IIC2523
Sistemas Distribuidos

Hernán F. Valdivieso López
(2025 - 2 / Clase 22)

Monitoreo de Seguridad
Vigilar y actuar para proteger el sistema

Temas de la clase

1. Objetivos y desafíos del monitoreo
2. Ciclo de vida del monitoreo
3. Mecanismos de monitoreo
4. Consideraciones legales

Fuente: OpenAI. (2025). [Definición de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Objetivos y desafíos del monitoreo

Objetivos y desafíos del monitoreo

- ¿Por qué monitorear si ya ciframos, autenticamos y autorizamos?
- Considerar cuando hay cuentas comprometidas con credenciales válidas.
- El monitoreo observa lo que los demás mecanismos no previenen.
- Sus objetivos son:
  - Detectar actividades maliciosas.
  - Reaccionar ante incidentes.
  - Recolectar evidencia.
  - Vigilar sin incumplir lo legal.
  - Mejorar la postura de seguridad.

Objetivos y desafíos del monitoreo

Frente a un entorno distribuido, existen varios desafíos:

- Latencia y asincronía.
- Volumen de eventos.
- Fragmentación de visibilidad.
- Puntos ciegos y fallas del monitoreo.
- Privacidad y cumplimiento normativo.

Objetivos y desafíos del monitoreo

Latencia y asincronía

Los latencia puede provocar que eventos llegan desordenados, o que los relojes no están sincronizados

La causalidad se puede perder.

¿Qué se hace ante este desafío?

- Algoritmos de sincronización de relojes físicos (NTP) o lógicos (vectoriales).
- **Correlación tolerante al desorden** que acepta ventanas de tiempo amplias o *buffer* temporal para reordenar eventos.
- *Logs con* **Identificadores de causalidad** explícita (ID de petición, flujo, transacción).

Objetivos y desafíos del monitoreo

Volumen de eventos

Demasiados logs, metricas y trazas para almacenarlos o analizarlos en tiempo real.

¿Qué se hace ante este desafío?

- **Filtrado local** de eventos irrelevantes antes de enviarlos al sistema central.
- ***Sampling* o agregación** de información para reducir granularidad de información. Por ejemplo, promedio de CPU cada 10s en vez de cada 1s.
- Procesamiento **paralelo de grandes volúmenes** de información con herramientas como Elasticsearch, Loki, Fluentd o Kafka.

Objetivos y desafíos del monitoreo

Fragmentación de visibilidad

Cada nodo ve sólo su propio contexto. Ataques distribuidos no se detectan localmente.

¿Qué se hace ante este desafío?

- Uso de Sistema de Gestión de Eventos e Información de Seguridad (SIEM) para el análisis de **correlación centralizada**
- incluir IDs de flujo, usuario, etc. en los *logs para* disponer la **trazabilidad**.
- Uso de ***dashboards* globales** como Prometheus + Grafana Loki.
- Aplicar **políticas de seguridad** como *Zero Trust* que dice nunca confiar en nadie y pedir identidad en cada solicitud, incluso a alguien dentro del sistema.

Objetivos y desafíos del monitoreo

Puntos ciegos y fallas del monitoreo

¿Qué pasa si el propio sistema de monitoreo es comprometido o falla?

¿Qué se hace ante este desafío?

- **Monitoreo del monitoreo (*watchdog*)**: agentes que verifican que los sistemas de detección estén operativos.
- ***Logs* inmutables** (*WORM storage*) y firmados criptográficamente para evitar que un atacante modifique evidencia.
- **Aislar** físicamente o lógicamente el canal de monitoreo del canal de control.

Objetivos y desafíos del monitoreo

Privacidad y cumplimiento normativo

Los datos recolectados pueden violar la privacidad del usuario o contradecir regulaciones.

¿Qué se hace ante este desafío?

- **Anonimización de logs sensibles** mediante uso de información no asociada a los datos personales: IP, id de usuario.
- Recolección con **consentimiento** o control configurado por el usuario.
- *Logs* por niveles de sensibilidad, no todos los eventos deben incluir datos identificables.

