Ciberseguridad

1. Adopción de pautas de seguridad informática

La seguridad informática se basa en el conjunto de medidas y prácticas destinadas a proteger los sistemas, dispositivos, redes y datos frente a accesos no autorizados, daños o interrupciones. Adoptar pautas adecuadas implica tener en cuenta los principios fundamentales de la seguridad, identificar los elementos vulnerables, conocer las posibles amenazas y aplicar mecanismos de prevención y respuesta.

a) Fiabilidad, confidencialidad, integridad y disponibilidad

Estos son los **cuatro pilares fundamentales** de la seguridad de la información (también conocidos como el modelo **CIA + F**):

- **Confidencialidad**: Garantiza que la información solo sea accesible para las personas autorizadas. Por ejemplo, el uso de contraseñas o cifrado evita que terceros accedan a datos sensibles.
- **Integridad**: Asegura que los datos no han sido modificados de forma no autorizada. Se busca que la información permanezca **completa y sin alteraciones**, lo cual se logra con mecanismos como el control de versiones o las firmas digitales.
- **Disponibilidad**: Implica que los sistemas y datos estén **accesibles cuando se necesiten**, sin interrupciones no deseadas. Esto requiere sistemas redundantes, copias de seguridad y planes de recuperación ante fallos.
- **Fiabilidad**: Se refiere a que los sistemas deben funcionar correctamente durante el tiempo previsto, sin

errores inesperados. Un sistema fiable es predecible y resistente a fallos, tanto físicos como lógicos.

b) Elementos vulnerables en el sistema informático: hardware, software y datos

Todo sistema informático está compuesto por varios elementos susceptibles de ser comprometidos:

- **Hardware**: Equipos físicos como servidores, ordenadores, routers, discos duros. Puede ser dañado por sobrecargas eléctricas, robos, incendios o desgaste. También puede sufrir sabotaje físico.
- **Software**: Sistemas operativos, programas y aplicaciones. Las vulnerabilidades en el software, como errores de programación o configuraciones inseguras, pueden permitir accesos no autorizados o ejecución de código malicioso.
- **Datos**: Son el objetivo principal de la mayoría de ataques. Los datos pueden verse expuestos, alterados o destruidos, afectando la continuidad del negocio y la privacidad de los usuarios.

Cada uno de estos elementos necesita medidas de protección específicas, tanto a nivel físico como lógico.

c) Análisis de las principales vulnerabilidades de un sistema informático

El análisis de vulnerabilidades consiste en identificar los puntos débiles del sistema que pueden ser explotados por atacantes. Algunas de las más comunes son:

- **Sistemas desactualizados**: Software o firmware que no ha

sido actualizado y contiene fallos conocidos.
- **Contraseñas débiles o mal gestionadas**: Uso de claves previsibles o reutilizadas.
- **Configuraciones incorrectas**: Permisos mal asignados, puertos abiertos innecesariamente o servicios expuestos a internet.
- **Falta de cifrado**: En la transmisión o almacenamiento de datos sensibles.
- **Falta de copia de seguridad**: Que impide la recuperación en caso de ataque (como ransomware) o fallo de hardware.
- **Ingeniería social**: Manipulación de usuarios para obtener información confidencial.

Detectar estas vulnerabilidades a tiempo permite corregirlas antes de que puedan ser explotadas.

d) Amenazas. Tipos:

Una **amenaza** es cualquier evento o acción que puede comprometer la seguridad del sistema informático. Se clasifican en **físicas** y **lógicas**:

i. Amenazas físicas

Estas afectan a la infraestructura física del sistema. Algunos ejemplos son:

- **Incendios, inundaciones o terremotos**
- **Cortes de suministro eléctrico**
- **Robo o vandalismo de equipos**
- **Desgaste o fallo del hardware**
- **Acceso físico no autorizado a salas de servidores o puestos de trabajo**

Para mitigarlas se aplican medidas como: sistemas de alimentación ininterrumpida (SAI), controles de acceso físicos, cámaras de vigilancia, almacenamiento seguro de los

equipos, etc.

ii. Amenazas lógicas

Son aquellas que atacan los sistemas mediante software o técnicas digitales. Incluyen:

- **Virus, gusanos y troyanos**: Programas maliciosos que dañan o roban información.
- **Ransomware**: Cifra los archivos y exige un rescate por su recuperación.
- **Spyware o keyloggers**: Recopilan datos personales sin consentimiento.
- **Phishing**: Suplantación de identidad para obtener datos sensibles.
- **Ataques DDoS**: Saturan servidores para provocar la caída del servicio.
- **Accesos no autorizados**: Por explotación de vulnerabilidades o robo de credenciales.

Estas amenazas requieren soluciones como antivirus, firewalls, autenticación multifactor, cifrado de datos, detección de intrusiones y educación en ciberseguridad para los usuarios.

