACADEMIA DE  
**CIBERSEGURIDAD**

# Presentación e Introducción

**Academia de Ciberseguridad**

# WHOAMI



**Lead Auditor**



**CTIA**  
Certified Threat Intelligence Analyst



Certified Professional Penetration Tester



**CSA**  
Certified SOC Analyst

**CEH**  
Certified Ethical Hacker  
**MASTER**  
Computer

**CFI**  
Hacking Forensic INVESTIGATOR



# Módulos que vamos a tener

- Módulo 1: Fundamentos de seguridad y redes informáticas
- Módulo 2: Fundamentos de ciberamenazas
- Módulo 3: Introducción al Centro de Operaciones de Seguridad
- Módulo 4: Componentes y arquitectura del SOC
- Módulo 5: Introducción a la gestión de registros
- Módulo 6: Detección y análisis de incidentes
- Módulo 7: Inteligencia y búsqueda de amenazas
- Módulo 8: Respuesta y gestión de incidentes



# Días y fecha de clases

- Clase #1 Sábado 20 de Septiembre
- Clase #2 Domingo 21 de Septiembre
- Clase #3 Sábado 27 de septiembre
- Clase #4 Domingo 28 de Septiembre
- Clase #5 Sábado 4 de Octubre





ACADEMIA DE  
**CIBERSEGURIDAD**

# Módulo #1

Redes de Computadora y Fundamentos de Ciberseguridad

**Academia de Ciberseguridad**

# Evolución de los Centros de Cómputo

En el pasado, los centros de cómputo eran **centralizados**, con todos los recursos ubicados en un solo lugar físico.

Con el crecimiento de las organizaciones y la demanda de servicios en línea, estos centros evolucionaron hacia **centros de datos distribuidos**, donde múltiples servidores trabajan de forma interconectada.

Esto permite **mayor disponibilidad, escalabilidad y resiliencia**, asegurando que los servicios se mantengan operativos incluso si una parte de la infraestructura falla.



# Introducción al SOC (Security Operations Center)

Un **SOC (Centro de Operaciones de Seguridad)** es el núcleo encargado de **monitorear, detectar, responder y prevenir incidentes de seguridad** en una organización.

Para comprender su funcionamiento, es fundamental tener **conocimientos básicos de computación, redes y arquitectura de sistemas**, ya que el SOC depende de estos elementos para operar de forma efectiva.

Su objetivo principal es **proteger los activos digitales**, garantizar la continuidad de negocio y coordinar las acciones ante amenazas cibernéticas.



# Fundamentos de Redes de Computadoras

Una **red de computadoras** conecta múltiples dispositivos para **compartir información y recursos**.

Estas redes pueden variar en tamaño, desde una pequeña red doméstica hasta redes globales como **Internet**.

Su función principal es permitir una **comunicación rápida y confiable**, utilizando diferentes tecnologías como cableado, conexiones inalámbricas, routers, switches y protocolos de comunicación.





# Redes Domésticas e IoT (Internet de las Cosas)

Las redes de computadoras se han expandido más allá de las empresas y organizaciones, llegando a los hogares.

Esto ha dado lugar a la integración de **dispositivos inteligentes** como cámaras, sistemas de seguridad, asistentes virtuales, electrodomésticos y otros equipos conectados.

Gracias a esta conectividad, se han creado **hogares inteligentes**, permitiendo mayor comodidad, control y automatización de tareas cotidianas. Esta evolución ha transformado la manera en la que las personas interactúan con la tecnología en su entorno doméstico.



# Desafíos de la Conectividad Global

Las redes corporativas necesitan **conectarse globalmente** para superar las limitaciones geográficas.

Uno de los principales retos es garantizar que estas conexiones sean **seguras y confiables**, permitiendo la transferencia de datos sin interrupciones.

- Las **VPNs (Virtual Private Networks)** se utilizan para unir redes dispersas alrededor del mundo, creando una conexión segura para el intercambio de información.
- Este proceso ayuda a mantener la **continuidad de las operaciones** y la comunicación entre sedes internacionales.
- La correcta implementación de estas tecnologías es esencial para proteger la información corporativa frente a amenazas externas.



# Escalabilidad en la Arquitectura Cliente-Servidor

La arquitectura **cliente-servidor** está diseñada para manejar **una gran cantidad de clientes de manera simultánea**.

Gracias a esta estructura:

- Los servidores centrales pueden **recibir, procesar y responder solicitudes** de múltiples clientes al mismo tiempo.
- Esto permite **flexibilidad y crecimiento**, adaptándose a organizaciones en expansión y a entornos de red de gran escala.



# Dependencia de las Redes de Computadoras

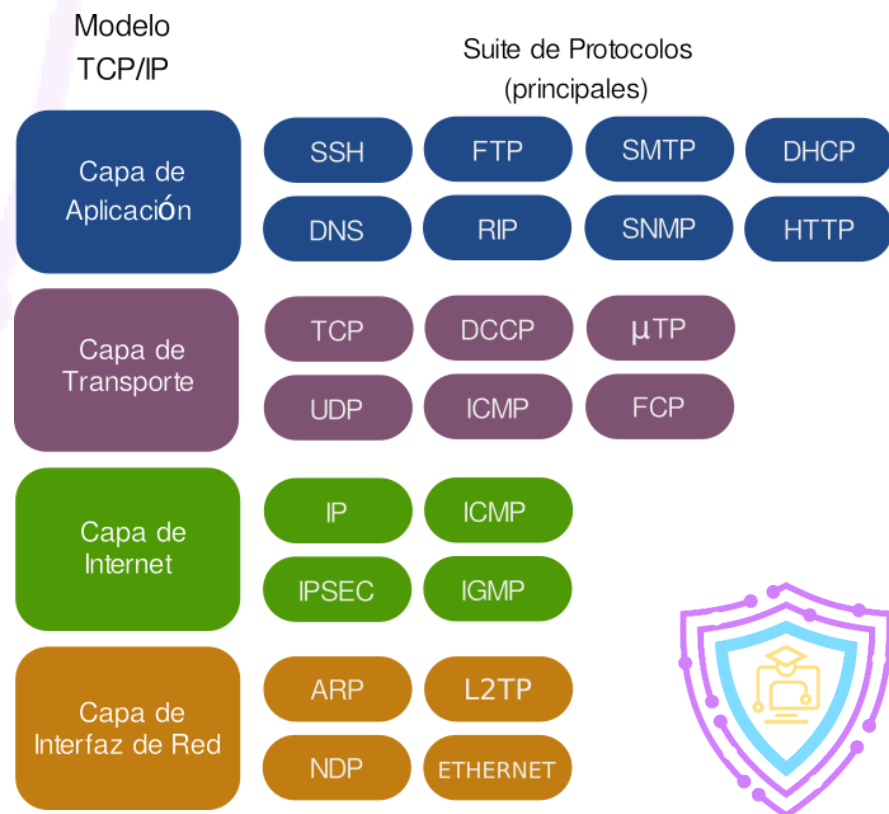
Actualmente, las empresas dependen de las redes para llevar a cabo sus **operaciones diarias**, desde la comunicación interna hasta la prestación de servicios críticos.

- Una **interrupción en la red** puede ocasionar graves consecuencias como pérdida de productividad, interrupción de servicios y daños económicos.
- Este nivel de dependencia resalta la **importancia de mantener la red confiable y segura**, con planes de contingencia y monitoreo constante.



# Modelo TCP/IP

El **modelo TCP/IP** es la base sobre la cual se diseñan y operan las redes de computadoras modernas. Se compone de **cuatro capas**, cada una con funciones específicas que permiten la transmisión de datos desde un dispositivo de origen hasta un dispositivo de destino.



# Capa de Aplicación (Application Layer)

Es la capa más cercana al usuario y sirve como **interfaz entre las aplicaciones y la red**. Define cómo los programas se comunican y establecen las reglas de intercambio de información.

## Protocolos principales:

- HTTP / HTTPS** → Navegación web segura.
- FTP** → Transferencia de archivos.
- SMTP** → Envío de correos electrónicos.
- DNS** → Resolución de nombres de dominio.

Cuando un usuario accede a [www.google.com](http://www.google.com), el navegador utiliza:

- DNS para convertir el nombre en una dirección IP.
- HTTP/HTTPS para solicitar y recibir el contenido de la página web.



# Capa de Transporte (Transport Layer)

Garantiza la **comunicación extremo a extremo** entre el dispositivo emisor y el receptor. Administra el **control de flujo, segmentación de datos y detección de errores**.

## •Protocolos principales:

- **TCP (Transmission Control Protocol):**
  - Confiable y orientado a la conexión.
  - Asegura que los datos lleguen completos y en el orden correcto.
  - Ejemplo: Navegar por un sitio web o descargar un archivo.
- **UDP (User Datagram Protocol):**
  - Más rápido pero sin control de errores.
  - Adecuado para transmisión en tiempo real.
  - Ejemplo: Streaming de video o videollamadas.
- **RTP (Real-time Transport Protocol):**
  - Optimizado para audio y video en tiempo real

## Ejemplo práctico:

**TCP:** Al descargar un archivo desde un servidor FTP, TCP verifica que cada parte llegue correctamente antes de reconstruir el archivo.

**UDP:** En una videollamada, si algunos paquetes se pierden, no se reenvían para evitar retrasos.



# Capa de Internet (Internet Layer)

Se encarga de **direccionar y enrutar los paquetes** a través de diferentes redes hasta llegar a su destino.

## •Protocolos principales:

- **IP (IPv4 / IPv6):** Define las direcciones únicas de cada dispositivo.
- **ICMP:** Diagnóstico y mensajes de error (ejemplo: comando *ping*).
- **ARP:** Traduce direcciones IP a direcciones físicas (MAC).
- **RARP:** Hace la traducción inversa de MAC a IP.

## •Ejemplo práctico:

- Cuando haces *ping* a un servidor, ICMP se encarga de enviar mensajes de prueba y recibir respuestas para verificar la conectividad.





# Capa de Enlace o Acceso a la Red

Administra la **conexión física** entre dispositivos que se encuentran en la **misma red**.  
Controla el **envío y recepción de datos**, gestionando:

- Encapsulación de la información en tramas.
- Direccionamiento físico mediante direcciones **MAC**.
- Detección de errores básicos en la transmisión.

## •Ejemplo práctico:

- En una red doméstica, esta capa maneja la comunicación entre una computadora y el router a través de Wi-Fi o cable Ethernet.
- Cuando envías datos a otro equipo en la misma red, primero se usa la dirección MAC para asegurarse de que el paquete llegue correctamente.



# Modelo OSI

El **Modelo OSI (Open Systems Interconnection)** es un marco de referencia desarrollado por la **ISO (International Organization for Standardization)** para **entender y estandarizar la comunicación en redes.**

- Divide la comunicación en **7 capas**, cada una con funciones específicas.
- Permite que diferentes dispositivos y tecnologías se comuniquen **de manera organizada y compatible.**
- Es esencial para:
  - Diseñar redes eficientes y escalables.
  - Desarrollar protocolos de comunicación.
  - Solucionar problemas de conectividad.



# Tipos de Redes

El objetivo de esta sección es **explicar los diferentes modelos y tipos de redes**, comprendiendo sus funcionalidades y aplicaciones.

Esto permite **elegir la arquitectura de red más adecuada** para cada escenario y necesidad específica, considerando factores como escalabilidad, tamaño y alcance geográfico.



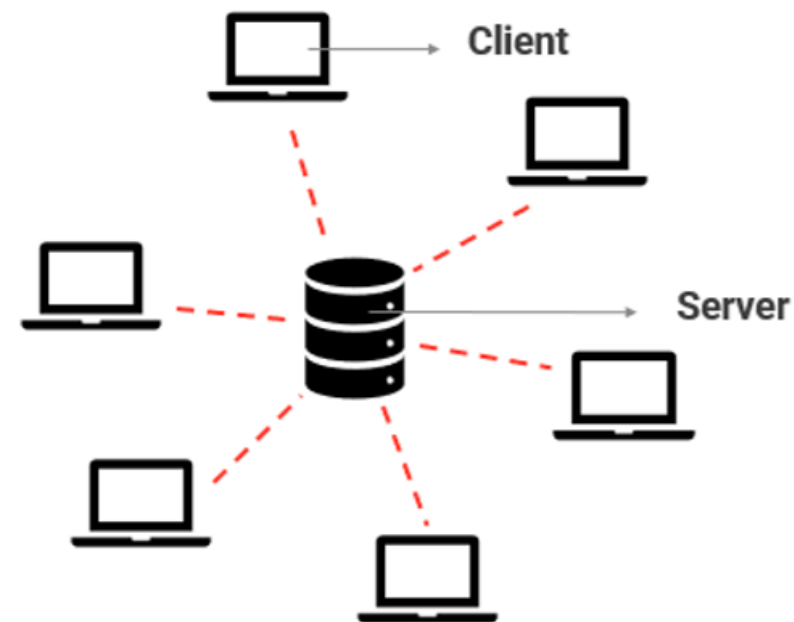
# Modelo Cliente/Servidor (Client/Server Model)

## •Cliente (Client):

- Dispositivo o aplicación que **solicita servicios o recursos** a un servidor.
- Puede ser una computadora, un teléfono móvil u otro dispositivo conectado.
- Utiliza aplicaciones como navegadores web, clientes de correo electrónico o programas de transferencia de archivos.

## •Servidor (Server):

- Sistema que **proporciona servicios, datos o recursos** a múltiples clientes.
- Diseñado para manejar múltiples solicitudes de forma simultánea.
- Tipos de servidores:
  - **Web server** (páginas web).
  - **Email server** (correo electrónico).
  - **File server** (archivos compartidos).
  - **Database server** (bases de datos).



# Tipos de Redes por Tamaño y Alcance

Las redes se clasifican según **su tamaño, extensión geográfica y escalabilidad**:

## 1. PAN (Personal Area Network):

1. Conecta dispositivos personales como teléfonos, laptops y tablets.
2. Alcance muy reducido (generalmente algunos metros).
3. Ejemplo: conexión por Bluetooth entre un celular y unos audífonos.

## 2. LAN (Local Area Network):

1. Conecta dispositivos dentro de un área pequeña, como una casa u oficina.
2. Usada comúnmente en empresas y redes domésticas.
3. Ejemplo: red de computadoras en una empresa conectadas a un servidor central.

## 3. WLAN (Wireless Local Area Network):

1. Similar a una LAN pero sin cables, utilizando Wi-Fi.
2. Permite movilidad dentro de un área determinada, como una oficina o cafetería.

## 4. MAN (Metropolitan Area Network):

1. Cubre un área geográfica mayor, como **una ciudad completa**.
2. Ejemplo: red de fibra óptica que conecta diferentes sedes de una empresa en la misma ciudad.

## 5. WAN (Wide Area Network):

1. Red de gran alcance, que puede cubrir **países o incluso continentes**.
2. Ejemplo: Internet es la **WAN más grande del mundo**.



# Controles de Seguridad en Redes

Los **controles de seguridad en redes** son **medidas y mecanismos de protección** implementados para proteger la **infraestructura de red** contra accesos no autorizados, ataques y amenazas de ciberseguridad.

Su objetivo es garantizar la **confidencialidad, integridad y disponibilidad (CIA)** de los datos, asegurando que la información esté protegida mientras se transmite y se almacena.

Estos controles regulan y monitorean el tráfico de red, aplican políticas de seguridad, y ayudan a **detectar, prevenir y mitigar riesgos y vulnerabilidades**.



# Ejemplos de Controles de Seguridad en Redes

Entre las soluciones más comunes para proteger la infraestructura de red se incluyen:

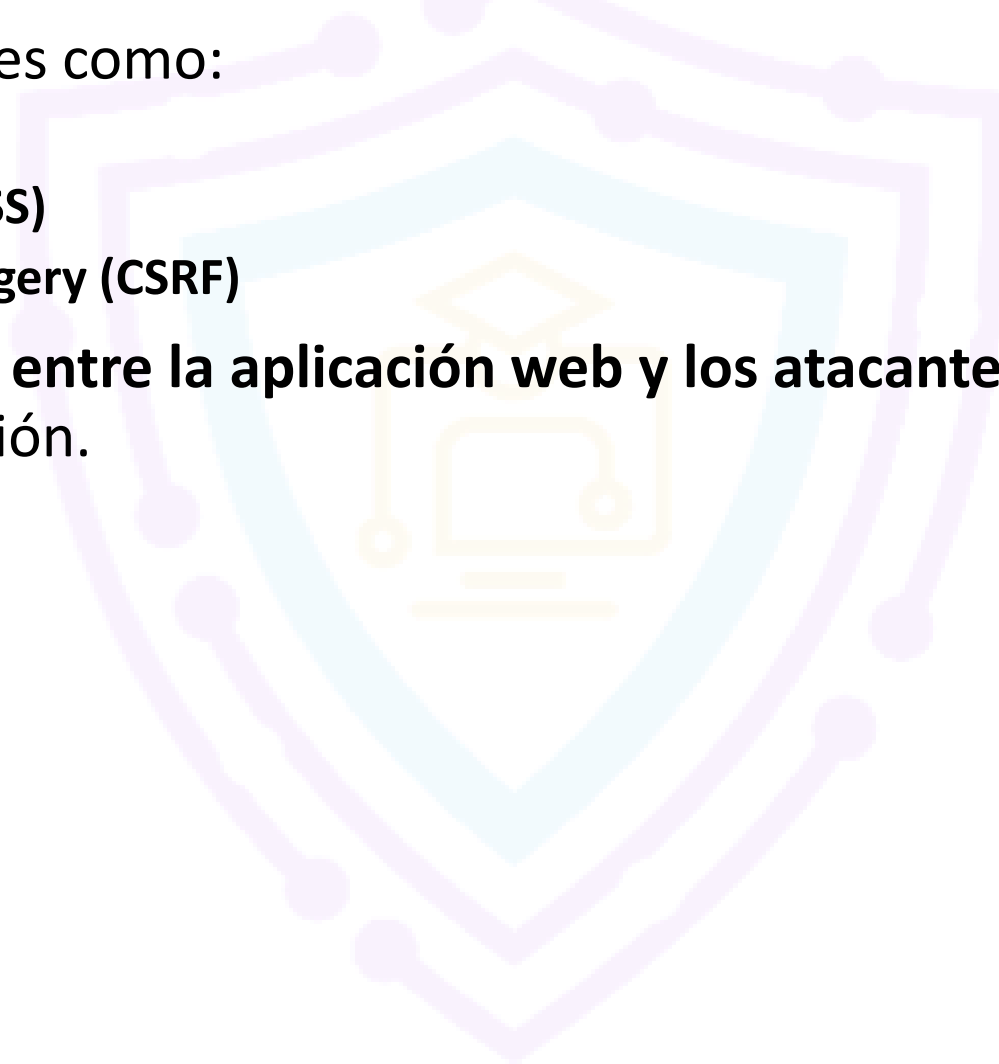
- **Firewalls (Cortafuegos)**
- **WAF (Web Application Firewall)**
- **IPS (Intrusion Prevention System)**
- **VPN (Virtual Private Network)**
- **NAC (Network Access Control)**
- **Antivirus y Antimalware**
- **Segmentación de Red (Network Segmentation)**
- **Cifrado de Red (Network Encryption)**
- **SIEM (Security Information and Event Management)**

Cada una cumple un papel específico en la defensa contra amenazas y ataques.



# Web Application Firewall (WAF)

- Protege las aplicaciones web filtrando y monitoreando el tráfico **HTTP y HTTPS**.
- Bloquea ataques comunes como:
  - **SQL Injection**
  - **Cross-Site Scripting (XSS)**
  - **Cross-Site Request Forgery (CSRF)**
- Actúa como una **barrera entre la aplicación web y los atacantes**, asegurando la integridad de la información.





# Firewalls (Cortafuegos)

- Controlan y monitorean el tráfico de red **entrante y saliente** según reglas predefinidas.

- **Tipos principales:**

- **Firewalls de hardware:**

- Ubicados en el **perímetro de la red** para proteger contra amenazas externas.

- **Firewalls de software:**

- Instalados en **dispositivos individuales** como una capa extra de protección.

**Función clave:**

Bloquear accesos no autorizados y actividades maliciosas.



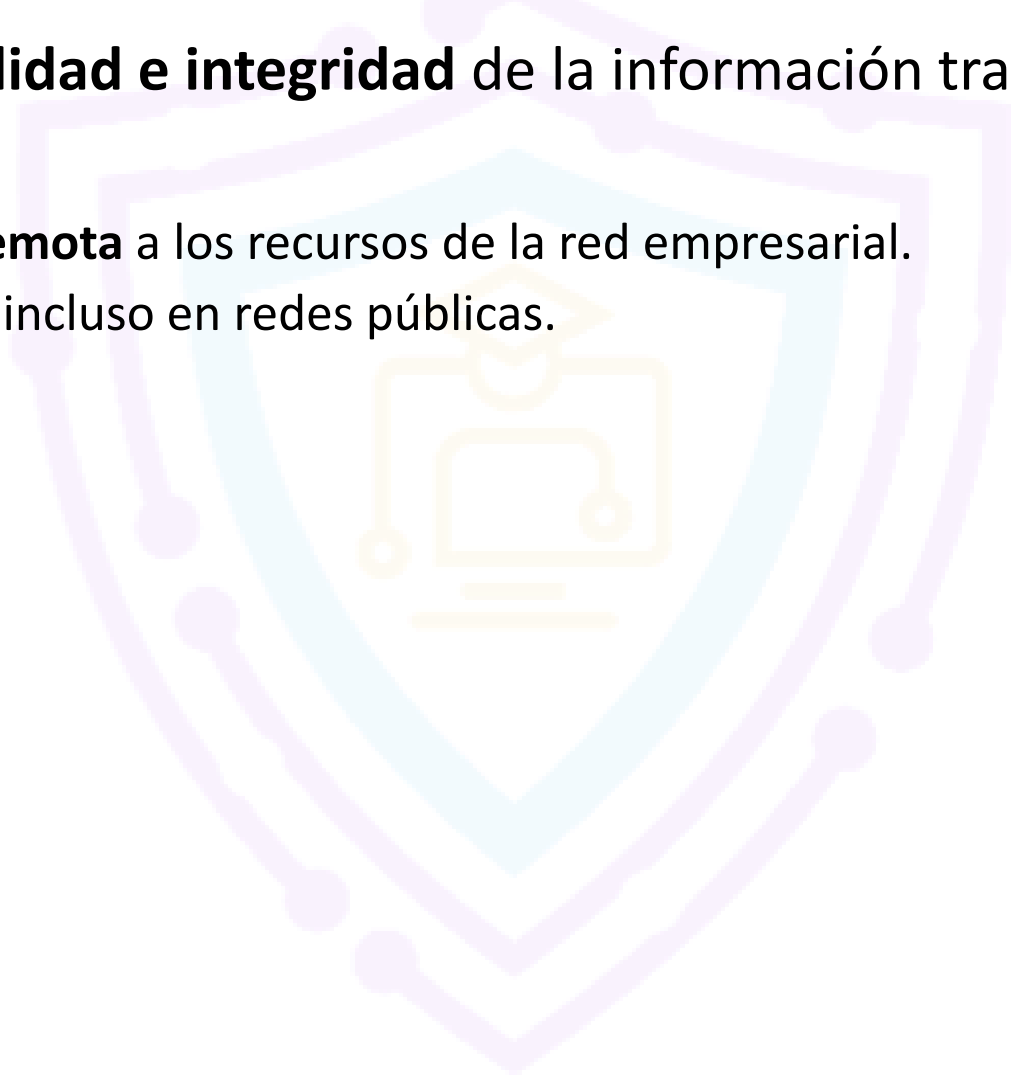
# Intrusion Prevention System (IPS)

- Solución **proactiva** que identifica y previene **actividades sospechosas o maliciosas**.
- Monitorea el tráfico de red en tiempo real y bloquea amenazas antes de que afecten la infraestructura.
- Puede operar:
  - A nivel de **red**, protegiendo múltiples dispositivos.
  - A nivel de **host**, defendiendo un sistema específico.



# Virtual Private Network (VPN)

- Crea un **canal seguro de comunicación** sobre Internet mediante el cifrado de datos.
- Garantiza la **confidencialidad e integridad** de la información transmitida.
- Permite a los usuarios:
  - Conectarse de forma **remota** a los recursos de la red empresarial.
  - Mantener la seguridad incluso en redes públicas.



# Network Access Control (NAC)

- Controla y gestiona el **acceso a la red** basándose en políticas de seguridad.

- **Funcionalidades:**

- Verifica la **autenticación** de usuarios y dispositivos.
- Evalúa el **cumplimiento de políticas** antes de permitir la conexión.
- Previene accesos no autorizados y brechas de seguridad.



# Segmentación de Red (Network Segmentation)

- Divide la red en **segmentos separados** para:

- Limitar el **movimiento lateral de amenazas**.
- Aislar activos críticos.

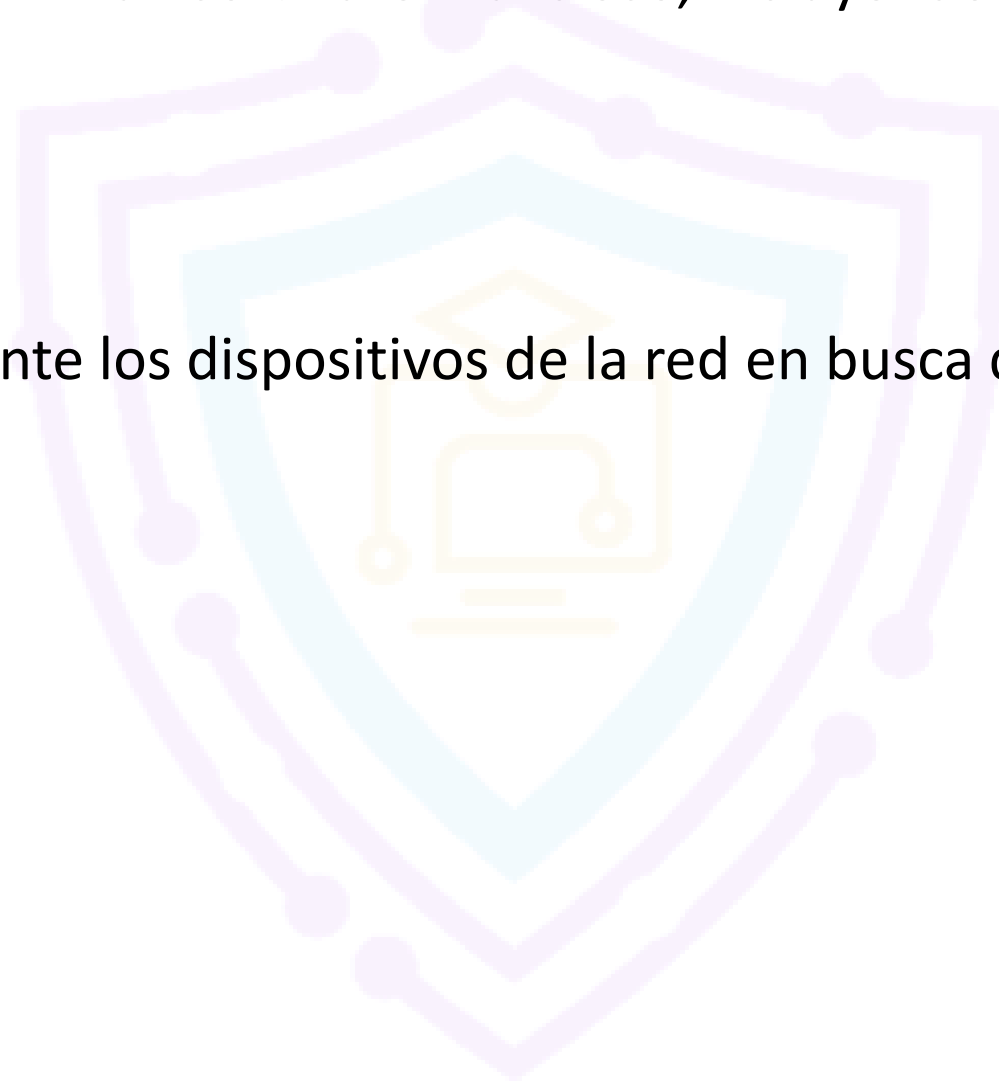
- Se implementa mediante:

- **Segmentación física** (hardware independiente).
- **VLANs** (Virtual Local Area Networks).



# Antivirus y Antimalware

- Detectan, previenen y eliminan software malicioso, incluyendo:
  - **Virus**
  - **Ransomware**
  - **Spyware**
  - **Troyanos**
- Monitorean continuamente los dispositivos de la red en busca de comportamientos sospechosos.



# Cifrado de Red (Network Encryption)

- Protege los datos **en tránsito**, evitando que sean interceptados por atacantes.
- Convierte la información en un **formato codificado** que solo puede descifrar un destinatario autorizado.

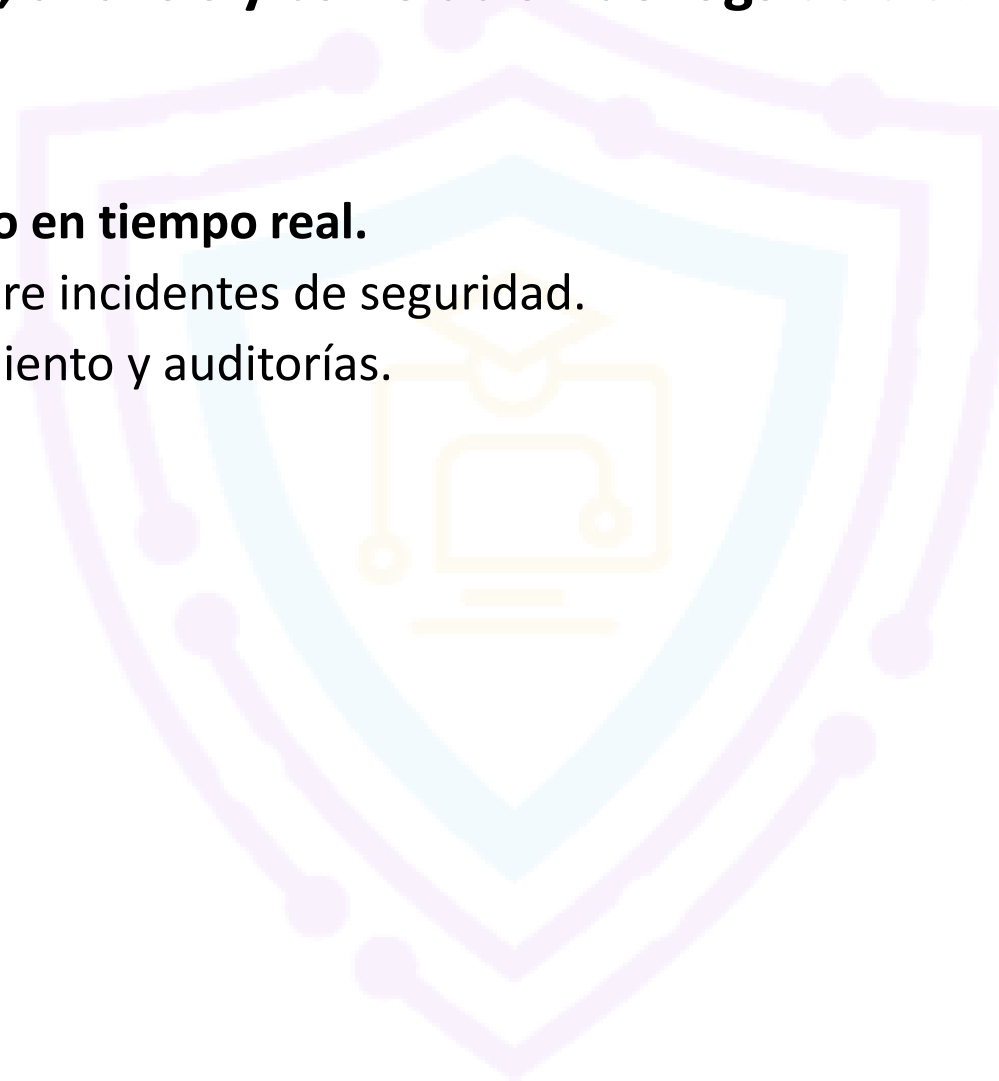
## Protocolos comunes:

- **SSL/TLS**: para navegación web segura.
- **IPSec**: para asegurar conexiones a nivel de red.



# Security Information and Event Management (SIEM)

- Centraliza la **recolección, análisis y correlación de logs** de distintos dispositivos y sistemas de la red.
- Proporciona:
  - **Monitoreo centralizado en tiempo real.**
  - **Alertas inmediatas** sobre incidentes de seguridad.
  - Reportes para cumplimiento y auditorías.





# Seguridad en Windows

**Windows Security** es un conjunto completo de **herramientas y características** diseñadas para proteger los sistemas operativos Microsoft Windows. Proporciona una **defensa en múltiples capas** contra riesgos de seguridad, asegurando la **confidencialidad, integridad y disponibilidad** de los datos.



# Componentes Clave de Windows Security

Los principales componentes de seguridad que ofrece Windows son:

- 1. Protección contra Malware (Malware Protection)**
- 2. Autenticación de Usuarios (User Authentication)**
- 3. Control de Acceso (Access Control)**
- 4. Cifrado y Protección de Datos (Encryption and Data Protection)**

Cada uno cumple un rol específico para mantener la seguridad integral del sistema.



# Protección contra Malware

La protección contra malware se centra en **detectar, prevenir y eliminar software malicioso**, como:

- Virus
- Ransomware
- Spyware
- Troyanos

Estas herramientas trabajan en tiempo real para proteger datos y recursos del sistema.



# Principales herramientas de protección:

## •Windows Defender Antivirus:

Antivirus integrado que opera en segundo plano, detectando y eliminando amenazas automáticamente.

## •Windows Defender SmartScreen:

Protege contra **phishing** y descargas maliciosas, analizando sitios web y archivos en busca de amenazas.

## •Microsoft Defender for Endpoint:

Solución empresarial que ofrece:

- Protección avanzada de endpoints.
- Gestión de vulnerabilidades.
- Respuesta automatizada ante incidentes.