Ciclo de vida del monitoreo

Ciclo de vida del monitoreo

Recolección de eventos

1

Respuesta

3

Permitir, bloquear y/o alertar

Análisis

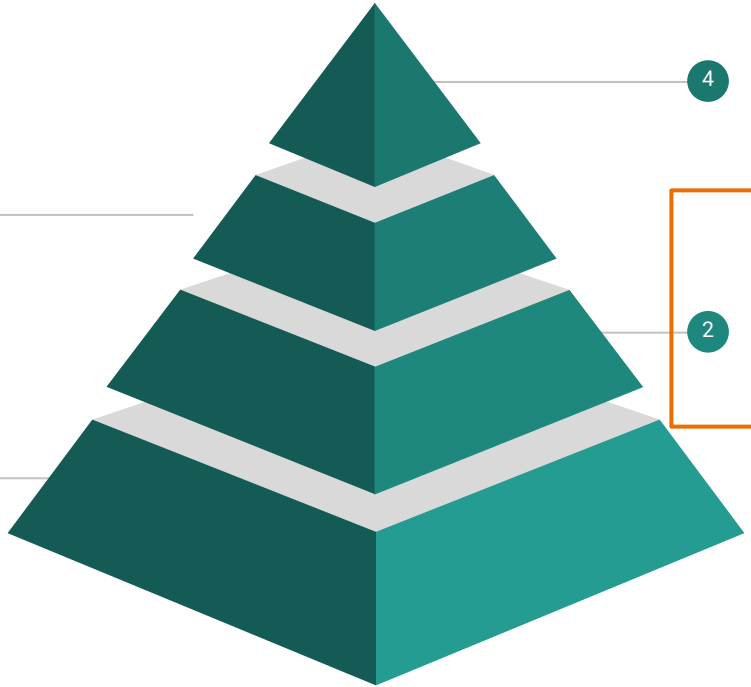
2

Verificar reglas, patrones, anomalías.

Registro para auditoría

4

Ciclo de vida del monitoreo



Recolección de eventos

1

Respuesta

Permitir, bloquear y/o alertar

3

Registro para auditoría

4

Análisis

2

Verificar reglas, patrones, anomalías.

Ciclo de vida del monitoreo - Análisis

Análisis basado en firmas

- Compara eventos contra una base de patrones conocidos de ataques.

Ejemplos:

- Detectar una petición HTTP con `../../../etc/passwd` que es un patrón típico de ataque de inyección de rutas.
- Comparar *hashes* de archivos con los de virus conocidos.

Ciclo de vida del monitoreo - Análisis

Análisis por anomalías

- Detecta comportamientos que se desvían del perfil "normal" del sistema.

Ejemplos:

- Un usuario *root* inicia sesión a las 3 a.m. desde una IP no habitual.
- Un servicio comienza a enviar 10 veces más tráfico que su promedio.
- Un archivo cambia de tamaño y tipo sin que haya una acción esperada.

Fuente: Network Anomaly Detection: A Comprehensive Guide | Kentik

Ciclo de vida del monitoreo - Análisis

Análisis basado en reglas o políticas

- Reglas definidas manualmente que activan alertas si se incumplen ciertas condiciones.

Ejemplos:

- Bloquear cualquier intento de conexión SSH desde fuera de la subred interna.
- Alertar si un mismo usuario accede desde dos países en menos de 5 minutos.
- Bloquear cualquier intento de Netflix desde la Eduroam UC 😭.

Fuente: GitHub - SigmaHQ/sigma: Main Sigma Rule Repository

Ciclo de vida del monitoreo - Análisis

Análisis por correlación de eventos

- Combina múltiples eventos dispersos en tiempo o espacio para detectar incidentes.
- Muchas veces requiere información bien normalizada: *timestamp*, IP de origen, ID de usuario, etc.

Ejemplos:

- Tres intentos fallidos de *login* desde distintas IPs seguidos de un login exitoso puede implicar un ataque distribuido de fuerza bruta.
- Acceso a un servidor de archivos seguido por conexión externa puede implicar un posible robo de datos.

Fuente: A conceptual framework for network management event correlation and filtering systems | IEEE Conference Publication

Ciclo de vida del monitoreo - Análisis

Análisis basado en *machine learning* o inteligencia artificial

- Aprende patrones normales y detecta anomalías desviaciones o agrupar eventos similares.
- Uso de herramientas como Elastic ML o Microsoft Sentinel

Ejemplos:

- Clasificación de *logs* por severidad usando NLP.
- *Clustering* de comportamientos de red para detectar "usuarios parecidos" y encontrar *outliers*.
- Detección de ataques que cambian constantemente su firma.

Fuente: Network Anomaly Detection: Machine Learning in Action | Fidelis Security

Ciclo de vida del monitoreo - Análisis

Tipo	Descripción	Ventaja principal	Desventaja principal
Firmas	Detecta ataques conocidos comparando patrones	Alta precisión frente a amenazas conocidas	No detecta nuevas amenazas
Anomalías	Detecta desviaciones del comportamiento normal	Detecta amenazas desconocidas	Alto número de falsos positivos
Correlación	Relaciona múltiples eventos para identificar ataques complejos	Proporciona contexto y reduce alertas falsas	Requiere gran capacidad de procesamiento y *logs*
Reglas	Usa condiciones predefinidas tipo "si pasa A, alerta"	Fácil de entender y controlar	Difícil de mantener y escalar
IA	Usa modelos para aprender patrones normales o maliciosos	Se adapta y detecta amenazas complejas	Requiere entrenamiento, recursos y validación

