Incidentes de Ciberseguridad – UD2.2

Auditorías de incidentes de Ciberseguridad

IES Chan do Monte – Curso 2025/26

Docente: Simal Paz, Daniel

Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes

---

Índice

---

1. Introducción

En cualquier organización —empresa, administración pública o centro educativo— los sistemas de información están expuestos a:

- ataques externos (hackers, malware, ransomware, phishing…),
- errores internos (configuraciones malas, usuarios despistados),
- y fallos técnicos (hardware, software, red).

Para poder **proteger** estos sistemas no basta con "poner un antivirus". Es necesario combinar:

- **Controles** (medidas preventivas y de protección),
- **Herramientas** (programas y dispositivos que vigilan y actúan),
- **Mecanismos de monitorización y alerta** (para detectar problemas),
- **Equipos especializados** (personas que analizan y responden a los incidentes).

El objetivo de esta unidad es:

- conocer los **tipos de controles** de ciberseguridad,
- entender cómo se **monitorizan** los sistemas,
- saber qué **herramientas** se usan para detectar y analizar incidentes,
- identificar qué **equipos de ciberseguridad** intervienen en la protección de una organización.

📌 **Ejemplo:**

Un ayuntamiento sufre un intento de ataque de fuerza bruta contra su servidor VPN.
Gracias a:

- las **alertas del SIEM**,
- los **registros del firewall**,
- y el trabajo del **equipo de ciberseguridad**,

se detecta rápidamente el patrón de intentos de acceso, se bloquea la IP atacante y se obliga a cambiar contraseñas a los usuarios afectados.

Sin monitorización ni alertas, ese ataque podría haber acabado en un acceso no autorizado.

---

2. Tipos de controles de ciberseguridad

Los **controles** son medidas que se aplican para reducir riesgos y proteger sistemas, datos y personas. Se suelen clasificar en:

- controles técnicos,
- controles físicos,
- controles personales u organizativos.

2.1 Controles técnicos

Son medidas basadas en **tecnología** (software y hardware) que protegen los sistemas.

Ejemplos habituales:

- **Firewalls** de red y de puesto de trabajo.
- **Antivirus / antimalware** instalados en los equipos.
- **Sistemas EDR** (protección avanzada de endpoints).
- **IDS/IPS** que vigilan el tráfico de red.
- **SIEM** que recopilan y analizan eventos de seguridad.
- **Cifrado** de discos y comunicaciones (BitLocker, HTTPS, VPN).
- **Autenticación multifactor (MFA)** para evitar accesos solo con contraseña.

🎯 **Objetivo:** reducir la posibilidad de que un ataque tenga éxito y detectar comportamientos sospechosos.

📌 **Ejemplo:**

Un alumno descarga un archivo infectado.
El **antivirus** detecta la firma del malware y lo pone en cuarentena.
El **firewall** impide que el programa malicioso se conecte a un servidor externo.
Gracias a estos **controles técnicos**, el incidente queda en nada.

2.2 Controles físicos

Protegen los **elementos físicos** de la infraestructura:

- servidores,
- routers, switches,
- CPD (centros de procesamiento de datos),
- puestos de trabajo, portátiles, etc.

Ejemplos de controles físicos:

- Cerraduras y puertas con llave o tarjeta.
- Control de acceso con tarjeta o biometría.
- Cámaras de videovigilancia en zonas sensibles.
- Armarios rack cerrados con llave.
- Sistemas antiincendios y de climatización en el CPD.

📌 **Ejemplo:**

En un instituto, la sala de servidores solo es accesible con una tarjeta personal.
Además, hay cámaras que graban quién entra y sale.
Esto evita que alguien pueda desconectar o robar un servidor sin quedar registrado.

2.3 Controles personales (organizativos)

Se centran en el **comportamiento de las personas**. El factor humano suele ser la causa de muchos incidentes (phishing, contraseñas débiles, uso inadecuado de dispositivos…).

Incluyen:

- Formación y concienciación en ciberseguridad.
- Políticas de uso aceptable de internet, correo y dispositivos USB.
- Normas sobre contraseñas (longitud, caducidad, no compartirlas…).
- Procedimientos de respuesta a incidentes (a quién avisar, cómo actuar).
- Acuerdos de confidencialidad, códigos de conducta, etc.