## •Controlled Folder Access:

Función que **bloquea accesos no autorizados a carpetas críticas**, protegiendo contra ataques de ransomware.

## •Microsoft Defender Offline:

Herramienta que **analiza y elimina malware antes de que Windows se inicie**, operando fuera del sistema operativo.



# Autenticación de Usuarios

El proceso de autenticación verifica que **solo usuarios autorizados** puedan acceder a los recursos del sistema.

## Métodos de autenticación:

- **Multi-Factor Authentication (MFA):**

Requiere varios factores de verificación (contraseña, código SMS, biometría), añadiendo una capa extra de seguridad.

- **Smart Card Authentication:**

Usa tarjetas físicas con **certificados digitales** para una autenticación segura y portátil.

- **Biometric Authentication:**

Utiliza **rasgos físicos únicos** como huellas digitales o reconocimiento facial.

- **Windows Hello:**

Permite iniciar sesión de forma rápida y segura mediante **biometría o PIN**, sustituyendo las contraseñas tradicionales.



# Control de Acceso

El control de acceso gestiona **los permisos y derechos** que tienen los usuarios sobre recursos y datos, asegurando que solo realicen las acciones autorizadas.

## Métodos principales:

### •User Account Control (UAC):

Solicita confirmación o credenciales antes de permitir cambios en el sistema.

### •File and Folder Permissions:

Define qué usuarios o grupos pueden:

- Leer (Read)
- Escribir (Write)
- Ejecutar (Execute)

### •Security Groups:

Agrupar usuarios y dispositivos con necesidades de acceso similares para simplificar la administración de permisos.

### •Active Directory (AD) Security:

Centraliza la administración de usuarios, políticas y permisos en entornos empresariales.

### •Role-Based Access Control (RBAC):

Asigna permisos según el **rol** que desempeña el usuario en la organización.

### •Dynamic Access Control (DAC):

Asigna permisos dinámicos basados en atributos como:

- Identidad del usuario.
- Tipo de dispositivo.
- Clasificación de los datos.

### •AppLocker:

Restringe qué aplicaciones y archivos pueden ejecutarse en el sistema, bloqueando software no autorizado.



# Cifrado y Protección de Datos

El cifrado es esencial para proteger la **información sensible**, asegurando que solo usuarios autorizados puedan acceder a ella.

## Herramientas principales:

### •BitLocker:

Cifra **unidades de disco completas** para proteger datos en caso de pérdida o robo del equipo.

### •Encrypting File System (EFS):

Proporciona **cifrado a nivel de archivo o carpeta**, permitiendo que solo usuarios autorizados accedan a la información.

### •Windows Information Protection (WIP):

Previene fugas accidentales de datos mediante:

- Clasificación de información sensible.
- Control de acceso y de uso entre aplicaciones y dispositivos.

### •Windows Defender Credential Guard:

Protege credenciales de inicio de sesión contra malware y ataques, dificultando su robo por parte de atacantes.



# Seguridad en Linux

El objetivo de esta sección es explicar los **principios de seguridad en sistemas UNIX/Linux** y las **mejores prácticas** para protegerlos frente a accesos no autorizados y diversas amenazas.

UNIX y Linux son conocidos por su **sólida arquitectura de seguridad**, que se basa en varios componentes fundamentales que trabajan en conjunto para garantizar la protección de los sistemas y datos.





# Componentes Clave en la Seguridad de UNIX/Linux

## 1. Kernel (Núcleo del Sistema):

1. Es el **componente central** que gestiona todos los recursos del sistema.
2. Administra procesos, memoria, controladores y la comunicación con el hardware.
3. Garantiza la estabilidad y la seguridad en la ejecución de tareas.

## 2. Shell:

1. Proporciona la **interfaz de línea de comandos (CLI)** para que los usuarios interactúen con el sistema.
2. Interpreta los comandos y los envía al kernel para su ejecución.

## 3. Sistema de Archivos:

1. Organiza la información de forma **jerárquica** bajo la filosofía de que *“todo es un archivo”*.
2. Permite aplicar permisos y políticas de control de acceso.



# Características de Seguridad en UNIX/Linux

## •Autenticación de Usuarios:

- Uso de **nombre de usuario y contraseña** para controlar el acceso.
- Almacenamiento seguro de credenciales en archivos de configuración, con contraseñas encriptadas.

## •Gestión de Procesos:

- Cada proceso se identifica con un **PID (Process ID)** único.
- Soporte para **multitarea y entornos multiusuario**, permitiendo que varios usuarios trabajen de forma segura en un mismo sistema.

## •Sistema Robusto de Permisos:

- Control detallado de acceso a archivos y directorios mediante permisos **de lectura, escritura y ejecución**.
- Soporte para administración avanzada de usuarios y grupos.

## •Capacidades de Red Seguras:

- Herramientas integradas para la comunicación segura y la protección del tráfico de red.



# Buenas Prácticas de Seguridad en UNIX/Linux

## Gestión Segura de Usuarios:

Aplicar el **principio de privilegios mínimos** para limitar el acceso a lo estrictamente necesario.  
Crear roles y grupos con permisos definidos.

## Políticas de Contraseñas Fuertes:

Configurar contraseñas complejas y únicas.  
Forzar cambios periódicos.  
Utilizar herramientas para auditar la fortaleza de contraseñas.

## Control de Acceso a Archivos:

Asignar permisos correctos a cada archivo y directorio.  
Utilizar el comando `chmod` para modificar permisos y proteger información sensible.

## Seguridad en Acceso Remoto:

Configurar **SSH** de forma segura para administrar servidores.  
Deshabilitar métodos de autenticación inseguros como contraseñas simples.

## Monitoreo y Auditoría:

Revisar **logs y registros** en busca de actividad sospechosa.  
Implementar alertas y herramientas de monitoreo.

## Detección y Prevención de Intrusiones:

Instalar sistemas IDS/IPS que detecten y bloqueen intentos de intrusión.

## Cifrado de Datos:

Cifrar sistemas de archivos y datos sensibles para garantizar confidencialidad e integridad.

## Actualizaciones del Kernel y Paquetes:

Mantener el sistema y el kernel actualizados para protegerlo contra nuevas vulnerabilidades.



# Fundamentos de Aplicaciones Web

Este módulo explica los conceptos esenciales para **proteger las aplicaciones web contra amenazas cibernéticas**, abordando aspectos clave como la **arquitectura cliente-servidor**, el uso seguro de **HTTP/HTTPS**, la **autenticación de usuarios** y la **protección de datos**.

Las aplicaciones web son altamente expuestas a ataques debido a que interactúan directamente con los usuarios y suelen manejar **información sensible**, por lo que requieren controles de seguridad sólidos.



# Aspectos Clave para la Seguridad en Aplicaciones Web

- Arquitectura Cliente-Servidor.
- Prácticas de codificación segura.
- Autenticación y autorización de usuarios.
- Protección de datos sensibles.
- Actualizaciones regulares para mitigar vulnerabilidades.

Enfocarse en estos puntos permite **mantener la integridad y confiabilidad** tanto de la aplicación como de los datos de los usuarios.



# Arquitectura Cliente-Servidor

La arquitectura cliente-servidor divide las tareas y procesos entre dos componentes principales:

- **Cliente (Front-End):**

- Interfaz visible para el usuario (GUI).
- Maneja la interacción y el procesamiento local.

- **Servidor (Back-End):**

- Procesa las solicitudes recibidas.
- Ejecuta la lógica de negocio, consultas a bases de datos y genera respuestas.



# Proceso de interacción

- 1.El usuario inicia una solicitud desde el cliente (ejemplo: llenar un formulario o hacer clic en un enlace).
- 2.La solicitud viaja por la red hasta el servidor con los datos y parámetros necesarios.
- 3.El servidor procesa la solicitud:
  1. Ejecuta reglas de negocio.
  2. Realiza cálculos o consultas a bases de datos.
- 4.El servidor genera una respuesta con la información solicitada o el resultado de la acción.
- 5.La respuesta es enviada nuevamente al cliente, completando el ciclo.



# Cliente-Servidor en Seguridad

Una comunicación segura entre el cliente y el servidor es fundamental para prevenir:

- Interceptación de datos.
- Manipulación de información.
- Suplantación de identidad.

Esto se logra principalmente mediante **protocolos de seguridad** como HTTPS.





# HTTP y HTTPS

## HTTP (Hypertext Transfer Protocol)

Protocolo para **transmitir páginas web** y otros recursos en Internet.

Es **sin estado y sin conexión persistente**, lo que significa:

- El cliente envía una solicitud.

- El servidor responde.

- La conexión se cierra después de la transacción.

### Métodos HTTP comunes:

**GET:** Recupera datos de un recurso específico.

**POST:** Envía datos para ser procesados en el servidor.

**PUT:** Actualiza un recurso existente con nueva información.

**DELETE:** Elimina un recurso específico.

### HTTP Headers:

Contienen información adicional sobre la solicitud o respuesta.

Ejemplos:

- Tipo de contenido (Content-Type).

- Credenciales de autenticación.

- Instrucciones de caché.



# Importancia de los Estándares y Leyes de Seguridad

- Establecen **reglas claras y específicas** para proteger información crítica.
- Proveen **estructuras organizativas y técnicas** para la gestión de la ciberseguridad.
- Obligan a las empresas a cumplir con **normativas nacionales e internacionales**.
- Fomentan la **confianza** entre usuarios, clientes y entidades reguladoras.
- Ayudan a **prevenir y responder** ante incidentes de ciberseguridad.



Diseñada para **mejorar la ciberseguridad** de servicios en línea e infraestructura crítica.

- Establece:

- **Medidas de seguridad obligatorias** para proveedores de servicios digitales.
- **Protocolos de reporte** en caso de incidentes de ciberseguridad.

- Su objetivo es fortalecer la capacidad de respuesta ante amenazas que puedan afectar sectores esenciales.

**Aplicación:**

Servicios en sectores como energía, transporte, salud, finanzas y tecnología digital.



Ley enfocada en la **protección de la información de salud** de las personas.

• Se compone de dos reglas principales:

- **Security Rule:**

- Define cómo proteger electrónicamente los datos de salud.
- Establece controles para garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Privacy Rule:**

- Regula **quién puede acceder y usar la información médica.**
- Establece lineamientos para el consentimiento y la divulgación de datos.

## **Aplicación:**

Hospitales, clínicas, aseguradoras y cualquier entidad que maneje información médica.



# NIST SP 800-53 – Estados Unidos

Publicación creada por el **National Institute of Standards and Technology (NIST)**.

- Proporciona una **guía completa de controles de seguridad y privacidad** para sistemas de información federales.

- Incluye:

- Familias de controles organizados por categorías.
- Configuraciones base para la implementación segura de sistemas.

- Ayuda a:

- Establecer un sistema robusto de ciberseguridad en agencias gubernamentales.
- **Gestionar riesgos** relacionados con la información sensible.



# ISO/IEC 27001 – Estándar Internacional

Estándar reconocido a nivel mundial para la **implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (ISMS)**.

## •Objetivos principales:

- **Identificar riesgos** relacionados con la información.
- Establecer **controles de seguridad personalizados** para mitigarlos.
- Promover la **mejora continua** en la protección de la información.

## **Aplicación:**

Empresas de todos los sectores que busquen certificarse y demostrar compromiso con la seguridad de la información.



# Relación entre ISO/IEC 27001 y un SOC

## 1. Lo que exige la norma

- ISO/IEC 27001 define la creación de un **Sistema de Gestión de Seguridad de la Información (ISMS)**.
- Este sistema debe incluir:
  - Identificación y evaluación de riesgos.
  - Controles para prevenir, detectar y responder a incidentes.
  - Monitoreo y mejora continua de la seguridad.
  - Evidencia documentada de que los controles están funcionando.

En el **Anexo A** de la norma, hay controles relacionados con la **monitorización y respuesta a incidentes**, por ejemplo:

- **A.12.4 – Registro y monitoreo de eventos (Logging and monitoring).**
- **A.16 – Gestión de incidentes de seguridad de la información.**





ACADEMIA DE  
**CIBERSEGURIDAD**

# Módulo #2

## Fundamentos de Amenazas Cibernéticas

**Academia de Ciberseguridad**



# Amenazas Cibernéticas

En la era digital, las **amenazas cibernéticas** representan riesgos constantes para la **confidencialidad, integridad y disponibilidad (CIA)** de la información.

Estas amenazas han evolucionado significativamente con el tiempo, pasando de ser actividades de exploración tecnológica a convertirse en herramientas de **delito, espionaje y conflicto geopolítico**.



# Orígenes de las Amenazas Cibernéticas

- En los primeros días de la computación, **hacking** surgió como una actividad enfocada en la **exploración de sistemas**.
- Con el crecimiento de Internet:
  - Se **amplió la superficie de ataque** a nivel global.
  - Las amenazas comenzaron a propagarse de forma rápida y masiva.
- Las motivaciones se diversificaron:
  - **Curiosidad y aprendizaje.**
  - **Ganancias financieras** (cibercrimen, ransomware, fraude).
  - **Agendas políticas** (hacktivismo, ciberespionaje).
  - **Conflictos ideológicos y geopolíticos.**

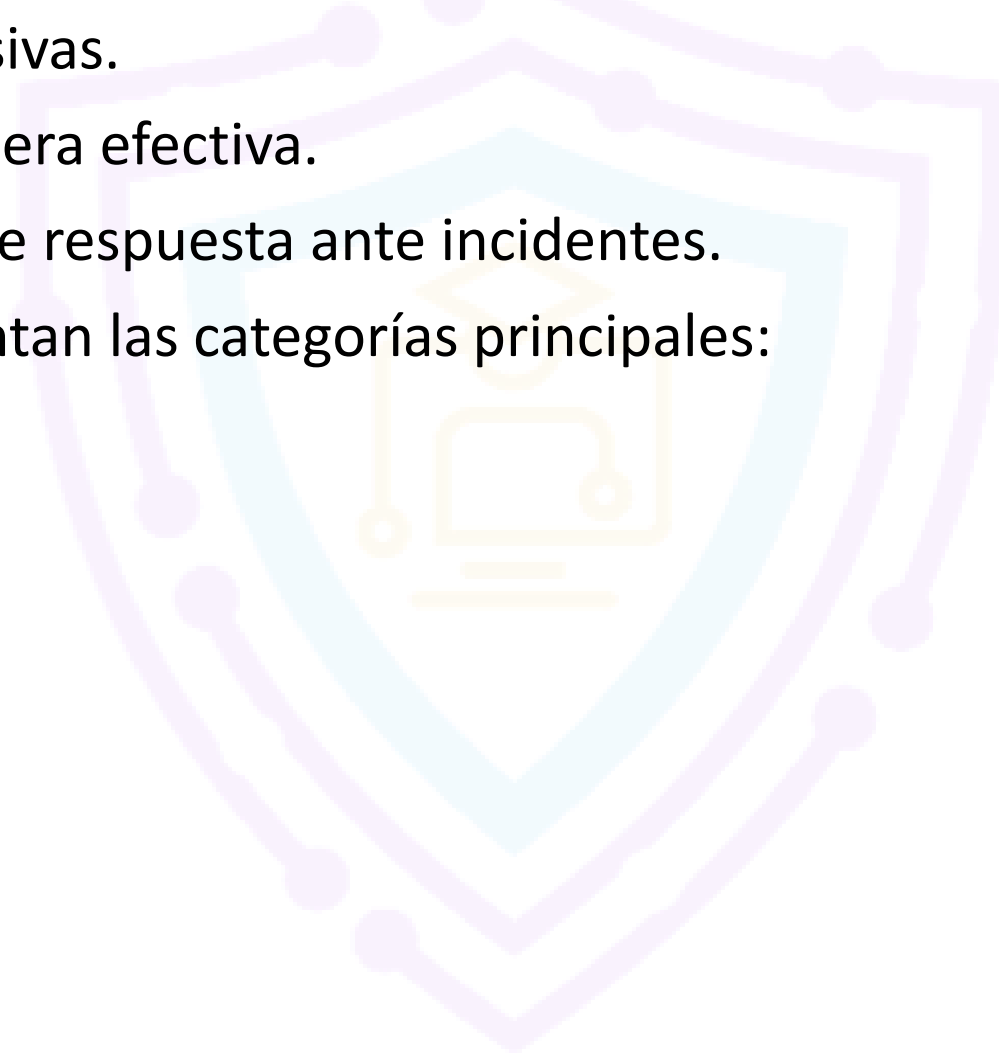


# Clasificación de las Amenazas Cibernéticas

Clasificar las amenazas permite a las organizaciones:

- Priorizar medidas defensivas.
- Asignar recursos de manera efectiva.
- Desarrollar estrategias de respuesta ante incidentes.

A continuación, se presentan las categorías principales:



# Malware (Software Malicioso)

El término **malware** abarca programas diseñados para infiltrarse y dañar sistemas informáticos.

Incluye:

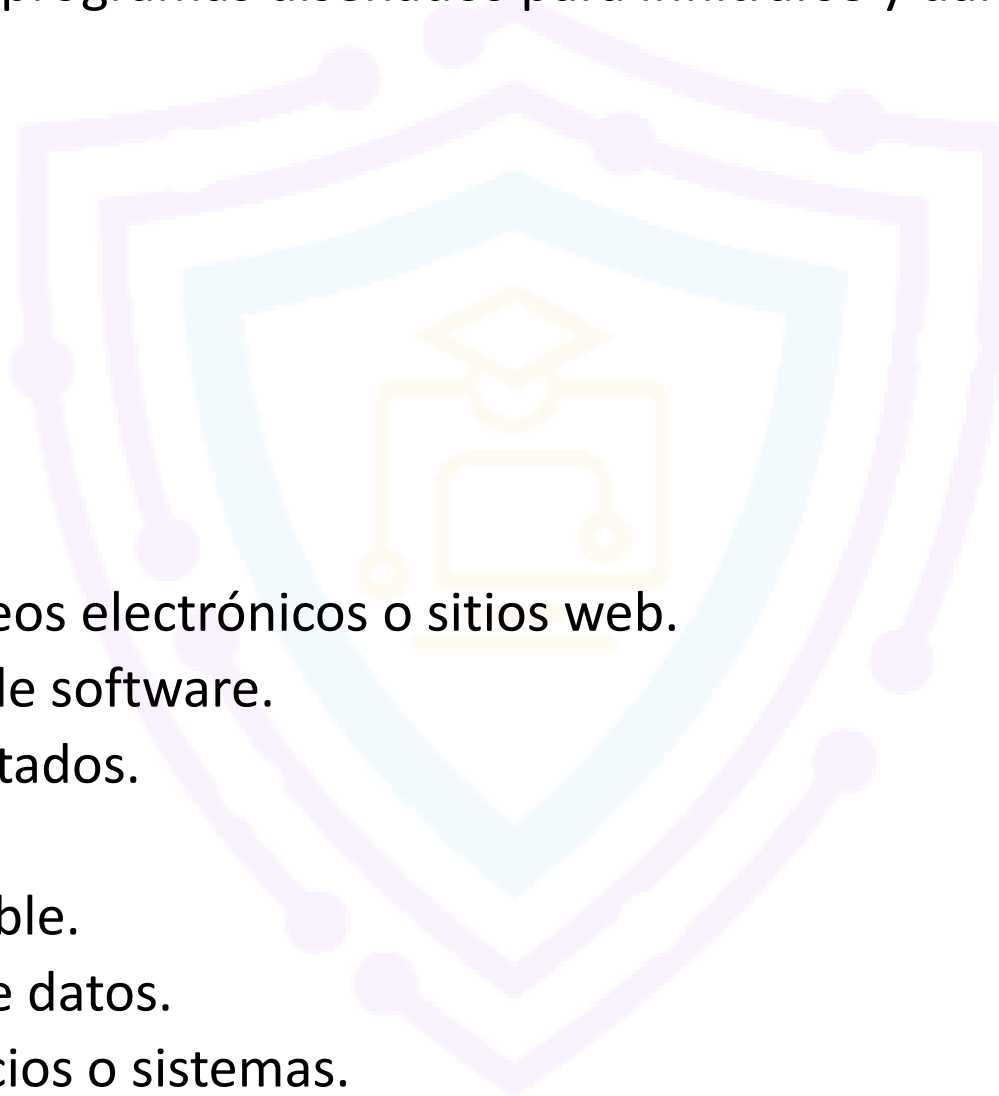
- **Virus**
- **Gusanos (Worms)**
- **Troyanos**
- **Ransomware**
- **Spyware**

**Vías de infección:**

- Enlaces maliciosos en correos electrónicos o sitios web.
- Descargas no autorizadas de software.
- Dispositivos externos infectados.

**Impacto:**

- Robo de información sensible.
- Bloqueo o manipulación de datos.
- Interrupción total de servicios o sistemas.



# Phishing (Suplantación de Identidad)

Técnica de **ingeniería social** utilizada para engañar a los usuarios y obtener datos confidenciales como contraseñas, información financiera o credenciales corporativas.

## Métodos comunes:

- **Correos electrónicos falsos** que imitan instituciones legítimas.
- **Páginas web fraudulentas** para capturar información.
- **Mensajes SMS o redes sociales** con enlaces maliciosos.

## Variantes:

- **Spear Phishing:** ataque dirigido a personas o grupos específicos.
- **Whaling:** ataques enfocados en ejecutivos o directivos de alto nivel.



# DDoS (Distributed Denial of Service)

Un ataque DDoS busca **saturar un sistema o servicio** con un volumen excesivo de tráfico para que deje de estar disponible para los usuarios legítimos.

• **Botnets:** redes de dispositivos comprometidos utilizados para amplificar el ataque.

• **Consecuencias:**

- Interrupción de servicios en línea.
- Pérdidas financieras por inactividad.
- Daño a la reputación de la empresa.



# Amenazas Internas (Insider Threats)

Se originan dentro de la organización e involucran a individuos con **acceso autorizado** a sistemas y datos.

## Tipos de amenazas internas:

- **Intencionales:** espionaje, robo de datos, sabotaje.
- **No intencionales:** errores humanos o negligencia.

## Desafío clave:

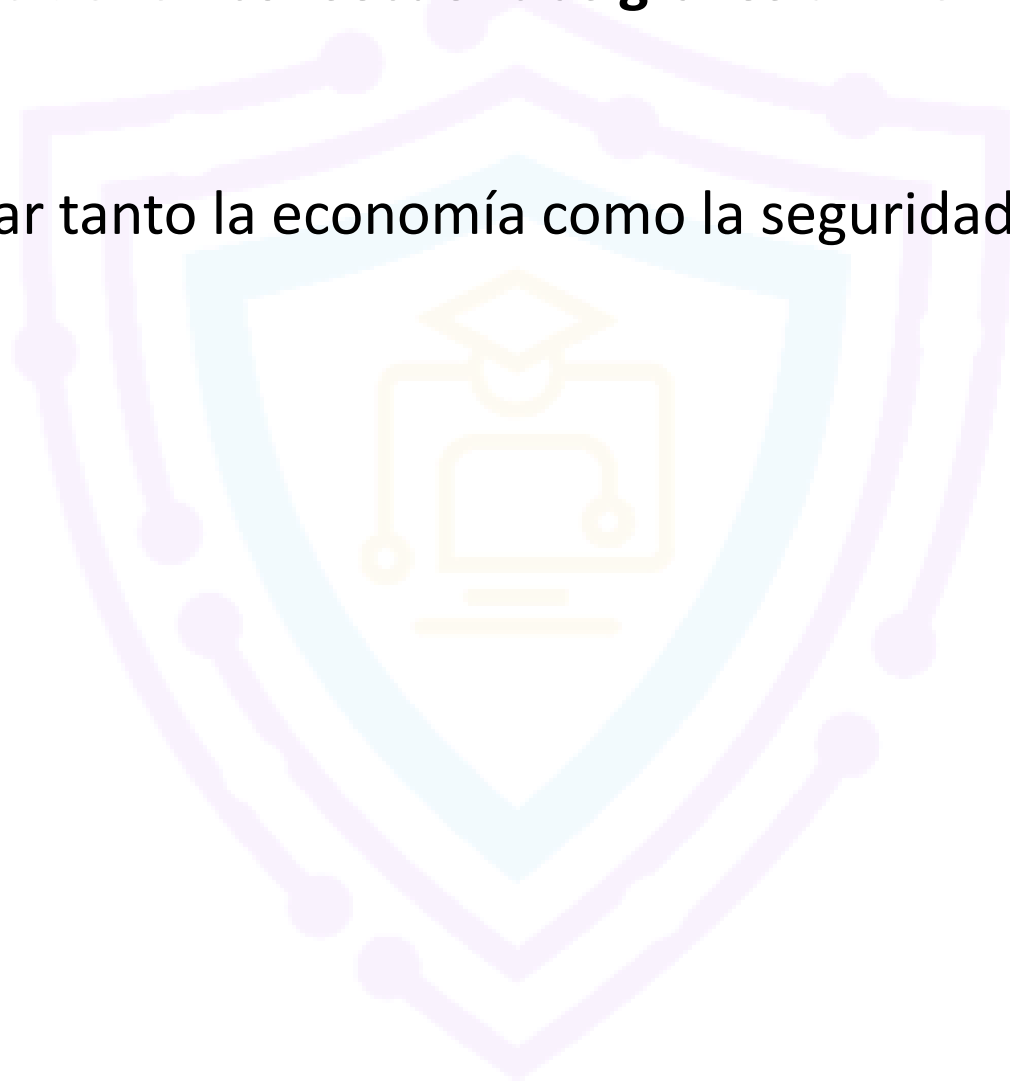
Diferenciar comportamientos normales de actividades potencialmente maliciosas.



# Impacto de las Amenazas Cibernéticas

Las amenazas cibernéticas tienen **consecuencias graves** a nivel individual, corporativo y gubernamental.

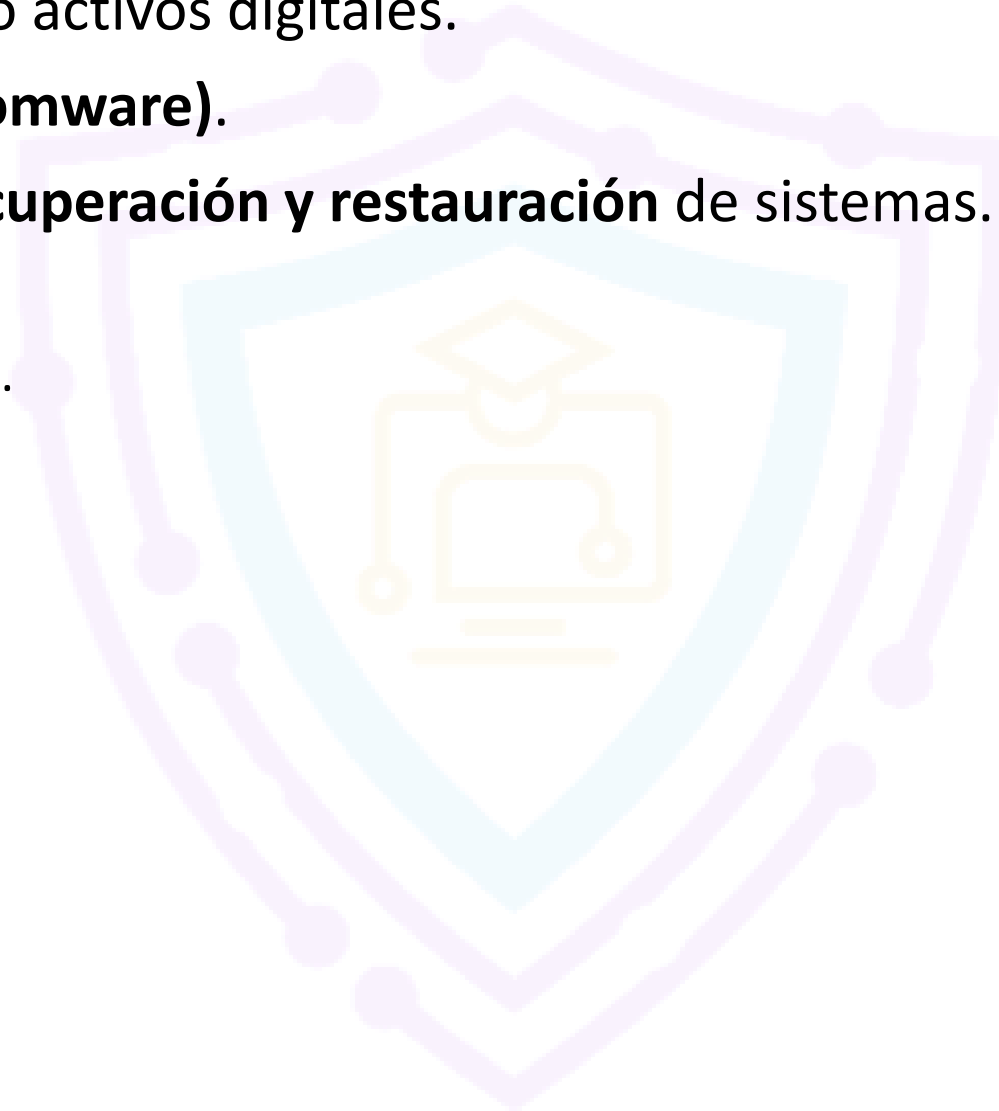
Sus efectos pueden afectar tanto la economía como la seguridad pública y nacional.





# Pérdidas Financieras

- Robo directo de fondos o activos digitales.
- Pagos de **rescates (ransomware)**.
- Costos asociados a la **recuperación y restauración** de sistemas.
- Pérdidas indirectas:
  - Productividad reducida.
  - Daños reputacionales.
  - Gastos legales.



# Brechas de Datos (Data Breaches)

Se producen cuando actores no autorizados **acceden o exponen información confidencial**, como:

- Datos personales.
- Información financiera.
- Propiedad intelectual.
- Datos clasificados.

## **Consecuencias:**

- Robo de identidad.
- Fraude financiero.
- Pérdida de confianza por parte de clientes y socios.



# Disrupción de Infraestructura Crítica

Sectores como **energía, salud y transporte** son objetivos frecuentes debido a su impacto social y económico.

## Posibles consecuencias:

- Apagones eléctricos a gran escala.
- Interrupción de servicios hospitalarios.
- Caos en sistemas de transporte.
- Riesgos para la seguridad pública.



# Amenazas a la Seguridad Nacional

Los **ciberataques patrocinados por estados** representan uno de los mayores riesgos actuales.

- **Objetivos comunes:**

- Sistemas militares.
- Redes gubernamentales.
- Infraestructura estratégica.

- **Riesgos:**

- Robo de información clasificada.
- Espionaje a gran escala.
- Potenciales conflictos geopolíticos.



# Vulnerabilidades en Ciberseguridad

Las **vulnerabilidades** representan **debilidades o fallos** en sistemas de información que los atacantes pueden explotar para:

- Obtener **acceso no autorizado**.
- Robar **información confidencial**.
- Interrumpir servicios críticos o causar daños.

Estas debilidades pueden encontrarse en:

- **Hardware** (equipos físicos).
- **Software** (aplicaciones y sistemas operativos).
- **Protocolos de red**.
- **Factores humanos**.



# Vulnerabilidades de Software

Las vulnerabilidades en software son **las más comunes** y provienen de errores en el diseño o desarrollo de aplicaciones.

## Causas principales:

- Código con errores o fallos de diseño.
- Versiones obsoletas y sin soporte.
- Falta de parches de seguridad.

## Riesgos:

- Acceso no autorizado a sistemas.
- Robo o manipulación de datos.
- Ejecución remota de código malicioso.

## Ejemplo práctico:

- Una aplicación web sin actualizar que contiene fallos conocidos, explotados mediante un ataque de **SQL Injection**.



# Factores Humanos

El **factor humano** es una de las mayores fuentes de vulnerabilidades.

## Errores frecuentes:

- Caer en ataques de **phishing** y proporcionar credenciales sensibles.
- Uso de **contraseñas débiles** o repetidas.
- Ignorar actualizaciones de seguridad.
- Desconocimiento o falta de capacitación en ciberseguridad.



# Internet de las Cosas (IoT)

Los dispositivos IoT (Internet of Things) presentan retos únicos en seguridad.

## Problemas comunes:

- Ausencia de mecanismos de seguridad robustos.
- Uso de **protocolos inseguros** para la comunicación.
- Configuraciones predeterminadas con **credenciales por defecto**.

## Vulnerabilidades frecuentes:

- **Ataques Man-in-the-Middle (MitM)**: interceptación de datos en tránsito.
- **Ataques de cifrado débiles**: violación de la confidencialidad de la información.

**Ejemplo:** cámaras de seguridad comprometidas para formar parte de una botnet en un ataque DDoS.





# Buenas Prácticas de Ciberseguridad

Adoptar buenas prácticas es fundamental para **proteger la información, reforzar los sistemas y garantizar la resiliencia** frente a amenazas.