Mecanismos de monitoreo

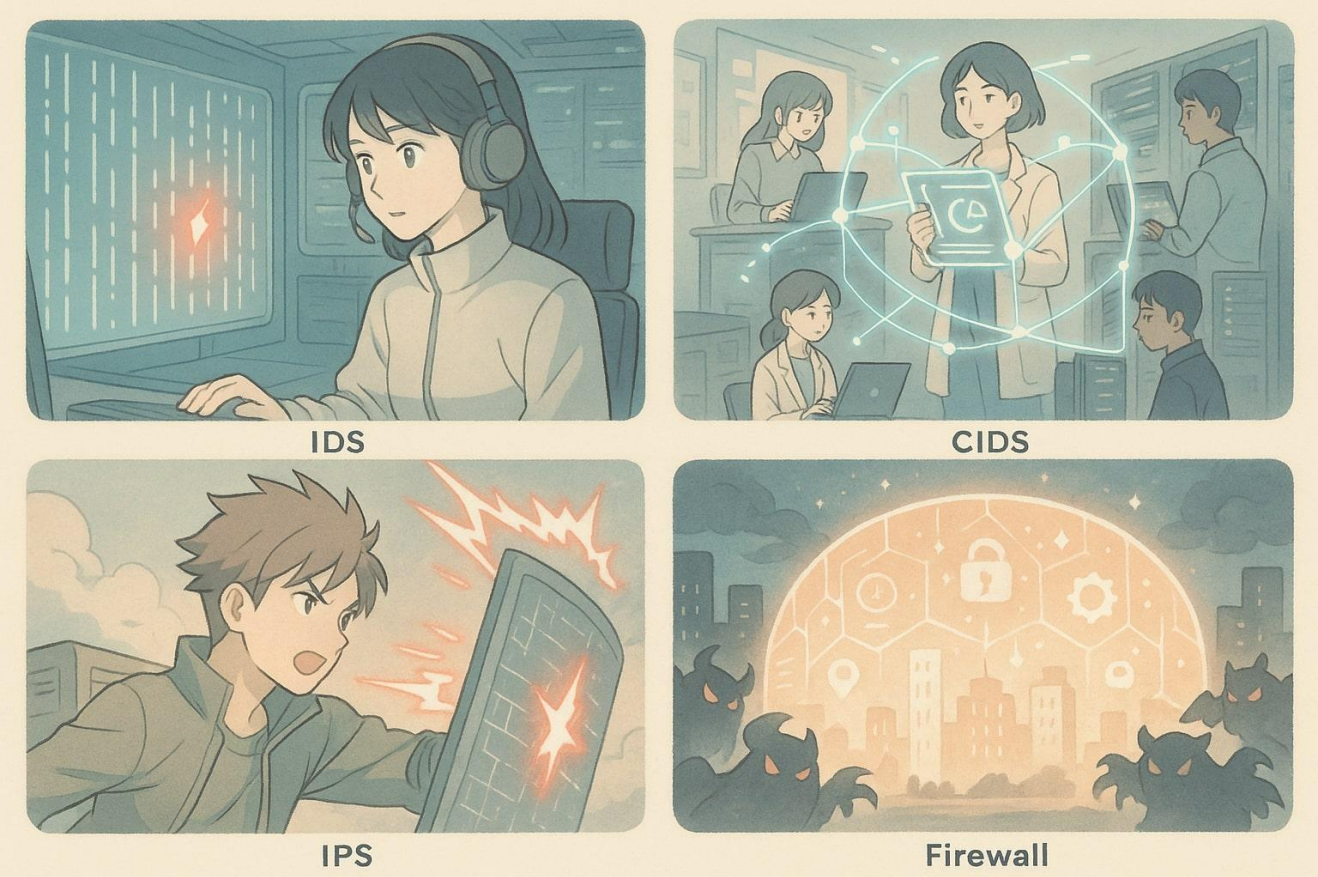
IDS - intrusion detection system

CIDS - Collaborative intrusion detection system

IPS - Intrusion prevention systems

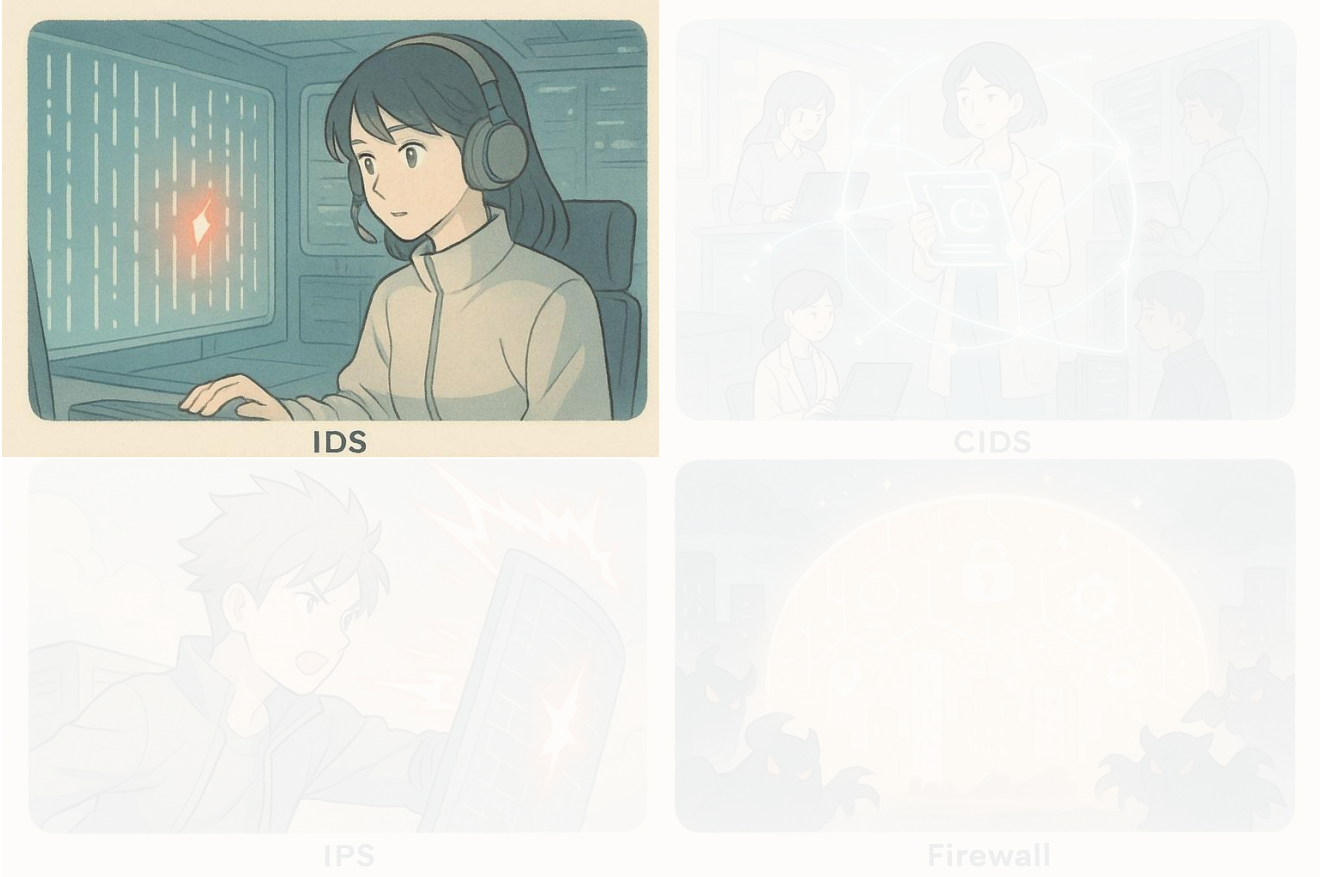
Firewalls

Mecanismos de monitoreo



Fuente: OpenAI. (2025). [Mecanismos de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Mecanismos de monitoreo - IDS



Fuente: OpenAI. (2025). [Mecanismos de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Mecanismos de monitoreo - IDS

- Detectan actividades no autorizadas (*Intrusion Detection System*)
- Se pueden clasificar según el tipo de análisis y donde realizan dicho análisis.

Mecanismos de monitoreo - IDS

- Detectan actividades no autorizadas (*Intrusion Detection System*)
- Se pueden clasificar según el **tipo de análisis** y donde realizan dicho análisis.