📌 **Ejemplo:**

Tras una campaña de formación, el personal reconoce mejor los correos de phishing.
Cuando llega un correo sospechoso, lo reenvían al departamento de TI en lugar de hacer clic.

---

3. Mecanismos de monitorización, identificación, detección y alerta

Para poder actuar, primero hay que **saber** que algo está pasando.
Ahí entran en juego la **monitorización**, la **recopilación de información** y el **análisis de eventos**.

3.1 Monitorización

La monitorización consiste en **vigilar de forma continua** el estado de:

- los sistemas (servidores, PCs, portátiles),
- las redes (routers, switches, firewalls),
- las aplicaciones (servidor web, correo, base de datos, ERP, etc.).

Se pueden monitorizar cosas como:

- uso de CPU, memoria, espacio en disco,
- servicios activos/caídos,
- número de peticiones a un servidor web,
- conexiones abiertas,
- cambios de configuración, etc.

🧠 **Idea importante:**
si nadie mira lo que ocurre en la red o en los sistemas, los ataques pueden pasar completamente desapercibidos.

3.2 Recopilación de información (logs)

La monitorización se basa en **recoger datos**.
Estos datos suelen ser **logs** (registros) generados por:

- sistemas operativos (Windows, Linux…),
- dispositivos de red (firewalls, routers),
- aplicaciones (servidor web, correo…),
- herramientas de seguridad (antivirus, IDS/IPS, EDR, etc.).

En esos logs se registran eventos como:

- inicios de sesión (correctos y fallidos),
- cambios de contraseña,
- instalación/desinstalación de programas,
- intentos de conexión bloqueados por el firewall,
- detección de malware por el antivirus.

📌 **Ejemplo práctico:**

Un usuario dice que su cuenta ha sido robada.
Revisando los **logs** se descubre que:

- hubo inicios de sesión desde un país extraño,
- el atacante cambió la contraseña,
- se descargaron muchos datos de golpe.

Gracias a los registros, se puede confirmar el incidente y tomar medidas (bloqueo, investigación…).

3.3 Análisis y correlación de eventos

Un evento aislado (por ejemplo, un inicio de sesión fallido) **no tiene por qué ser un ataque**.
Pero si se analizan **muchos eventos juntos**, se pueden ver patrones.

Ahí entran herramientas como los **SIEM**, que:

- reciben logs de muchas fuentes diferentes,
- los normalizan y almacenan,
- permiten hacer búsquedas y paneles (dashboards),
- y aplican reglas para **correlacionar** eventos.

💡 **Ejemplo de correlación:**

1. 20 intentos de inicio de sesión fallidos de un usuario.
2. Inicio de sesión correcto desde una IP de otro país.
3. Poco después, acceso a un volumen inusual de ficheros.

El SIEM une estos eventos y genera una **alerta** de posible compromiso de cuenta.

3.4 Alertas y respuesta inicial

Cuando se detecta algo sospechoso, las herramientas de seguridad generan **alertas**:

- El antivirus detecta un archivo malicioso.
- El IDS detecta un intento de exploit.
- El SIEM detecta un patrón anómalo.

La **respuesta inicial** suele incluir:

1. Identificar el alcance (qué equipo, qué usuario, qué servicio).
2. Recoger información (logs, capturas de pantalla, mensaje de error…).
3. Aislar el sistema si es necesario (por ejemplo, desconectar de la red).
4. Escalar el incidente al **equipo de ciberseguridad** (interno o externo, SOC, CSIRT, etc.).

4. Equipos de ciberseguridad

Las herramientas por sí solas no son suficientes: tiene que haber **personas** que las configuren, vigilen, interpreten y tomen decisiones.

4.1 Equipo interno de seguridad

Formado por personal propio de la organización:

- técnicos de sistemas,
- administradores de redes,
- responsables de seguridad de la información.

✅ **Ventajas:**

- Conocen muy bien la organización, sus procesos y sus necesidades.
- Tienen control directo sobre los sistemas y cambios.