2. Seguridad física y ambiental

La seguridad física y ambiental se refiere al **conjunto de medidas destinadas a proteger los recursos informáticos frente a riesgos físicos**, ambientales o humanos que puedan provocar daños, interrupciones del servicio o pérdida de información. No basta con protegerse de amenazas lógicas; sin una adecuada infraestructura física, cualquier sistema puede verse comprometido.

a) Ubicación y protección física de los

equipos y servidores

La localización y protección física de los equipos, especialmente de los servidores y dispositivos de red, es fundamental para preservar su funcionamiento continuo y su integridad. Algunas prácticas recomendadas:

- **Ubicación adecuada**:
  - Los **servidores deben instalarse en salas específicas (centros de datos o CPD)**, con acceso controlado y restringido.
  - Deben estar **alejados de ventanas o zonas húmedas**, y situados en plantas no propensas a inundaciones.
  - Es recomendable que se encuentren en **zonas interiores, ventiladas y de difícil acceso** desde el exterior.

- **Medidas de seguridad física**:
  - **Controles de acceso**: cerraduras electrónicas, tarjetas de acceso, identificación biométrica.
  - **Sistemas de videovigilancia y alarmas**: para detectar intrusiones o actividades sospechosas.
  - **Armarios o racks de seguridad**: los servidores suelen instalarse en racks metálicos con cerradura, protegidos frente a golpes o manipulación.
  - **Anclaje y protección del cableado**: para evitar sabotajes o desconexiones accidentales.

- **Protección contra incendios**:
  - Instalación de **detectores de humo y sistemas de extinción específicos para equipos eléctricos** (por ejemplo, sistemas de gas inerte, no de agua).
  - Uso de **material ignífugo** en paredes, techos y suelo.

- **Protección contra sobrecalentamientos**:
  - Uso de **sistemas de refrigeración y control de temperatura** constantes.
  - Evitar la acumulación de polvo y realizar mantenimientos periódicos.

b) Sistemas de alimentación ininterrumpida

Un fallo en el suministro eléctrico puede provocar **pérdida de datos, corrupción de archivos o daños en el hardware**. Por ello, se implementan sistemas que garanticen una fuente de energía estable y continua:

- **SAI (Sistema de Alimentación Ininterrumpida)**:
  - Es un **dispositivo que suministra energía temporal** a los equipos informáticos cuando se produce un corte de corriente.
  - Contiene **baterías internas** que proporcionan electricidad durante unos minutos, permitiendo guardar el trabajo y apagar el sistema de forma segura.
  - También **protege frente a picos de tensión o caídas de voltaje**.

- **Grupos electrógenos**:
  - Para instalaciones críticas, se combinan los SAIs con **generadores eléctricos de respaldo** que entran en funcionamiento automáticamente si el corte eléctrico se prolonga.
  - Estos permiten **mantener activos los servidores, routers, sistemas de refrigeración y control**, asegurando la continuidad del servicio.

- **Supervisión del sistema eléctrico**:
  - Se emplean **sensores y software de monitorización** para detectar fallos, consumo anómalo o deterioro de las baterías.

- **Distribución eléctrica redundante**:
  - En entornos de alta disponibilidad, se utilizan **dos líneas eléctricas independientes**, dos SAIs y dos fuentes de alimentación por servidor, para garantizar que el fallo de un componente no interrumpa el funcionamiento.

3. Seguridad lógica

La seguridad lógica comprende el **conjunto de técnicas, herramientas y normas que protegen los recursos informáticos a nivel de software**, garantizando el acceso autorizado, la integridad de los datos y la continuidad del servicio. A diferencia de la seguridad física, se aplica directamente sobre los sistemas operativos, aplicaciones, redes y archivos.

a) Criptografía

La criptografía es una técnica fundamental de seguridad lógica que permite **cifrar la información para que solo pueda ser comprendida por quien posea la clave adecuada**. Sus principales objetivos son:

- **Confidencialidad**: evitar que terceros lean la información.
- **Integridad**: asegurar que los datos no han sido alterados.
- **Autenticidad**: verificar la identidad del emisor.
- **No repudio**: el emisor no puede negar que envió la

información.

Tipos:

- **Cifrado simétrico** (una sola clave): más rápido, pero menos seguro.
- **Cifrado asimétrico** (clave pública y privada): más seguro, base del correo seguro o del protocolo HTTPS.
- **Hashing**: genera un resumen de los datos para verificar su integridad.

Aplicaciones comunes: certificados digitales, firmas electrónicas, conexiones seguras (SSL/TLS), almacenamiento cifrado.

b) Listas de control de acceso

Las **Listas de Control de Acceso** son mecanismos que **determinan qué usuarios o grupos pueden acceder a determinados recursos** y con qué permisos (lectura, escritura, ejecución, eliminación…).

- Se utilizan en sistemas operativos, bases de datos, servidores y redes.
- Permiten una gestión granular y personalizada del acceso.
- Refuerzan el principio del **mínimo privilegio**, otorgando solo los permisos estrictamente necesarios.

c) Establecimiento de políticas de contraseñas

Las contraseñas son la **primera barrera contra accesos no autorizados**, por lo que su fortaleza es clave en la seguridad lógica. Las políticas deben incluir:

- **Longitud mínima** (al menos 8-12 caracteres).
- **Uso de caracteres variados** (mayúsculas, minúsculas, números, símbolos).
- **Prohibición de contraseñas comunes o personales** (como «123456», fechas de nacimiento…).
- **Cambio periódico obligatorio** (cada 3-6 meses, por ejemplo).
- **Evitar el almacenamiento en texto plano** (usar hashing y salting).