Signature-based IDS

- Detecta ataques conocidos.
- Requiere base de datos de patrones predefinidos.
- Baja tasa de falsos positivos.
- No detecta ataques nuevos o "zero-day".

Anomaly-based IDS

- Detecta comportamientos anómalos, incluso desconocidos.
- Requiere entrenamiento previo con datos normales.
- Puede generar falsos positivos si el modelo está mal entrenado.

Mecanismos de monitoreo - IDS

- Detectan actividades no autorizadas (*Intrusion Detection System*)
- Se pueden clasificar según el tipo de análisis y **donde realizan dicho análisis.**

HIDS (Host-based IDS)

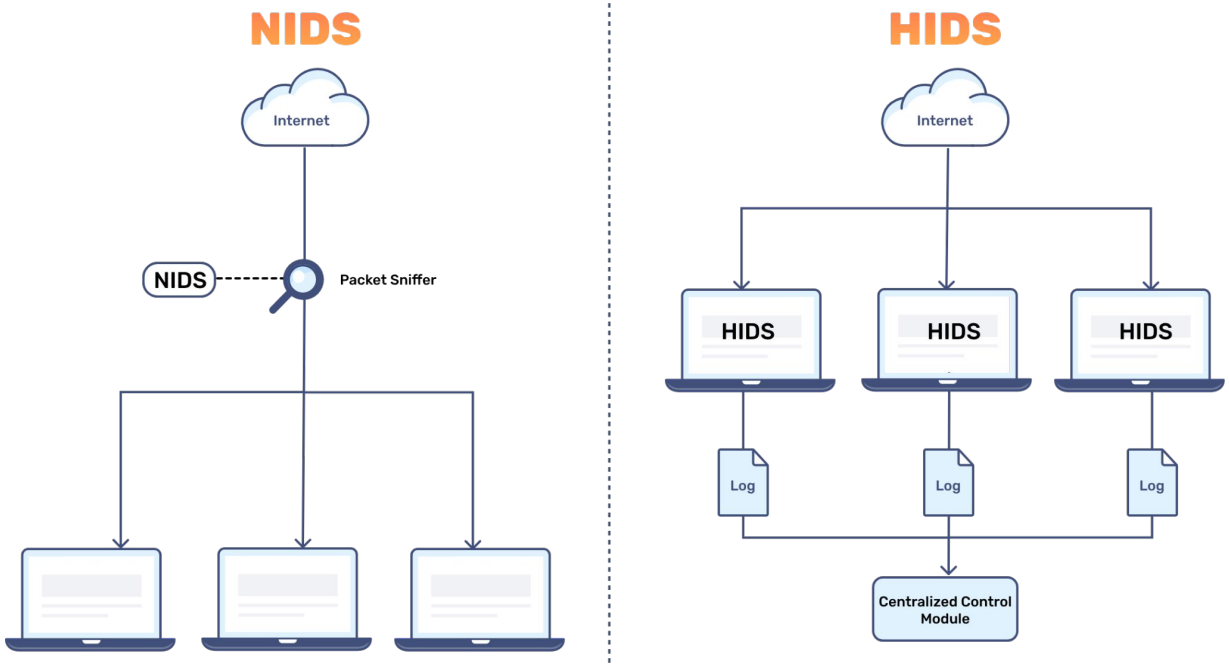
- Se enfoca en analizar un servidor (*host)*.
- Revisa *logs*, llamadas al sistema, integridad de los archivos.
- Detecta ataques internos o posteriores a la intrusión.