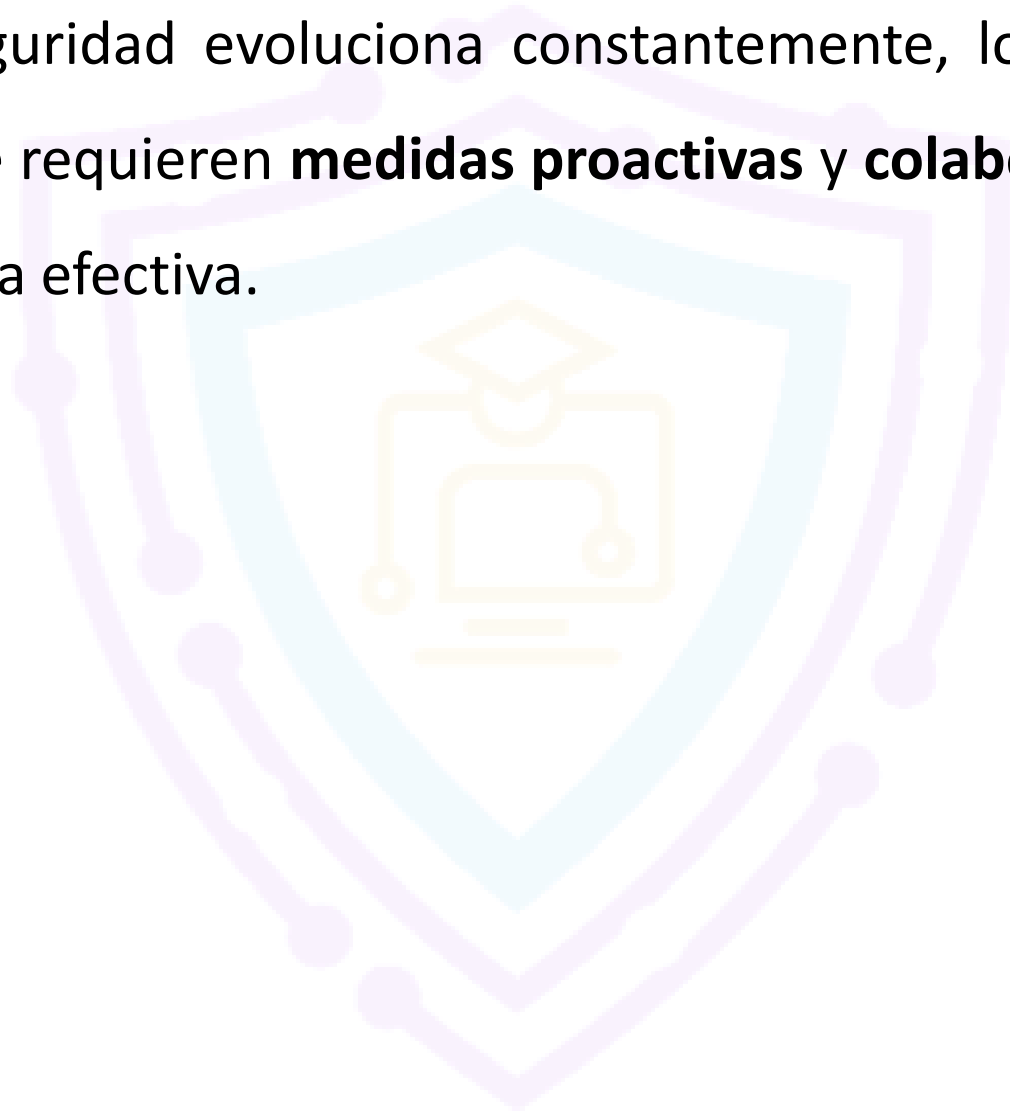
Estas prácticas se dividen en cuatro pilares principales:

- 1.Cifrado (Encryption)**
- 2.Seguridad en la Red (Network Security)**
- 3.Respuesta a Incidentes (Incident Response)**
- 4.Recuperación (Recovery)**



# Amenazas Emergentes y Retos Futuros

El mundo de la ciberseguridad evoluciona constantemente, lo que genera **nuevas amenazas y desafíos** que requieren **medidas proactivas y colaboración internacional** para mitigarlos de manera efectiva.



# Inteligencia Artificial y Machine Learning en Ciberamenazas

La convergencia de **IA y aprendizaje automático** ha transformado el panorama de la ciberseguridad.

- Los **ciberdelincuentes** usan IA para:
  - Crear ataques **sofisticados y dirigidos**.
  - Desarrollar malware que **adapta su comportamiento** para evadir las defensas tradicionales.
  - Automatizar ataques masivos con mayor efectividad.
- Los **profesionales de ciberseguridad** también utilizan IA para:
  - **Detectar y responder** a amenazas en tiempo real.
  - Analizar grandes volúmenes de datos y patrones anómalos.
  - Mejorar la **precisión en la detección** y reducir falsos positivos.



# Computación Cuántica y Ciberseguridad

La **computación cuántica** ofrece un avance revolucionario, pero también **representa un riesgo importante** para la seguridad actual.

## •Amenaza principal:

- Puede **debilitar o romper los algoritmos de cifrado actuales**, como RSA y ECC, dejando datos críticos expuestos.

## •Implicaciones:

- Información previamente segura podría ser descifrada en segundos.
- Urge la **adopción de algoritmos cuántico-resistentes** para proteger datos a largo plazo.

## •Acciones necesarias:

- Actualizar protocolos de cifrado.
- Desarrollar estrategias de seguridad para la era cuántica.
- Prepararse para el impacto a nivel global.



# Cooperación Internacional en Ciberseguridad

Las amenazas cibernéticas **no conocen fronteras** y afectan a gobiernos, empresas y ciudadanos en todo el mundo.

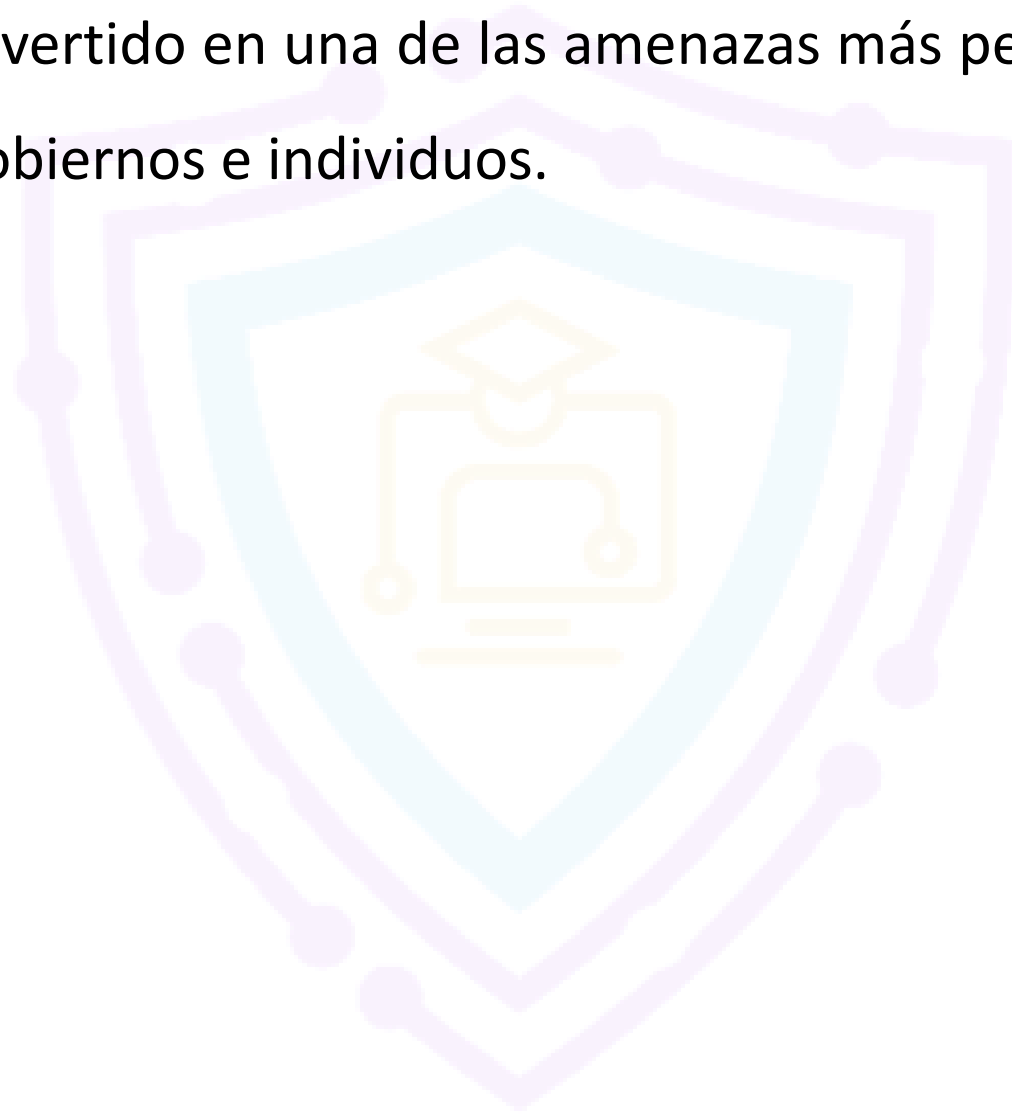
## Medidas clave:

- **Compartir información** entre gobiernos y sectores privados.
- Desarrollar **inteligencia de amenazas conjunta**.
- Crear **mecanismos coordinados de respuesta** ante ataques transnacionales.
- Establecer **estándares y marcos globales de ciberseguridad** para fortalecer la resiliencia mundial.



# Ransomware: Una Amenaza Creciente

El **ransomware** se ha convertido en una de las amenazas más peligrosas y frecuentes, afectando a empresas, gobiernos e individuos.



# Definición y Proceso Básico

El ransomware **cifra los archivos de la víctima**, dejándolos inaccesibles y exigiendo un pago en criptomonedas para recuperar el acceso.

## Flujo básico:

- 1.El ataque inicia con un **correo de phishing** o un **enlace malicioso**.
- 2.El usuario interactúa con el contenido, permitiendo la **infiltración del malware**.
- 3.El ransomware **cifra los archivos** con algoritmos como AES o RSA.
- 4.Se entrega una **nota de rescate** con instrucciones de pago.
- 5.El atacante exige **pagos anónimos** en criptomonedas.



# Las 9 Fases de un Ataque de Ransomware

## 1.Explotación e Infección

1. Se aprovechan vulnerabilidades en software para instalar el ransomware.

## 2.Comunicación con Servidor C&C (Command and Control)

1. El ransomware se conecta con el servidor del atacante para recibir instrucciones.

## 3.Descubrimiento y Análisis

1. Evalúa el sistema para identificar los archivos y recursos más valiosos.

## 4.Cifrado de Datos

1. Los archivos son encriptados con algoritmos robustos, dificultando su recuperación.

## 5.Entrega de Nota de Rescate

1. Se comunica a la víctima cómo y cuánto debe pagar.

## 6.Cobro del Rescate

1. El atacante recibe el pago, generalmente en criptomonedas.

## 7.Entrega de Clave de Descriptación (Opcional)

1. Puede entregar una clave para descifrar los datos, aunque **no está garantizado**.

## 8.Recuperación de Datos

1. Se intentan restaurar archivos mediante backups o herramientas de recuperación.

## 9.Análisis Post-Ataque

1. Se identifican las causas y se fortalecen las defensas para prevenir futuros incidentes.





# Impacto del Ransomware

## Principales Consecuencias:

### Interrupción Operativa y Pérdida de Productividad

Paraliza procesos empresariales.

Genera tiempo de inactividad que afecta la generación de ingresos.

### Consecuencias Potencialmente Letales

En sectores como **salud** o **infraestructura crítica**, puede poner vidas en riesgo.

### Brechas de Datos y Consecuencias Legales

Exposición de información sensible.

Demandas legales y multas regulatorias.

### Estrés Psicológico y Desconfianza

Ansiedad, miedo y pérdida de confianza en la organización afectada.

### Ataques Dirigidos y Personalizados

Los ciberdelincuentes realizan **reconocimiento previo** para maximizar el daño.

### Evasión de Medidas de Seguridad

El ransomware evoluciona constantemente para **burlar defensas tradicionales**.

### Daños Reputacionales y Pérdidas Financieras

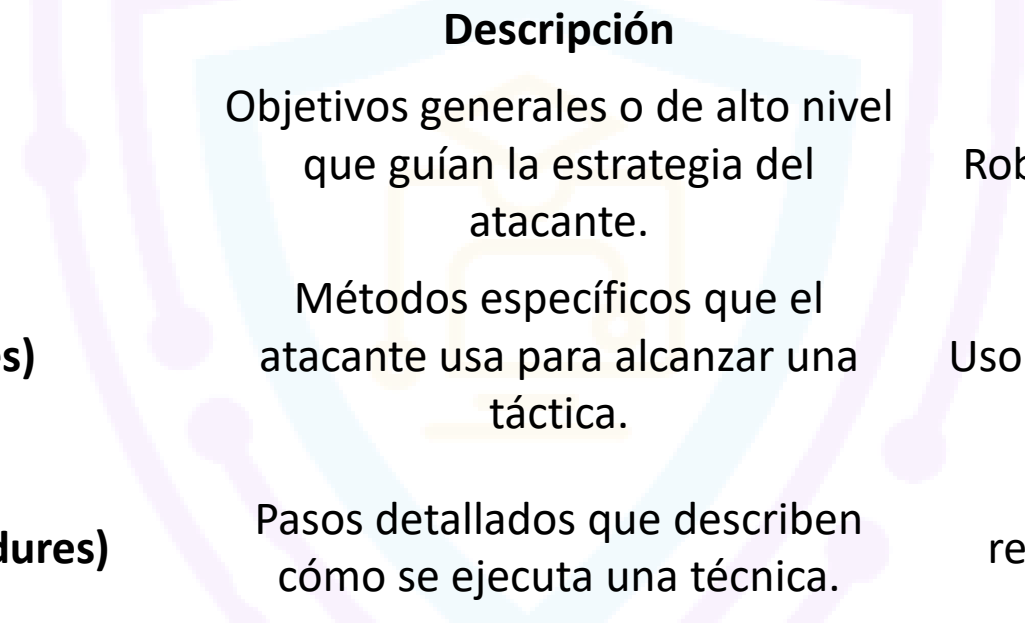
Impacto negativo en la imagen corporativa.

Dificultad para retener clientes y socios estratégicos.



Concepto	Definición	Ejemplo
Intención (Intent)	Propósito principal del ataque, es decir, <b>lo que el atacante quiere lograr</b> .	Robo de datos o interrupción de un servicio.
Motivación (Motive)	Razón subyacente que impulsa al atacante a realizar la acción.	Obtener dinero, motivos políticos o ideológicos.
Objetivo (Goal)	Resultado final que el atacante espera obtener.	Control total de un sistema, espionaje o extorsión.





Concepto	Descripción	Ejemplo
<b>Tácticas (Tactics)</b>	Objetivos generales o de alto nivel que guían la estrategia del atacante.	Robo de información confidencial.
<b>Técnicas (Techniques)</b>	Métodos específicos que el atacante usa para alcanzar una táctica.	Uso de malware para extraer datos.
<b>Procedimientos (Procedures)</b>	Pasos detallados que describen cómo se ejecuta una técnica.	Fases de un ataque: reconocimiento, malware, C&C, exfiltración.



# Tácticas (Tactics)

Las tácticas representan **los objetivos estratégicos** de un ataque cibernético. Son el “**por qué**” detrás de las acciones del atacante.

## Ejemplos comunes:

- **Exfiltración de datos:** robar información sensible.
- **Destrucción de datos:** eliminar información para causar daño.
- **Interrupción de sistemas:** afectar operaciones críticas.
- **Acceso no autorizado:** infiltrarse en sistemas protegidos.



# Técnicas (Techniques)

Las técnicas describen **cómo** el atacante ejecuta una táctica. Son el “**qué**” y los **métodos específicos** que se utilizan.

## Ejemplos:

- En una táctica de **exfiltración de datos**, la técnica podría incluir:
  - Uso de malware para robar archivos.
  - Compresión y cifrado de datos para evadir detección.
  - Envío de datos a un servidor externo controlado por el atacante.

Otras técnicas incluyen:

- **Phishing** para obtener credenciales.
- **Ingeniería social** para manipular usuarios.
- **Explotación de vulnerabilidades** en software o hardware.



# Procedimientos (Procedures)

Los procedimientos son el nivel más detallado y describen **paso a paso cómo se ejecuta una técnica.**

Son el “**cómo exacto**” de la operación.

**Ejemplo de procedimiento para exfiltración de datos:**

- 1.Reconocimiento:** identificar objetivos y recopilar información.
- 2.Entrega de malware:** infectar el sistema objetivo.
- 3.Establecer comunicación C&C:** conectar con el servidor de comando y control.
- 4.Cifrado y extracción de datos:** enviar información robada de manera encubierta.



# Ejemplo de APT (Advanced Persistent Threat)

Un **APT** es un tipo de ataque avanzado, persistente y dirigido que representa una gran amenaza para organizaciones y gobiernos.

## Escenario:

### 1. Acceso inicial mediante spear phishing

1. El atacante envía un correo electrónico cuidadosamente diseñado.
2. El mensaje contiene un enlace o archivo malicioso.
3. La víctima lo abre, permitiendo la instalación de malware.

### 2. Exploración de la red

1. El atacante identifica activos críticos y vulnerabilidades.
2. Mapas de red y usuarios clave son recopilados.

### 3. Movimiento lateral (Lateral Movement)

1. El atacante se desplaza entre sistemas internos.
2. Escala privilegios y obtiene mayor control.

### 4. Comunicación encubierta (Covert Communication)

1. El malware se comunica con servidores C&C utilizando **canales cifrados** para evitar ser detectado.

### 5. Exfiltración de datos (Data Exfiltration)

1. Los datos son robados en pequeños fragmentos para no levantar sospechas.
2. Los archivos suelen ser comprimidos y cifrados.

### 6. Persistencia (Persistence)

1. El atacante instala **backdoors y rootkits** para permanecer dentro de la red durante semanas o meses sin ser detectado.



# Oportunidad (Opportunity)

La **oportunidad** se refiere a las **condiciones o circunstancias** que permiten a un atacante **aprovechar vulnerabilidades o debilidades** en un sistema.

Factor	Descripción	Ejemplo
Contraseñas débiles	Credenciales fáciles de adivinar o repetidas.	Usuario con clave "123456".
Falta de medidas de seguridad	Datos sin cifrar o software obsoleto.	Base de datos sin encriptación.
Sistemas sin parches	Retrasos en la actualización de parches críticos.	Ataques a vulnerabilidades conocidas como Log4j.
Ingeniería social	Engaño a usuarios para comprometer la seguridad.	Phishing con enlaces maliciosos.
Errores de configuración	Configuraciones inseguras que exponen servicios.	Puertos abiertos sin necesidad.
Dependencias de terceros	Riesgos por servicios externos inseguros.	Brecha en proveedor de nube que afecta a clientes.





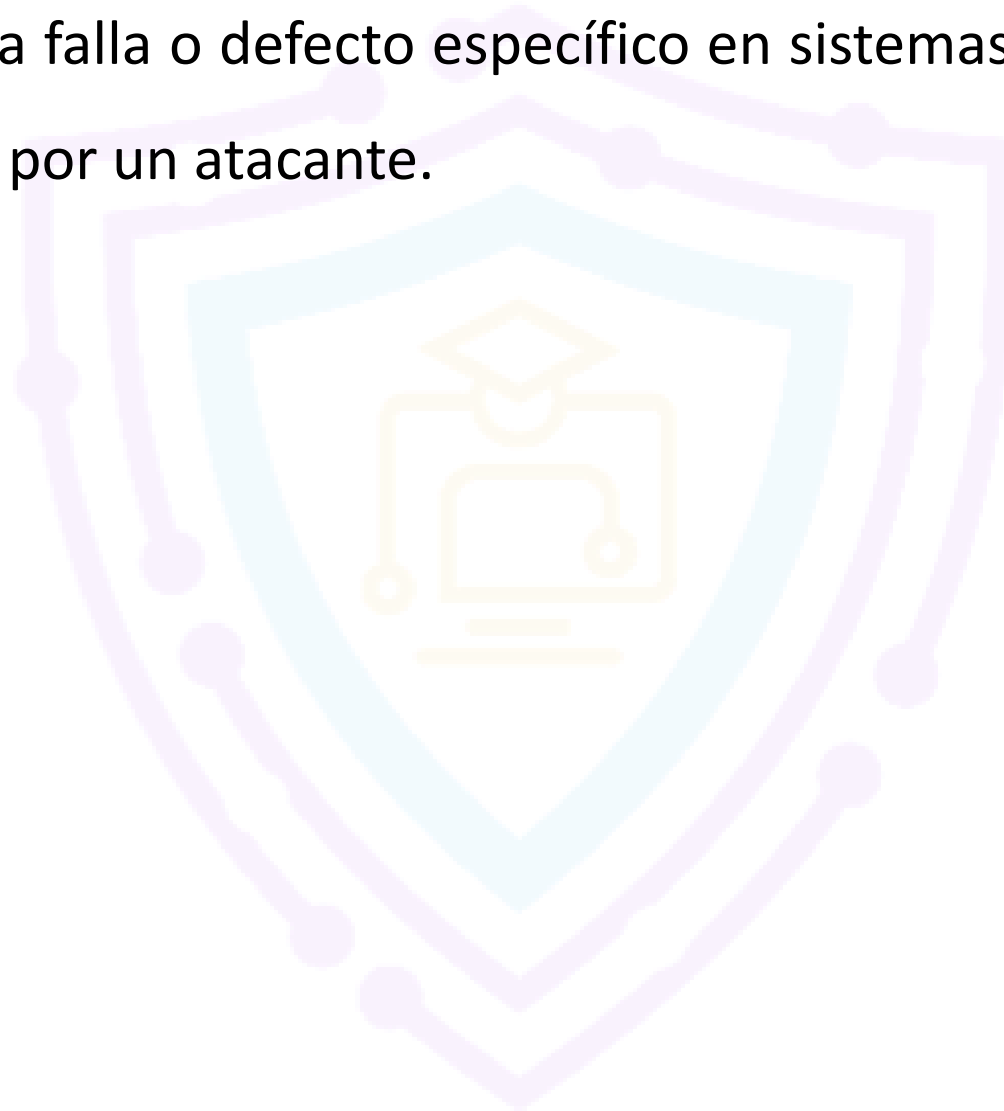
# Ejemplo práctico

Un servidor web que no tiene implementado HTTPS y utiliza contraseñas por defecto **crea la oportunidad perfecta** para que un atacante robe datos de usuarios mediante un ataque de intermediario (*Man-in-the-Middle*).



# Vulnerabilidad (Vulnerability)

Una vulnerabilidad es una falla o defecto específico en sistemas, aplicaciones o redes que puede ser explotado por un atacante.



# Tipos de Vulnerabilidades

Tipo	Descripción	Ejemplo
Software	Errores en el código de aplicaciones o sistemas operativos.	SQL Injection, XSS, Buffer Overflow.
Hardware	Fallas físicas en componentes o dispositivos.	Firmware desactualizado, ataque a procesadores (Meltdown, Spectre).
Configuración	Ajustes incorrectos que exponen el sistema a riesgos.	Contraseñas por defecto, permisos excesivos.
Humanas	Errores o comportamientos inseguros de los usuarios.	Empleado que cae en un ataque de phishing.



# Debilidad (Weakness)

Una **debilidad** es una **limitación fundamental** en la organización, el diseño de un sistema o la cultura de seguridad que **aumenta la probabilidad de vulnerabilidades**.

Tipo de Debilidad	Descripción	Ejemplo
Arquitectónica	Fallas en el diseño general de sistemas.	Falta de segmentación de red en la infraestructura.
Políticas y Cumplimiento	Ausencia de reglas o procedimientos adecuados.	No contar con una política de contraseñas segura.
Recursos Limitados	Falta de presupuesto, personal o tecnología.	Una empresa sin equipo SOC dedicado.
Cultural	Actitudes que no priorizan la ciberseguridad.	Empleados que ignoran protocolos de seguridad.

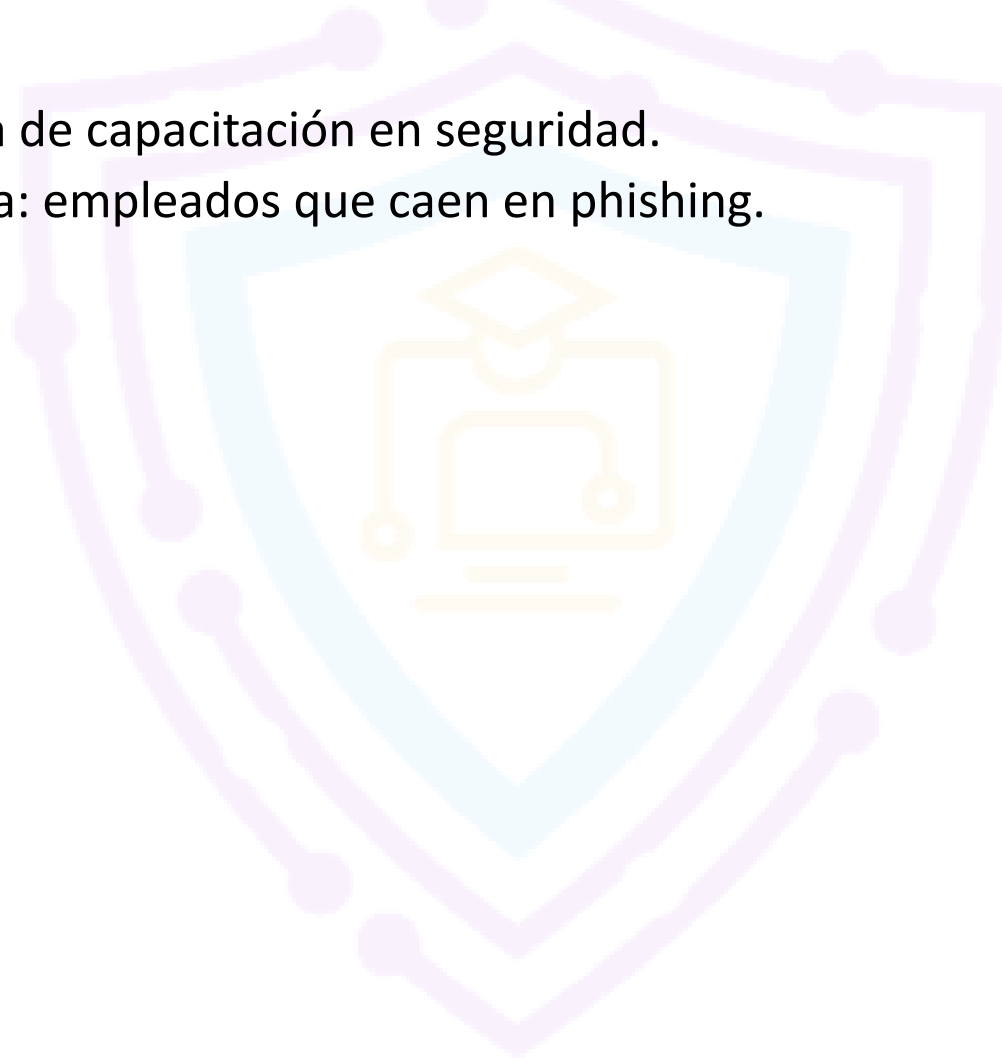


# Relación entre Vulnerabilidad y Debilidad

- Una **debilidad** puede **originar múltiples vulnerabilidades**.

- Ejemplo:

- Debilidad cultural: falta de capacitación en seguridad.
- Vulnerabilidad derivada: empleados que caen en phishing.



# Ciclo de Vida de una Vulnerabilidad

Comprender el ciclo de vida de una vulnerabilidad es clave para **gestionar y mitigar riesgos**.

## Fase

### 1. Descubrimiento

### 2. Divulgación

### 3. Explotación

### 4. Mitigación

## Descripción

La vulnerabilidad es detectada por investigadores, pruebas internas o reportes de usuarios.

Se comunica al proveedor o a la comunidad, priorizando su impacto y criticidad.

El atacante aprovecha la vulnerabilidad si no existe parche o no se ha aplicado.

Aplicación de parches, cambios de configuración y medidas de protección.



# Buenas Prácticas para la Mitigación

- 1.Gestión de parches:** aplicar actualizaciones de seguridad rápidamente.
- 2.Configuración segura:** eliminar servicios y puertos innecesarios.
- 3.Control de accesos:** aplicar el principio de menor privilegio.
- 4.Pruebas de seguridad:** realizar escaneos y pentests regularmente.
- 5.Educación de usuarios:** capacitaciones sobre phishing y seguridad básica.
- 6.Gestión de proveedores:** evaluar la seguridad de servicios externos.



# Blended Cyberattack

Un **Blended Cyberattack** es un ataque **sofisticado y multifacético** que utiliza **múltiples vectores y técnicas simultáneamente**.

Su objetivo es aumentar las probabilidades de éxito y dificultar la detección por parte de los equipos de ciberseguridad.

A diferencia de ataques simples que usan un solo método (ej. solo phishing), un blended attack puede combinar **ingeniería social, malware, ransomware y APT** en un mismo incidente.





# Objetivo del ataque

- Obtener acceso inicial a la red de una institución financiera.
- Robar datos sensibles como información de clientes y datos financieros.
- Extorsionar a la víctima mediante ransomware y amenazas de filtración de información.
- Mantener presencia oculta durante el mayor tiempo posible.



# Etapas de un Blended Cyberattack

Etapa	Descripción	Ejemplo en una institución financiera
1. Identificación del objetivo	Los atacantes seleccionan una organización y analizan su infraestructura.	Selección de un banco local para robar datos financieros.
2. Reconocimiento (Research)	Recolección de información pública y privada sobre la empresa y empleados clave.	Uso de LinkedIn para identificar personal de TI.
3. Phishing	Envío de correos falsos para engañar a empleados y obtener acceso inicial.	Correo simulando ser del área de soporte solicitando credenciales.
4. Acceso inicial	El empleado cae en la trampa, permitiendo que el atacante entre a la red.	Instalación de malware vía archivo adjunto.
5. Inyección de malware	El atacante instala malware personalizado para persistir en la red.	Backdoor que evade el antivirus y permanece activo.
6. Explotación de vulnerabilidades	Escalada de privilegios y movimiento lateral dentro de la red.	Robo de credenciales administrativas usando Pass-the-Hash.
7. APT (Advanced Persistent Threat)	Operación encubierta para evadir detección y extraer información.	Monitoreo de tráfico de red y exfiltración lenta de datos.
8. Ransomware	Cifrado de datos críticos seguido de una demanda de rescate.	Servidores de clientes inaccesibles hasta pagar rescate.
9. Robo de datos y extorsión	Uso de la información robada para extorsionar a la organización.	Amenaza de publicar datos de clientes si no se paga.
10. Mitigación y recuperación	Aislamiento, restauración y fortalecimiento de la seguridad.	Colaboración con autoridades y refuerzo de políticas internas.



# ¿Qué es Cross-Site Scripting (XSS)?

Vulnerabilidad en la que el atacante **inyecta scripts maliciosos** en la aplicación web.

- Cuando el usuario carga la página comprometida, su **navegador ejecuta el código malicioso**.

- Esto permite al atacante:

- Robar **credenciales** y **cookies de sesión**.
- **Modificar contenido** de la página.
- Redirigir a sitios falsos (*phishing*).
- **Controlar la sesión** del usuario.

## Flujo básico:

1. El atacante inyecta código malicioso en la aplicación.
2. El servidor lo refleja o almacena sin validación.
3. El navegador de la víctima ejecuta el código como si fuera legítimo.



# Tipos de XSS

Tipo de XSS	Característica principal	Riesgo común
Reflected (No persistente)	El script se refleja en la respuesta inmediata del servidor.	Phishing, robo de credenciales
Stored (Persistente)	El script se <b>almacena</b> en la base de datos o servidor.	Robo masivo de datos, cookies
DOM-based (Cliente)	El ataque ocurre <b>directamente en el navegador</b> a través de JavaScript inseguro.	Redirecciones, manipulación del DOM



# Reflected Cross-Site Scripting (Reflected XSS)

- Ocurre cuando la aplicación refleja la entrada del usuario **directamente en la respuesta**, sin validación.
- Común en **formularios, parámetros de URL o búsquedas**.

## Ejemplo práctico:

- 1.El atacante envía un correo *phishing* con un link malicioso.
- 2.La víctima hace clic en el link → el servidor refleja el script.
- 3.El navegador ejecuta el script sin saber que es malicioso.
- 4.El atacante roba cookies o credenciales.

## Caso visual:

[https://sitio.com/search?q=<script>alert\('Hacked!'\)</script>](https://sitio.com/search?q=<script>alert('Hacked!')</script>)



# Stored Cross-Site Scripting (Stored XSS)

El código malicioso **se guarda de forma permanente** en el servidor, como:

- Comentarios en foros.
- Mensajes en chats.
- Perfiles de usuario.

## Ejemplo práctico:

- 1.El atacante publica un comentario con `<script>` malicioso.
- 2.Ese código queda guardado en la base de datos.
- 3.Otros usuarios cargan la página y ejecutan el script automáticamente.
- 4.El atacante roba cookies y secuestra sesiones.

## Peligro:

- Ataques **masivos** porque afecta a todos los usuarios que visiten la página comprometida.

## Mitigación:

- Validar y limpiar toda la entrada antes de guardarla.
- Codificar los datos antes de mostrarlos en el HTML.
- Monitorear logs en busca de actividad sospechosa.



# DOM-Based Cross-Site Scripting (DOM XSS)

- Ocurre **en el lado del cliente**, no en el servidor.
- El navegador ejecuta código inseguro cuando el sitio web **manipula el DOM** usando datos no validados.

## Ejemplo práctico:

- Una función JavaScript insegura toma datos de la URL:

```
document.write(location.href);
```

Si el atacante manipula la URL con un <script>, el navegador lo ejecutará.



# Flujo de un ataque XSS

## Etapas:

- 1.Inyección:** El atacante introduce el código malicioso.
- 2.Almacenamiento o reflexión:** El servidor no valida y entrega el script.
- 3.Ejecución en el cliente:** El navegador ejecuta el script.
- 4.Explotación:**
  1. Robo de cookies/sesiones.
  2. Redirecciones.
  3. Modificación de la página.
- 5.Escalamiento:** El atacante usa la información robada para acceder a más recursos.





# Medidas de prevención

Estrategia	Descripción
Validación y sanitización	Nunca confiar en la entrada del usuario. Validar y limpiar todos los datos.
Escaping de salida	Codificar caracteres especiales antes de mostrarlos en HTML, JS o URLs.
Content Security Policy (CSP)	Limitar qué scripts pueden ejecutarse en la aplicación.
Uso de frameworks seguros	React, Angular y otros frameworks modernos manejan automáticamente la sanitización.
Capacitación del equipo	Entrenar a desarrolladores y testers sobre OWASP y buenas prácticas.



# ¿Qué son los Application-Based Attacks?

- Son ataques que explotan **vulnerabilidades en software y aplicaciones web**.
- El objetivo del atacante es **ganar acceso no autorizado** a datos o sistemas.
- Ejemplos comunes:
  - **Cross-Site Scripting (XSS)**.
  - **SQL Injection**.
  - **Buffer Overflow**.
  - **Command Injection**.