Además, se puede complementar con **doble factor de autenticación (2FA)** para mayor seguridad.

d) Políticas de almacenamiento

Estas políticas definen **cómo, dónde y quién puede almacenar información dentro de una organización**. Su objetivo es garantizar la protección y disponibilidad de los datos:

- **Restricciones de acceso a carpetas o unidades** según el rol del usuario.
- **Cifrado de discos duros, USBs o dispositivos móviles**.
- **Prohibición de almacenamiento local en dispositivos no seguros**.
- **Ubicación prioritaria en servidores seguros o nubes con respaldo cifrado**.
- **Control de uso de servicios en la nube externos (Google Drive, Dropbox, etc.)**.

e) Copias de seguridad e imágenes de respaldo

Las **copias de seguridad** (backups) son esenciales para **recuperar la información en caso de fallo, ataque o pérdida**. Deben seguir una política clara:

- **Tipos**:
    - **Completas**: toda la información.
    - **Incrementales**: solo lo que ha cambiado desde la última copia.
    - **Diferenciales**: cambios desde la última copia completa.

- **Frecuencia**: diaria, semanal, etc., según la criticidad.
- **Ubicación**: externa al sistema principal, idealmente **en la nube y/o en servidores offline**.
- **Pruebas periódicas de restauración**, para asegurar su funcionalidad.

Las **imágenes de respaldo** son una copia exacta de todo un sistema, incluida su configuración, útil para **recuperar rápidamente un equipo tras un fallo completo o un ciberataque** (como un ransomware).

f) Medios de almacenamiento

Es fundamental controlar y asegurar los **dispositivos donde se almacenan datos**, ya sean físicos o virtuales. Ejemplos:

- **Discos duros, SSD, USBs, DVDs**: deben estar protegidos contra accesos no autorizados y cifrados si contienen información sensible.
- **Servidores y NAS**: requieren monitorización, actualización y control de accesos.
- **Almacenamiento en la nube**: se debe garantizar el cumplimiento de la legislación (como el RGPD), uso de cifrado de extremo a extremo y proveedores confiables.
- **Dispositivos móviles**: deben incluir bloqueo, cifrado y borrado remoto en caso de pérdida.

4. Análisis forense en sistemas informáticos

El **análisis forense informático** consiste en la **identificación, preservación, análisis y presentación de evidencias digitales** tras un incidente de seguridad (por ejemplo, un ataque, una fuga de datos o sabotaje interno). Su objetivo es reconstruir los hechos de forma precisa y legalmente válida, apoyando tanto la **recuperación del sistema** como posibles procesos judiciales o disciplinarios.

a) Aplicación de metodologías de análisis forenses

El proceso de análisis forense sigue unas fases claramente estructuradas, basadas en metodologías aceptadas internacionalmente, como las propuestas por NIST, ISO/IEC 27037 o SANS Institute. Estas fases son:

1. **Identificación del incidente y planificación**:
    - Detección del evento que motiva el análisis (acceso no autorizado, malware, manipulación de archivos…).
    - Definición del alcance, recursos y objetivos del análisis.

2. **Adquisición y preservación de evidencias**:
    - Recogida de datos sin alterarlos, siguiendo la **cadena de custodia**.
    - Copias forenses (bit a bit) de discos, memorias, logs, correos, redes…
    - Uso de herramientas como FTK Imager, EnCase o dd.

3. **Análisis técnico detallado**:
    - Búsqueda de indicios (timestamps, archivos

sospechosos, cuentas no autorizadas, tráfico de red…).
   - Análisis de logs, memoria RAM, discos duros, registros de eventos, metadatos.
   - Uso de herramientas especializadas (Autopsy, Volatility, Sleuth Kit, Wireshark…).

4. **Interpretación de resultados y reconstrucción de la línea temporal**:
   - Determinar cómo ocurrió el ataque, qué se comprometió, cuándo y por quién.
   - Evaluación del impacto y de posibles vulnerabilidades explotadas.

5. **Contención y respuesta**:
   - Recomendaciones para evitar nuevos ataques (parches, refuerzo de contraseñas, cambios en políticas de acceso…).

b) Documentación y elaboración de informes de análisis forenses

La **documentación exhaustiva** es una parte esencial del análisis forense, tanto para fines técnicos como legales. Debe permitir que un tercero reproduzca el análisis si es necesario.

Aspectos clave del informe forense:

- **Objetivo del análisis** y resumen del incidente.
- **Procedimientos realizados**, con fechas, herramientas utilizadas y responsables.
- **Evidencias recopiladas**: descripciones técnicas, ubicación, formato y hash de verificación.
- **Hallazgos relevantes**: ficheros sospechosos, accesos no

autorizados, actividad inusual.
- **Línea temporal de eventos**, si es posible.
- **Conclusiones**: explicación detallada de lo sucedido.
- **Recomendaciones**: medidas correctoras o preventivas.

El informe debe estar escrito con **precisión técnica y claridad**, de forma comprensible para equipos directivos o jurídicos, manteniendo siempre la **cadena de custodia de las pruebas** y garantizando su **validez legal**.

5. Implantación de mecanismos de seguridad activa

La **seguridad activa** en los sistemas informáticos consiste en el **conjunto de medidas, herramientas y prácticas que previenen, detectan y reaccionan ante ataques o vulnerabilidades**. Su objetivo es garantizar la continuidad del servicio y minimizar el impacto de las amenazas.

a) Ataques y contramedidas en sistemas personales

Los **sistemas personales (PC, móviles, portátiles, tablets)** son especialmente vulnerables debido a su exposición continua a redes públicas, software de terceros y prácticas poco seguras del usuario.