NIDS (Network-based IDS)

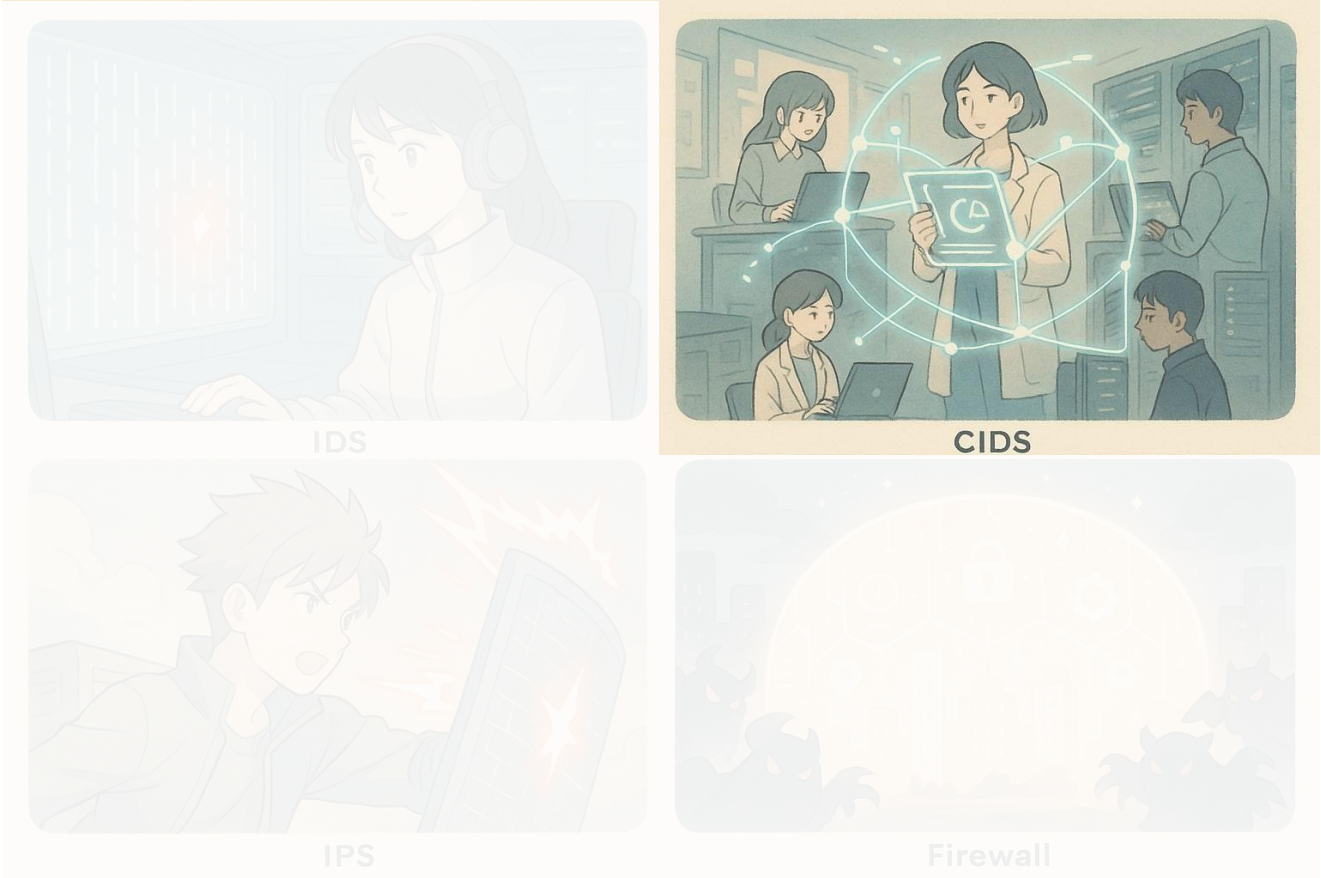
- Se enfoca en analizar la comunicación entre sistemas.
- Revisa el tráfico de red: paquetes en tiempo real.
- Detecta ataques en tránsito o intentos de intrusión.