## Por qué son peligrosos:

- Pueden ser usados para **robo de credenciales**, fraude financiero, espionaje corporativo y ataques dirigidos (*phishing*).
- Un solo error en el código puede permitir comprometer miles de usuarios.



# El proceso de un ataque XSS

El ataque sigue un flujo estructurado. Conocer estas etapas ayuda a detectar y detener ataques a tiempo.

Etapa	Descripción
1. Identificación de la vulnerabilidad	El atacante analiza la aplicación web en busca de puntos débiles usando <b>scanners automáticos</b> o revisión manual del código.
2. Creación del payload malicioso	Diseña un script, generalmente en <b>JavaScript</b> , para robar cookies, sesiones o manipular contenido.
3. Inyección del payload	Inserta el código malicioso en el campo vulnerable, como comentarios, formularios o parámetros de URL.
4. Interacción de la víctima	El usuario interactúa con la página comprometida, ejecutando el script sin saberlo.
5. Explotación y robo de datos	El script roba información (cookies, credenciales) o realiza acciones en nombre del usuario.
6. Impacto y consecuencias	El atacante obtiene acceso no autorizado y puede causar <b>daños financieros y reputacionales</b> .



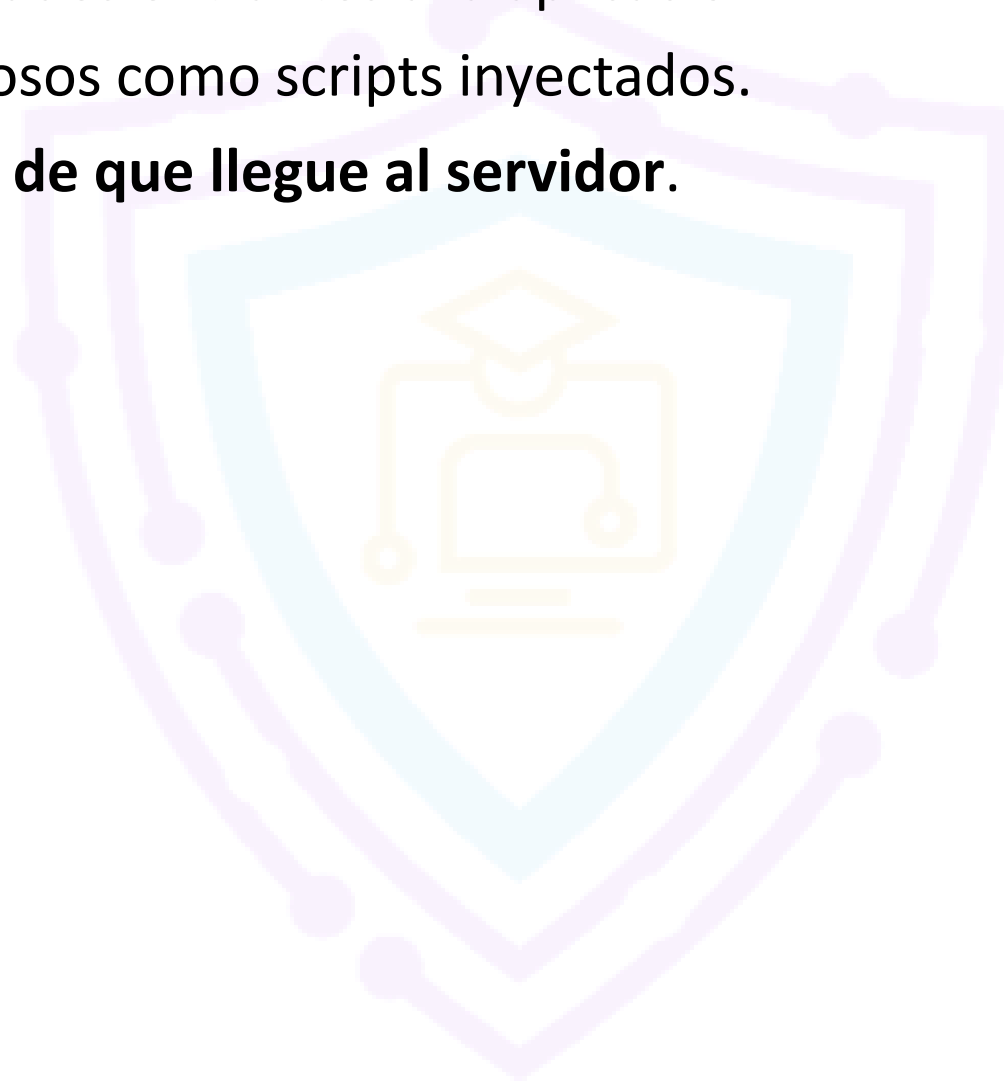
# Flujo visual de ataque

- 1.El atacante identifica la falla.
- 2.Envía el link malicioso o inserta el script en la aplicación.
- 3.El usuario abre la página.
- 4.El navegador ejecuta el código malicioso.
- 5.El atacante roba la información o controla la cuenta.



# Mitigación práctica con WAF

- El **WAF** analiza las solicitudes entrantes a la aplicación.
- Detecta patrones maliciosos como scripts inyectados.
- Bloquea el ataque **antes de que llegue al servidor**.



# ¿Qué son los Host-Based Attacks?

Un **host-based attack** se centra en comprometer equipos específicos (hosts), como:

- Computadoras de usuarios clave.
- Servidores internos.
- Equipos con información crítica.

## **Objetivos comunes de los atacantes:**

- Robar propiedad intelectual o datos confidenciales.
- Obtener control administrativo del sistema.
- Instalar malware o rootkits para persistencia.
- Movimientos laterales dentro de la red.

Estos ataques suelen ser **dirigidos y planeados** (APT – Advanced Persistent Threat).



# Caso de estudio: Ataque a investigación cuántica

Este escenario describe un ataque avanzado de 8 meses a una institución científica dedicada a investigación cuántica.

Mes	Etapas del ataque	Descripción
1	<b>Social Engineering</b>	Atacantes envían <b>correos spear-phishing</b> a investigadores, haciéndose pasar por colegas.
2	<b>Malware Deployment</b>	Investigadores descargan malware disfrazado de herramienta legítima.
3	<b>Zero-Day Exploitation</b>	Se explota una vulnerabilidad <b>desconocida (zero-day)</b> para obtener privilegios elevados.
4-5	<b>Lateral Movement</b>	El atacante se mueve entre equipos buscando servidores con datos valiosos.
6	<b>Data Exfiltration</b>	Se roba la información, <b>cifrándola y comprimiéndola</b> para evadir detección.
7	<b>Covering Tracks</b>	Limpieza de logs y uso de <b>rootkits</b> para ocultar rastros.
8	<b>Publicación de datos</b>	Los atacantes publican la investigación robada como si fuera suya, causando daño reputacional.



# Técnicas utilizadas

Técnica	Descripción	Ejemplo
<b>Spear Phishing</b>	Engañar a usuarios específicos con correos creíbles.	Correo que parece venir de un colega.
<b>Malware Avanzado</b>	Software que se oculta y espera ser activado.	Troyano disfrazado de herramienta de investigación.
<b>Explotación Zero-Day</b>	Aprovechar una vulnerabilidad desconocida por el fabricante.	Fallo sin parche en Windows o Linux.
<b>Lateral Movement</b>	Acceder a otros equipos en la red para escalar privilegios.	Uso de Pass-the-Hash.
<b>Rootkits</b>	Herramientas que ocultan procesos maliciosos en el sistema.	Ocultación en kernel o drivers.
<b>Data Exfiltration</b>	Robo de datos cifrándolos para evadir detección.	SFTP oculto o tráfico HTTPS falso.





# Impacto del ataque

Impacto	Descripción
1. Robo de propiedad intelectual	Años de investigación se pierden y benefician a un competidor o nación rival.
2. Retrasos en proyectos	Proyectos clave se ven afectados y retrasados meses o años.
3. Daño reputacional	La organización pierde credibilidad ante la comunidad científica y socios.
4. Vulnerabilidad humana	Empleados no entrenados caen en phishing, facilitando el ataque inicial.
5. Explotación de Zero-Day	Falta de control proactivo permite ataques sin ser detectados.
6. Falta de detección avanzada	Sin herramientas como EDR o SIEM, el ataque se extiende por meses.
7. Respuesta lenta	La ausencia de un plan de incidentes incrementa el daño.



# Medidas preventivas

Estrategia	Descripción
Entrenamiento en phishing	Simulaciones y capacitaciones regulares para reconocer correos maliciosos.
Gestión de parches	Actualizaciones constantes para reducir exposición a zero-days conocidos.
Implementar EDR y SIEM	Detectar anomalías y comportamientos sospechosos en tiempo real.
Monitoreo proactivo	Revisión continua de logs y alertas.
Plan de respuesta a incidentes	Procedimientos claros para detección, contención y erradicación.
Segmentación de red	Limitar el movimiento lateral de atacantes.
Uso de MFA (Multi-Factor Authentication)	Protege accesos críticos, incluso si se comprometen credenciales.



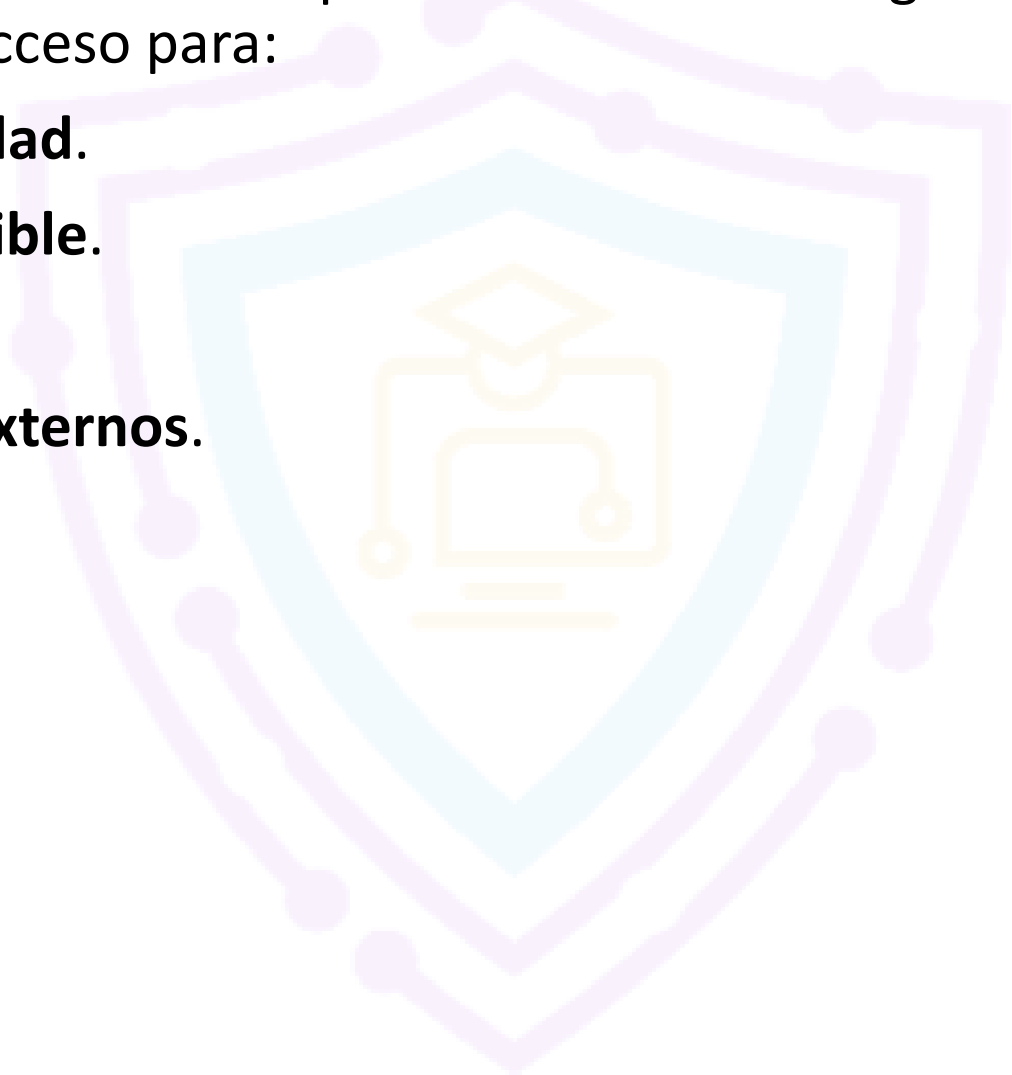
# ¿Qué es un Insider Attack?

Un **Insider Attack** ocurre cuando una persona con acceso legítimo a los sistemas de la organización utiliza ese acceso para:

- **Comprometer la seguridad.**
- **Robar información sensible.**
- **Sabotear operaciones.**
- **Colaborar con actores externos.**

## **Actores comunes:**

- Empleados actuales.
- Ex-empleados.
- Contratistas.



# Tipos de Insider Attacks

Los ataques internos pueden clasificarse en dos grandes grupos: **intencionales** y **no intencionales**.

Tipo	Descripción	Ejemplo
Malicious Insider	El empleado actúa con intención maliciosa, robando datos, sabotando sistemas o ayudando a atacantes externos.	Ex-empleado resentido que borra bases de datos críticas.
Unintentional Insider	El empleado causa un incidente por <b>error, negligencia o falta de conocimiento</b> , sin intención de dañar.	Caer en un phishing y comprometer credenciales.



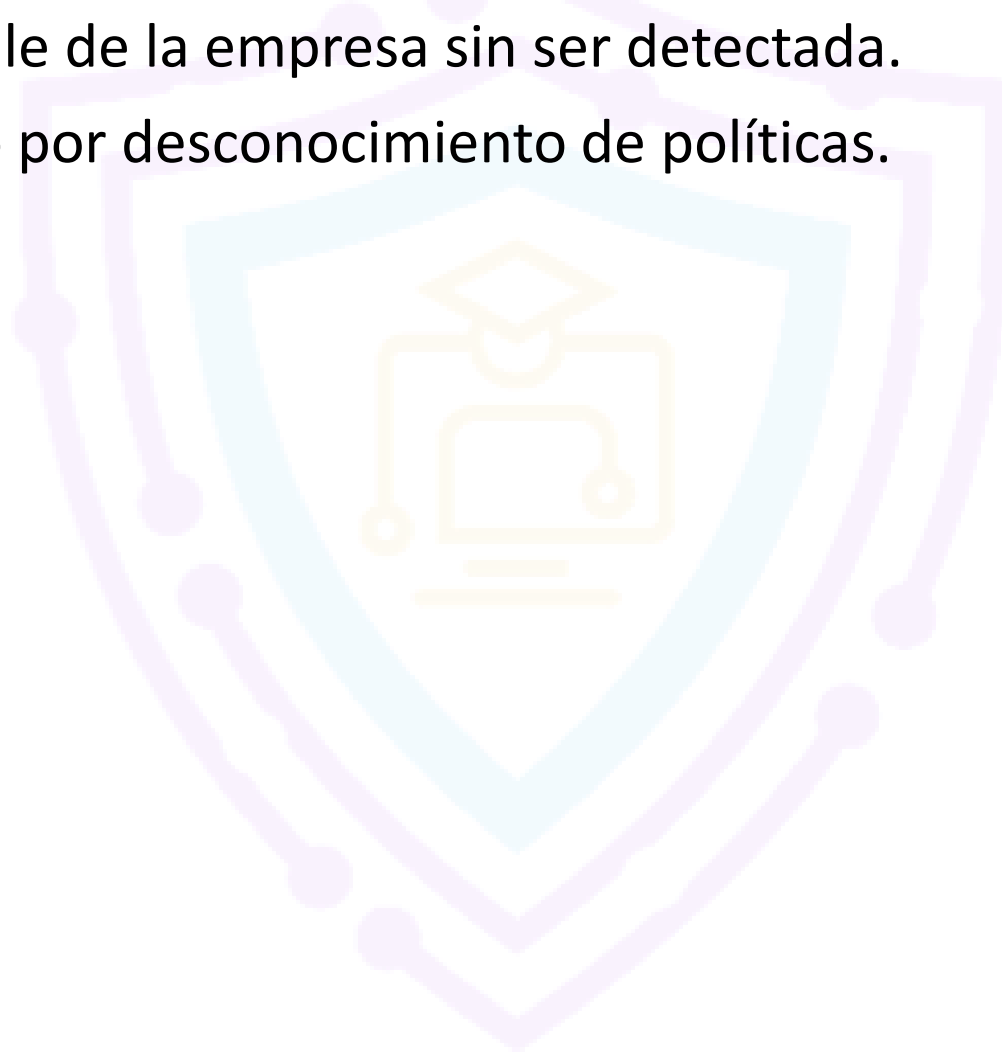
# Categorías detalladas de ataques internos

Categoría	Descripción	Motivación
<b>Malicious Insider Threat</b>	Empleado que deliberadamente roba información o daña la organización.	Venganza, dinero, extorsión.
<b>Espionaje</b>	Robo de datos confidenciales para beneficio externo, como un competidor o gobierno.	Ventaja competitiva, intereses geopolíticos.
<b>Privilege Abuse</b>	Uso indebido de privilegios de acceso más allá del rol asignado.	Curiosidad, fraude, sabotaje.
<b>Insider Trading</b>	Uso de información privilegiada para manipular mercados financieros.	Ganancias económicas.
<b>Data Exfiltration</b>	Transferencia no autorizada de información fuera de la empresa.	Robo de propiedad intelectual o fuga por descuido.
<b>Sabotaje</b>	Destrucción o alteración deliberada de datos y sistemas.	Ideología, resentimiento, venganza.
<b>Credential Theft and Misuse</b>	Robo y uso indebido de credenciales para accesos ilegítimos.	Suplantación, fraude interno.



# Ejemplo visual: Data Exfiltration

1. Empleado descarga datos en una USB o los envía por correo personal.
2. Información sensible sale de la empresa sin ser detectada.
3. Puede ser intencional o por desconocimiento de políticas.



# Ejemplo práctico de ataque interno

## Escenario: Robo de propiedad intelectual

- **Perfil:** Investigador con acceso a datos de investigación confidencial.
- **Acción:** Copia archivos a un disco duro externo durante semanas.
- **Objetivo:** Vender la información a un competidor extranjero.
- **Consecuencias:**
  - Pérdida de años de investigación.
  - Daño reputacional.
  - Problemas legales y pérdida de inversionistas.



# Factores de riesgo en insider attacks

## Factor

## Cómo incrementa el riesgo

Falta de entrenamiento	Empleados no identifican amenazas como phishing.
Exceso de privilegios	Usuarios tienen más acceso del necesario.
Ausencia de monitoreo	No se detectan actividades anómalas a tiempo.
Cultura organizacional débil	Falta de confianza y comunicación favorece ataques internos.
Ausencia de políticas claras	Los empleados desconocen las reglas y consecuencias.





# Estrategias de prevención y mitigación

Estrategia	Descripción
<b>Access Control &amp; Least Privilege</b>	Limitar accesos estrictamente a lo necesario para cada rol.
<b>User Monitoring &amp; Behavioral Analytics</b>	Detectar comportamientos anómalos en tiempo real.
<b>Employee Education &amp; Awareness</b>	Capacitar sobre phishing, buenas prácticas y amenazas internas.
<b>Políticas claras</b>	Definir normas sobre uso de datos y consecuencias de incumplimiento.
<b>Incident Response Plan</b>	Plan específico para responder ante amenazas internas.
<b>Data Encryption &amp; DLP</b>	Cifrar información y prevenir fugas mediante monitoreo.
<b>Privileged Access Management (PAM)</b>	Control estricto de accesos privilegiados.
<b>Whistleblower Programs</b>	Canal anónimo para reportar comportamientos sospechosos.
<b>Auditorías regulares</b>	Revisiones periódicas para detectar vulnerabilidades internas.
<b>Insider Threat Detection Tools</b>	Uso de herramientas dedicadas a amenazas internas.



# ¿Qué es Malware?

Malware es software **diseñado para dañar, explotar o comprometer** sistemas y redes.

## Efectos comunes:

- Pérdida de datos.
- Robos de identidad.
- Caídas de sistemas y servicios.
- Pérdidas financieras.
- Integración del sistema comprometido en redes de ataque (botnets).

## Vectores de infección:

- Correos de **phishing**.
- **Websites maliciosos** o comprometidos.
- Software infectado.
- Vulnerabilidades sin parchear.



# Tipos de Malware

Tipo	Características	Comportamiento
<b>Virus</b>	Se adjunta a archivos legítimos y necesita ejecución por parte del usuario.	Se replica y puede corromper datos o abrir puertas para otros ataques.
<b>Worm</b>	Se propaga automáticamente sin intervención humana ni archivos anfitrión.	Rápida propagación en redes, genera congestión y puede entregar payloads adicionales.
<b>Trojan</b>	Se disfraza como software legítimo. Requiere engaño (ingeniería social).	Robo de información, acceso remoto, backdoors persistentes.
<b>Ransomware</b>	Cifra archivos y exige pago en criptomonedas para su liberación.	Interrumpe operaciones, genera pérdidas financieras y afecta la confidencialidad.
<b>Spyware</b>	Monitorea y recopila información de manera oculta.	Robo de credenciales, espionaje corporativo, seguimiento de actividad.
<b>Adware</b>	Muestra publicidad no deseada. Puede recolectar información del usuario.	Pop-ups, redirecciones, degradación del rendimiento.
<b>Keylogger</b>	Captura las pulsaciones del teclado.	Robo de contraseñas, información financiera y datos sensibles.
<b>Botnet</b>	Grupo de dispositivos infectados controlados remotamente.	DDoS, spam, ataques coordinados a gran escala.



# Métodos de Distribución

Los cibercriminales utilizan múltiples estrategias para distribuir malware. Conocerlas permite **anticipar y prevenir infecciones**.

Método	Descripción
Phishing	Correos fraudulentos con enlaces o adjuntos maliciosos que parecen legítimos.
Drive-By Downloads	Descarga silenciosa de malware al visitar un sitio web comprometido.
Software infectado	Programas legítimos modificados para incluir malware o plataformas de distribución comprometidas.
Removable Media	USBs o discos externos infectados que, al conectarse, ejecutan malware automáticamente.



# Técnicas de Prevención

Técnica	Descripción
Antivirus y Antimalware actualizados	Detectan, bloquean y eliminan malware conocido y nuevo.
Firewalls	Controlan el tráfico de red y bloquean accesos no autorizados.
Educación del usuario	Capacitación en phishing, descargas seguras y buenas prácticas digitales.
Actualización de software	Parches frecuentes para cerrar vulnerabilidades explotadas por malware.
Segmentación de red	Limita el movimiento lateral del malware dentro de la infraestructura.
Backups regulares	Permiten recuperar datos en caso de un ataque de ransomware.

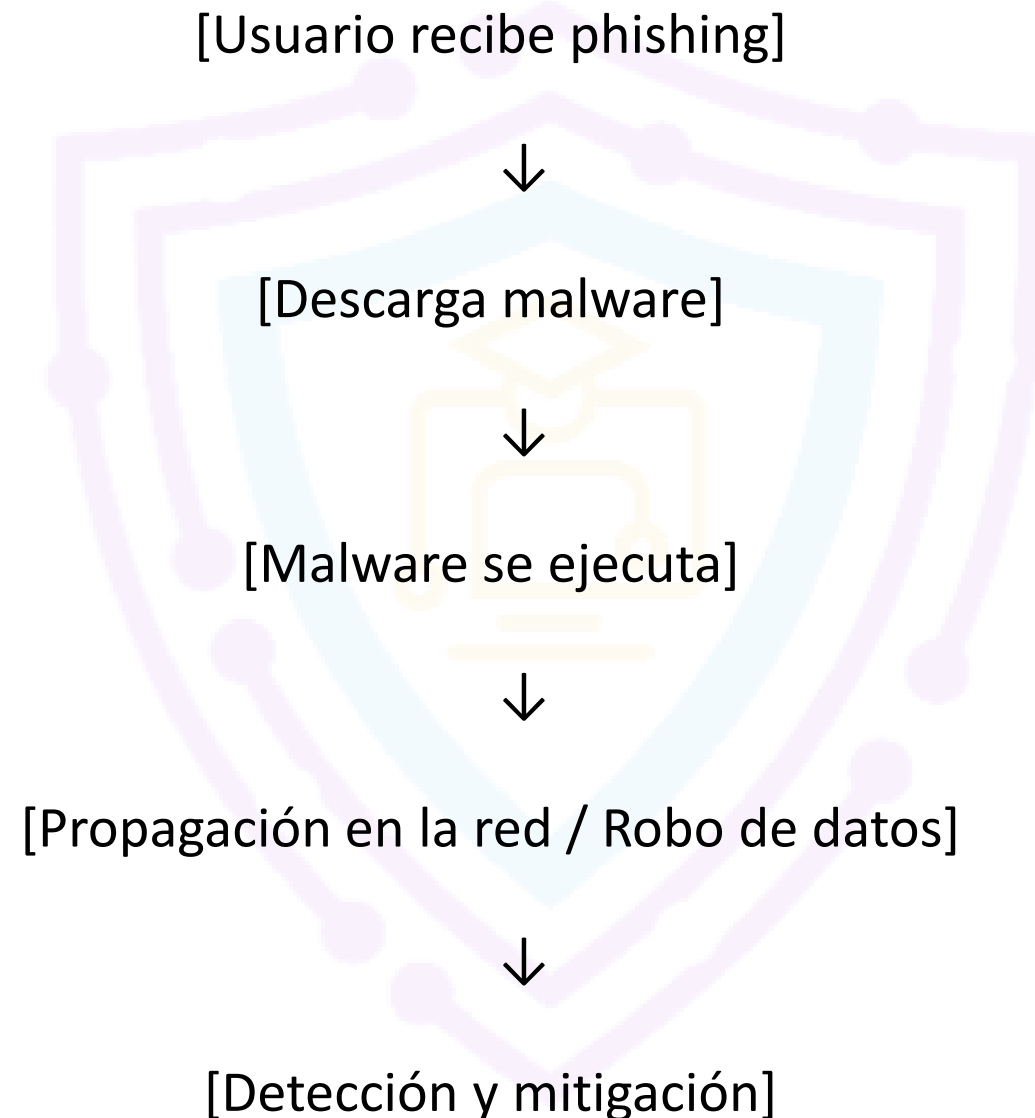


# Técnicas de Mitigación

Técnica	Descripción
<b>Detección temprana</b>	Monitoreo constante con antivirus, EDR y alertas en tiempo real.
<b>Aislamiento</b>	Desconectar el dispositivo afectado para evitar la propagación.
<b>Eliminación</b>	Uso de herramientas de limpieza o formateo completo del sistema.
<b>Reporte</b>	Notificar a equipos internos y autoridades para investigación y prevención futura.



# Flujo de ataque típico





ACADEMIA DE  
**CIBERSEGURIDAD**

# Módulo #3

Introducción a los Centros de Operaciones de Ciberseguridad

**Academia de Ciberseguridad**



# ¿Qué es un SOC?

Un Security Operations Center (SOC) es una unidad centralizada dentro de una organización, responsable de **monitorear, detectar, responder y mitigar amenazas de ciberseguridad**.

- Funciona como el **centro de control** de la seguridad de la empresa.
- Está conformado por analistas y profesionales que usan herramientas especializadas para **vigilar continuamente la infraestructura TI**.
- Su objetivo es **identificar y gestionar incidentes de seguridad** antes de que causen un impacto grave.



# ¿Por qué es importante?

1. **Detección temprana de amenazas:** Identificar ataques en fases iniciales antes de que causen daños graves.
2. **Threat Hunting proactivo:** Buscar amenazas ocultas que evaden herramientas automatizadas.
3. **Respuesta rápida a incidentes:** Contener y mitigar ataques de forma inmediata.
4. **Reducción del tiempo de exposición:** Limitar el tiempo que un atacante permanece dentro de la red.
5. **Gestión de vulnerabilidades:** Detectar, priorizar y corregir fallos críticos en sistemas y aplicaciones.
6. **Cumplimiento normativo:** Garantizar que la organización cumpla con regulaciones y estándares.
7. **Análisis forense:** Investigar incidentes para comprender el ataque y recolectar evidencia.
8. **Integración de inteligencia de amenazas:** Usar información actualizada para anticipar ataques.
9. **Concientización y capacitación:** Educar al personal para evitar errores humanos.



## SOC Center Manager / Director

- **Rol:** Dirige y supervisa todas las operaciones del SOC.
- **Responsabilidades:**
  - Administrar personal, presupuesto y recursos.
  - Definir estrategias y políticas alineadas a los objetivos de seguridad.
  - Coordinar con otras áreas de la organización.

## Team Leader / Manager

- **Rol:** Supervisar y guiar al equipo de analistas del SOC.
- **Responsabilidades:**
  - Asignar tareas y gestionar la carga de trabajo.
  - Coordinar la respuesta a incidentes.
  - Evaluar desempeño y promover la cultura de seguridad.



# Operaciones y Monitoreo

## Security Analyst (Nivel 1, 2 y 3)

- **Rol:** Monitorear eventos, analizar alertas y responder incidentes.
- **Responsabilidades:**
  - **Nivel 1:** Triage de alertas y escalamiento de incidentes.
  - **Nivel 2:** Análisis profundo y determinación de la causa raíz.
  - **Nivel 3:** Liderar incidentes complejos y optimizar controles.

## Operator / Technician

- **Rol:** Operar y mantener herramientas de monitoreo.
- **Responsabilidades:**
  - Responder alertas de seguridad.
  - Dar mantenimiento rutinario.
  - Escalar problemas a analistas de mayor nivel.

## Network Security Analyst

- **Rol:** Supervisar el tráfico de red.
- **Responsabilidades:**
  - Configurar y administrar firewalls, IDS y otros dispositivos.
  - Detectar intrusiones y brechas en la red.



## Endpoint Security Analyst

- **Rol:** Proteger equipos finales (desktops, laptops, móviles).
- **Responsabilidades:**
  - Implementar soluciones de seguridad en endpoints.
  - Realizar evaluaciones de vulnerabilidades y responder incidentes.

## Cloud Security Analyst

- **Rol:** Proteger entornos y servicios en la nube.
- **Responsabilidades:**
  - Evaluar riesgos en plataformas cloud.
  - Monitorear y controlar accesos y configuraciones.



# Respuesta e Investigación

## Incident Responder

•**Rol:** Liderar la respuesta a incidentes críticos.

•**Responsabilidades:**

- Contener y erradicar amenazas.
- Coordinar acciones con las partes involucradas.
- Documentar aprendizajes post-incidente.

## Threat Hunter

•**Rol:** Buscar amenazas avanzadas que evaden defensas automáticas.

•**Responsabilidades:**

- Analizar datos en busca de patrones sospechosos.
- Detectar ataques avanzados antes de que ocurran.

## Forensic Analyst

•**Rol:** Analizar evidencia digital tras un incidente.

•**Responsabilidades:**

- Preservar evidencia para procesos legales.
- Reconstruir eventos para comprender el ataque.



# Inteligencia, Cumplimiento y Riesgo

## Threat Intelligence Analyst

- **Rol:** Recopilar y analizar inteligencia de amenazas.
- **Responsabilidades:**
  - Monitorear actores maliciosos y tendencias globales.
  - Generar reportes de inteligencia accionable.

## Compliance Analyst

- **Rol:** Garantizar cumplimiento normativo.
- **Responsabilidades:**
  - Realizar auditorías internas.
  - Evaluar políticas y regulaciones.
  - Recomendar mejoras para cerrar brechas.

## Vendor Risk Management Analyst

- **Rol:** Gestionar riesgos de ciberseguridad de terceros y proveedores.
- **Responsabilidades:**
  - Evaluar prácticas de seguridad de proveedores.
  - Asegurar cumplimiento de requisitos de seguridad.

## Data Privacy Officer

- **Rol:** Supervisar cumplimiento de leyes de protección de datos.
- **Responsabilidades:**
  - Desarrollar políticas de privacidad.
  - Manejar incidentes relacionados con datos personales.



## Security Engineer

- **Rol:** Diseñar e implementar soluciones técnicas de seguridad.
- **Responsabilidades:**
  - Evaluar riesgos técnicos.
  - Implementar herramientas y sistemas de protección.

## Security Architect

- **Rol:** Diseñar la arquitectura general de seguridad.
- **Responsabilidades:**
  - Definir políticas y estándares.
  - Garantizar que las medidas estén alineadas con los objetivos de negocio.

## SOC Auditor

- **Rol:** Auditar procesos y operaciones del SOC.
- **Responsabilidades:**
  - Evaluar la efectividad de los controles.
  - Recomendar mejoras y detectar fallas.





# Comunicación y Capacitación

## Communication and Coordination Specialist

- **Rol:** Coordinar la comunicación durante incidentes.
- **Responsabilidades:**
  - Facilitar la comunicación entre equipos y stakeholders.
  - Mantener la información clara y precisa durante crisis.

## Security Awareness and Training Specialist

- **Rol:** Capacitar a empleados en buenas prácticas de ciberseguridad.
- **Responsabilidades:**
  - Crear campañas de concientización.
  - Evaluar la efectividad de la formación.

## SOC Trainer

- **Rol:** Entrenar a miembros del SOC.
- **Responsabilidades:**
  - Desarrollar programas de formación interna.
  - Mejorar habilidades técnicas y operativas.



# Roles Avanzados y Especializados

## Penetration Tester

- **Rol:** Evaluar la infraestructura mediante pruebas de penetración.
- **Responsabilidades:**
  - Identificar vulnerabilidades y puntos débiles.
  - Recomendar medidas correctivas.

## Emergency Response & Crisis Management Coordinator

- **Rol:** Coordinar la respuesta durante crisis y emergencias.
- **Responsabilidades:**
  - Establecer planes de contingencia.
  - Comunicar y coordinar acciones durante incidentes graves.

## Physical Security Analyst

- **Rol:** Asegurar activos físicos como edificios y equipos.
- **Responsabilidades:**
  - Identificar riesgos físicos.
  - Implementar controles de seguridad física.