Ataques frecuentes:

- Phishing
- Malware (troyanos, ransomware, spyware)
- Robo de credenciales
- Instalación de software no autorizado
- Ingeniería social

Contramedidas comunes:

- Antivirus actualizado
- Firewall personal
- Autenticación multifactor
- Navegadores seguros y extensiones de bloqueo
- Control de permisos de aplicaciones

b) Clasificación de los ataques

Los ataques informáticos pueden clasificarse en función de varios criterios:

Según el objetivo:

- Contra la confidencialidad (espionaje, sniffing)
- Contra la integridad (alteración de datos)
- Contra la disponibilidad (DoS, ransomware)

Según el medio:

- Ataques físicos (robo de dispositivos)
- Ataques lógicos (software malicioso, exploits)
- Ataques humanos (ingeniería social)

Según la visibilidad:

- Ataques activos: modifican el sistema o sus datos.
- Ataques pasivos: solo observan o capturan información.

c) Anatomía de ataques y análisis de software malicioso

El **análisis de un ataque** permite comprender su estructura y su funcionamiento. Suele implicar:

- **Vectores de entrada**: correo electrónico, web,

dispositivos USB, aplicaciones.
- **Carga maliciosa**: código ejecutado que daña, espía o toma control.
- **Mecanismos de persistencia**: ocultación, reinfección, modificación del registro.
- **Comportamiento en el sistema**: cambios en archivos, procesos, conexiones.

El **análisis de malware** se puede realizar:

- **Estáticamente**: sin ejecutar el archivo (lectura de código, hash, firmas).
- **Dinámicamente**: en entornos controlados (sandbox) para observar su comportamiento.

d) Herramientas preventivas. Instalación y configuración

Las herramientas **preventivas** se enfocan en evitar que ocurran ataques. Algunas esenciales:

- **Antivirus y antimalware**: escaneo en tiempo real.
- **Firewalls personales y de red**: filtrado de tráfico.
- **Navegadores seguros y extensiones anti-rastreo**.
- **Sistemas de detección de intrusos (IDS)**.
- **Antispam y filtros DNS seguros**.

Instalarlas correctamente implica:

- Configurar actualizaciones automáticas.
- Personalizar niveles de análisis.
- Programar escaneos periódicos.

e) Herramientas paliativas. Instalación y configuración

Las herramientas **paliativas** ayudan a **minimizar el daño y recuperar el sistema** tras un ataque:

- **Sistemas de backup automático**.
- **Herramientas de restauración del sistema**.
- **Sistemas de contención y aislamiento (sandbox, máquinas virtuales)**.
- **Eliminadores de malware especializados (ej. RKill, Malwarebytes Anti-Rootkit)**.

f) Actualización de sistemas y aplicaciones

Mantener el sistema operativo, el navegador y los programas siempre **actualizados** es crucial para cerrar vulnerabilidades conocidas.

Las **actualizaciones automáticas** y la **revisión periódica de parches de seguridad** son prácticas recomendadas.

g) Seguridad en la conexión con redes públicas

Conectarse a redes Wi-Fi públicas puede exponer al dispositivo a numerosos riesgos:

Riesgos:

- Interceptación de tráfico (ataques MITM).
- Captura de credenciales.
- Redireccionamiento a sitios falsos.

Medidas de protección:

- Usar **VPNs**.
- Evitar servicios sensibles (banca, compras).
- No conectarse automáticamente a redes abiertas.
- Desactivar el uso compartido.

h) Pautas y prácticas seguras

Listado de prácticas seguras:

- Utilizar contraseñas fuertes y únicas, y cambiarlas regularmente.
- No instalar software de fuentes desconocidas.
- Cifrar los datos sensibles del dispositivo.
- Activar el bloqueo automático del equipo.
- Controlar los permisos de aplicaciones móviles.
- Educar en **conciencia de ciberseguridad** (formación continua).

6. Seguridad en la red corporativa

La **seguridad en redes corporativas** busca proteger la infraestructura, los dispositivos conectados y los datos que circulan a través de la red frente a accesos no autorizados, ataques, fugas de información y otras amenazas. Requiere una **estrategia integral**, incluyendo vigilancia constante, configuración segura de servicios y respuesta rápida ante incidentes.

a) Monitorización del tráfico en redes

La **monitorización del tráfico** permite detectar patrones anómalos, accesos no autorizados y posibles ciberataques en tiempo real.

Herramientas comunes:

- **IDS/IPS (Intrusion Detection/Prevention Systems)**: detectan y/o bloquean tráfico sospechoso (Snort, Suricata).
- **SIEM (Security Information and Event Management)**: centraliza logs y permite correlación de eventos (ej. Splunk, AlienVault).
- **NetFlow/sFlow**: recopilan y analizan flujos de datos en red.
- **Wireshark**: análisis profundo de paquetes en red.