Mecanismos de monitoreo - IDS

- Detectan actividades no autorizadas (*Intrusion Detection System*)
- Se pueden clasificar según el tipo de análisis y **donde realizan dicho análisis.**



Mecanismos de monitoreo - CIDS

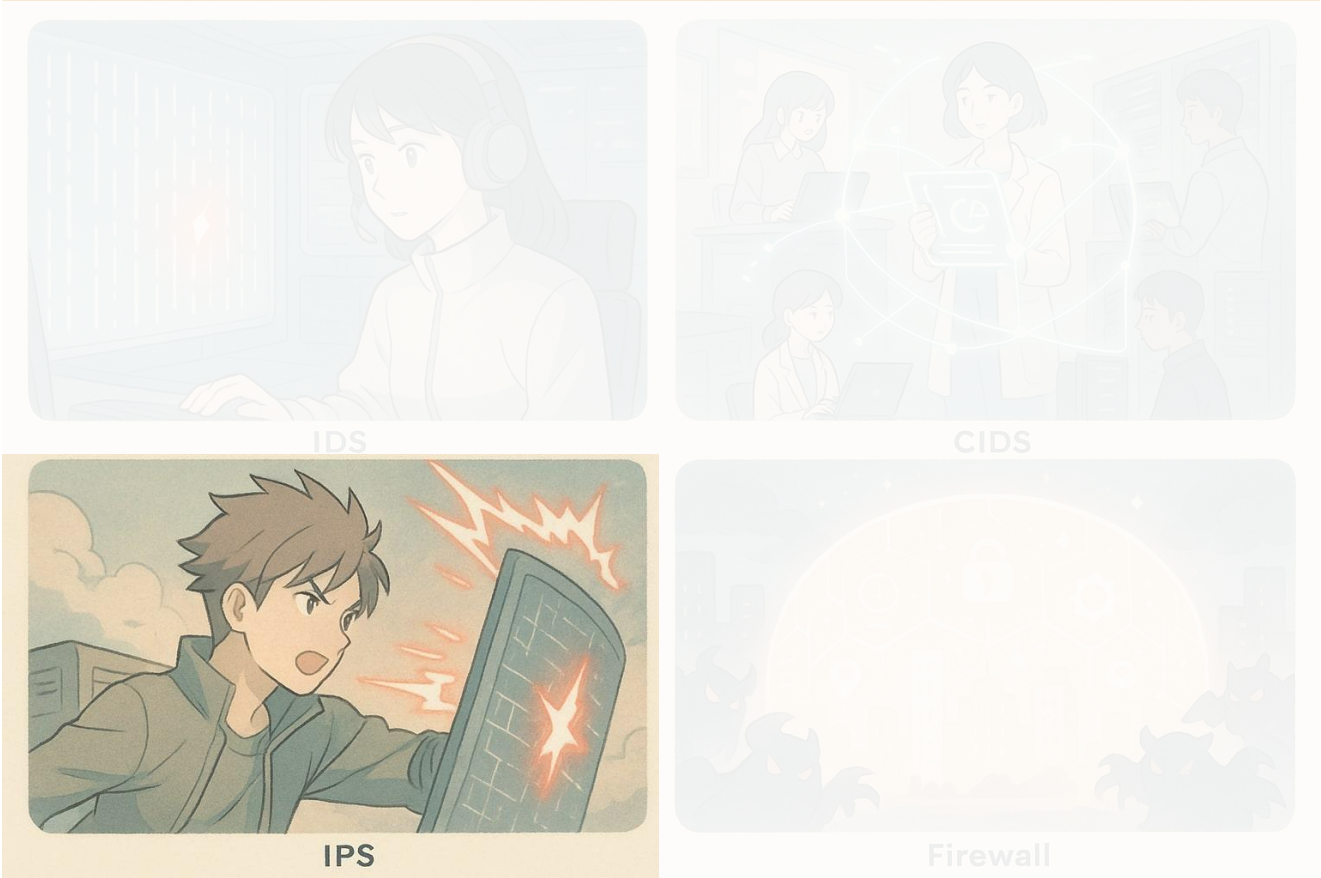


Fuente: OpenAI. (2025). [Mecanismos de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Mecanismos de monitoreo - CIDS

- Una colección de sistemas de detección de intrusos que comparten detecciones y análisis (*Collaborative Intrusion Detection System*).
- Los dispositivos encargados de recoger y analizar datos se agrupan en comunidades, cada una con un líder que es responsable de recopilar y analizar los datos de sus miembros.
- Las comunidades se pueden superponer.

Mecanismos de monitoreo - IPS



Fuente: OpenAI. (2025). [Mecanismos de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Mecanismos de monitoreo - IPS

- Detectan y previenen actividades no autorizadas (*Intrusion Prevention System*).
- Funciona como un *IDS* + capacidad de intervenir:
- Pueden clasificarse según el tipo de análisis que realizan y según su ubicación en el sistema
  - *NIPS*: analizar y previenen ataques a la red (*Network-based*)
  - *HIPS*: analizan y previenen ataques al servidor (*Host-based*)
  - *Anomaly-based IPS*: analizan y previenen anomalías.
  - *Signature-based IPS*: analizan y previenen firmas.