## Legal and Compliance Liaison

- **Rol:** Asegurar que las actividades del SOC cumplan con leyes y regulaciones.
- **Responsabilidades:**
  - Asistir en procesos legales relacionados con incidentes.
  - Guiar al SOC en temas regulatorios.



# Indicadores Clave de Desempeño (KPIs) del SOC

Los **KPIs (Key Performance Indicators)** son métricas esenciales utilizadas para **medir la efectividad, eficiencia y desempeño** de un SOC.

Permiten:

- Evaluar la calidad de las operaciones de seguridad.
- Identificar áreas de mejora.
- Demostrar el valor del SOC a la organización y stakeholders.
- Mejorar la detección, respuesta y prevención de incidentes.

**Beneficio clave:**

Un SOC que monitorea sus KPIs puede **mitigar riesgos**, cumplir con regulaciones y optimizar procesos.



## 1. Detección y Respuesta

### •MTTD (Mean Time to Detect)

- **Descripción:** Tiempo promedio que tarda el SOC en detectar un incidente.
- **Importancia:** Un MTTD bajo indica **detección rápida y eficiente**, reduciendo el impacto.

### •MTTR (Mean Time to Resolve)

- **Descripción:** Tiempo promedio para resolver un incidente después de detectarlo.
- **Importancia:** Un MTTR bajo implica **mitigación rápida** y mínima interrupción operativa.

### •Tasa de Cierre de Incidentes

- **Descripción:** Porcentaje de incidentes resueltos exitosamente.
- **Importancia:** Un valor alto refleja **eficacia en la resolución** y mantenimiento de un entorno seguro.

### •Porcentaje de Falsos Positivos

- **Descripción:** Alertas generadas incorrectamente que no representan amenazas reales.
- **Importancia:** Un porcentaje bajo reduce la carga de trabajo y mejora la eficiencia del SOC.



## 2. Priorización y Calidad de Respuesta

### •Distribución por Severidad de Incidentes

- **Descripción:** Clasificación de incidentes según su nivel de severidad.
- **Importancia:** Permite **priorizar recursos** para amenazas críticas.

### •Uso de Inteligencia de Amenazas

- **Descripción:** Medición de cómo la inteligencia de amenazas mejora las operaciones.
- **Importancia:** Incrementa la **capacidad de prevención y respuesta**.

### •Número Total de Incidentes Detectados

- **Descripción:** Volumen de incidentes en un período específico.
- **Importancia:** Indica la **efectividad de los mecanismos de detección**.



## 3. Concientización y Capacitación

### •Phishing Click Rate

- **Descripción:** Porcentaje de usuarios que hicieron clic en simulaciones de phishing.
- **Importancia:** Evalúa la **eficacia de la capacitación** y la vulnerabilidad de los usuarios.

### •Capacitación y Desarrollo de Habilidades

- **Descripción:** Programas para fortalecer las habilidades del equipo SOC.
- **Importancia:** Garantiza que el personal esté preparado para **amenazas emergentes**.



## 4. Vulnerabilidades y Cumplimiento

### •Vulnerabilidades Abiertas

- **Descripción:** Cantidad de fallos conocidos sin corregir en sistemas y aplicaciones.
- **Importancia:** Indica **riesgos pendientes de mitigación**.

### •Tasa de Cumplimiento de Parches (Patch Compliance)

- **Descripción:** Porcentaje de sistemas actualizados con parches de seguridad.
- **Importancia:** Reduce la exposición a ataques por vulnerabilidades conocidas.

### •Exactitud del Inventario de Activos

- **Descripción:** Precisión en la identificación de hardware, software y dispositivos.
- **Importancia:** Evita que existan **activos no controlados o inseguros**.

### •Cumplimiento Normativo y Regulatorio

- **Descripción:** Nivel de alineación con leyes y regulaciones aplicables.
- **Importancia:** Evita multas y problemas legales.



## 5. Eficiencia Operativa

### •Efectividad de Herramientas de Seguridad

- **Descripción:** Evaluación del desempeño de SIEM, EDR, IDS, etc.
- **Importancia:** Garantiza que las herramientas brinden **protección real**.

### •Tendencias y Patrones de Incidentes

- **Descripción:** Análisis de incidentes a lo largo del tiempo.
- **Importancia:** Permite **anticipar ataques recurrentes**.

### •Utilización de Recursos y Carga de Trabajo

- **Descripción:** Medición de la asignación de recursos en el SOC.
- **Importancia:** Evita la **sobrecarga de analistas** y mejora la eficiencia.

### •Costo por Incidente

- **Descripción:** Costo promedio que implica atender un incidente.
- **Importancia:** Ayuda a **optimizar presupuestos** y justificar inversiones.





## 6. Comunicación y Coordinación

### •Efectividad de la Comunicación

- **Descripción:** Calidad y rapidez de la comunicación interna y externa durante incidentes.
- **Importancia:** Favorece decisiones rápidas y coordinación efectiva.

### •Colaboración con Entidades Externas

- **Descripción:** Trabajo conjunto con proveedores, pares de la industria y autoridades.
- **Importancia:** Mejora el intercambio de inteligencia y fortalece la defensa.

### •Reporte de Incidentes Legales y Regulatorios

- **Descripción:** Proceso de informar incidentes a autoridades competentes.
- **Importancia:** Garantiza cumplimiento y colaboración con organismos legales.



## 7. Preparación y Mejora Continua

### •Ejercicios de Red Team

- **Descripción:** Resultados de simulaciones de ataques reales.
- **Importancia:** Mide la **capacidad de respuesta ante ataques avanzados**.

### •Manejo de Zero-Day y Amenazas Desconocidas

- **Descripción:** Habilidad para detectar y responder a amenazas no identificadas previamente.
- **Importancia:** Protege contra ataques emergentes.

### •Monitoreo de Amenazas Internas

- **Descripción:** Supervisión de actividades sospechosas de empleados o socios.
- **Importancia:** Previene daños desde dentro de la organización.

### •Preparación ante DDoS

- **Descripción:** Capacidad de respuesta frente a ataques de denegación de servicio.
- **Importancia:** Garantiza la **continuidad operativa**.

### •Mejora Continua

- **Descripción:** Actualización constante de procesos y tecnologías.
- **Importancia:** Mantiene al SOC **adaptado a amenazas en evolución**.



# Métricas del SOC

Las **métricas del SOC** son indicadores utilizados para medir la **efectividad del SOC** en la detección, respuesta y mitigación de amenazas de ciberseguridad.

## Objetivos principales:

- Evaluar el desempeño del equipo de seguridad.
- Identificar áreas de mejora en procesos y herramientas.
- Tomar decisiones basadas en datos para fortalecer la postura de seguridad.
- Mostrar la evolución y madurez del SOC a lo largo del tiempo.

## Diferencia con KPIs:

- **KPIs:** Visión estratégica y de negocio.
- **Métricas:** Datos operativos y técnicos para la gestión diaria.



# Métricas de Incidentes

## •Número de Incidentes de Seguridad

- **Descripción:** Total de incidentes detectados en un periodo específico.
- **Importancia:** Ayuda a visualizar la **frecuencia y tendencia** de amenazas.

## •Tasa de Detección de Incidentes

- **Descripción:** Porcentaje de incidentes detectados por el SOC frente al total real.
- **Importancia:** Mide la **efectividad de los mecanismos de monitoreo**.

## •Tiempo de Respuesta a Incidentes

- **Descripción:** Tiempo promedio que tarda el SOC en **responder** a un incidente.
- **Importancia:** Refleja la agilidad en la **contención y mitigación** de amenazas.

## •Tiempo para Cerrar Incidentes

- **Descripción:** Tiempo promedio desde la **detección hasta la resolución**.
- **Importancia:** Indica la **eficiencia en la gestión y resolución** de incidentes.

## •Distribución por Severidad de Incidentes

- **Descripción:** Clasificación de incidentes en bajo, medio y alto impacto.
- **Importancia:** Permite **priorizar recursos y esfuerzos**.

## •Tiempo Promedio Entre Incidentes (MTBSI)

- **Descripción:** Intervalo promedio entre incidentes consecutivos.
- **Importancia:** Indica la **resiliencia de la organización** frente a ataques recurrentes.



# Inteligencia de Amenazas y Detección

## •Uso de Inteligencia de Amenazas

- **Descripción:** Medición de cuánto se aprovecha la inteligencia para decisiones de seguridad.
- **Importancia:** Mejora la **detección y respuesta proactiva** ante amenazas emergentes.

## •Tasa de Falsos Positivos

- **Descripción:** Porcentaje de alertas incorrectas que no corresponden a amenazas reales.
- **Importancia:** Una tasa baja **optimiza recursos y reduce ruido operativo**.

## •Tasa de Verdaderos Positivos

- **Descripción:** Porcentaje de alertas correctas que representan amenazas reales.
- **Importancia:** Garantiza la **precisión en la detección**.

## •Análisis de Tendencias y Patrones de Incidentes

- **Descripción:** Estudio de amenazas recurrentes y su evolución.
- **Importancia:** Permite **anticipar ataques y fortalecer controles**.

## •Manejo de Zero-Day y Amenazas Desconocidas

- **Descripción:** Capacidad para detectar y mitigar amenazas **sin firmas conocidas**.
- **Importancia:** Fundamental para **defenderse de ataques avanzados**.



# Concientización y Capacitación

## •Tasa de Simulación de Phishing

- **Descripción:** Porcentaje de empleados que caen en simulaciones de phishing.
- **Importancia:** Mide la **eficacia de la formación en ciberseguridad**.

## •Mejora en Conciencia de Usuarios

- **Descripción:** Evolución en el comportamiento seguro de los usuarios a lo largo del tiempo.
- **Importancia:** Indica si los programas de capacitación **reducen riesgos humanos**.

## •Efectividad de la Capacitación y Desarrollo de Habilidades

- **Descripción:** Impacto de la capacitación en la reducción de incidentes y errores.
- **Importancia:** Justifica la **inversión en formación** y mide su ROI.



# Vulnerabilidades y Gestión de Activos

## •Número de Vulnerabilidades Identificadas

- **Descripción:** Total de vulnerabilidades encontradas en sistemas y aplicaciones.
- **Importancia:** Ayuda a **priorizar esfuerzos de remediación.**

## •Tasa de Cumplimiento de Parches

- **Descripción:** Porcentaje de sistemas actualizados con parches recientes.
- **Importancia:** Reduce la **exposición a ataques conocidos.**

## •MTTP (Mean Time to Patch)

- **Descripción:** Tiempo promedio para aplicar parches después de su liberación.
- **Importancia:** Mide la **eficiencia en la gestión de vulnerabilidades.**

## •Exactitud del Inventario de Activos

- **Descripción:** Precisión en el registro de hardware, software y dispositivos.
- **Importancia:** Evita **activos no controlados** y riesgos asociados.

## •Postura de Seguridad en Endpoints

- **Descripción:** Nivel general de protección de equipos finales.
- **Importancia:** Evalúa la **efectividad de controles en dispositivos de usuario final.**



## •Efectividad de la Colaboración Interna

- **Descripción:** Medición del trabajo en equipo dentro del SOC.
- **Importancia:** Favorece **respuesta rápida y coordinada** a incidentes.

## •Colaboración con Entidades Externas

- **Descripción:** Nivel de cooperación con vendors, peers y autoridades.
- **Importancia:** Mejora la **resiliencia y el intercambio de inteligencia**.

## •Costo por Incidente

- **Descripción:** Promedio de costos derivados de la gestión de un incidente.
- **Importancia:** Identifica áreas de **optimización financiera**.

## •Resultados de Ejercicios Red Team

- **Descripción:** Evaluación basada en simulaciones de ataques reales.
- **Importancia:** Mide la **capacidad defensiva ante amenazas avanzadas**.





## •Adherencia a Regulaciones y Normativas

- **Descripción:** Nivel de cumplimiento con leyes y estándares de ciberseguridad.
- **Importancia:** Evita sanciones legales y pérdida de confianza.

## •Cumplimiento de Políticas Internas

- **Descripción:** Porcentaje de cumplimiento con políticas de seguridad internas.
- **Importancia:** Garantiza consistencia en las prácticas de seguridad.

## •Satisfacción de Clientes y Retroalimentación

- **Descripción:** Opinión de clientes internos y externos sobre el desempeño del SOC.
- **Importancia:** Mide la calidad percibida del servicio de seguridad.



# Mejora Continua

## •Iniciativas de Mejora Continua

- **Descripción:** Actividades para evolucionar procesos y controles del SOC.
- **Importancia:** Mantiene la **adaptabilidad ante nuevas amenazas**.

## •Innovación Tecnológica

- **Descripción:** Uso de tecnologías emergentes en operaciones SOC.
- **Importancia:** Mejora la **detección y respuesta ante ataques avanzados**.



# Modelos de Madurez de un SOC

Los **modelos de madurez de SOC** son marcos que permiten evaluar y mejorar la **efectividad y capacidades** de un Security Operations Center.

Estos modelos ayudan a:

- Medir el **nivel actual de madurez** del SOC.
- Identificar **brechas y áreas de mejora**.
- Definir un **plan estratégico** para fortalecer la ciberseguridad.
- Priorizar inversiones y recursos de forma eficiente.



# Componentes Clave del Modelo de Madurez

## 1. Personas (People)

1. Se enfoca en las **habilidades, conocimientos y capacitación** del equipo SOC.
2. SOC's más maduros cuentan con analistas **altamente capacitados** para detectar, responder y mitigar amenazas.

## 2. Procesos (Process)

1. Incluye **SOPs (Procedimientos Operativos Estándar)** y flujos de trabajo claros.
2. Garantiza una **respuesta consistente y eficiente** ante incidentes.

## 3. Tecnología (Technology)

1. Uso de herramientas como **SIEM, EDR, SOAR, IDS/IPS**.
2. La tecnología adecuada mejora la **detección y respuesta en tiempo real**.

## 4. Gobernanza (Governance)

1. Supervisión y toma de decisiones estratégicas.
2. Alinea las operaciones del SOC con los **objetivos del negocio y regulaciones vigentes**.

## 5. Integración de Inteligencia de Amenazas (Threat Intelligence)

1. Combina inteligencia de amenazas con las operaciones del SOC.
2. Mejora la **capacidad de detección proactiva** y reduce riesgos.

## 6. Comunicación y Colaboración

1. Fomenta la **coordinación entre equipos** y departamentos.
2. Asegura respuestas rápidas y efectivas durante incidentes.

## 7. Mejora Continua (Continuous Improvement)

1. Evaluaciones regulares para **adaptarse a nuevas amenazas**.
2. Optimización constante de procesos, personas y tecnología.



# Beneficios de Implementar un Modelo de Madurez

## 1. Planificación Estratégica

- Define una **estrategia a largo plazo** para fortalecer el SOC.
- Prioriza proyectos alineados con los **objetivos de negocio y seguridad**.

## 2. Mejora Continua

- Evaluaciones periódicas para detectar **áreas de optimización**.
- Impulsa la evolución constante frente a amenazas cambiantes.

## 3. Optimización de Recursos

- Uso eficiente de **tecnología, personal e inversión**.
- Identifica áreas que requieren **más inversión o reasignación**.

## 4. Mitigación de Riesgos

- Detecta **vulnerabilidades y deficiencias** en procesos de seguridad.
- Permite una **respuesta proactiva** para minimizar el impacto de incidentes.



# Beneficios de Implementar un Modelo de Madurez

## 5. Adaptabilidad ante Nuevas Amenazas

- Prepara a la organización para **amenazas emergentes**.
- Anticipa riesgos y facilita la implementación rápida de medidas.

## 6. Comunicación y Colaboración

- Fomenta la integración entre **equipos internos y externos**.
- Mejora la **coordinación y la defensa integral**.

## 7. Cumplimiento Regulatorio

- Simplifica la **gestión de regulaciones y auditorías**.
- Reduce el riesgo de sanciones y mejora la **transparencia**.



# Desafíos en la Operación de un SOC

Operar un **SOC (Security Operations Center)** es una tarea crítica pero compleja, ya que implica proteger a la organización contra un panorama de amenazas cibernéticas en constante cambio.

Los equipos SOC deben enfrentarse a retos que afectan su **eficacia, eficiencia y capacidad de respuesta**, lo que puede poner en riesgo la seguridad de la organización.

## **Factores clave que complican la operación:**

- Evolución constante de amenazas cibernéticas.
- Gran volumen de alertas y datos a analizar.
- Escasez de profesionales capacitados.
- Complejidad en la integración de herramientas y procesos.
- Exigencias regulatorias cada vez más estrictas.



# Volumen de Alertas

Los sistemas de seguridad generan miles de alertas diariamente, muchas de ellas irrelevantes.

## •Impacto:

- Sobrecarga en los analistas (**alert fatigue**).
- Riesgo de que **alertas críticas pasen desapercibidas**.
- Retrasos en la detección y respuesta a incidentes.





# Escasez de Talento (Skills Shortage)

Falta de profesionales capacitados en ciberseguridad, especialmente en áreas especializadas de SOC.

## •Impacto:

- Dificultad para **reclutar y retener talento**.
- Sobrecarga de trabajo en equipos pequeños.
- Gaps en la cobertura de seguridad y reducción de la eficiencia.



# Amenazas Avanzadas (Advanced Threats)

Amenazas como **APTs (Advanced Persistent Threats)** y **zero-day exploits** que evaden mecanismos tradicionales de defensa.

## •Impacto:

- Mayor probabilidad de ataques exitosos.
- Necesidad constante de **actualización en técnicas y conocimientos**.
- Incremento en el nivel de sofisticación de las defensas requeridas.



# Fatiga de Alertas (Alert Fatigue)

Cuando los analistas se saturan por la gran cantidad de alertas repetitivas o irrelevantes.

## •Impacto:

- Pérdida de foco y disminución de efectividad.
- Respuesta lenta o nula ante incidentes graves.
- Posibles amenazas no detectadas.



# Complejidad de la Infraestructura IT

Ambientes híbridos con sistemas **legados y modernos**, múltiples herramientas y plataformas.

## •Impacto:

- Dificultad para correlacionar eventos y amenazas.
- Mayor riesgo de **brechas de seguridad**.
- Procesos lentos y poco integrados.



# Tiempos de Respuesta a Incidentes

La detección y respuesta deben ser **rápidas** para minimizar daños.

## •Impacto:

- Respuestas tardías generan **mayor impacto y pérdidas**.
- Mayor tiempo de inactividad en sistemas críticos.
- Deterioro de la postura de seguridad.

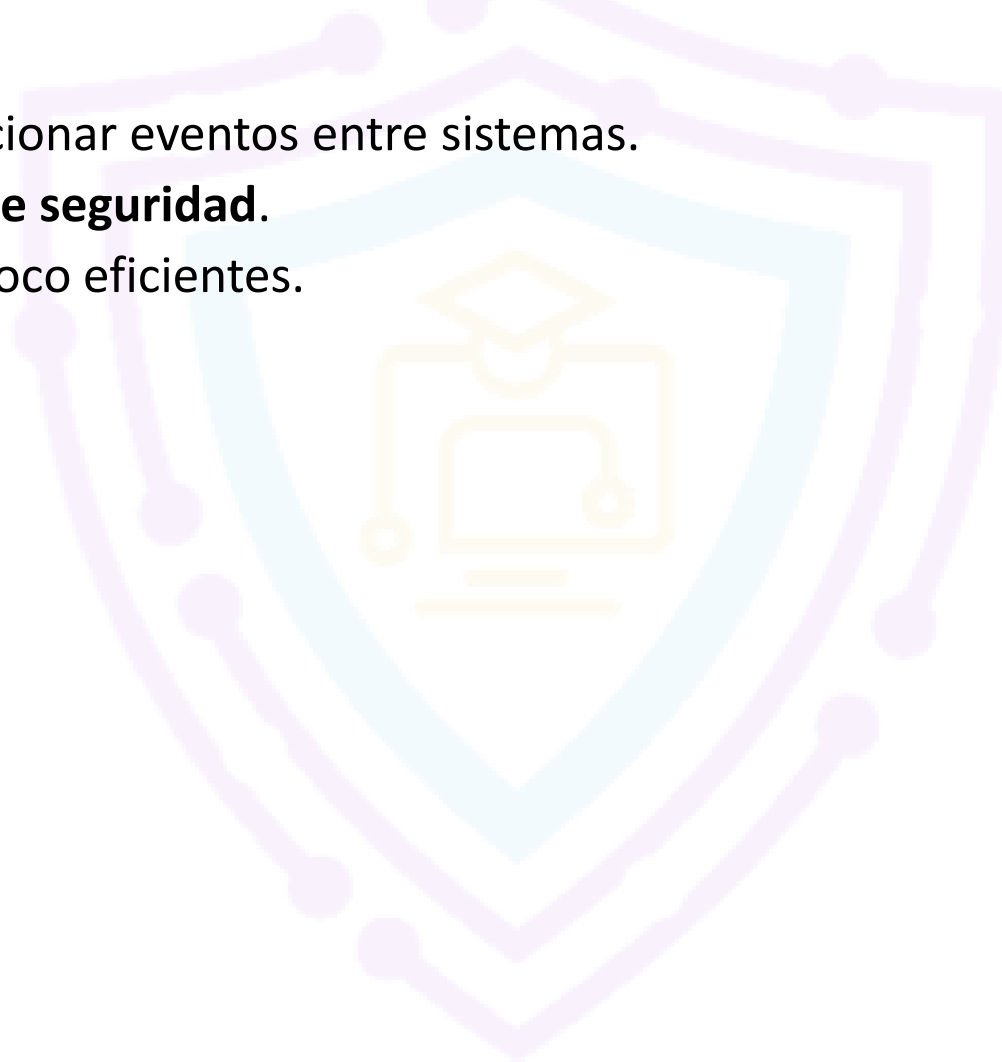


# Integración de Tecnologías

Los SOC suelen usar diversas herramientas que no siempre están bien integradas.

## •Impacto:

- Dificultad para correlacionar eventos entre sistemas.
- **Gaps en la cobertura de seguridad.**
- Procesos manuales y poco eficientes.



# Cumplimiento Regulatorio

Obligación de cumplir con leyes y regulaciones como GDPR, HIPAA, ISO 27001, etc.

## •Impacto:

- Riesgo de **multas y sanciones financieras**.
- Pérdida de confianza por incumplimiento.
- Procesos adicionales de auditoría y documentación.



# Amenazas Internas (Insider Threats)

Riesgos causados por **empleados, contratistas o socios**, ya sea por error o intención maliciosa.

## •Impacto:

- Detección más difícil que ataques externos.
- Brechas internas con acceso privilegiado.
- Necesidad de tecnologías especializadas para monitoreo de comportamiento.





# Presupuesto Limitado

Los SOC requieren inversión constante en:

- Tecnología.
- Personal.
- Capacitación.

## •Impacto:

- Limitaciones en la compra de herramientas avanzadas.
- Plantillas reducidas y sobrecarga operativa.
- Aumento en el riesgo de incidentes.



# Capacitación y Desarrollo Continuo

La ciberseguridad cambia rápidamente, por lo que el equipo SOC debe **actualizarse de forma constante**.

## •Impacto:

- Mejora continua de habilidades frente a amenazas emergentes.
- Reducción de errores y tiempos de respuesta.
- Fortalecimiento de la resiliencia del SOC.





ACADEMIA DE  
**CIBERSEGURIDAD**

# Módulo #4

## SOC: Componentes y Arquitectura

**Academia de Ciberseguridad**

# Tareas Principales en Operaciones de Seguridad

## 1. Monitoreo de Seguridad:

1. Recolección y análisis de datos para detectar comportamientos anómalos en la red.
2. Escalamiento de actividades maliciosas hacia sistemas de respuesta a incidentes.

## 2. Gestión de Incidentes de Seguridad:

1. Detección, gestión y seguimiento de vulnerabilidades en tiempo real.
2. Minimizar el impacto negativo sobre las operaciones.

## 3. Gestión de Vulnerabilidades:

1. Identificación, evaluación y mitigación continua de fallos en sistemas y redes.

## 4. Gestión de Dispositivos de Seguridad:

1. Administración de la infraestructura y dispositivos de seguridad.
2. Actualizaciones y mantenimiento para cumplir regulaciones.

## 5. Monitoreo de Flujos de Red (Network-Flow Monitoring):

1. Análisis de tráfico de red para detectar patrones sospechosos y generar alertas.



# El Rol del SOC en la Organización

El **SOC (Security Operations Center)** es la unidad central encargada de **monitorear, gestionar y analizar la seguridad en tiempo real**, permitiendo:

- Detectar y responder a intrusiones antes de que afecten las operaciones.
- Servir como **centro de control** y defensa de la ciberseguridad.
- Generar **alertas en tiempo real** para amenazas activas.

## **Fuentes de información clave:**

- Logs de sistemas y servidores.
- IDS/IPS.
- Firewalls.
- Endpoints.
- Flujos de red y datos.



# Modelo de Cooperación del SOC

El SOC opera bajo un **triángulo clave**:

**1.Personas:** Analistas, operadores y especialistas, internos o externos.

**2.Procesos:** Flujos y procedimientos estandarizados para gestionar incidentes.

**3.Tecnología:** Herramientas que permiten automatización y análisis avanzado.

*Objetivo:* Mantener comunicación constante y respuesta inmediata a incidentes.



# Componentes Clave de un SOC

## 1. SOC Analysts (Analistas SOC)

Monitorean alertas y eventos en tiempo real.

Analizan incidentes y aplican medidas de mitigación.

Requieren conocimientos sólidos de redes, ciberseguridad y sistemas.

## 2. Incident Responders (Respondedores de Incidentes)

Especialistas en **contener y erradicar amenazas**.

Investigan la causa raíz y aplican medidas correctivas.

Buscan minimizar el impacto en las operaciones del negocio.

## 3. Security Engineers (Ingenieros de Seguridad)

Diseñan y mantienen la **infraestructura de seguridad**.

Configuran firewalls, IDS/IPS y herramientas avanzadas.

Garantizan que los controles de seguridad estén correctamente integrados.



# Componentes Clave de un SOC

## 4. Threat Intelligence Analysts (Analistas de Inteligencia de Amenazas)

Recolectan y analizan información sobre amenazas emergentes.

Priorizan riesgos y proporcionan información crítica para la defensa proactiva.

Integran feeds de inteligencia para anticiparse a ataques.

## 5. Incident Detection & Response (IDR)

Procesos para **detectar, clasificar y responder** a incidentes de seguridad.

Flujos de trabajo estandarizados que aseguran respuestas rápidas y coordinadas.

## 6. Procedimientos de Escalamiento

Definen **niveles de intervención** según la gravedad del incidente.

Determinan qué equipos o personal deben actuar en cada fase.

Reducen tiempos de respuesta y aseguran la continuidad del negocio.





# Componentes Clave de un SOC

## 7. Integración de Inteligencia de Amenazas

Mejora la capacidad de **detección en tiempo real**.

Proporciona contexto para interpretar eventos de seguridad.

Permite una defensa basada en información actualizada.

## 8. Documentación

Registro detallado de incidentes, procedimientos y lecciones aprendidas.

Facilita **mejora continua** y cumplimiento normativo.

Permite análisis histórico de tendencias y debilidades.

## 9. SIEM (Security Information and Event Management)

Herramienta central para recolectar y analizar logs en tiempo real.

Correlaciona información de diversas fuentes.

Prioriza alertas y optimiza la investigación de incidentes.



# Componentes Clave de un SOC

## 10. IDPS (Intrusion Detection & Prevention Systems)

Detectan y previenen actividades sospechosas en la red.

Pueden actuar automáticamente para bloquear amenazas.

Protegen datos sensibles y sistemas críticos.

## 11. Firewalls y Proxies

**Firewalls:** Filtran tráfico por IPs, puertos y protocolos.

**Proxies:** Inspeccionan tráfico web y actúan como intermediarios.

Previenen accesos no autorizados y reducen riesgos de ataques.

## 12. Endpoint Protection (Protección de Dispositivos Finales)

Incluye **antivirus, EDR y mecanismos avanzados**.

Defiende equipos como laptops, móviles y estaciones de trabajo.

Reduce riesgos de malware, ransomware y phishing.



# Personas en el SOC

El recurso más importante de un SOC son **las personas**.

Cada miembro del SOC cumple un rol específico, con tareas, habilidades y responsabilidades definidas que permiten:

- **Monitorear** eventos de seguridad.
- **Analizar y responder** a incidentes.
- **Gestionar la infraestructura de seguridad**.
- **Definir estrategias y políticas** que fortalezcan la ciberseguridad.

## Factores clave:

- Cada rol debe contar con **descripción de puesto**, habilidades requeridas y certificaciones recomendadas.
- Las responsabilidades dependen de factores como el **tamaño de la empresa**, el **presupuesto**, la **estructura organizacional** y sus **objetivos de seguridad**.
- Uno de los mayores desafíos es la **escasez de personal capacitado**, lo que puede generar sobrecarga laboral y menor eficiencia.



# Roles Principales en un SOC

Estos roles son comunes en la mayoría de SOC's, aunque la cantidad de personal y su nivel de especialización varían según la organización.

## 1. SOC Analysts (Analistas SOC)

Los **analistas SOC** son la **primera línea de defensa** digital.

Se encargan de monitorear y analizar alertas, además de responder a amenazas para proteger los activos de la organización.



# Nivel 1 - Monitoreo y Detección Inicial

## •Rol:

Ejecutar tareas operativas diarias y monitorear alertas automáticas.

## •Responsabilidades:

- Monitorear eventos en firewalls, antivirus, IDS/IPS y otros sistemas.
- Analizar logs para identificar actividades sospechosas.
- Realizar investigación inicial de alertas y determinar su relevancia.
- Mantener comunicación y documentación actualizada de incidentes.
- Monitorear vulnerabilidades y apoyar en auditorías internas y externas.
- Investigar tendencias de amenazas emergentes para fortalecer la postura de seguridad.



# Nivel 2 - Análisis Profundo y Remediación Básica

## •Rol:

Gestionar colas de alertas y realizar análisis avanzados para determinar causas raíz.

## •Responsabilidades:

- **Priorizar alertas** según su criticidad e impacto.
- Realizar investigaciones profundas y correlacionar eventos.
- Identificar **falsos positivos** y filtrarlos para optimizar recursos.
- Gestionar tickets y asegurar tiempos de respuesta adecuados.
- Ejecutar **acciones básicas de remediación** para contener incidentes.



## 2. Incident Responders (Respondedores de Incidentes)

### Rol:

Investigar y responder de forma inmediata a incidentes críticos.  
También conocidos como *intrusion analysts*.

### Responsabilidades:

Análisis detallado de redes y sistemas comprometidos.

Detección de **Indicadores de Compromiso (IoCs)** y amenazas activas.

**Análisis de malware y reverse engineering** para entender ataques.

Creación de reportes de riesgo para la alta dirección.

Coordinación con equipos legales, de IT y comunicación.

Definir planes de respuesta y estrategias de mitigación.



# Security Engineers (Ingenieros de Seguridad)

## •Rol:

Diseñar, implementar y mantener la **infraestructura tecnológica de seguridad**.

## •Responsabilidades:

- Implementar y gestionar herramientas clave como SIEM, IDS/IPS y firewalls.
- Revisar y actualizar la arquitectura de seguridad regularmente.
- Aplicar parches y configuraciones para cerrar brechas de seguridad.
- Colaborar con equipos de IT, redes y desarrollo.
- Evaluar nuevas tecnologías y amenazas para mejorar el SOC.





## •Rol:

Recolectar, analizar e interpretar información sobre **amenazas emergentes** para anticiparse a ataques.

## •Responsabilidades:

- Monitorear fuentes de inteligencia, incluyendo:
  - OSINT (fuentes abiertas).
  - Foros de la dark web.
  - Feeds especializados.
- Correlacionar datos externos con eventos internos.
- Crear reportes con IoCs y recomendaciones para el equipo SOC.
- Compartir información con comunidades, grupos industriales y agencias gubernamentales.



# SOC Managers (Gerentes de SOC)

## •Rol:

Liderar el SOC, proporcionando dirección estratégica y asegurando que las operaciones se alineen con los objetivos de la organización.

## •Responsabilidades:

- Desarrollar planes estratégicos y políticas de seguridad.
- Administrar recursos como personal, presupuesto y tecnología.
- Reclutar, capacitar y retener talento especializado.
- Comunicar avances y riesgos a la alta dirección.
- Garantizar el cumplimiento de regulaciones y estándares de la industria.
- Coordinar la relación entre el SOC y otras áreas de la empresa.