Ventajas:

- Permite la detección temprana de amenazas.
- Ayuda a identificar cuellos de botella o mal uso de la red.
- Genera alertas ante patrones de tráfico inusuales.

b) Seguridad en los protocolos para comunicaciones inalámbricas

Las comunicaciones inalámbricas (Wi-Fi) son vulnerables si no se configuran adecuadamente. Es esencial usar protocolos de seguridad robustos:

Protocolos de seguridad Wi-Fi:

- **WEP (obsoleto)**: débil y fácilmente vulnerable.
- **WPA/WPA2**: mejora la seguridad con cifrado TKIP/AES.
- **WPA3 (actual)**: añade cifrado más fuerte, protección ante ataques de diccionario y mayor seguridad para redes abiertas.

Medidas complementarias:

- Cambiar SSID por defecto.

- Ocultar la red (SSID broadcasting).
- Usar listas blancas de direcciones MAC (aunque pueden ser suplantadas).
- Activar aislamiento de clientes.
- Usar VPN corporativa incluso sobre Wi-Fi interno.

c) Riesgos potenciales de los servicios de red

Los servicios de red (DNS, DHCP, correo, web, FTP, etc.) pueden convertirse en vectores de ataque si no se gestionan adecuadamente.

Riesgos comunes:

- **DNS poisoning**: redireccionamiento a sitios maliciosos.
- **Open relays en servidores de correo**: pueden usarse para spam.
- **Servicios no actualizados**: con vulnerabilidades explotables.
- **Puertos abiertos innecesarios**: amplían la superficie de ataque.
- **Servicios mal configurados**: acceso sin autenticación, permisos excesivos, etc.

Recomendaciones:

- Aplicar el principio de **mínimos privilegios**.
- Cerrar puertos innecesarios.
- Usar **firewalls perimetrales e internos**.
- Aislar servicios críticos en zonas desmilitarizadas (**DMZ**).

d) Intentos de penetración

Los **intentos de penetración** son acciones deliberadas para encontrar fallos en una red y obtener acceso no autorizado.

Tipos de ataque habituales:

- **Escaneos de puertos** (ej. Nmap): para identificar servicios abiertos.
- **Ataques por fuerza bruta**: probar múltiples combinaciones de credenciales.
- **Exploits sobre vulnerabilidades**: aprovechar fallos conocidos.
- **Sniffing de tráfico**: especialmente si no está cifrado.
- **Ataques internos**: desde empleados o dispositivos comprometidos.

Medidas de defensa:

- Sistemas de detección de intrusos (IDS).
- Registro y análisis de logs (SIEM).
- Configuración segura y actualización de servicios.
- Autenticación fuerte y control de acceso por roles.
- Auditorías de seguridad periódicas y tests de penetración controlados.

7. Implantación de técnicas de acceso remoto. Seguridad perimetral

En un entorno corporativo, donde es habitual el acceso remoto a recursos internos, resulta prioritario establecer mecanismos de **seguridad perimetral** y **acceso seguro**. Esto implica controlar los puntos de entrada y salida de la red, segmentar adecuadamente los servicios, y emplear tecnologías como **VPNs** y cifrado robusto.

a) Elementos básicos de la seguridad perimetral

La **seguridad perimetral** consiste en proteger la frontera de la red corporativa frente a amenazas externas. Los elementos básicos son:

- **Firewall (cortafuegos)**: filtra el tráfico de red entrante y saliente según reglas definidas.
- **IDS/IPS**: detectan y bloquean comportamientos anómalos o ataques.
- **Proxies**: intermedian el tráfico web, filtrando contenidos y ocultando identidades.
- **Gateways de seguridad**: controlan accesos a servicios específicos.
- **Filtros de correo**: bloquean spam y malware en el correo electrónico.

b) Perímetros de red. Zonas desmilitarizadas

Una **zona desmilitarizada (DMZ)** es un área intermedia entre la red interna y la externa (Internet), usada para alojar servicios que deben ser accesibles desde fuera (como servidores web, correo, DNS).

Objetivo: Aislar la red interna de accesos directos desde el exterior, minimizando riesgos.

Características de una DMZ:

- Se configura entre dos firewalls o con un firewall de tres zonas.
- Los servidores dentro de la DMZ están protegidos y aislados del resto de la red.
- Permite controlar estrictamente el flujo de tráfico

hacia la red interna.

c) Arquitectura débil de subred protegida

Una **arquitectura débil** se refiere a una configuración de seguridad mínima o poco segmentada.

Ejemplo típico:

- Un solo firewall entre la red interna y externa.
- Todos los servicios (internos y públicos) alojados en la misma subred.
- Ausencia de DMZ o segmentación de tráfico.

Consecuencias:

- Mayor riesgo en caso de compromiso de un servidor.
- Difícil detección de intrusiones.
- Mal control del tráfico lateral.

d) Arquitectura fuerte de subred protegida

Una **arquitectura fuerte** implica una protección multicapa, segmentación de servicios y monitorización constante.

Elementos comunes:

- Firewall perimetral + firewall interno.
- Red segmentada en VLANs o subredes según funciones.
- DMZ bien definida para servicios públicos.
- Monitorización y reglas específicas por zona.
- Autenticación fuerte y control de acceso granular.

Ventajas:

- Mejora el aislamiento de los servicios críticos.
- Minimiza el impacto de un ataque lateral.
- Facilita la detección y respuesta ante incidentes.

e) Redes privadas virtuales. VPN

Una **VPN (Virtual Private Network)** permite establecer una conexión cifrada a la red corporativa desde ubicaciones remotas, como si el usuario estuviera físicamente en la red interna.