Mecanismos de monitoreo - IPS

- Detectan y previenen actividades no autorizadas (*Intrusion Prevention System*).
- Funciona como un *IDS* + capacidad de intervenir:
- Pueden clasificarse según el tipo de análisis que realizan y según su ubicación en el sistema
  - *NIPS*: analizar y previenen ataques a la red (*Network-based*)
  - *HIPS*: analizan y previenen ataques al servidor (*Host-based*)
  - *Anomaly-based IPS*: analizan y previenen anomalías.
  - *Signature-based IPS*: analizan y previenen firmas.
- Actúa rápido ante amenazas, **pero** está el riesgo de falsos positivos ante anomalías, es decir, bloquear una acción sospechosa que no correspondía bloquear.

Mecanismos de monitoreo - *Firewall*

Fuente: OpenAI. (2025). [Mecanismos de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Mecanismos de monitoreo - *Firewall*

- Dispositivo (hardware o software) que filtra el tráfico entre zonas de red, bloqueando o permitiendo conexiones.
- Primera línea de defensa.
- Sus acciones principalmente son:
  - Permitir o bloquear puertos, IPs, protocolos.
  - Controlar tráfico entrante como saliente.
- Se pueden catalogar según el tipo de análisis realizado y donde operan.

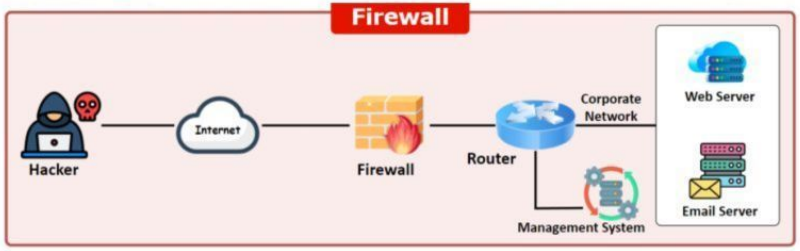
Mecanismos de monitoreo - *Firewall*

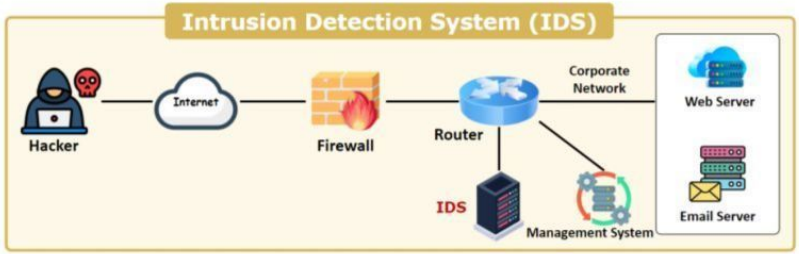
- Se pueden catalogar según el **tipo de análisis** realizado y donde operan.
- **Pasarelas de Filtrado de Paquetes (*Packet Filtering*)**
  - Operan a nivel de red (como un *router*) y deciden el paso de paquetes basándose en las direcciones de origen y destino en el encabezado del paquete IP.
- **Pasarelas a Nivel de Aplicación (*Application Layer Firewall*)**
  - Inspeccionan el contenido de los mensajes entrantes o salientes.

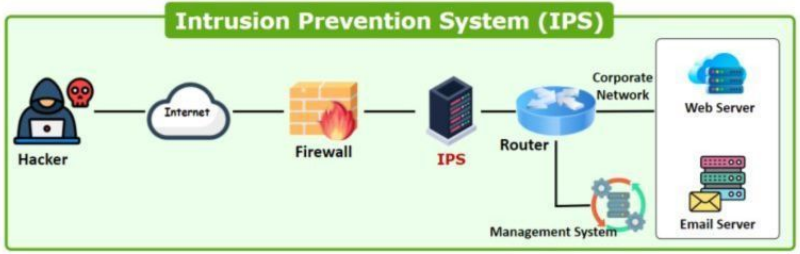
Mecanismos de monitoreo - *Firewall*

- Se pueden catalogar según el tipo de análisis realizado y **donde operan**.
- **Perimetral**
  - Protege el borde entre red interna y externa (entre Lan e Internet)
- **Por servidor**
  - Reglas locales en cada máquina (*Windows Defender Firewall*).
- **De nivel de capa de aplicación**
  - Inspeccionan el tráfico según protocolos específicos (HTTP, SQL, DNS, etc.).
- **Distribuidos**
  - *Firewalls* definidos por *software* que permiten aplicar políticas de seguridad individualizadas en cada componente del sistema.

Mecanismos de monitoreo - Resumen







Firewall:
Primera línea de defensa. Filtra tráfico según reglas.