# Cadena de Mando en un SOC

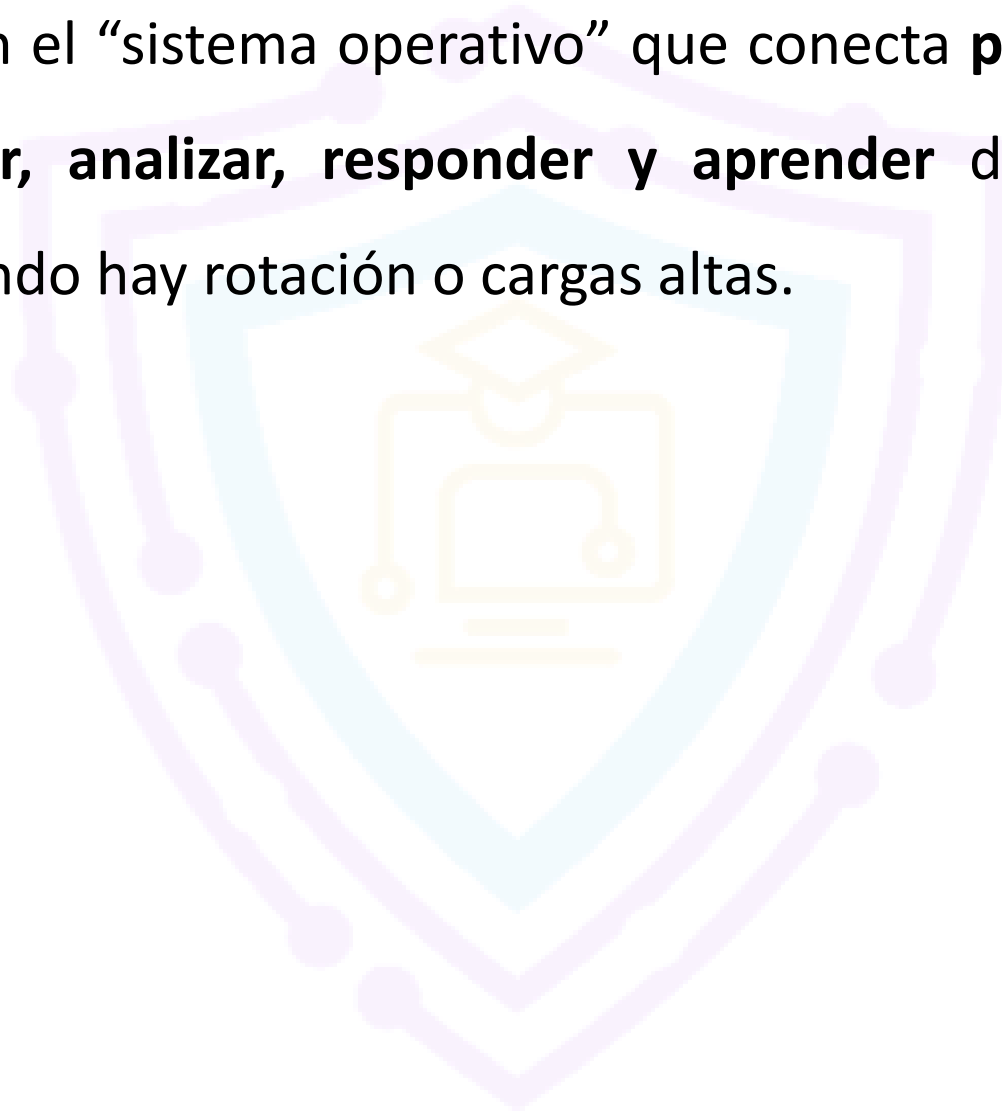
Un SOC efectivo cuenta con una estructura jerárquica clara:

- 1. Analistas Nivel 1 y 2** → Monitoreo y respuesta inicial.
- 2. Incident Responders y Analistas de Inteligencia** → Profundización y mitigación.
- 3. Ingenieros de Seguridad** → Gestión de infraestructura y herramientas.
- 4. SOC Manager** → Supervisión y decisiones estratégicas.
- 5. CISO (Chief Information Security Officer)** → Dirección general de la estrategia de seguridad.



# Procesos en un SOC

Los procesos del SOC son el “sistema operativo” que conecta **personas, tecnología y playbooks** para **detectar, analizar, responder y aprender** de los incidentes con consistencia, incluso cuando hay rotación o cargas altas.



# Proceso 1: Detección de incidentes

## Qué es

Detección temprana de actividad maliciosa mediante **correlación** y **analítica**.

## Entradas

- Logs (SIEM), **telemetría** (EDR/NDR), IDS/IPS, UBA/UEBA, TI feeds, NetFlow.

## Actividades

- Correlación de eventos y **detección por firmas** (conocidas) y **comportamiento** (desconocidas).
- Enriquecimiento con **IoCs** (IPs, dominios, hashes).

## Salidas

- **Alertas calificadas** (sospecha fundada) → pasan a **triage**.
- **Ruido filtrado** (descartes y supresión de reglas/uso).

## Métricas

- **MTTD**, tasa de verdaderos positivos, % **falsos positivos**, cobertura de fuentes.



# Proceso 2: Triage de alertas

## Objetivo

Priorizar lo crítico y reducir el ruido.

## Actividades

- Evaluar **contexto e impacto** (activo afectado, criticidad, exposición).
- Asignar **severidad** (Alta/Media/Baja) y **SLA**.
- Decidir **FP/TP** y **siguiente acción** (investigar, contener, cerrar).

## Salidas

- Ticket con **prioridad, propietario, SLA**, hipótesis inicial y evidencia.
- Reglas de **tuning** (umbral, listas de confianza/bloqueo).

## Métricas

- Tiempo de triage, % **FP**, cumplimiento de SLA en P1/P2.



# Proceso 3: Investigación y análisis

## Objetivo

Confirmar el incidente, **alcance** y **causa raíz**.

## Actividades

- **Forense**: imagen de disco/memoria, timeline, artefactos (prefetch, logs).
- **Análisis de malware**: estático/dinámico, TTPs y C2, firmas/loCs.
- **Integración de Threat Intel**: contexto de actor/campaña.
- **Reconstrucción**: vector inicial, privilegios, **movimiento lateral**, exfiltración.

## Salidas

- Informe técnico con **causa raíz**, loCs, hipótesis confirmada, riesgo/impacto.
- Recomendaciones tácticas y estratégicas.

## Métricas

- **Tiempo a causa raíz**, % investigaciones concluidas, repetición por misma causa.



# Proceso 4: Respuesta a incidentes

**Contener, erradicar y recuperar** con mínima interrupción.

## Playbooks

- Ransomware, Phishing BEC, WebShell, EDR-Detection, Lateral Movement, Cloud Key Leak.

## Actividades

- **Contención:** aislar host/segmento, bloquear IoCs, revocar credenciales.
- **Erradicación:** limpieza artefactos, parcheo, rotación de llaves/secretos.
- **Recuperación:** restaurar servicios/backup, validaciones post-recovery.
- **Coordinación:** IT, Legal/Compliance, Comunicaciones, RR.HH. (si aplica).

## Salidas

- Estado de incidente (**P1/P2**), acciones ejecutadas, lecciones inmediatas.

## Métricas

- **MTTR**, cumplimiento de **SLA** de contención/erradicación, tiempo de caída.





# Proceso 5: Gestión de vulnerabilidades

## Objetivo

Reducir superficie de ataque **antes** de que ocurra el incidente.

## Actividades

- **Inventario** y clasificación de activos.
- **Escaneo** continuo (red, app, cloud, contenedores).
- **Riesgo**: CVSS + **explotabilidad** (EPSS), exposición pública, valor del activo.
- **Remediación**: parches, mitigaciones compensatorias, excepciones con fecha.

## Métricas

- **MTTP** (Mean Time To Patch), % parches críticos en SLA, vulnerabilidades abiertas (por severidad).



# Proceso 6: Monitoreo de seguridad

## Objetivo

Observabilidad continua para **detección en tiempo real**.

## Capas

- **Red** (NDR/IDS, NetFlow, DNS).
- **Endpoint** (EDR, integridad de archivos).
- **Identidad** (IAM/IdP, MFA, UBA).
- **Cloud/SaaS** (CSPM, CWPP, logs nativos).
- **Aplicaciones** (WAF, logs app, API).

## Métricas

- Cobertura de **fuentes** en SIEM, latencia de ingesta, integridad de logs.



# Proceso 7: SOAR (Orquestación y Automatización)

Bajar **MTTD/MTTR** y **carga manual**.

## Automatizar

- Enriquecimiento (VT/Whois/GeoIP), bloqueo de IoCs, cuarentena EDR, avisos a usuarios, creación/actualización de tickets, notificaciones a on-call.

## Orquestar

- Flujos multi-herramienta con **aprobaciones humanas** para acciones disruptivas.

## Métricas

- % de casos con **auto-enriquecimiento**, acciones automáticas exitosas, minutos ahorrados.



# Proceso 8: Caza de amenazas (Threat Hunting)

## Objetivo

Encontrar **lo que no alertó**.

## Enfoques

- **Hypothesis-driven** (MITRE ATT&CK/TTPs).
- **Data-driven** (anomalías en telemetría).
- **Intel-driven** (actor/campaña).

## Entregables

- Hallazgos, **nuevas reglas/detecciones**, hardening, IoCs y consultas reutilizables.

## Métricas

- Hunts ejecutados/mes, **detecciones nuevas** creadas, incidentes prevenidos.



# Proceso 9: Mejora continua

## Ciclo

- **Post-mortem** sin culpables → acciones correctivas.
- **Métricas/KPIs** (MTTD/MTTR, cierre, FP/TP).
- **Actualización** de playbooks, casos de prueba y capacitación.

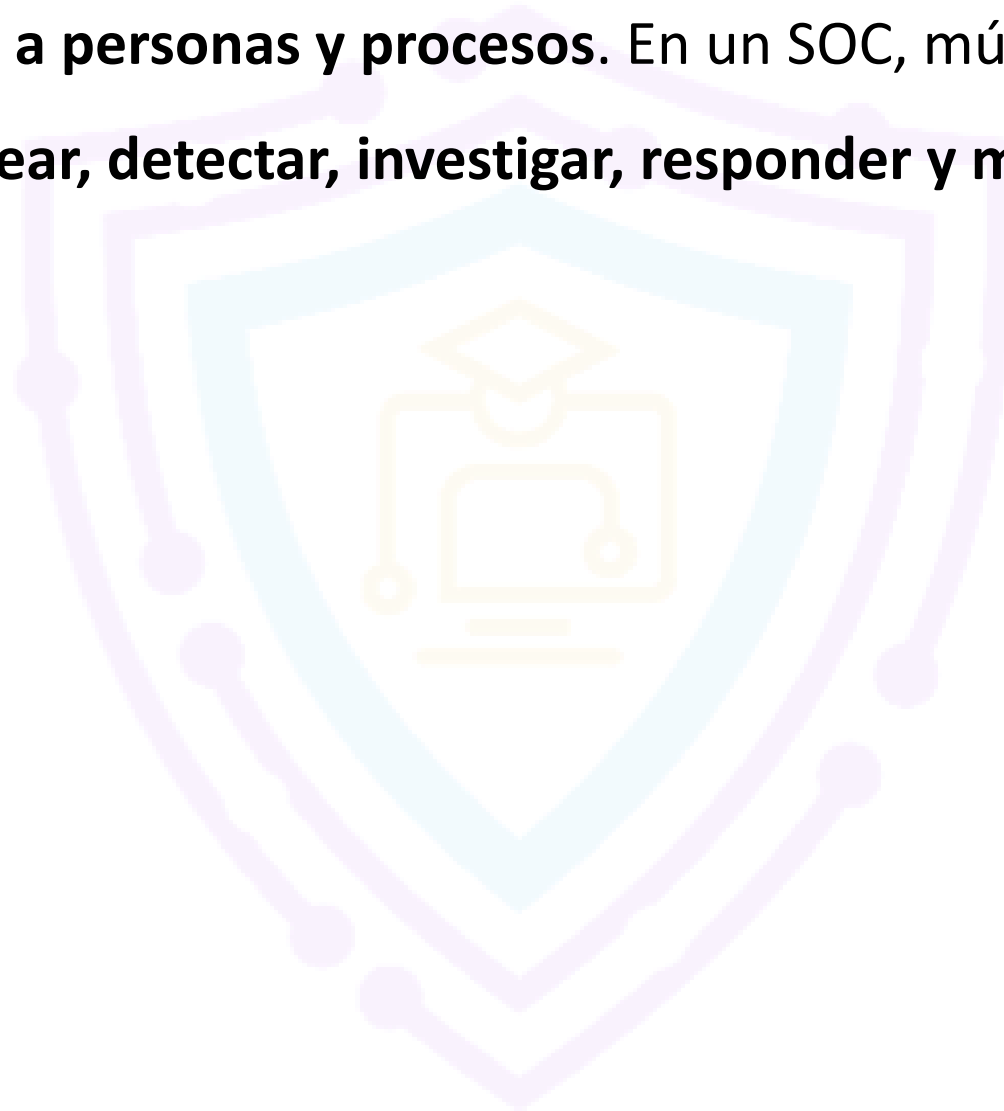
## Métricas

- % acciones post-mortem cerradas a tiempo, reducción de reincidencias.



# Tecnologías en un SOC

La tecnología debe **servir a personas y procesos**. En un SOC, múltiples herramientas se integran para **monitorear, detectar, investigar, responder y mejorar** continuamente.



# Mapa de Tecnologías (visión global)

- **Detección & Monitoreo:** SIEM, IDPS, EDR, UEBA, NTA, Log Management.
- **Respuesta & Eficiencia:** SOAR, IR Platforms, Ticketing, Integración/Interoperabilidad.
- **Postura & Exposición:** Vulnerability Management, Patch Management, CSPM/CWPP (Cloud), WIPS, IoT Security.
- **Identidad & Acceso:** IAM, MFA, Zero Trust.
- **Protección de Datos:** DLP, Cifrado/Tokenización, Backups/Recovery.
- **Perímetro/Red:** Firewalls/NGFW, SWG, VPN.
- **Especializadas:** Deception, Security Analytics (ML/AI), AppSec Testing, Virtualization Security, TIP (Threat Intel), Training/Awareness, GRC/Compliance, MSS.



# SIEM (Security Information & Event Management)

## Función

Agrega/normaliza logs, **correlación en tiempo real**, detección y reporting.

## Uso en SOC

Visibilidad centralizada, priorización de alertas, investigación.

## Ejemplos

Splunk, IBM QRadar, LogRhythm.





# IDPS (IDS/IPS)

## Función

**IDS:** Detecta actividad maliciosa. **IPS:** Bloquea/previene en tiempo real.

## Uso en SOC

Detección de intrusiones, firma y comportamiento, alertas y bloqueos.

## Ejemplos

Snort (IDS), Cisco Firepower (IPS).



# EDR (Endpoint Detection & Response)

## Función

Telemetría de endpoints, detección, contención y forense en host.

## Uso en SOC

Aislar equipos, erradicar malware, trazabilidad de acciones.

## Ejemplos

CrowdStrike Falcon, Carbon Black.



# Log Management

## Función

Recolección/retención de logs a escala; búsqueda y auditoría.

## Uso en SOC

Evidencia forense y cumplimiento de retención.

## Ejemplos

ELK (Elastic, Logstash, Kibana), Splunk.



# SOAR (Orquestación, Automatización y Respuesta)

## Función

- Integra herramientas, automatiza **tareas repetitivas** y flujos con aprobaciones.

## Uso en SOC

- Reducir **MTTD/MTTR**, estandarizar playbooks.

## Ejemplos

- Cortex XSOAR (Palo Alto), (Demisto/Phantom heredados).



# Plataformas de Respuesta a Incidentes (IR Platforms)

## **Función**

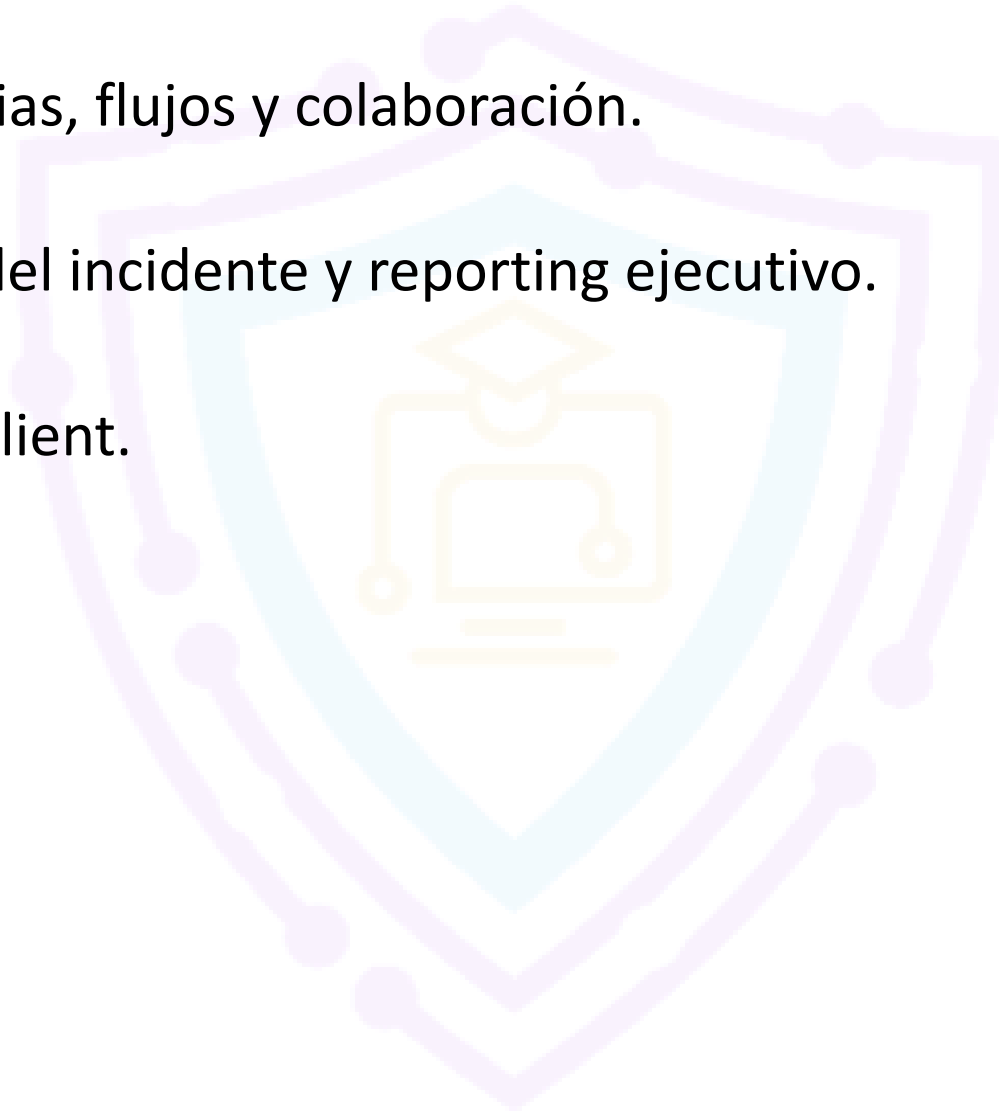
Gestionan casos, evidencias, flujos y colaboración.

## **Uso en SOC**

Trazabilidad end-to-end del incidente y reporting ejecutivo.

## **Ejemplos**

ServiceNow SIR, IBM Resilient.



# Threat Intelligence Platforms (TIP)

## Función

Agregan y enriquecen IoCs/TTPs; **comparten** inteligencia.

## Uso en SOC

Contexto en detección y priorización; feeds hacia SIEM/SOAR.

## Ejemplos

ThreatConnect, Anomali ThreatStream.



# Vulnerability Management

## Función

Descubrir, evaluar (CVSS+EPSS), priorizar y remediar vulnerabilidades.

## Uso en SOC

Reducir superficie de ataque; alimentar **Patch Management**.

## Ejemplos

Qualys, Tenable.io.



# Firewalls / NGFW & Appliances de Red

## Función

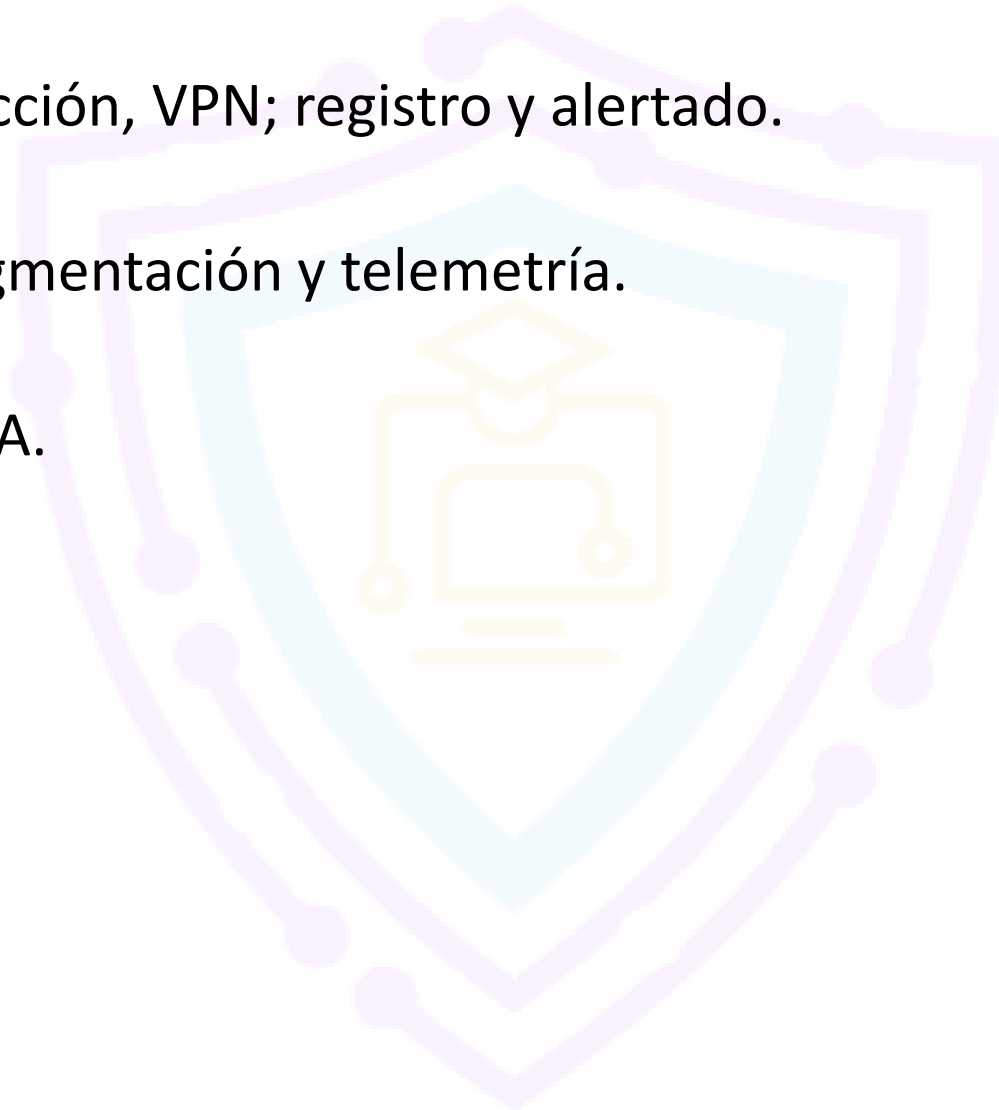
Políticas de tráfico, inspección, VPN; registro y alertado.

## Uso en SOC

Control de perímetro, segmentación y telemetría.

## Ejemplos

Palo Alto NGFW, Cisco ASA.





# Arquitectura e Infraestructura del SOC

Un SOC eficaz integra **personas, procesos y tecnología** sobre una **infraestructura robusta** (física y lógica) para **monitorear, detectar, responder y mejorar** continuamente.



# Componentes esenciales (visión general)

**Personas:** SOC Manager, analistas (L1/L2/L3), incident responders, ingenieros, threat hunters.

**Procesos:** gestión de incidentes, integración de inteligencia, gestión de vulnerabilidades, cambio y mejora continua.

**Tecnología:** SIEM, IDS/IPS, EDR, SOAR, TIP, IR, forense, VM/PM, IAM/MFA, DLP, etc.

**Objetivo:** detectar, responder y **mitigar** amenazas para fortalecer la postura de seguridad.



# Infraestructura física

- **Ubicación:** on-prem, cloud o **híbrido** según requisitos y riesgos.
- **Instalaciones:** control de acceso físico, CCTV, biometría, registros de visitantes.
- **Energía y HVAC:** energía redundante (UPS/generador), cooling y monitoreo ambiental.
- **Resiliencia:** redundancia de sistemas críticos y planes de continuidad.



# Infraestructura de red

- **Segmentación:** segmentar la red del SOC (gestión/forense) del resto de la organización.
- **Conectividad:** enlaces de **alta velocidad** y baja latencia para ingesta y análisis.
- **Controles perimetrales:** **firewalls/NGFW** y **IPS** dedicados al entorno del SOC.



# Tecnologías

- **Monitoreo/detección:** SIEM, IDS/IPS, EDR, NTA/NDR, UEBA.
- **Respuesta/eficiencia:** SOAR, plataformas de IR, ticketing.
- **Reducción de riesgo:** VM/PM, firewalls, WIPS, IoT security, DLP, backup.
- **Identidad y acceso:** IAM, **MFA**, políticas de mínimo privilegio.
- **Soporte forense:** herramientas de adquisición y análisis.



# Tipos de SOC y sus Propósitos

## 1) Enterprise SOC (ESOC)

- **Propósito:** centro **centralizado** para toda la empresa (múltiples áreas/unidades).
- **Foco:** monitoreo, detección y respuesta a escala empresarial.
- **Ventaja:** servicios integrales alineados a objetivos corporativos.

## 2) Global SOC (GSOC)

- **Propósito:** operación **global** con cobertura multi-región.
- **Foco:** consistencia de políticas y coordinación mundial.
- **Ventaja:** visibilidad central + ejecución local/seguimiento de husos horarios.

## 3) Cloud SOC (CSOC)

- **Propósito:** proteger **activos y servicios en la nube**.
- **Foco:** postura cloud (CSPM/CWPP), eventos nativos, identidades/llaves, APIs.
- **Ventaja:** controles y playbooks **cloud-first**.

## 4) MSSP (Proveedor de Servicios Gestionados)

- **Propósito:** **terceriza** capacidades SOC (24/7, tecnologías, talento).
- **Foco:** monitoreo/detección/IR y VM para múltiples clientes.
- **Ventaja:** **escala y experiencia**; modelo flexible según necesidades.



# Tipos de SOC y sus Propósitos

## 5) ICS SOC (Industrial Control Systems)

- **Propósito:** proteger **infraestructura crítica** (OT/ICS/SCADA).
- **Foco:** continuidad y **seguridad funcional** sin impactar producción.
- **Ventaja:** controles y telemetría **especializados** para entornos industriales.

## 6) Financial SOC (FSOC)

- **Propósito:** sector **financiero** (banca/fintech).
- **Foco:** protección de datos sensibles, **anti-fraude** y cumplimiento sectorial.
- **Ventaja:** monitoreo transaccional en tiempo real y marcos regulatorios estrictos.

## 7) Healthcare SOC (HSOC)

- **Propósito:** **salud** (hospitales/clinics).
- **Foco:** EHR, dispositivos médicos, regulación sanitaria y privacidad.
- **Ventaja:** controles contra **ransomware** y seguridad de dispositivos.

## 8) Government SOC (GSOC, gubernamental)

- **Propósito:** proteger **infraestructura y datos del Estado**.
- **Foco:** amenazas estatales/espionaje, coordinación con inteligencia y LEAs.
- **Ventaja:** mandato nacional y cooperación interagencia.



# Tipos de SOC y sus Propósitos

## 9) Incident Response Center (IRC)

**Propósito:** centro **especializado** en respuesta (post-detección).

**Foco:** causa raíz, contención, erradicación y recuperación.

**Ventaja:** rapidez y profundidad en IR; complementa al SOC de monitoreo.

## 10) Threat Intelligence Center (TIC)

**Propósito:** recolectar/analizar/distribuir inteligencia de amenazas.

**Foco:** actores, TTPs, vulnerabilidades y **anticipación**.

**Ventaja:** acciona al SOC con **insights** y comparte con la comunidad.

## 11) Virtual SOC (VSOC)

**Propósito:** operación **virtual** con infraestructura cloud y equipos distribuidos.

**Foco:** visibilidad central remota y automatización.

**Ventaja:** **flexibilidad**, escalabilidad y costo optimizado.

## 12) Collaborative SOC (CSOC, colaborativo)

**Propósito:** defensa colectiva entre **múltiples organizaciones**.

**Foco:** **intercambio** de inteligencia y co-respuesta.

**Ventaja:** detección más temprana y respuesta **acelerada**.





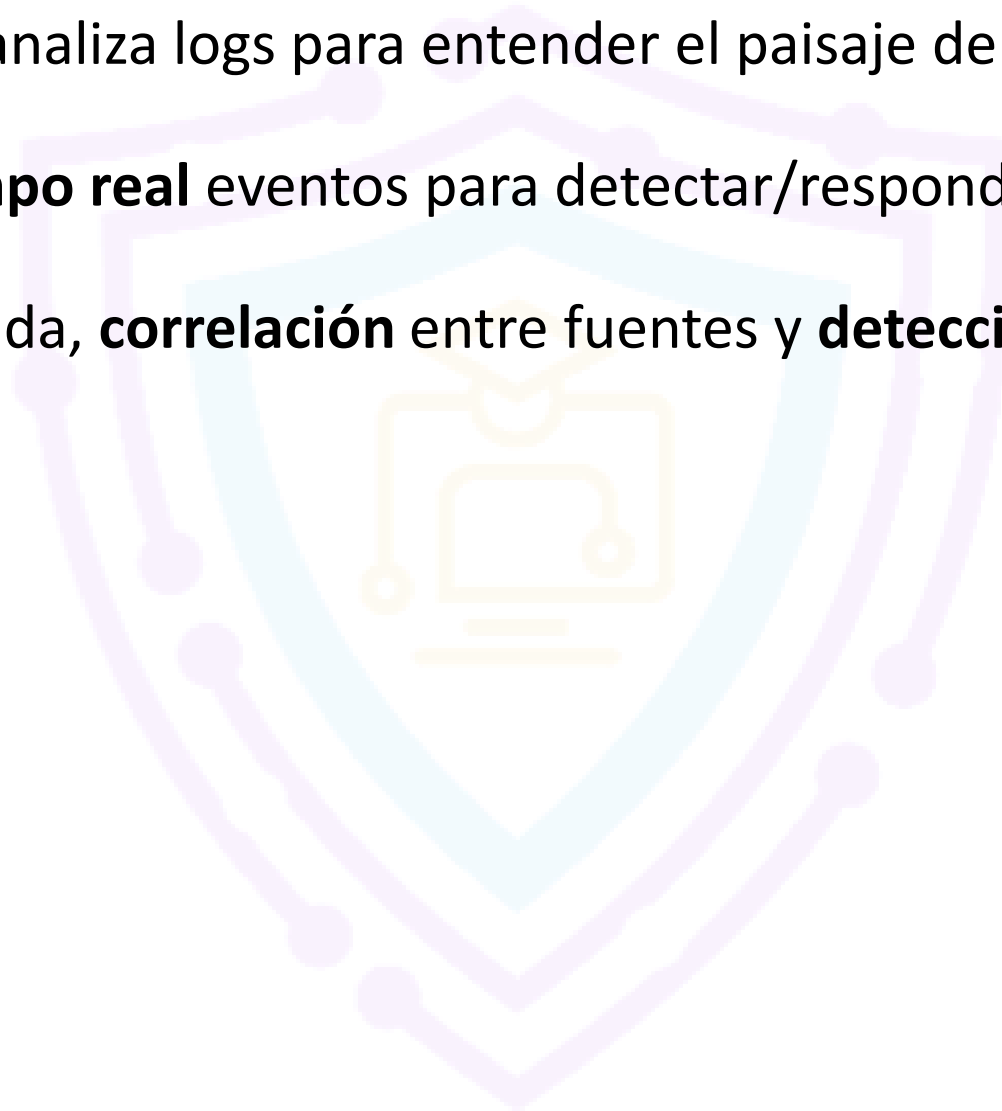
# Introducción a SIEM

Un **SIEM** combina **SIM** (recolección/almacenamiento/análisis de logs) y **SEM** (monitoreo/analítica en tiempo real) para **correlacionar eventos, detectar amenazas, responder y cumplir** regulaciones desde una **plataforma centralizada**.



# ¿Qué es un SIEM? (SIM + SEM)

- **SIM:** recopila, guarda y analiza logs para entender el paisaje de seguridad.
- **SEM:** monitorea en **tiempo real** eventos para detectar/responder cuando ocurren.
- **Resultado:** visión unificada, **correlación** entre fuentes y **detección proactiva**.



# Componentes Clave del SIEM (1/2)

1. **Recolección de Logs:** dispositivos, apps, sistemas, nube, identidades, redes.
2. **Normalización:** transformar formatos dispares a un esquema común.
3. **Correlación:** unir eventos multi-fuente para hallar **patrones/técnicas**.
4. **Almacenamiento de Eventos:** histórico para **forense y cumplimiento**.
5. **Alertas/Notificaciones:** avisos por actividad sospechosa con **prioridad/SLA**.
6. **Dashboards/Reportes:** vistas en tiempo real + informes personalizados.
7. **Monitoreo de Actividad de Usuario:** detección de **anomalías/insider**.
8. **Cumplimiento:** auditoría/trazas para marcos regulatorios.
9. **Integración de Threat Intel (TI):** enriquecimiento con **IoCs/TTPs**.



# Beneficios del SIEM

- **Visibilidad centralizada** del entorno.
- **Detección y respuesta** más rápida (menos **MTTD/MTTR**).
- **Cumplimiento** (GDPR, HIPAA, PCI-DSS, etc.).
- **Automatización/orquestación** al integrarse con SOAR.
- **Monitoreo en tiempo real y análisis forense** robusto.
- **Hunting e histórico** para tendencias y mejora continua.



# Desafíos Comunes del SIEM

- **Onboarding de datos** (parsers/conectores, calidad de logs).
- **Ruido y falsos positivos** si no se ajustan reglas/umbrales.
- **Costos de ingesta/retención y escala.**
- **Tuning continuo** (reglas, lists, pipeline).
- **Skillset** requerido para contenido/detecciones.



# Casos de Uso Típicos

- **Compromiso de cuentas** (anomalías de inicio de sesión/MFA/privilegios).
- **Ransomware** (cadena: entrega → ejecución → cifrado → exfiltración).
- **Exfiltración de datos** (DLP, DNS/HTTP inusuales).
- **Amenazas internas** (accesos fuera de patrón, movimientos laterales).
- **Seguridad cloud** (config/identity/keys; eventos nativos).
- **Cumplimiento/auditoría** (quién hizo qué, cuándo y desde dónde).



# Implementación del SIEM (Fases)

1. **Descubrir & Planear:** alcance, fuentes críticas, requisitos de cumplimiento.
2. **Onboarding de Datos:** priorizar **identidad/red/endpoint/cloud**; validar parsers.
3. **Contenido Inicial:** reglas base (autenticación, admin, malware, exfil).
4. **Dashboards & Reportes:** por caso de uso y audiencia (SOC vs. ejecutivos).
5. **Integraciones:** SOAR (playbooks), EDR, IAM, TIP, ITSM.
6. **Piloto & Ajustes:** tuning de ruido/SLA y documentación.
7. **Producción 24/7:** operación, métricas, mejora continua.