Tipos:

- **VPN de acceso remoto (client-to-site)**: para empleados que se conectan desde fuera.
- **VPN de sitio a sitio (site-to-site)**: conecta redes completas entre ubicaciones distintas.

Protocolos habituales:

- **IPSec**, **L2TP**, **OpenVPN**, **SSL-VPN**.

f) Beneficios y desventajas con respecto a las líneas dedicadas

Aspecto	VPN	Línea dedicada
Coste	Bajo (usa Internet)	Alto (infraestructura propia)
Flexibilidad	Alta (desde cualquier lugar)	Limitada (fija)
Seguridad	Alta si se cifra adecuadamente	Muy alta (sin paso por Internet)
Mantenimiento	Medio (depende del proveedor y TI)	Alto (revisiones constantes)

Aspecto	VPN	Línea dedicada
Rendimiento	Variable (según ancho de banda y latencia)	Estable

Conclusión: Las VPN son más económicas y flexibles, ideales para la mayoría de escenarios actuales, aunque las líneas dedicadas siguen siendo válidas en entornos críticos con gran exigencia de rendimiento y seguridad.

g) Técnicas de cifrado. Clave pública y clave privada

El **cifrado** garantiza la confidencialidad y autenticidad de los datos. Se basa en algoritmos que convierten la información en ilegible para quien no tenga la clave adecuada.

Tipos de cifrado:

- **Cifrado simétrico**: usa una sola clave para cifrar y descifrar (ej. AES). Rápido, pero con el problema del intercambio seguro de la clave.
- **Cifrado asimétrico**: usa un **par de claves**:
  - **Clave pública**: se comparte abiertamente.
  - **Clave privada**: se mantiene en secreto.
  - Lo que se cifra con una clave solo puede descifrarse con la otra (ej. RSA).

Usos combinados:

- En comunicaciones seguras (HTTPS, VPN), se usa cifrado asimétrico para intercambiar una clave simétrica, que luego cifra el resto del tráfico.

Ejemplo práctico: en una conexión VPN, el túnel puede establecerse con autenticación basada en clave pública

(certificados digitales) y luego cifrarse con un algoritmo simétrico de alto rendimiento como AES.

8. Bastionado de redes y sistemas

El **bastionado** consiste en aplicar un conjunto de medidas técnicas para **reforzar la seguridad de sistemas, dispositivos y redes informáticas**, eliminando servicios innecesarios, configurando adecuadamente accesos y minimizando superficies de ataque. Es un proceso clave en la **ciberseguridad preventiva**.

a) Diseño de planes de securización

Un **plan de securización** es un conjunto planificado de acciones que permiten establecer mecanismos de protección adecuados en una red o sistema. Suele incluir:

- **Análisis del entorno**: dispositivos, servicios y topología de red.
- **Identificación de riesgos y amenazas**.
- **Establecimiento de medidas preventivas y reactivas** (bastionado, backup, monitorización).
- **Definición de roles y responsabilidades**.
- **Documentación de configuraciones seguras**.
- **Planificación de auditorías periódicas**.

Su objetivo es **minimizar vulnerabilidades antes de que sean explotadas**.

b) Configuración de sistemas de control de acceso y autenticación de personas

El acceso debe estar **estrictamente controlado** en función del principio de **privilegio mínimo** (cada usuario accede solo a lo que necesita).

Medidas típicas:

- **Autenticación multifactor (MFA)**: combinación de contraseña + token, huella o app.
- **Servidores de autenticación centralizada**: LDAP, RADIUS, Active Directory.
- **Políticas de expiración y complejidad de contraseñas**.
- **Gestión de cuentas privilegiadas (PAM)**.
- **Desactivación de cuentas inactivas o por baja**.

c) Administración de credenciales de acceso a sistemas informáticos

Una **gestión segura de credenciales** implica evitar malas prácticas (como contraseñas repetidas, almacenadas en texto plano o compartidas entre usuarios).

Buenas prácticas:

- Uso de **gestores de contraseñas cifrados**.
- Aplicación de **rotación periódica** de contraseñas.
- Auditoría de accesos y control de cambios.
- Eliminación de credenciales por defecto en software y dispositivos.
- Registro de actividad (logs) de autenticaciones.

d) Diseño de redes de computadores seguras

Una **red segura** debe estar segmentada, supervisada y contener mecanismos de aislamiento entre recursos.

Principios del diseño seguro:

- **Segmentación de red** mediante VLANs o subredes.

- Uso de **firewalls internos** para separar zonas (DMZ, red de datos, red de gestión).
- **Redundancia y tolerancia a fallos** en componentes críticos.
- Aplicación de **políticas de acceso por capas**.
- **Enrutamiento seguro** y detección de tráfico anómalo (IDS/IPS).

e) Configuración de dispositivos y sistemas informáticos

Todo dispositivo que se conecte a la red debe estar correctamente configurado para reducir posibles vectores de ataque.

Medidas comunes de bastionado:

- **Desactivación de servicios no necesarios**.
- **Actualización de firmware y parches del sistema operativo**.
- **Bloqueo de puertos y servicios no usados**.
- Aplicación de **reglas de firewall local**.
- **Registro y auditoría** del uso del sistema.