❌ **Inconvenientes:**

- Requiere presupuesto y personal especializado.
- Es necesario estar en formación constante (las amenazas cambian rápido).

4.2 Servicios externos de ciberseguridad

Muchas organizaciones pequeñas o medianas no pueden tener un equipo propio completo, así que contratan:

- empresas de servicios de seguridad gestionada (MSSP),
- consultoras de ciberseguridad,
- servicios de SOC externalizado, auditorías, pentesting, etc.

✅ **Ventajas:**

- Alto nivel de especialización.
- Acceso a herramientas avanzadas (SIEM, EDR, escáneres de vulnerabilidades, etc.).
- Se paga por servicio (más flexible).

❌ **Inconvenientes:**

- Menor conocimiento interno de la organización.
- Dependencia de contratos, tiempos de respuesta y acuerdos de nivel de servicio (SLA).

4.3 SOC, CSIRT/CERT y otros equipos especializados

SOC (Security Operations Center)
Centro de operaciones de seguridad que:

- monitoriza 24/7 los sistemas y redes,
- analiza alertas de SIEM, IDS, antivirus, etc.,
- coordina la respuesta a incidentes en tiempo real.

CSIRT / CERT
Equipos de Respuesta a Incidentes (a nivel de organización, sector, país…):

- reciben notificaciones de incidentes,
- ayudan a analizarlos, contenerlos y solucionarlos,
- elaboran informes y recomendaciones.

Blue Team, Red Team, Purple Team

- **Blue Team:** equipo defensor. Vigila, endurece sistemas, responde a incidentes.
- **Red Team:** equipo atacante (ético). Simula ataques reales para poner a prueba las defensas.
- **Purple Team:** colaboración entre Red y Blue para aprender y mejorar.

📌 **Ejemplo:**

Una organización encarga a un **Red Team** que simule un ataque de phishing y de intrusión en la red.
El **Blue Team** debe detectar y bloquear el ataque.
Después, el **Purple Team** hace un informe con lo que se hizo bien y mal, y se mejoran las defensas.

---

5. Herramientas de identificación y monitorización

Estas herramientas aumentan la capacidad de detectar, investigar y responder a incidentes.

5.1 EPP (antivirus y protección básica de endpoint)

Las plataformas de protección de endpoint (EPP) son los **antivirus y antimalware clásicos**.

Funciones básicas:

- escaneo de archivos en busca de firmas de malware,
- análisis en tiempo real (protección residente),
- cuarentena o eliminación de archivos peligrosos,
- a veces, firewall personal.

Ejemplos conocidos:

- Microsoft Defender,
- Bitdefender,
- Avast,
- Kaspersky, etc.

Limitación: un EPP tradicional puede no detectar amenazas nuevas (desconocidas) o ataques que no usan archivos (fileless).

5.2 EDR (Endpoint Detection & Response)

El EDR es la evolución avanzada de la protección de endpoint.

Funciones principales:

- monitoriza continuamente lo que ocurre en el equipo (procesos, conexiones, cambios de sistema),
- detecta comportamientos sospechosos, aunque no exista firma conocida,
- puede **actuar automáticamente**: aislar el equipo, matar un proceso, bloquear una conexión, etc.,
- almacena información útil para investigar incidentes.

📌 **Ejemplo:**
Un usuario abre un documento aparentemente normal.
El EDR detecta que, al abrirse, el proceso de Word intenta:

- descargar un script desde una web extraña,
- ejecutar comandos en PowerShell.

Aunque no se trate de un virus conocido, el EDR considera ese comportamiento anómalo y bloquea la acción.

5.3 Escáneres de vulnerabilidades

Son herramientas que buscan **fallos de seguridad** en:

- sistemas operativos,
- servicios (servidor web, servidor de correo…),
- aplicaciones web,
- dispositivos de red.

Realizan pruebas automatizadas para comprobar:

- versiones sin actualizar,
- puertos innecesarios abiertos,
- configuraciones inseguras,
- vulnerabilidades conocidas (CVE).