# Desafíos Comunes en SIEM

## 1. Complejidad

**Reto:** Configurar y administrar un SIEM requiere **conocimientos especializados** y un ajuste continuo.

**Impacto:**

Configuraciones avanzadas para adaptarlo a la empresa.  
Actualizaciones frecuentes para mantener la eficacia.  
Puede volverse difícil de escalar sin una estrategia clara.





# Desafíos Comunes en SIEM

## 2. Falsos Positivos

**Reto:** Alertas incorrectas debido a **reglas desactualizadas** o **mala configuración**.

**Impacto:**

- Saturación del equipo SOC.

- Distracción de amenazas reales.

- Dificultad para priorizar incidentes críticos.

**Solución:**

- Ajuste y tuning constante de reglas y umbrales.

- Uso de inteligencia de amenazas para validar alertas.



# Desafíos Comunes en SIEM

## 3. Integración

**Reto:** El SIEM debe integrarse con múltiples herramientas y fuentes de datos.

**Impacto:**

Información aislada → "**silos**" de datos.

Dificultad para correlacionar eventos.

Procesos de respuesta más lentos.

**Solución:**

Planificación e integración gradual.

Uso de **APIs** y conectores estandarizados.



# Casos de Uso del SIEM

## 1. Detección y Respuesta a Incidentes

Monitoreo en tiempo real de actividades sospechosas.

Alertas inmediatas para respuesta rápida.

Prevención de brechas antes de que escalen.

## 2. Cumplimiento Normativo

Generación de **reportes auditables**.

Evidencia de cumplimiento con GDPR, HIPAA, PCI-DSS, etc.

Conservación de logs según requerimientos legales.

## 3. Detección de Amenazas Internas

Análisis de comportamiento de usuarios.

Identificación de **acciones anómalas**.

Mitigación de accesos indebidos o abusos.

## 4. Integración con Threat Intelligence

Conexión con **feeds externos** de IoCs.

Correlación con eventos internos.

Respuesta proactiva ante amenazas conocidas.

## 5. Análisis Forense

Registro detallado de eventos e incidentes.

Reconstrucción de la cadena de ataque.

Identificación de brechas y vulnerabilidades.



# Flujo de Trabajo de un SIEM

## 1. Log Collection (Recolección de Logs)

### Fuente de datos:

Dispositivos de red, servidores, endpoints, aplicaciones y appliances de seguridad.

### Propósito:

Capturar eventos críticos y actividades dentro de la infraestructura TI.

Garantizar visibilidad completa de todo el entorno.

## 2. Log Transmission (Transmisión de Logs)

### Proceso:

Los agentes o colectores instalan en las fuentes de datos.

Transmiten de forma **continua y segura** los logs al servidor SIEM.

### Beneficio:

Evita pérdida de datos.

Asegura flujo constante de información para análisis en tiempo real.



# Flujo de Trabajo de un SIEM

## 3. Normalization (Normalización)

### •Objetivo:

- Estandarizar los datos recibidos para que tengan un formato uniforme.

### •Incluye:

- Ajuste de timestamps.
- Conversión de estructuras de logs dispares.
- Unificación de atributos para análisis coherente.

## 4. Correlation (Correlación)

### •Función clave:

- El motor de correlación analiza eventos para detectar **patrones y anomalías**.
- Relaciona logs de diferentes sistemas y dispositivos.

### •Resultado:

- Identificación de amenazas complejas como APTs, intrusiones y ataques distribuidos.



## 5. Alerting (Generación de Alertas)

### •Proceso:

- Se crean alertas basadas en resultados de la correlación.
- Se asigna **prioridad** según la severidad y el contexto.

### •Beneficio:

- Los equipos SOC se enfocan en **amenazas críticas** primero.

## 6. Investigation (Investigación)

### •Herramientas clave: Consola y dashboards del SIEM.

### •Acciones:

- Filtrar y consultar datos históricos.
- Visualizar incidentes y su contexto.
- Identificar causa raíz y alcance de la amenaza.



# Flujo de Trabajo de un SIEM

## 7. Reporting (Reportes)

### •Usos principales:

- Auditorías de seguridad.
- Evidencia de cumplimiento normativo.
- Análisis de tendencias y métricas clave.

### •Valor agregado:

- Demostrar la efectividad de la estrategia de ciberseguridad ante la alta dirección.

## 8. Archiving (Archivado)

### •Objetivo:

- Retener logs históricos a largo plazo.

### •Aplicaciones:

- Investigaciones forenses.
- Threat hunting.
- Análisis de tendencias y patrones.

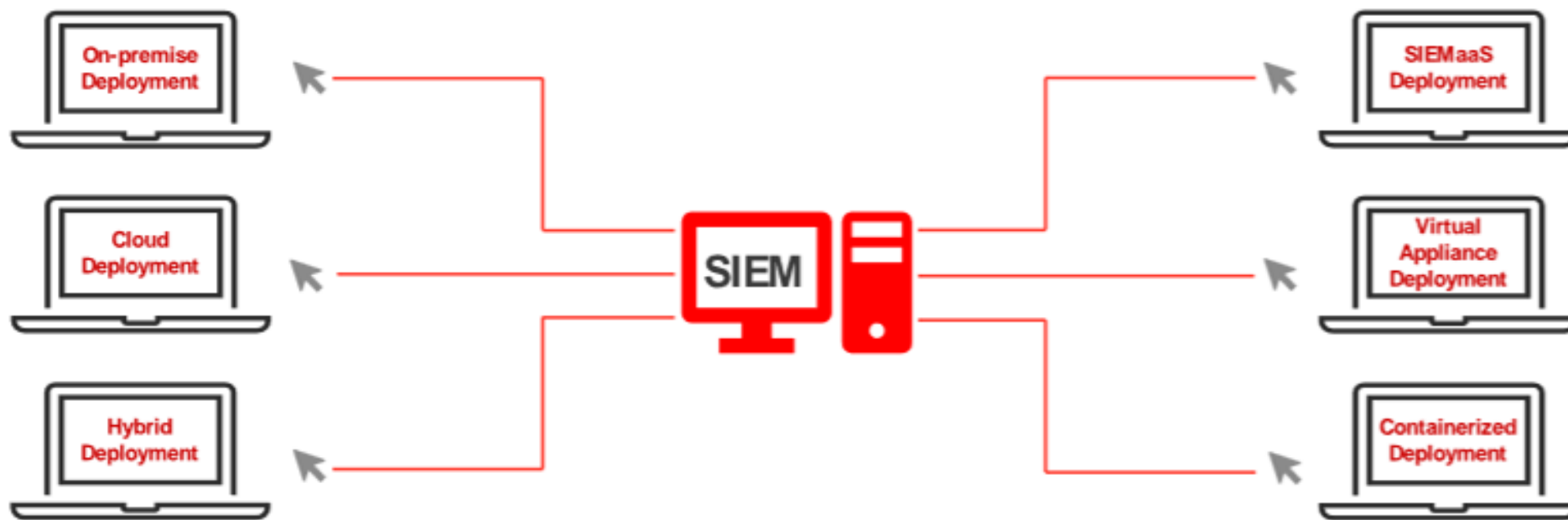
### •Importancia:

- Cumplimiento legal y normativo.



# Modelos de Despliegue de SIEM

Los SIEM pueden implementarse de varias formas según el tamaño, presupuesto y necesidades de la organización.



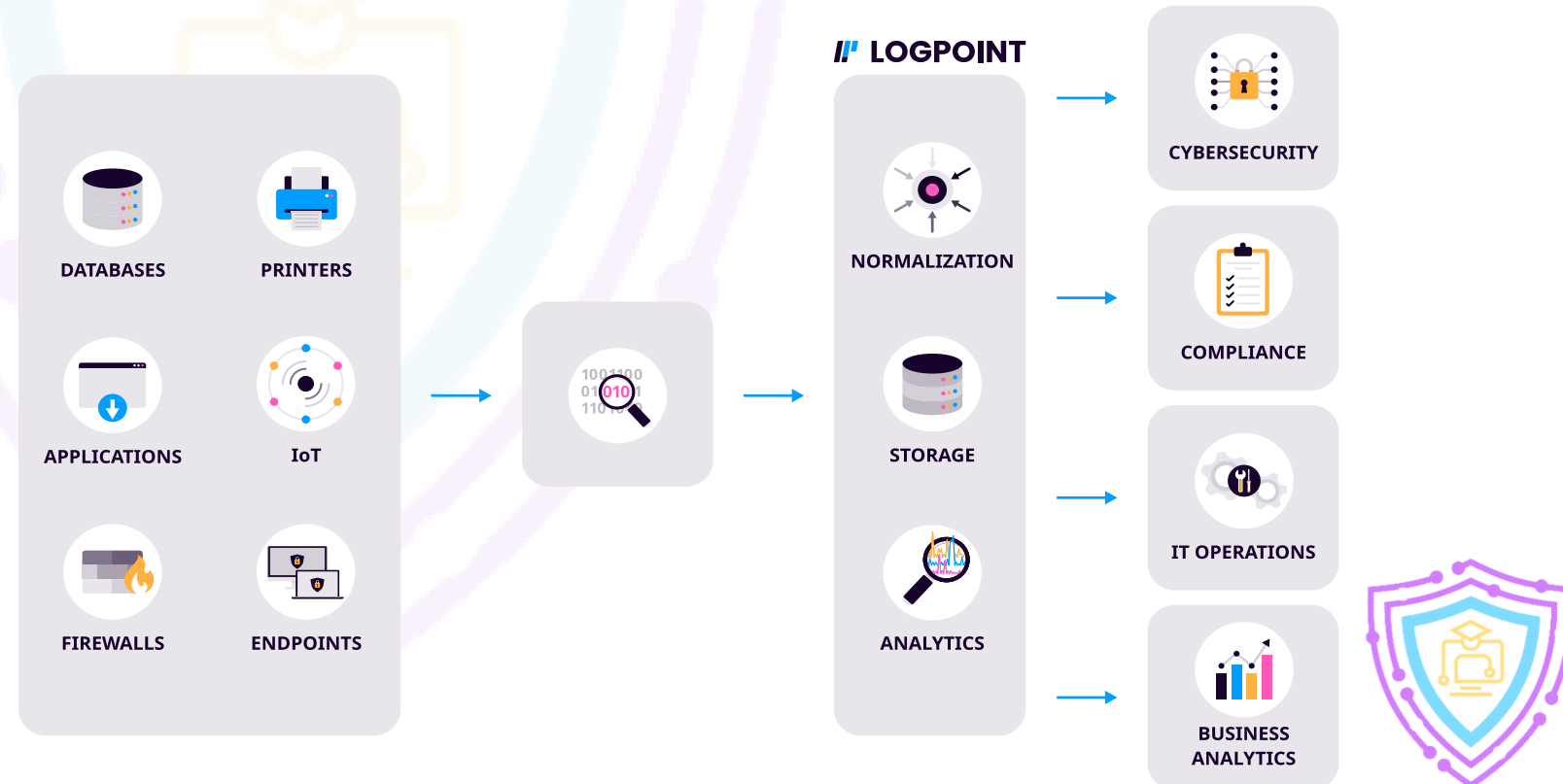


# ¿Qué son los Data Sources en SIEM?

Son **puntos de origen de logs y eventos** en la infraestructura de TI.

• Proveen información crítica para:

- Monitorear la seguridad en tiempo real.
- Detectar anomalías y amenazas.
- Generar alertas y reportes para cumplimiento normativo.



# Categorías Principales de Data Sources

- Infraestructura de red
- Servidores y sistemas operativos
- Dispositivos de seguridad
- Aplicaciones empresariales
- Servicios en la nube
- Usuarios y control de accesos
- Dispositivos móviles e IoT
- Sistemas físicos de seguridad



# Categorías Principales de Data Sources

Categoría	Ejemplos de Dispositivos	Propósito Principal
Red	Routers, Firewalls, IDS/IPS	Detectar ataques y accesos indebidos
Servidores	Web, Domain Controllers, App Servers	Identificar actividad sospechosa
Endpoints	PC, Laptops, EDR	Malware, amenazas internas
Seguridad Física	CCTV, Control de Acceso	Correlación físico-digital
Cloud	AWS, Azure, SaaS	Visibilidad en entornos híbridos
Vulnerabilidades	Qualys, Tenable.io	Priorización de parches

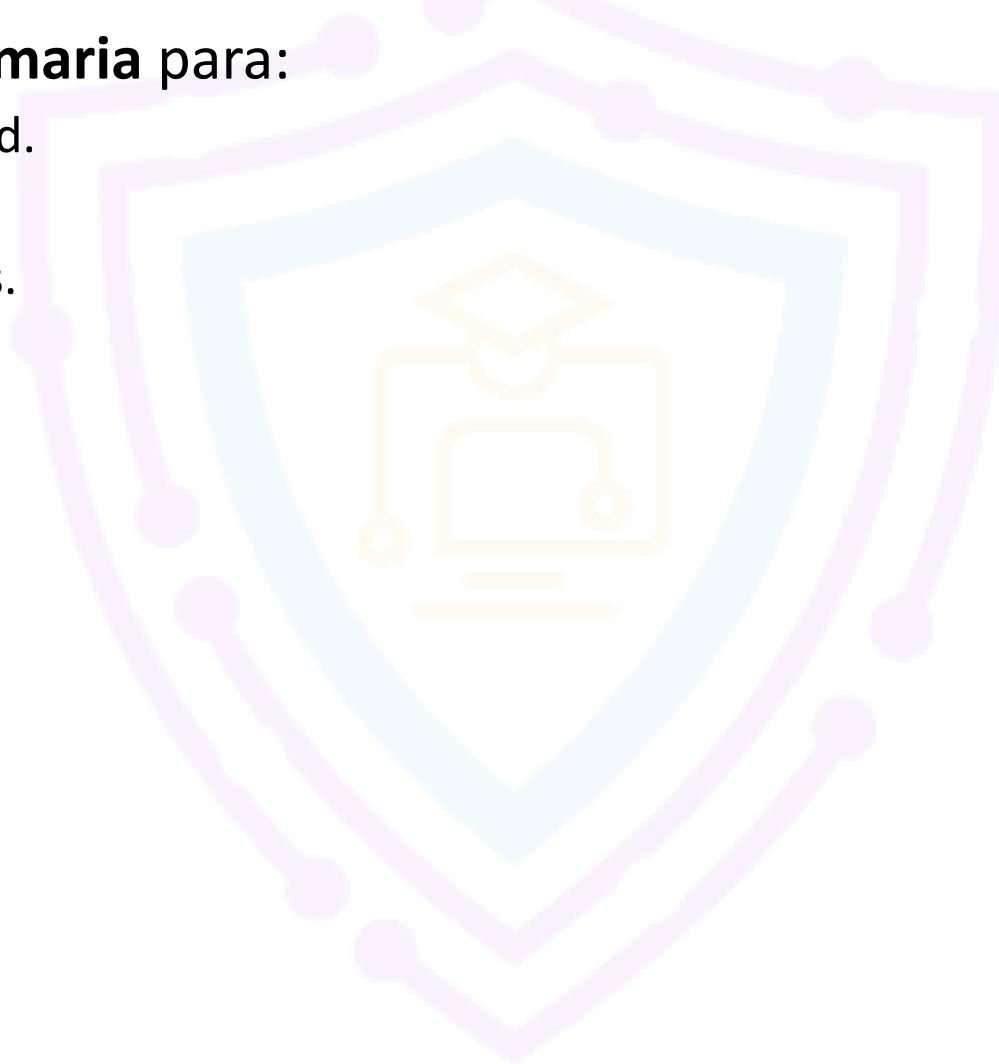


# Introducción a los SIEM Logs

Los **logs** son **registros detallados de eventos y actividades** en la infraestructura de TI.

• Son la **base de datos primaria** para:

- Monitorear la seguridad.
- Detectar amenazas.
- Responder a incidentes.



# Importancia de los Logs en un SIEM

- Detectar **ataques y anomalías** en tiempo real.
- Generar **alertas** basadas en eventos críticos.
- Mantener **evidencia histórica** para investigaciones.
- Facilitar el **cumplimiento regulatorio** y auditorías.
- Apoyar análisis forense y threat hunting.



# Tipos de Logs en un SIEM

Tipo de Log	Descripción	Ejemplos Clave
<b>Security Logs</b>	Registros relacionados con seguridad y accesos.	Inicios de sesión fallidos, cambios de privilegios, violaciones de políticas.
<b>System Logs</b>	Información sobre salud y rendimiento de sistemas.	Errores del sistema, advertencias, eventos de hardware.
<b>Application Logs</b>	Actividad interna de aplicaciones.	Transacciones en BD, llamadas API, errores de aplicación.
<b>Network Logs</b>	Tráfico y comunicación entre dispositivos.	IPs origen/destino, puertos, protocolos, volumen de datos.
<b>Audit Logs</b>	Auditoría de acciones de usuarios y administradores.	Accesos a archivos, cambios de configuración, tareas administrativas.



# Flujo de Trabajo de Logs en SIEM

## 1. Log Sources (Fuentes)

1. Servidores, endpoints, firewalls, bases de datos, aplicaciones, etc.

## 2. Log Collection (Recolección)

1. Uso de **agentes o colectores** instalados en cada fuente.

## 3. Log Transmission (Transmisión)

1. Envío seguro usando **TLS/SSL** hacia el SIEM central.

## 4. Normalization (Normalización)

1. Conversión a un **formato estándar** para facilitar el análisis.

## 5. Log Analysis (Análisis)

1. Correlación de eventos para detectar patrones y anomalías.

## 6. Alerting (Alertas)

1. Notificación inmediata a analistas SOC según severidad.

## 7. Storage & Retention (Almacenamiento y Retención)

1. Guardado histórico para cumplir regulaciones y análisis forense.





ACADEMIA DE  
**CIBERSEGURIDAD**

# Módulo #5

## Introducción a la gestión de logs

**Academia de Ciberseguridad**



# ¿Qué es un incidente en ciberseguridad?

Un incidente en ciberseguridad es cualquier evento o acción que pone en riesgo la seguridad, integridad o disponibilidad de los sistemas, redes o datos de una organización.

Estos eventos pueden ser accidentales o maliciosos, y tienen el potencial de causar interrupciones, pérdidas de información o daños a la reputación.

Su detección y gestión temprana son esenciales para proteger los activos digitales.



# Importancia de la respuesta a incidentes

La respuesta a incidentes busca minimizar el impacto de los eventos de seguridad y restaurar la operación normal lo antes posible.

Implica la coordinación entre diferentes áreas, como TI, seguridad, legal y comunicación.

Contar con un plan de respuesta bien estructurado permite actuar rápidamente, reducir pérdidas y mantener la confianza de clientes y socios.



# Ejemplos de incidentes de ciberseguridad

Los incidentes pueden variar en tipo y severidad. Algunos de los más comunes incluyen:

- Infecciones de malware
- Phishing
- Ataques DoS / DDoS
- Amenazas internas
- Accesos no autorizados
- Brechas de datos
- Ransomware
- Errores de configuración
- Incidentes físicos
- Ingeniería social



# ¿Qué son los registros (logs) en ciberseguridad?

Los logs son colecciones de información generadas por los componentes de los sistemas de información, como redes, aplicaciones, sistemas operativos y servicios. Funcionan como una huella de auditoría que registra todo lo que ocurre en el entorno digital, permitiendo detectar comportamientos anómalos, errores o actividades sospechosas.

Aunque un log por sí mismo no siempre indica una falla, su análisis conjunto permite descubrir incidentes de seguridad y garantizar la trazabilidad.



# Importancia de los logs

Los logs son fundamentales para la ciberseguridad, ya que permiten detectar, investigar y responder a incidentes.

Proveen información detallada sobre actividades del sistema, rendimiento y eventos críticos.

El análisis adecuado de los logs permite identificar amenazas, anomalías y violaciones a políticas de seguridad antes de que se conviertan en incidentes graves.



# Tipos de logs en ciberseguridad

Los logs reflejan los eventos y acciones que ocurren dentro de sistemas, redes o aplicaciones.

Cada tipo de log aporta una perspectiva diferente sobre el comportamiento del entorno y ayuda a detectar problemas técnicos o de seguridad.

A continuación se presentan los más importantes.



# Tipos de logs en ciberseguridad

## Logs del sistema

Registros que documentan eventos relacionados con el sistema operativo, hardware y servicios esenciales. Incluyen errores del sistema, advertencias, inicios y apagados, así como fallos en controladores o componentes. Son útiles para diagnosticar problemas de estabilidad y seguridad.

## Logs de aplicación

Registros específicos de cada aplicación que detallan la interacción con los usuarios, errores y métricas de rendimiento. Por ejemplo, un servidor web genera logs HTTP con las solicitudes recibidas y el estado de las respuestas. Estos logs ayudan a identificar fallos funcionales o intentos de explotación en aplicaciones.

## Logs de seguridad

Registran todos los eventos relacionados con la seguridad, como autenticaciones, autorizaciones y controles de acceso. Incluyen intentos de inicio de sesión exitosos y fallidos, cambios de permisos o modificaciones en políticas. Son esenciales para detectar accesos indebidos y comportamientos sospechosos.

## Logs de firewall

Capturan la información sobre el tráfico de red que pasa por el firewall, incluyendo conexiones permitidas, bloqueadas y sospechosas.

Ayudan a identificar ataques externos, intentos de intrusión o configuraciones incorrectas que puedan exponer el sistema.



# Tipos de logs en ciberseguridad

## Logs de autenticación

Documentan todos los eventos relacionados con el inicio de sesión de usuarios, cambios de contraseñas y accesos fallidos. Estos registros permiten rastrear intentos de fuerza bruta, accesos no autorizados o abuso de credenciales.

## Logs de auditoría

Registros críticos que documentan actividades de seguridad dentro del entorno TI, como cambios de privilegios, modificaciones de políticas y accesos a información sensible. Permiten rastrear acciones administrativas y mantener la trazabilidad necesaria para auditorías y cumplimiento normativo.

## Logs de red

Incluyen información de routers, switches, IDS/IPS y otros dispositivos de red. Proveen detalles sobre conexiones, paquetes, protocolos y posibles amenazas. Ayudan a detectar tráfico malicioso, escaneos o accesos no autorizados.

## Logs de base de datos

Registros provenientes de los servidores de bases de datos que incluyen consultas, transacciones, errores y cambios en los registros. Permiten detectar accesos indebidos o manipulaciones de datos sensibles.





# Tipos de logs en ciberseguridad

## Logs de endpoints

Provenientes de dispositivos finales como laptops, tablets o smartphones. Registran actividades como inicios de sesión, accesos a archivos, actualizaciones o instalación de software. Son esenciales para monitorear el comportamiento del usuario y detectar compromisos locales.

## Logs de DNS

Capturan las consultas y respuestas DNS realizadas por los sistemas. Permiten identificar comportamientos maliciosos como tunneling DNS o el uso de dominios sospechosos. Son una fuente clave para la detección temprana de amenazas.

## Logs de puntos de acceso inalámbricos

Registros generados por los access points Wi-Fi que documentan los dispositivos conectados, tiempos de conexión y direcciones MAC. Ayudan a controlar accesos no autorizados y mantener la seguridad de la red inalámbrica.

## Logs de servicios en la nube

Recogen información sobre las actividades de usuarios, uso de recursos y eventos de seguridad dentro de plataformas cloud. Son esenciales para monitorear la actividad en entornos AWS, Azure o Google Cloud y detectar accesos indebidos o configuraciones inseguras.

## Logs de acceso físico

Registran entradas y salidas en áreas seguras, como centros de datos o laboratorios. Ayudan a monitorear el control de acceso físico y mantener la trazabilidad de quién entra o sale. Su análisis permite vincular incidentes físicos con incidentes digitales.



# Importancia de los registros (logs) en el SOC

Los logs son una fuente esencial de información que permite al equipo del SOC monitorear, detectar, responder e investigar incidentes de seguridad.

A través de ellos, los analistas pueden entender el comportamiento del sistema, identificar amenazas y mantener un control continuo sobre la infraestructura tecnológica.



# Detección de incidentes de seguridad

Los logs de firewall permiten identificar patrones inusuales de conexión.

Por ejemplo, un aumento repentino de solicitudes desde una misma dirección IP puede indicar un posible ataque DDoS.

El análisis de estos registros permite tomar medidas preventivas y mitigar el impacto.



# Detección de anomalías

El SIEM analiza registros de autenticación de usuarios para identificar comportamientos fuera de lo normal, como accesos desde ubicaciones desconocidas o en horarios inusuales.

Estas alertas ayudan a detectar uso indebido de credenciales o intentos de intrusión en tiempo real.



Tras un incidente de seguridad, los logs son clave para reconstruir la línea de tiempo de los hechos.

Permiten identificar cómo se produjo la intrusión, qué sistemas se vieron comprometidos y cuáles fueron las acciones del atacante.

Sin registros detallados, una investigación forense sería prácticamente imposible.



# Monitoreo de actividad del usuario

El seguimiento de logs de autenticación y autorización permite detectar comportamientos sospechosos de empleados o contratistas.

Por ejemplo, un intento de acceder a archivos sensibles fuera del rol asignado puede evidenciar una posible amenaza interna.



# Monitoreo de cumplimiento

Los logs ayudan a demostrar que una organización cumple con regulaciones como ISO 27001, GDPR o HIPAA.

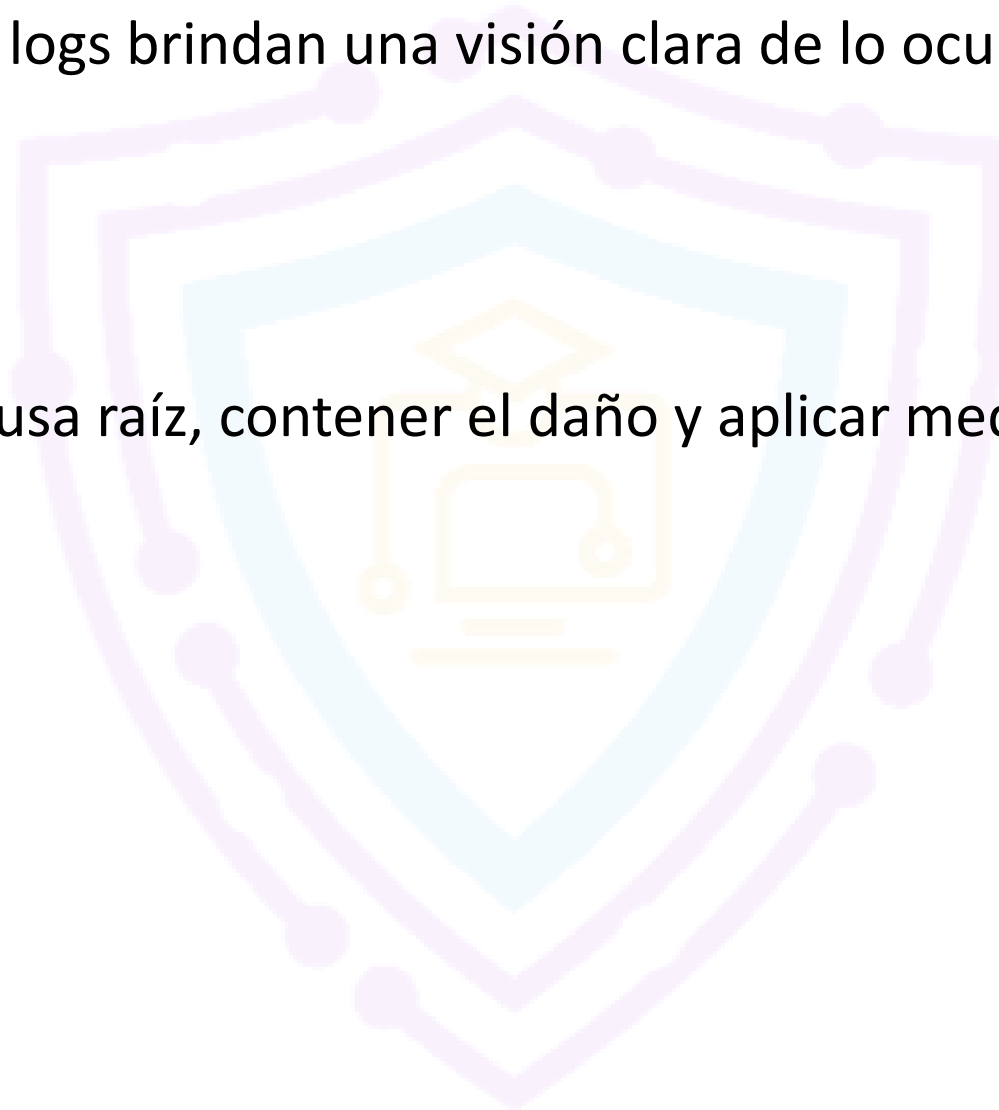
Permiten rastrear quién accedió a qué datos, cuándo y desde dónde, garantizando transparencia y trazabilidad en los procesos.



# Respuesta a incidentes

Durante un incidente, los logs brindan una visión clara de lo ocurrido antes, durante y después del ataque.

Ayudan a identificar la causa raíz, contener el daño y aplicar medidas para prevenir incidentes futuros.





# Análisis del tráfico de red

Los logs de red permiten visualizar el volumen, origen y destino del tráfico.

A través de su análisis se pueden detectar comportamientos anómalos, intentos de exfiltración de datos o conexiones no autorizadas hacia el exterior.



# Detección de malware

Los registros generados por antivirus o EDR revelan la presencia de archivos maliciosos, conexiones sospechosas o cambios no autorizados en el sistema.

El análisis de estos logs permite identificar infecciones y eliminar malware antes de que se propague.



# Detección de amenazas internas

El monitoreo de la actividad de los usuarios es esencial para identificar accesos no autorizados, robos de información o intentos de eludir controles de seguridad.

Por ejemplo, un empleado que accede a datos fuera de su horario habitual puede estar realizando una acción maliciosa.



# Estructura típica de un registro (log)

Aunque los logs pueden variar según el sistema, dispositivo o aplicación que los genera, todos siguen un formato estructurado con elementos clave.

Este formato permite a los analistas del SOC entender rápidamente qué ocurrió, cuándo, dónde y cómo, facilitando la correlación de eventos y la detección de incidentes.



# Timestamp (marca de tiempo)

Cada entrada de log incluye la fecha y hora exactas del evento registrado.

La marca de tiempo es fundamental para reconstruir la secuencia de actividades, determinar la duración de un ataque o identificar el momento en que un sistema fue comprometido.

Sin un timestamp preciso, el análisis forense o la correlación entre múltiples fuentes se vuelve imprecisa.



# Tipo o ID del evento

Cada evento dentro de un log tiene un **identificador único (Event ID)** o tipo de evento.

Esto permite clasificar rápidamente las actividades registradas, como accesos exitosos, intentos fallidos, errores de sistema, cambios de configuración o eventos críticos de seguridad.

Los IDs ayudan a automatizar la detección de patrones y priorizar incidentes.



# Dirección IP y puerto de origen

El log registra la dirección IP y el puerto desde los cuales se originó la actividad.

Esta información es clave para identificar el origen del tráfico, el país o la red desde la que se ejecutó el evento.

Ayuda a reconocer ataques externos, movimientos laterales o accesos no autorizados dentro de la red.



# Información del usuario o cuenta

Muchos registros incluyen el nombre del usuario o la cuenta involucrada en el evento.

Esto permite identificar quién realizó una acción específica, si el acceso fue autorizado o si se usaron credenciales comprometidas.

La trazabilidad de usuarios es esencial para detectar abuso de privilegios o actividad interna sospechosa.





# Acción u operación realizada

Describe la actividad que ocurrió dentro del sistema o red. Puede incluir operaciones como “inicio de sesión”, “eliminación de archivo”, “modificación de permisos” o “ejecución de comando”.

Este campo permite entender qué acción concreta se realizó y su impacto potencial en la seguridad.



# Estado o resultado del evento

Cada registro indica si la acción fue **exitosa** o **fallida**.

Por ejemplo, un intento de autenticación fallido puede ser un simple error del usuario o un intento de fuerza bruta.

Analizar los estados ayuda a identificar patrones de error y posibles ataques en progreso.



# Descripción o mensaje del evento

Incluye una descripción detallada o mensaje generado por el sistema que da contexto adicional sobre el evento. Puede contener información técnica, como nombres de procesos, rutas de archivos o resultados de ejecución.

Este campo ayuda al analista a comprender la causa y el impacto del suceso registrado.



# ¿Qué es la gestión local de logs?

La gestión local de logs consiste en recopilar, almacenar y analizar los registros generados por sistemas, aplicaciones y dispositivos dentro de una organización directamente en el mismo equipo o entorno donde se originan. Este enfoque permite mantener una copia inmediata y confiable de los eventos ocurridos antes de que se envíen a sistemas centralizados.



# Beneficios de la gestión local de logs

La gestión local mejora la disponibilidad, confiabilidad y velocidad de respuesta del SOC.

Permite realizar análisis inmediatos, mantener copias redundantes y asegurar la integridad de la información incluso si el sistema central falla.

También reduce la dependencia de la red y mejora la eficiencia del monitoreo.



# Herramientas de gestión de logs

Las herramientas de gestión de logs permiten recopilar, centralizar, analizar y visualizar los registros generados por diferentes sistemas dentro de una organización. Son esenciales para el trabajo del SOC, ya que facilitan la detección de amenazas, el cumplimiento normativo y la toma de decisiones basadas en datos.



# SIEM (Security Information and Event Management)

Los sistemas SIEM están diseñados para recopilar y correlacionar logs provenientes de múltiples fuentes como servidores, dispositivos de red y aplicaciones.

Permiten monitoreo en tiempo real, detección de patrones sospechosos, generación de alertas automáticas y reportes de cumplimiento.

Ejemplos de SIEM: **Splunk, LogRhythm, IBM QRadar, Wazuh.**



# Colectores y reenviadores de logs

Los **log collectors** y **forwarders** se encargan de recopilar los registros desde distintos dispositivos y enviarlos a un destino central o SIEM.