Ejemplo: un router o switch debe tener cambiadas las contraseñas por defecto, limitar el acceso remoto, registrar eventos y tener habilitado el cifrado en sus interfaces de administración.

f) Configuración de dispositivos para la instalación de sistemas informáticos

En la fase previa a la instalación de un sistema, los **dispositivos hardware** deben configurarse correctamente:

- Activación de **Secure Boot** (UEFI).

- Desactivación de puertos físicos no necesarios (USB, lector de tarjetas).
- Uso de discos cifrados (BitLocker, LUKS).
- Configuración de **RAID** para tolerancia a fallos.
- Establecimiento de claves de BIOS o firmware.

Todo esto evita accesos no autorizados desde el arranque o manipulación física.

g) Configuración de los sistemas informáticos

Una vez instalado el sistema operativo y las aplicaciones, se deben seguir pautas de configuración segura:

- **Aplicación de políticas de grupo (GPO)** en entornos Windows.
- Desactivación de **cuentas administrativas por defecto**.
- Configuración de **logs del sistema y eventos críticos**.
- Establecimiento de **roles y permisos de usuarios**.
- **Automatización de actualizaciones** críticas de seguridad.
- Restricciones de ejecución de scripts o macros según entorno.

Además, se recomienda el uso de herramientas de **end-point protection** y **plataformas de gestión centralizada de seguridad** (EDR, MDM).

9. Hacking ético

El **hacking ético** consiste en aplicar las técnicas de un atacante, pero con fines **legítimos y autorizados**, con el objetivo de **evaluar la seguridad de sistemas y redes**. Los profesionales que lo llevan a cabo son conocidos como **pentesters** o **hackers de sombrero blanco**.

El proceso suele desarrollarse en **entornos controlados** o de pruebas, simulando ataques reales, con el fin de **identificar vulnerabilidades, evaluar el impacto potencial** y proponer **medidas de mejora**.

a) Determinación de las herramientas de monitorización para detectar vulnerabilidades

El primer paso es la **identificación de debilidades** en redes, sistemas o aplicaciones. Para ello, se utilizan herramientas de escaneo, auditoría y análisis.

Herramientas habituales:

- **Nmap**: escaneo de puertos y detección de servicios.
- **Wireshark**: análisis de tráfico de red.
- **Nessus / OpenVAS**: escáneres de vulnerabilidades.
- **Nikto**: escáner de servidores web.
- **Burp Suite**: análisis de seguridad de aplicaciones web.
- **Metasploit**: framework de explotación.
- **Aircrack-ng**: análisis de redes Wi-Fi.

El objetivo es **detectar puntos débiles** que puedan ser explotados por un atacante.

b) Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas

Las redes inalámbricas presentan riesgos específicos. En entornos de laboratorio se simulan ataques para comprobar la robustez de las comunicaciones Wi-Fi.

Ataques comunes simulados:

- **Captura de handshakes** y crackeo de contraseñas (WPA/WPA2).
- **Ataques de desautenticación (deauth)** para forzar reconexión y captura.
- **Evil twin**: crear un punto de acceso falso.
- **Man-in-the-middle (MITM)**: interceptar tráfico.

Contramedidas evaluadas:

- Uso de **WPA3 o WPA2-Enterprise**.
- **Filtrado MAC**, ocultación de SSID (aunque no son medidas fuertes).
- Segmentación de la red y aislamiento de clientes.
- **Autenticación RADIUS** en redes corporativas.

c) Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros

Aquí se simulan accesos no autorizados mediante vulnerabilidades en servicios de red, sistemas operativos o configuraciones débiles.

Ejemplos de pruebas ofensivas:

- **Explotación de servicios desactualizados** con vulnerabilidades conocidas (como SMB, RDP, FTP).
- **Fuerza bruta de credenciales**.
- **Escalada de privilegios** una vez dentro del sistema.
- **Pivoting** para moverse lateralmente dentro de la red.

Defensas evaluadas:

- **Firewalls y filtrado de puertos**.
- Sistemas de detección de intrusiones (**IDS/IPS**).

- **End-point protection** y control de integridad.
- Políticas de acceso restrictivas (ACLs, listas blancas).
- Segmentación de redes y sistemas honeypot.

d) Consolidación y utilización de sistemas comprometidos

Una vez que un sistema ha sido comprometido, el atacante ético simula cómo podría **mantener el acceso** y utilizar ese sistema como plataforma de ataque o de exfiltración de datos.

Técnicas comunes:

- Instalación de **backdoors** o puertas traseras persistentes.
- **Creación de usuarios ocultos** o con privilegios elevados.
- Uso de **túneles cifrados** para evadir detección.
- **Rootkits** para ocultar procesos y archivos maliciosos.
- Lanzamiento de ataques internos desde ese nodo (pivoting).

Esto permite al pentester evaluar el nivel de **persistencia** que podría lograr un atacante real y cómo detectar su presencia.

e) Ataque y defensa en entorno de pruebas, a aplicaciones web

Las aplicaciones web son uno de los objetivos más comunes. El hacking ético analiza la seguridad de formularios, sesiones, entradas de usuario, APIs, etc.

Pruebas ofensivas típicas:

- **Inyección SQL (SQLi)**.
- **Cross-site scripting (XSS)**.
- **Cross-site request forgery (CSRF)**.

- **Directory traversal**.
- **Upload de ficheros maliciosos**.
- **Robo de sesiones o cookies**.