Ejemplos muy utilizados:

- **Nessus**
  👉 https://www.tenable.com/products/nessus
- **OpenVAS / Greenbone**
  👉 https://www.openvas.org/
  👉 https://www.greenbone.net/en/

💡 **Ejemplo práctico:**

Se pasa un escáner sobre la red de un instituto y se detecta que:

- un servidor Windows no tiene instalados los parches de seguridad críticos,
- un router tiene la contraseña por defecto del fabricante.

Con esta información, el departamento TIC puede corregir los problemas antes de que los aproveche un atacante.

5.4 IDS/IPS

IDS (Intrusion Detection System)
Sistema de **detección de intrusiones**.
Analiza el tráfico de red y otros datos para detectar:

- intentos de ataque,
- patrones conocidos de malware,
- tráfico anómalo.

Genera **alertas**, pero no actúa por sí mismo.

IPS (Intrusion Prevention System)
Sistema de **prevención** de intrusiones.
Además de detectar, puede:

- bloquear conexiones,
- descartar paquetes,
- resetear sesiones.

Ejemplos de motores IDS/IPS:

- **Snort**
- **Suricata** (open source, muy usado en entornos modernos)
  👉 https://suricata.io/
  👉 Documentación de reglas: https://docs.suricata.io/en/latest/rules/index.html

📌 **Ejemplo:**

Suricata está configurado en la red de una empresa.
Detecta un patrón de tráfico que coincide con un exploit de una vulnerabilidad crítica en un servidor web.
El IDS genera una alerta que llega al SIEM y al equipo de seguridad.

5.5 SIEM (Security Information and Event Management)

Un SIEM es una solución central que:

- recibe logs y eventos de muchos sistemas (servidores, firewalls, IDS, aplicaciones…),
- los normaliza y almacena en una base de datos,
- permite buscar, visualizar y crear paneles (dashboards),
- aplica reglas de correlación para detectar patrones de ataque,
- genera alertas y, en algunos casos, orquesta respuestas automáticas.

Es una de las herramientas clave en un **SOC**.

📌 **Recursos de consulta sobre SIEM (en general):**

- IBM – “What is SIEM?”
- Microsoft – “What is SIEM?”
- Cisco – “What is SIEM?”

💡 **Ejemplo de uso:**

El SIEM recibe:

- los logs del firewall,
- los eventos del servidor de correo,
- las alertas del antivirus,
- y los logs de autenticación de los servidores.

Con esta información puede detectar, por ejemplo:

- intentos de fuerza bruta,
- campañas de phishing exitosas,
- movimientos laterales dentro de la red (un atacante que pasa de una máquina a otra).

5.6 DLP (Data Loss Prevention)

Las herramientas DLP se centran en evitar la **pérdida o fuga de datos sensibles** (por ejemplo, datos personales, información confidencial de la empresa, etc.).

Pueden:

- analizar correos salientes,
- controlar copias a dispositivos USB,
- vigilar impresiones,
- analizar ficheros que se suben a la nube.

Si detectan datos sensibles (por ejemplo, números de DNI, tarjetas bancarias, historiales médicos…), pueden:

- bloquear la acción,
- pedir autorización,
- o registrar la incidencia.

📌 **Ejemplo:**

Un empleado intenta mandar por correo un Excel con datos de clientes (DNI, teléfono, dirección). El sistema DLP analiza el contenido, detecta patrones de DNI y bloquea el envío o lanza una alerta al responsable de seguridad.

---

6. Elastic Stack como solución de monitorización y SIEM

Elastic Stack (antes conocido como ELK) está formado por:

- **Elasticsearch** – motor de búsqueda y base de datos donde se almacenan los eventos.
- **Logstash** – herramienta de ingesta y procesamiento de datos (parsing de logs, filtros, transformaciones).
- **Kibana** – interfaz web para visualizar datos, crear dashboards y realizar consultas.
- **Beats** – agentes ligeros que se instalan en los sistemas para enviar logs (Filebeat, Winlogbeat, Packetbeat, Auditbeat, etc.).

👉 Página oficial: https://www.elastic.co/elastic-stack

Con la configuración adecuada, Elastic Stack puede funcionar como un **SIEM**:

- los Beats recogen los logs (sistemas, aplicaciones, redes),
- Logstash los procesa y los envía a Elasticsearch,
- Kibana permite crear cuadros de mando, buscar eventos y configurar alertas.