Utilizan protocolos como **Syslog**, **SNMP** o **API** para transmitir la información.

Ejemplos: **Syslog-ng**, **Winlogbeat**, **Filebeat**.





# Herramientas de análisis y visualización de logs

Estas soluciones permiten interpretar los registros mediante paneles, métricas y gráficos dinámicos.

Ayudan a los analistas a identificar patrones, anomalías y eventos críticos con rapidez.

Ejemplos: **Kibana**, **Grafana**, **Graylog**.



# Plataformas EDR (Endpoint Detection and Response)

Los sistemas EDR supervisan y protegen endpoints como estaciones de trabajo, servidores y dispositivos móviles.

Analizan los logs locales de los equipos para detectar comportamientos sospechosos, malware o movimientos laterales dentro de la red.

Ejemplos: **CrowdStrike Falcon, Carbon Black (VMware), SentinelOne.**



# Dispositivos de seguridad y firewall

Los **firewalls** y **appliances de seguridad de red** generan logs detallados sobre tráfico, intentos de conexión, ataques bloqueados y violaciones de políticas.

Estos registros ayudan al SOC a identificar comportamientos sospechosos y a reforzar las reglas de filtrado.

Ejemplos: **Cisco FMC, Palo Alto Networks Panorama, FortiAnalyzer.**



# Herramientas de monitoreo en la nube

Estas soluciones recolectan y analizan logs de entornos cloud como AWS, Azure o Google Cloud.

Permiten detectar accesos no autorizados, violaciones de políticas y optimizar el rendimiento de los recursos.

Ejemplos: **AWS CloudWatch, Azure Monitor, Google Cloud Operations Suite.**



# Soluciones DAM (Database Activity Monitoring)

Los sistemas DAM registran y analizan todas las actividades realizadas en bases de datos. Ayudan a detectar accesos no autorizados, consultas anómalas y manipulaciones de datos sensibles.

Ejemplos: **Imperva SecureSphere, IBM Guardium.**



# Herramientas APM (Application Performance Monitoring)

Las herramientas APM analizan logs de aplicaciones para evaluar su rendimiento, disponibilidad y estabilidad.

Detectan errores, tiempos de respuesta lentos o fallos de comunicación entre servicios.

Ejemplos: **New Relic, AppDynamics, Dynatrace.**



# Sistemas IDS / IPS

Los sistemas de detección y prevención de intrusiones (IDS/IPS) generan logs que registran intentos de ataque, violaciones de políticas y tráfico malicioso.

Permiten analizar el comportamiento de la red en tiempo real y bloquear amenazas activas.

Ejemplos: **Snort**, **Suricata**, **Zeek**.



# Herramientas FIM (File Integrity Monitoring)

Las herramientas FIM supervisan los cambios realizados en archivos y directorios críticos del sistema.

Detectan modificaciones no autorizadas, cambios de permisos o alteraciones de contenido.

Ejemplos: **Tripwire, OSSEC, Wazuh FIM.**







ACADEMIA DE  
**CIBERSEGURIDAD**

# Módulo #6

## Detección de incidentes y análisis

**Academia de Ciberseguridad**

# ¿Qué es un SIEM Use Case?

Un **caso de uso en SIEM** define cómo se utilizará el sistema para detectar, analizar y responder a incidentes de seguridad específicos.

Ayuda a establecer reglas, fuentes de datos y acciones automáticas que mejoran la detección y la respuesta ante amenazas.



# Comprensión del entorno

El primer paso es conocer la infraestructura de la organización:

- Tipos de sistemas y dispositivos.
- Sistemas operativos utilizados.
- Aplicaciones y servicios en uso.

Este análisis permite determinar qué logs son relevantes para el monitoreo de seguridad.

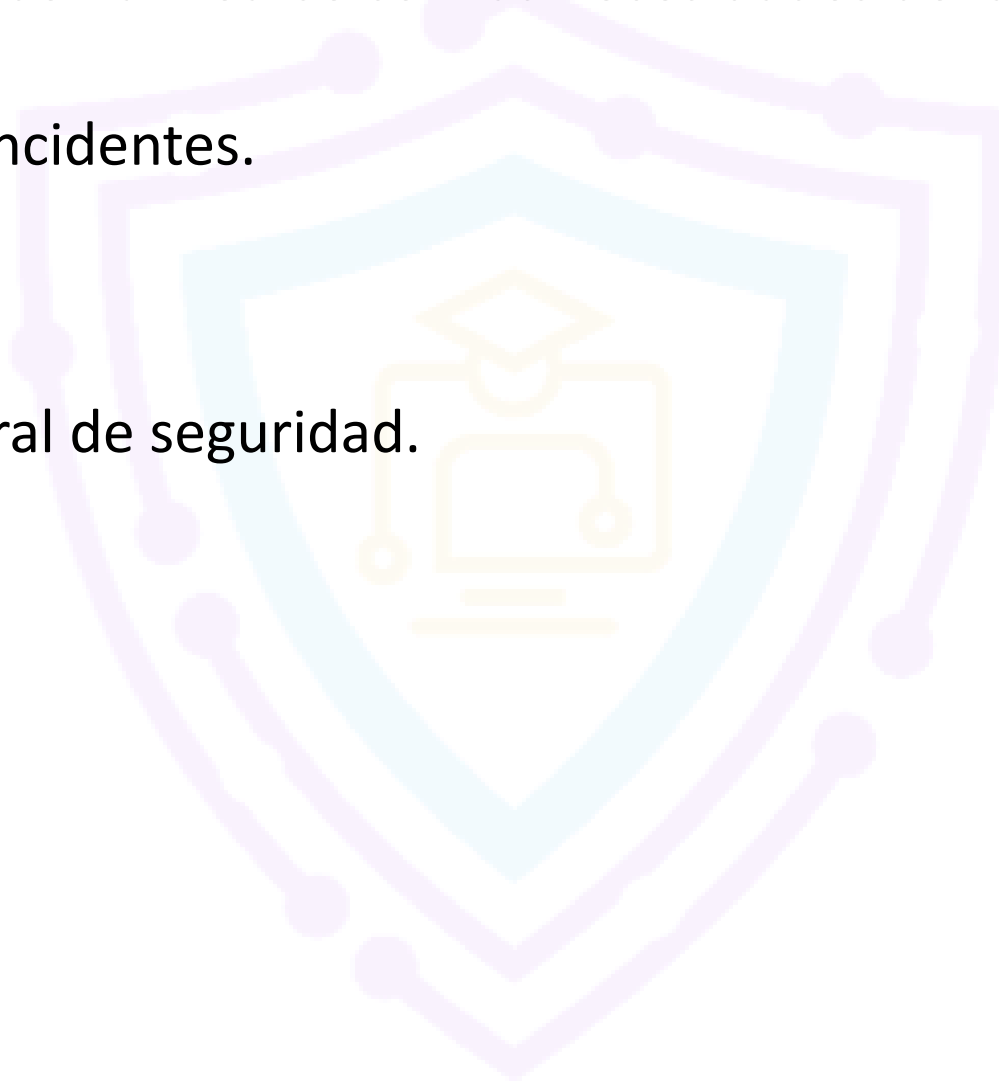


# Definición de objetivos de seguridad

Los objetivos del SIEM deben alinearse con las necesidades de la organización.

Ejemplos:

- Detectar y responder a incidentes.
- Investigar amenazas.
- Cumplir con normativas.
- Mejorar la postura general de seguridad.



# Recolección de requisitos

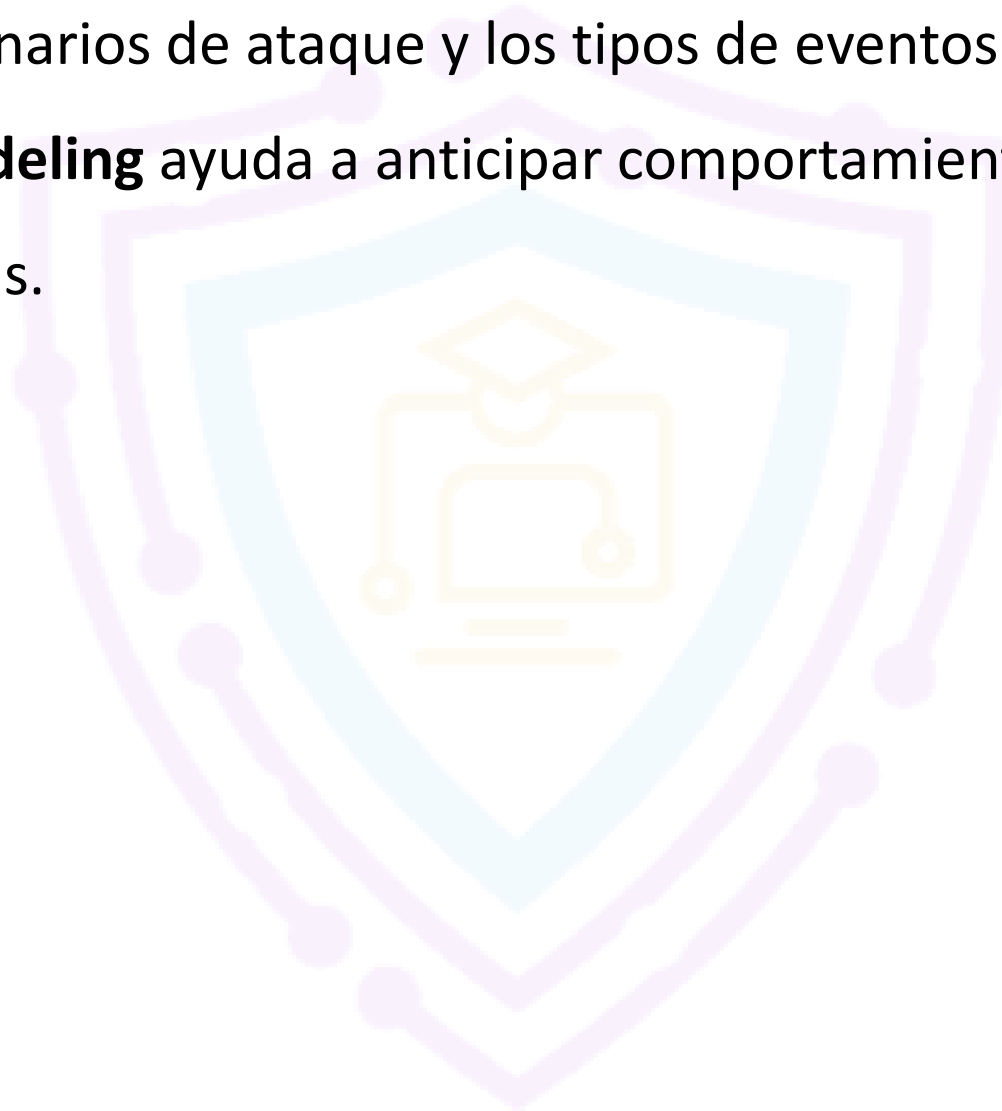
Se identifican los elementos que el SIEM debe cubrir:

- Fuentes de logs y eventos a recopilar.
- Reglas y filtros para detección.
- Nivel de automatización deseado en respuesta a incidentes.



# Modelado de amenazas

Se analizan posibles escenarios de ataque y los tipos de eventos que estos generarían. El **threat modeling** ayuda a anticipar comportamientos maliciosos y definir reglas más precisas.



# Creación y ajuste de reglas

Las reglas del SIEM determinan qué condiciones disparan una alerta.

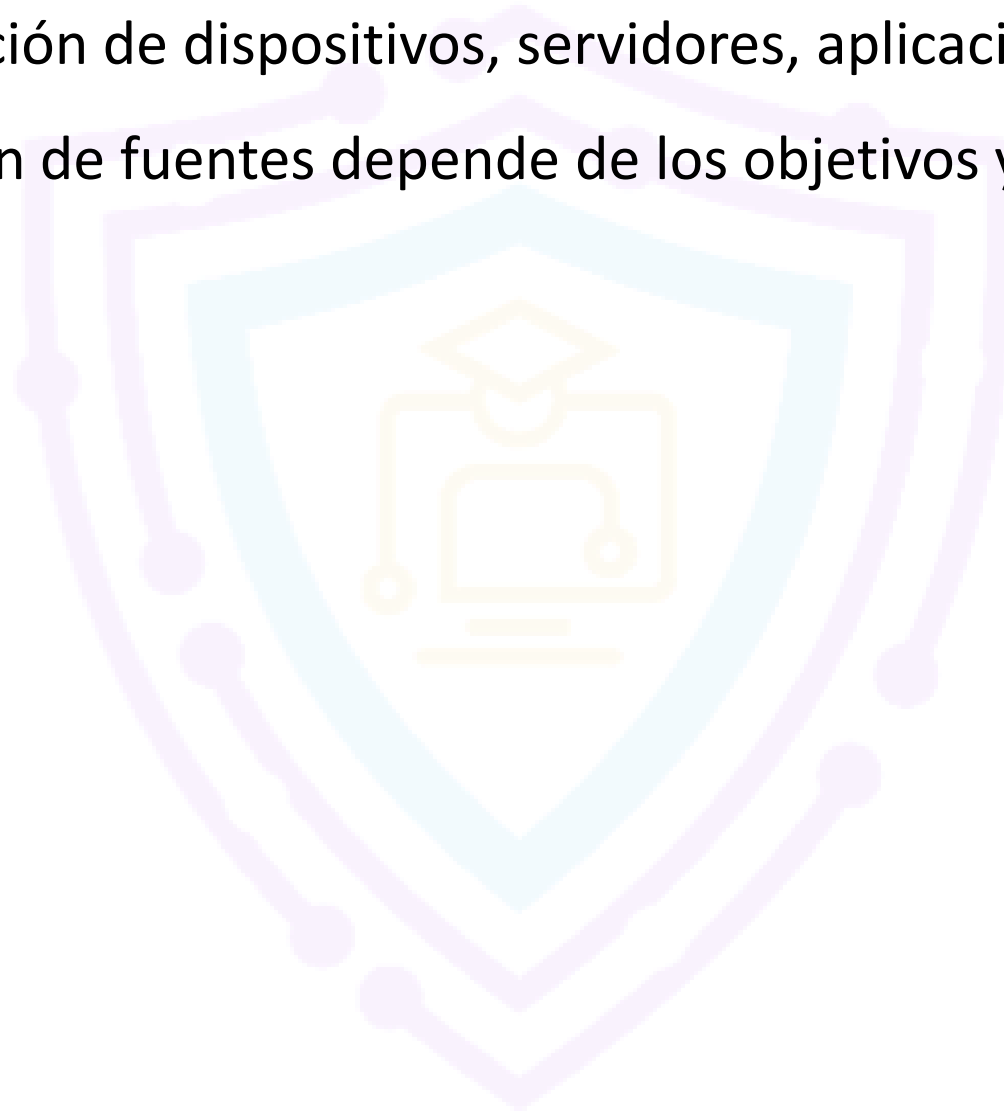
Se basan en actividades sospechosas, patrones de red o comportamientos de usuario.

Es un proceso iterativo que debe ajustarse constantemente para reducir falsos positivos.



# Fuentes de datos y recolección de logs

El SIEM recopila información de dispositivos, servidores, aplicaciones y herramientas de seguridad. La selección de fuentes depende de los objetivos y casos de uso definidos.

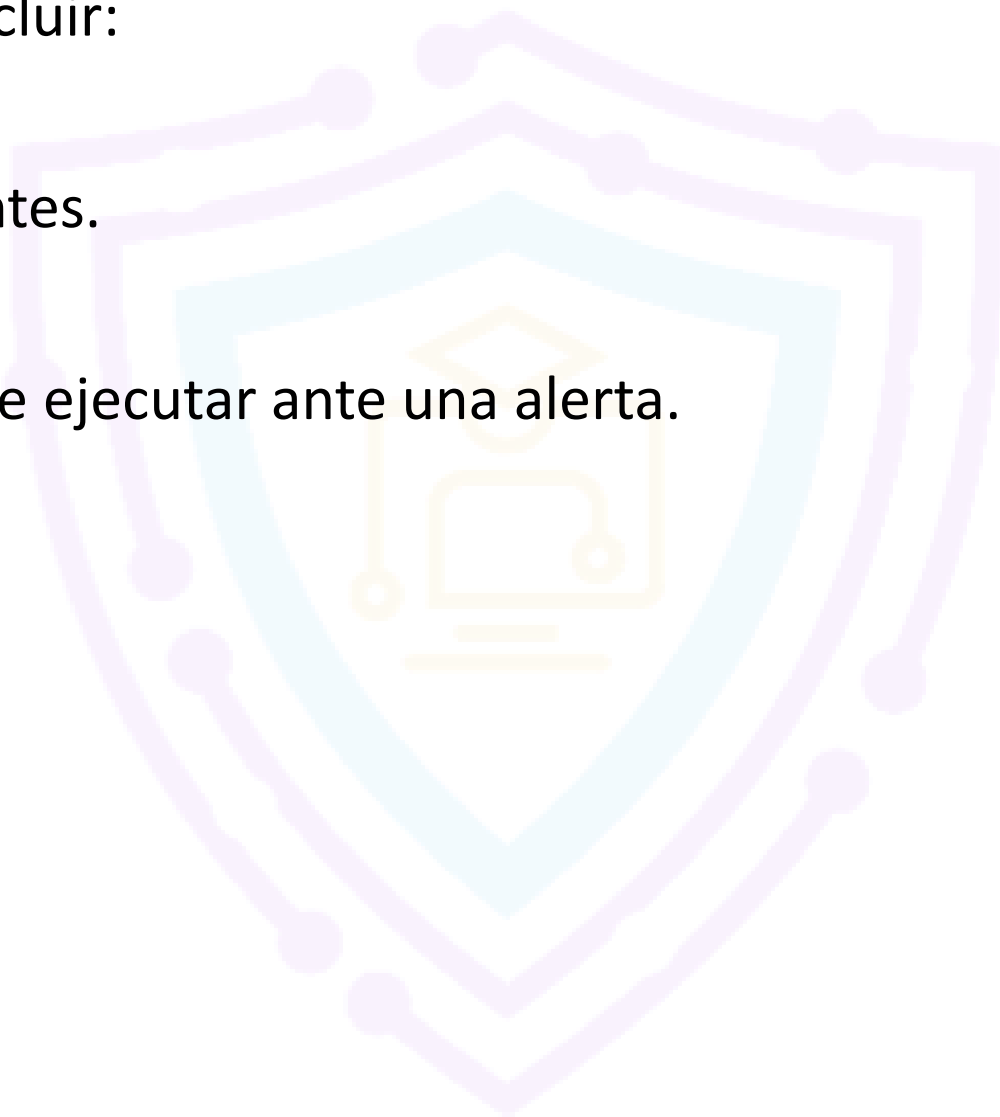




# Definición del caso de uso

Cada caso de uso debe incluir:

- Objetivo de seguridad.
- Fuentes de datos relevantes.
- Reglas que lo activan.
- Acciones que el SOC debe ejecutar ante una alerta.



# Clasificación de casos de uso

Los casos de uso pueden dividirse en categorías como:

- Seguridad de red.
- Seguridad de endpoints.
- Monitoreo de actividad de usuarios.

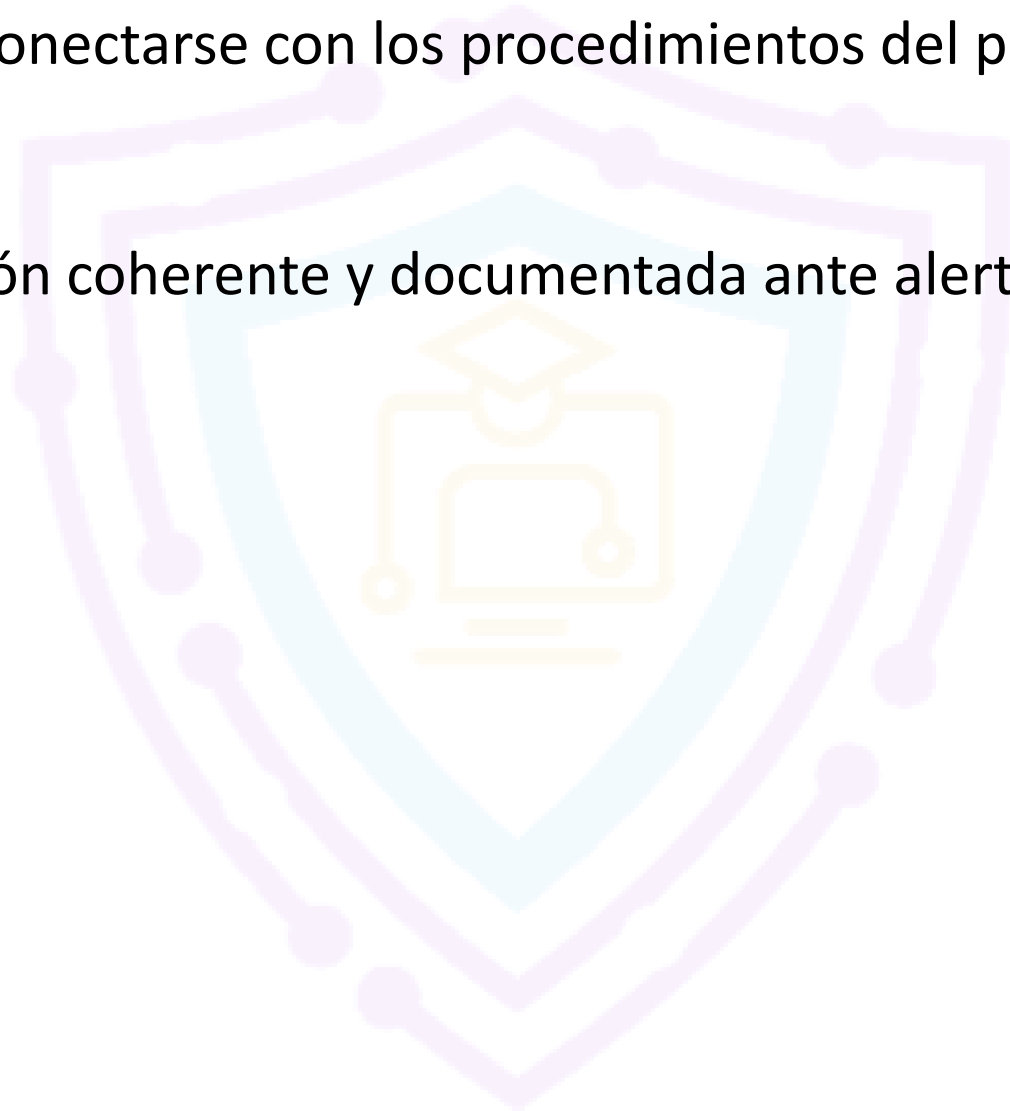
Esta clasificación facilita la priorización y mantenimiento.



# Integración con respuesta a incidentes

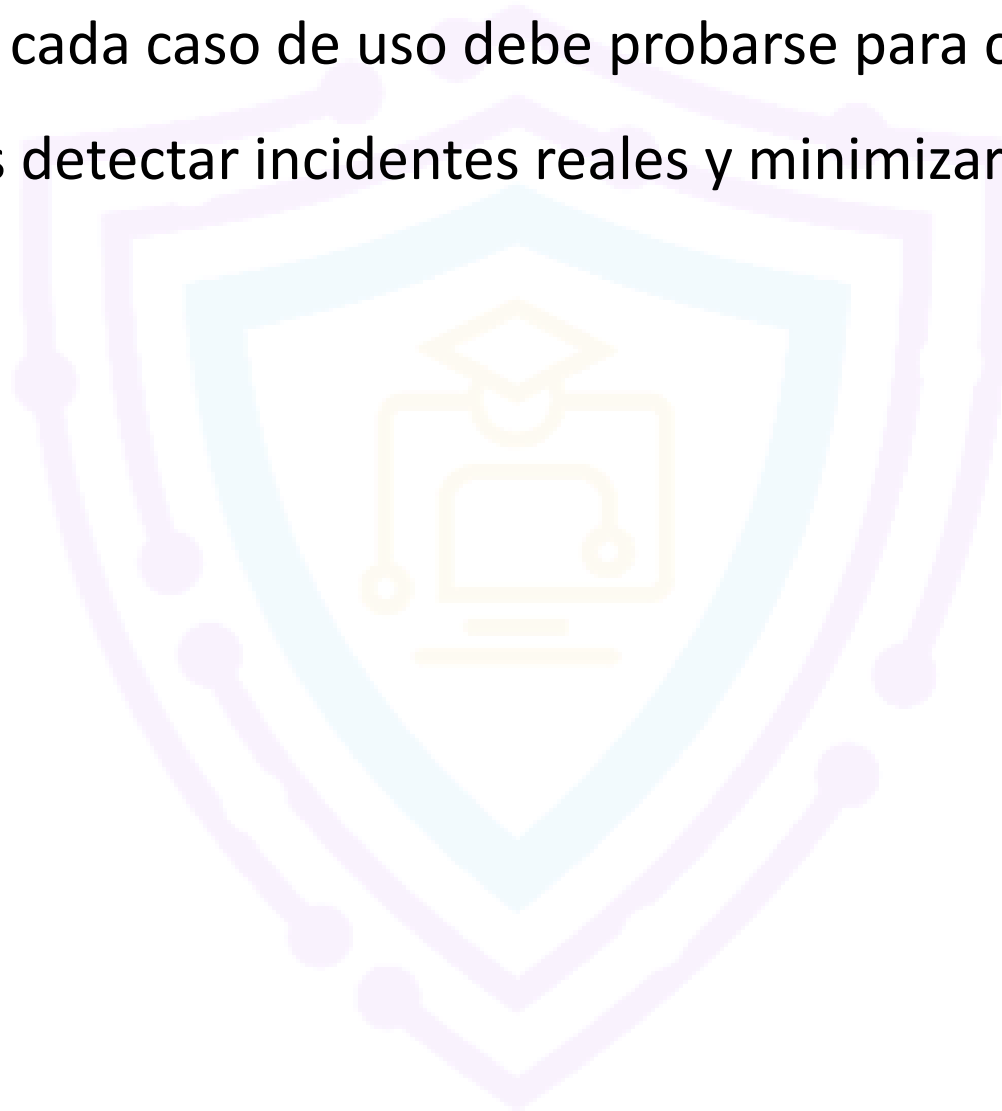
Los casos de uso deben conectarse con los procedimientos del plan de respuesta del SOC.

Esto garantiza una reacción coherente y documentada ante alertas del SIEM.



# Pruebas y validación

Antes de implementarse, cada caso de uso debe probarse para confirmar su efectividad. El objetivo es detectar incidentes reales y minimizar falsos positivos.



# Mejora continua

Los casos de uso deben actualizarse regularmente según nuevas amenazas, vulnerabilidades o cambios en la infraestructura.

La mejora constante asegura que el SIEM siga siendo eficaz frente al entorno cambiante.



# Conceptos básicos de monitoreo

- **Vigilancia continua:** observación constante de redes y sistemas.
- **Fuentes de datos:** logs de red, sistemas, aplicaciones y dispositivos de seguridad.
- **Detección en tiempo real:** identificación inmediata de amenazas.
- **Correlación de eventos:** conexión entre alertas para detectar ataques complejos.
- **Generación de alertas:** notificación a los analistas ante eventos críticos.



# Conceptos básicos de análisis de seguridad

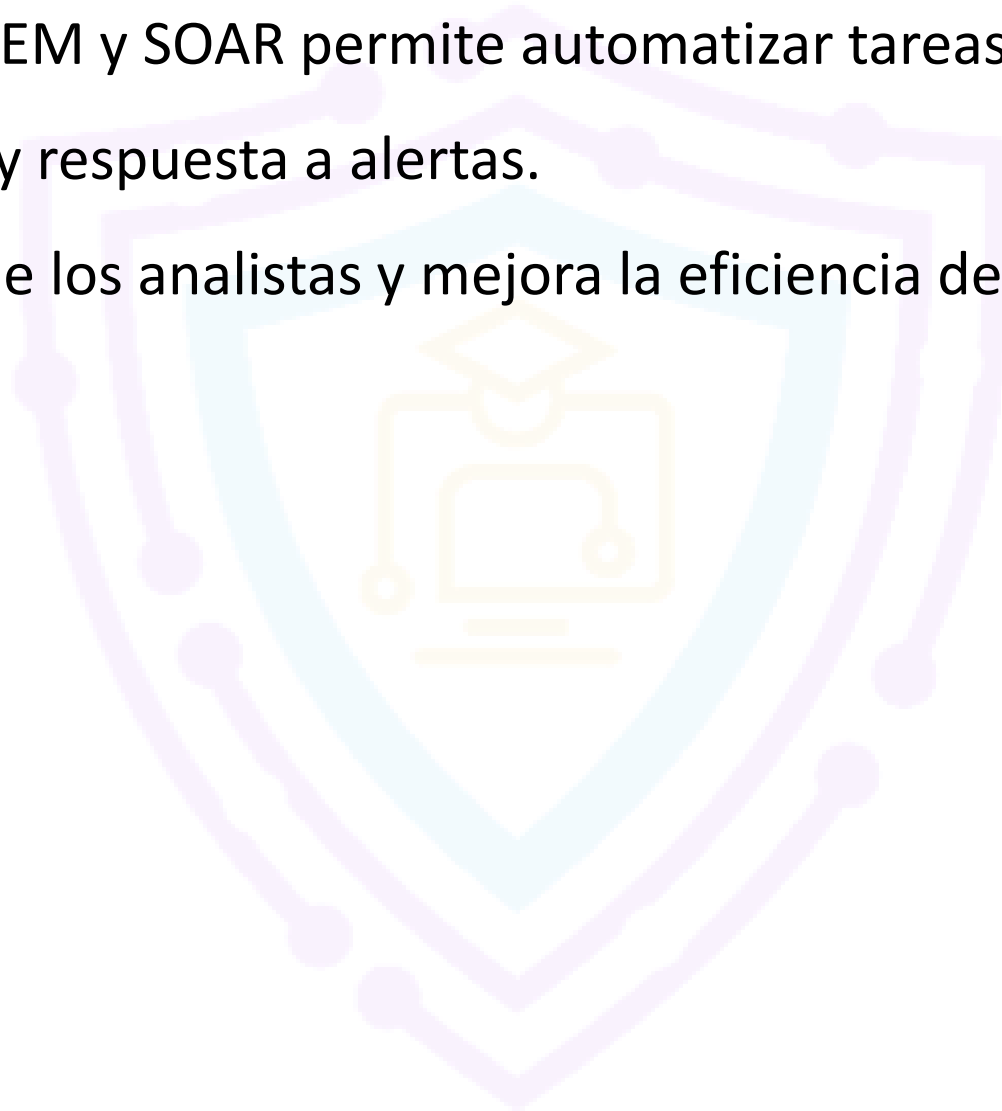
- **Investigación de incidentes:** examen detallado de alertas para determinar causa y alcance.
- **Análisis forense:** reconstrucción de eventos para obtener evidencia y comprensión total del ataque.
- **Integración de inteligencia de amenazas:** uso de IoCs y fuentes externas para contextualizar incidentes.
- **Análisis de comportamiento:** detección de anomalías mediante la observación de patrones de usuario o red.
- **Evaluación de riesgos:** priorización de incidentes según su impacto y probabilidad.



# Automatización y orquestación

El uso de herramientas SIEM y SOAR permite automatizar tareas repetitivas como la correlación, clasificación y respuesta a alertas.

Esto optimiza el tiempo de los analistas y mejora la eficiencia del SOC.





# Proceso de monitoreo y análisis

- 1.Recolección de datos:** obtención de logs, tráfico y métricas.
- 2.Detección de eventos:** análisis para descubrir anomalías o patrones sospechosos.
- 3.Generación de alertas:** priorización según gravedad e impacto.
- 4.Investigación:** análisis profundo y correlación con inteligencia de amenazas.
- 5.Respuesta:** contención, mitigación y recuperación.
- 6.Mejora continua:** revisión periódica de reglas y procedimientos.



# Detección y análisis de malware

Un sistema de seguridad de endpoints genera una alerta sobre actividad maliciosa en la estación de trabajo de un empleado. Los registros del antivirus y del endpoint se analizan para identificar modificaciones de archivos, conexiones de red sospechosas y procesos anómalos.

Los analistas examinan el comportamiento del malware, su método de propagación y el impacto potencial en la organización.

## **Respuesta:**

El dispositivo afectado se aísla de la red, se ejecutan herramientas de limpieza y se actualizan las firmas del antivirus.

## **Prevención:**

- Refuerzo de la protección de endpoints.
- Filtrado de correos con archivos adjuntos maliciosos.
- Capacitación a empleados sobre prevención de malware.



# Detección de comportamiento anómalo del usuario

Un usuario accede a archivos y sistemas sensibles fuera de su horario laboral. Se recopilan y analizan los logs de autenticación, accesos y tráfico de red para comparar su comportamiento con patrones históricos. Los analistas revisan los permisos y funciones del usuario para determinar si los accesos fueron legítimos.

## Respuesta:

La cuenta se suspende temporalmente mientras se realiza la investigación. Se analizan los eventos para detectar accesos no autorizados o indicios de compromiso.

## Prevención:

- Implementación de **User Behavior Analytics (UBA)** para detectar desviaciones.
- Aplicación de **RBAC** para limitar accesos según roles.
- Revisiones periódicas de permisos de usuario.



# Detección y respuesta ante ataque de phishing

Varios empleados reportan correos sospechosos con enlaces falsos de un supuesto proveedor. Se analizan los registros del servidor de correo, pasarela de seguridad y herramientas antiphishing para identificar los mensajes maliciosos.

Los analistas revisan encabezados de correo, dominios de remitente y enlaces para confirmar el ataque.

## Respuesta:

Se informa a todos los empleados sobre la campaña activa y se actualizan los filtros de correo para bloquear mensajes similares.

Se revisan posibles clics o accesos realizados por los usuarios.

## Prevención:

- Implementar soluciones de filtrado y detección temprana de phishing.
- Realizar simulaciones de phishing y capacitaciones periódicas.
- Habilitar **autenticación multifactor (MFA)** para proteger las cuentas frente a robo de credenciales.