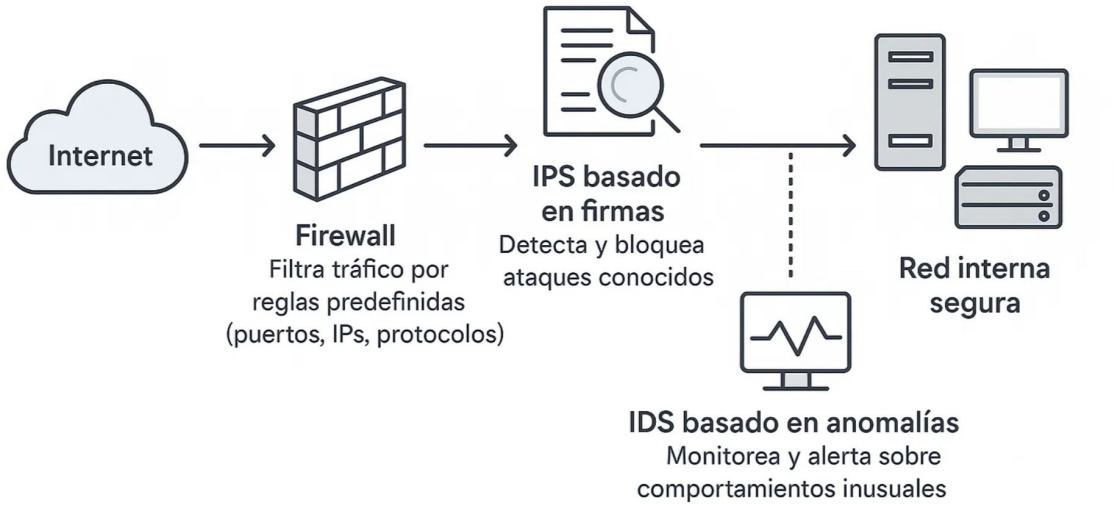
IDS:
Detecta actividades sospechosas, pero no interviene.

IPS:
Detecta y bloquea amenazas en tiempo real.

Fuente: 🚀 Firewall vs IDS vs IPS – Key Differences Explained! | Nasir Amin y OpenAI. (2025). [Firewall, IDS e IPS] (Generada por IA con Sora)

Mecanismos de monitoreo - Ojo 👀

- Si bien muchas veces se elige IDS o IPS, nada obliga a no usar ambos.
  - Por ejemplo, *Signature-based IPS + AIDS*



Fuente: OpenAI. (2025). [*Signature-based IPS + Anomaly-based IDS*] [Imagen generada por IA con Sora]. https://openai.com/sora

Consideraciones legales

Consideraciones legales

- El monitoreo implica el registro de eventos, por ejemplo, las acciones de los usuarios.
- En términos de privacidad, el usuario puede sentirse vulnerado.
- Se requiere un marco regulatorio para definir cómo y hasta donde se puede monitorear al usuario en un sistema.

Consideraciones legales

GDPR: El Marco Europeo de Protección de Datos

- Reglamento General de Protección de Datos de la UE.
- Establece la privacidad como un derecho fundamental.

Consideraciones legales

GDPR: El Marco Europeo de Protección de Datos

- Reglamento General de Protección de Datos de la UE.
- Establece la privacidad como un derecho fundamental.

Objetivos

- Protección de los datos personales contra **accesos no autorizados**.
- **Control del usuario**: acceso, corrección y eliminación de los datos personales.
- **Transparencia** en el uso de los datos.

Consideraciones legales

Para cumplir aspectos legales, muchos sistemas de monitoreo cumplen con:

- Guardar solo datos **estrictamente necesarios** (minimización).
- **Anonimizar** o pseudonimizar información personal cuando sea posible.
- Registrar solo **metadatos relevantes** sin datos sensibles.
    - Tiempo, IP de acceso, tipo de evento, resultado, ubicación general, identificador anónimo, tipo de dispositivo, sistema operativo
- Documentar consentimiento o aviso previo al usuario (Términos y condiciones).
- Restringir acceso a personal autorizado.
- Mantener datos solo el tiempo necesario y luego eliminarlos.

Poniendo a prueba lo que hemos aprendido 👀

En sistemas distribuidos, el monitoreo debe balancear retos técnicos y éticos para garantizar un correcto funcionamiento en la seguridad dentro del ámbito legal.

¿Cuál de las siguientes alternativas representa el **principal desafío** para la identificación de **patrones maliciosos** en el sistema?

a. La exigencia de no almacenar todos los eventos realizados por el usuario en el servidor.

b. La asincronía y desincronización de relojes entre nodos.

c. Un alto volumen de eventos a analizar.

d. La existencia de múltiples algoritmos de cifrado para comunicarse entre los nodos.

e. La exigencia de eliminar periódicamente las acciones del usuario para garantizar su privacidad.

Poniendo a prueba lo que hemos aprendido 👀

En sistemas distribuidos, el monitoreo debe balancear retos técnicos y éticos para garantizar un correcto funcionamiento en la seguridad dentro del ámbito legal.

¿Cuál de las siguientes alternativas representa el **principal desafío** para la identificación de **patrones maliciosos** en el sistema?

a. La exigencia de no almacenar todos los eventos realizados por el usuario en el servidor.

b. La asincronía y desincronización de relojes entre nodos.

c. Un alto volumen de eventos a analizar.

d. La existencia de múltiples algoritmos de cifrado para comunicarse entre los nodos.

e. La exigencia de eliminar periódicamente las acciones del usuario para garantizar su privacidad.

Próximos eventos

Próxima clase

- Arquitecturas *Peer to Peer* (*P2P*),
- Cuando el cliente también es servidor... ¿como garantizamos la seguridad? ¿como buscamos datos en este sistema?

Evaluación

- Estamos con la investigación. Se entrega el lunes 24 de noviembre.

IIC2523
Sistemas Distribuidos

Hernán F. Valdivieso López
(2025 - 2 / Clase 22)