💡 **Ejemplo sencillo:**

1. En los servidores Windows se instala **Winlogbeat** para enviar los eventos de seguridad.
2. En el servidor web se instala **Filebeat** para enviar el log de accesos de Apache o Nginx.
3. En Kibana se crean paneles que muestran:
    - número de inicios de sesión fallidos,
    - códigos de error HTTP (404, 500…),
    - picos de tráfico.
4. Se configuran alertas cuando:
    - un usuario supera cierto número de intentos fallidos,
    - un servidor deja de enviar logs,
    - aparece un patrón concreto de ataque.

---

7. Reglas IDS (Suricata/Snort): estructura y ejemplos

Herramientas como **Suricata** y **Snort** utilizan **reglas** para detectar ataques.

Una regla tiene dos partes:

1. **Cabecera** – indica:
    - acción (alert, drop, pass…),
    - protocolo (tcp, udp, icmp…),
    - IP y puerto de origen,
    - IP y puerto de destino,
    - dirección del tráfico (-> o <>).
2. **Opciones** – van entre paréntesis y se separan con `;`.
   Algunas típicas son:
    - `msg:"texto descriptivo";` → mensaje que aparecerá en la alerta.
    - `content:"cadena";` → cadena de texto a buscar en el tráfico.
    - `sid:100001;` → identificador único de la regla.
    - `rev:1;` → versión de la regla.

📌 **Ejemplo 1 – Detectar “cmd.exe” en tráfico HTTP**

```
alert tcp any any -> any 80 (
  msg:"Posible uso de cmd.exe en HTTP";
  content:"cmd.exe";
  sid:100001;
  rev:1;
)
```

- Acción: `alert` → genera una alerta.
- Protocolo: `tcp`.
- Origen: `any any` → cualquier IP, cualquier puerto.
- Destino: `any 80` → cualquier IP, puerto 80 (HTTP).
- Opciones: busca la cadena `"cmd.exe"` y, si la encuentra, dispara la alerta con el mensaje indicado.

📌 **Ejemplo 2 – Detectar acceso a `/admin` en una web**

```
alert http any any -> any any (
  msg:"Acceso a /admin detectado";
  content:"GET /admin";
  http_method;
  sid:100002;
  rev:1;
)
```

- Cuando en una petición HTTP aparezca `GET /admin`, se genera una alerta.
- Puede servir para vigilar accesos a paneles de administración.

📌 Documentación de reglas Suricata:
https://docs.suricata.io/en/latest/rules/index.html

---

8. Glosario de términos

Antivirus / EPP: software que protege los endpoints contra malware conocido.
EDR: herramienta avanzada que detecta comportamientos sospechosos en el endpoint y puede responder automáticamente.
IDS: sistema de detección de intrusiones en la red o sistemas.
IPS: sistema que, además de detectar, bloquea las intrusiones.
SIEM: plataforma que centraliza logs, los analiza y genera alertas de seguridad.
DLP: sistema de prevención de fuga de datos.
SOC: centro de operaciones de seguridad.
CSIRT/CERT: equipo de respuesta ante incidentes de seguridad.
Elastic Stack (ELK): conjunto de herramientas para ingesta, almacenamiento y visualización de datos (Elasticsearch, Logstash, Kibana, Beats).
Regla IDS: instrucción que define qué patrón se considera sospechoso y qué hacer cuando se detecta.

---

9. Conclusiones

- La seguridad de una organización se basa en una combinación de **controles técnicos, físicos y personales**.
- La **monitorización continua** y la **recopilación de logs** son esenciales para poder detectar incidentes a tiempo.
- Herramientas como **antivirus, EDR, escáneres de vulnerabilidades, IDS/IPS, SIEM y DLP** forman parte de un ecosistema de defensa.
- Plataformas como **Elastic Stack** permiten construir soluciones de monitorización y detección muy potentes.
- Los **equipos de ciberseguridad** (internos, externos, SOC, CSIRT, Blue/Red/Purple Team) son los encargados de interpretar la información y coordinar la respuesta ante incidentes.