Herramientas empleadas:

- **OWASP ZAP**, **Burp Suite**, **SQLmap**, **Wfuzz**.

Defensas evaluadas:

- Uso correcto de **validación de entrada/salida**.
- Aplicación de **WAF (Web Application Firewall)**.
- Configuración segura del servidor y cabeceras HTTP.
- Políticas de seguridad como **CSP** (Content Security Policy).
- Auditoría de código y actualizaciones regulares.

10. Normativa de ciberseguridad

El cumplimiento normativo en ciberseguridad es esencial para garantizar la **legalidad, la protección de datos, la integridad de los sistemas** y la **responsabilidad de las organizaciones** frente a incidentes de seguridad. Las empresas deben integrar estos requisitos en sus políticas, procedimientos técnicos y estructuras organizativas.

a) Puntos principales de aplicación para un correcto cumplimiento normativo

Para cumplir con la normativa de ciberseguridad, deben contemplarse los siguientes aspectos clave:

- **Confidencialidad, integridad y disponibilidad de los datos** (principios básicos de la seguridad).
- **Gestión del riesgo**: identificación, evaluación y

mitigación de amenazas.

- **Protección de datos personales** conforme al RGPD y la LOPDGDD.
- **Auditorías de seguridad periódicas** y documentación de procesos.
- **Notificación de brechas de seguridad** en los plazos legales.
- **Concienciación y formación del personal** en seguridad y privacidad.
- **Designación de un responsable de seguridad** o DPO, si procede.
- **Sistemas de trazabilidad y evidencias** para cumplir con la ley en caso de inspección.

b) Diseño de sistemas de cumplimiento normativo

Implica la creación de un **marco interno de gestión** que garantice el cumplimiento legal. Requiere:

- **Políticas internas de seguridad y privacidad**.
- **Inventario de activos** y control de accesos.
- **Evaluaciones de impacto (PIA)** en tratamiento de datos.
- **Canales de denuncia interna** (compliance penal y protección de informantes).
- Implementación de **sistemas de gestión basados en normas ISO** (como ISO/IEC 27001).
- **Revisión y actualización periódica** del sistema de cumplimiento.

c) Legislación para el cumplimiento de la responsabilidad penal

La **LO 1/2015** reformó el Código Penal español y atribuyó **responsabilidad penal a las personas jurídicas**, lo que implica

que una empresa puede ser penalmente responsable si:

- No ha adoptado **medidas de vigilancia y control** para evitar delitos (como accesos ilícitos, sabotajes, robo de datos, etc.).
- No cuenta con un **programa de cumplimiento normativo (compliance penal)**.

Por tanto, se exige:

- Diseño de un **plan de prevención de delitos**.
- Identificación de **riesgos penales** tecnológicos.
- Supervisión del cumplimiento por un **órgano de control** (compliance officer).
- Pruebas de que se han tomado medidas **antes del delito**, no después.

d) Legislación y jurisprudencia en materia de protección de datos

Marco normativo principal:

- **Reglamento General de Protección de Datos (RGPD – UE 2016/679)**
- **Ley Orgánica 3/2018 (LOPDGDD)**, adaptación nacional del RGPD

Aspectos clave:

- Principios de **licitud, lealtad, transparencia, minimización de datos y responsabilidad proactiva**.
- Requiere realizar **análisis de riesgos y evaluaciones de impacto (EIPD)**.
- Necesita el **consentimiento expreso**, salvo excepciones

legales.
- Impone **plazos para notificar violaciones de seguridad** (máx. 72h).
- **Derechos ARSULIPO**: Acceso, Rectificación, Supresión, Limitación, Portabilidad y Oposición.
- Jurisprudencia creciente en casos de **filtraciones de datos, videovigilancia ilegal, brechas sin notificar**, etc.

e) Normativa vigente de ciberseguridad de ámbito nacional e internacional

A nivel nacional (España):

- **Ley 43/2021**, de seguridad informática en el sector público.
- **Ley 9/2014**, General de Telecomunicaciones.
- **Esquema Nacional de Seguridad (ENS)**: obligatorio para administraciones públicas.
- **Ley de Protección de Infraestructuras Críticas (Ley PIC).**

A nivel europeo/internacional:

- **NIS 2 Directive (2022)**: seguridad de redes y sistemas de información críticos (entra en vigor en 2024).
- **ISO/IEC 27001**: norma internacional de SGSI (Sistemas de Gestión de Seguridad de la Información).
- **ENISA**: Agencia de la Unión Europea para la Ciberseguridad.
- **Convenio de Budapest sobre cibercriminalidad**.

f) Ley PIC (Protección de infraestructuras críticas)

Ley 8/2011, de protección de infraestructuras críticas (PIC), con su reglamento RD 704/2011.

Tiene como objetivo **proteger los servicios esenciales** cuya interrupción tendría un fuerte impacto en la sociedad, economía o seguridad nacional.

Sectores cubiertos:

- Energía, transporte, agua, salud, administración digital, financiero, etc.

Componentes principales:

- Elaboración del **Catálogo Nacional de Infraestructuras Críticas**.
- Asignación de un **Responsable de Seguridad y Enlace (RSE)**.
- Diseño de **Planes de Seguridad del Operador (PSO)**.
- Coordinación con **CNPIC** (Centro Nacional para la Protección de las Infraestructuras Críticas).