

Sistemas de Almacenamiento

CE1.1 – Nomenclatura y codificación de archivos

1 – ¿Qué es la nomenclatura en los sistemas de archivos?

- En los sistemas operativos, la nomenclatura se refiere a las reglas que definen cómo se nombran archivos y carpetas. Estas reglas incluyen el uso de caracteres válidos, longitud del nombre y formato. Un buen sistema de nomenclatura ayuda a mantener el orden y facilita la búsqueda y clasificación de la información.

2 – Importancia de la codificación

- La codificación estandarizada de nombres y extensiones permite que los programas reconozcan rápidamente el tipo de archivo. Por ejemplo, un archivo .txt indica texto plano, mientras que .jpg señala una imagen. Esta codificación también afecta a cómo se gestionan las copias, migraciones y permisos.

3 – Jerarquías y organización de almacenamiento

- Los archivos se organizan en estructuras jerárquicas: directorios, subdirectorios y volúmenes. Un sistema bien estructurado mejora la eficiencia del almacenamiento y reduce los errores en entornos multiusuario. La nomenclatura coherente refuerza esta estructura.

CE1.2 – Nomenclatura estandarizada de máquinas y servicios

4 – ¿Qué es la nomenclatura estandarizada?

- En redes y sistemas, se utiliza una nomenclatura estandarizada para identificar claramente cada equipo, servicio o aplicación. Por ejemplo, un servidor de correo puede llamarse srv-mail-01, indicando que es el primero en su clase. Este tipo de nombre facilita la administración, el soporte técnico y la documentación.

CE1.2 – Nomenclatura estandarizada de máquinas y servicios

5 – Beneficios en entornos profesionales

- **Aplicar una nomenclatura estandarizada permite una rápida localización y diagnóstico de incidencias, facilita la automatización de tareas y garantiza consistencia en entornos distribuidos. Además, permite mantener una trazabilidad clara en entornos grandes.**

CE1.2 – Nomenclatura estandarizada de máquinas y servicios

6 – Ejemplos prácticos

- **Ejemplos válidos:**

- srv-db-01: primer servidor de base de datos.
- cli-ventas-23: cliente número 23 del departamento de ventas.
- Nombres como “ordenador nuevo” o “pepe-portátil” deben evitarse, ya que dificultan el control técnico y la escalabilidad del sistema.

CE1.3 – Políticas de migración y archivado

7 – ¿Qué es una política de migración de archivos?

- Una política de migración de datos es una estrategia que define cuándo y cómo mover archivos desde un almacenamiento activo a otro más económico o con diferentes características. Se suele aplicar a archivos antiguos, poco consultados / usados o duplicados.



DATA MIGRATION

8 – Archivado: eficiencia y recuperación

- El archivado permite mantener una copia de los datos que no se usan frecuentemente pero que deben conservarse por razones legales, históricas o operativas. Esto mejora el rendimiento del sistema, libera espacio y asegura disponibilidad futura.

9 – Aplicación práctica

- En un servidor de archivos, los documentos de más de 3 años sin modificar pueden migrarse automáticamente a una unidad de almacenamiento más lenta pero más económica. Este proceso puede realizarse de forma manual o mediante herramientas automáticas.

CE1.4 – Redes y servidores DNS

- **10 – Mapas de red y direccionamiento IP**
- **Un mapa de direcciones IP representa la distribución de dispositivos en una red TCP/IP. Permite identificar qué IP está asignada a cada máquina o servicio, y garantiza un direccionamiento coherente y seguro.**

11 – ¿Qué es un servidor DNS?

- El servidor DNS (Domain Name System) traduce nombres de dominio legibles (servidor.empresa.local) en direcciones IP numéricas (192.168.1.10). Esto facilita el acceso a servicios sin necesidad de memorizar direcciones IP.

12 – Implantación básica de un servidor DNS

- Para implantar un servidor DNS se define una zona de dominio, se asignan registros (A, CNAME, MX, etc.) y se integra con el mapa IP. Es fundamental en redes empresariales con múltiples servicios y equipos conectados.

13 – Estructura de los sistemas de archivos

- Los sistemas de archivos contienen metadatos como: fecha de creación, última modificación, usuario propietario, permisos de acceso y jerarquía. Estos datos permiten auditar el uso del sistema y aplicar políticas de seguridad.

14 – Usuarios autorizados y control de acceso

- Cada archivo o carpeta puede tener usuarios autorizados para leer, escribir o ejecutar el contenido. Los sistemas permiten definir reglas de acceso por usuario o grupo, lo cual es vital para entornos multiusuario o con datos sensibles.

15 – Políticas de migración aplicadas a estructuras reales

- Cuando una carpeta contiene archivos muy antiguos o que han sido modificados por última vez hace años, puede aplicarse una política de migración o archivado, siempre identificando fechas y permisos para no afectar el funcionamiento de otros usuarios o servicios.

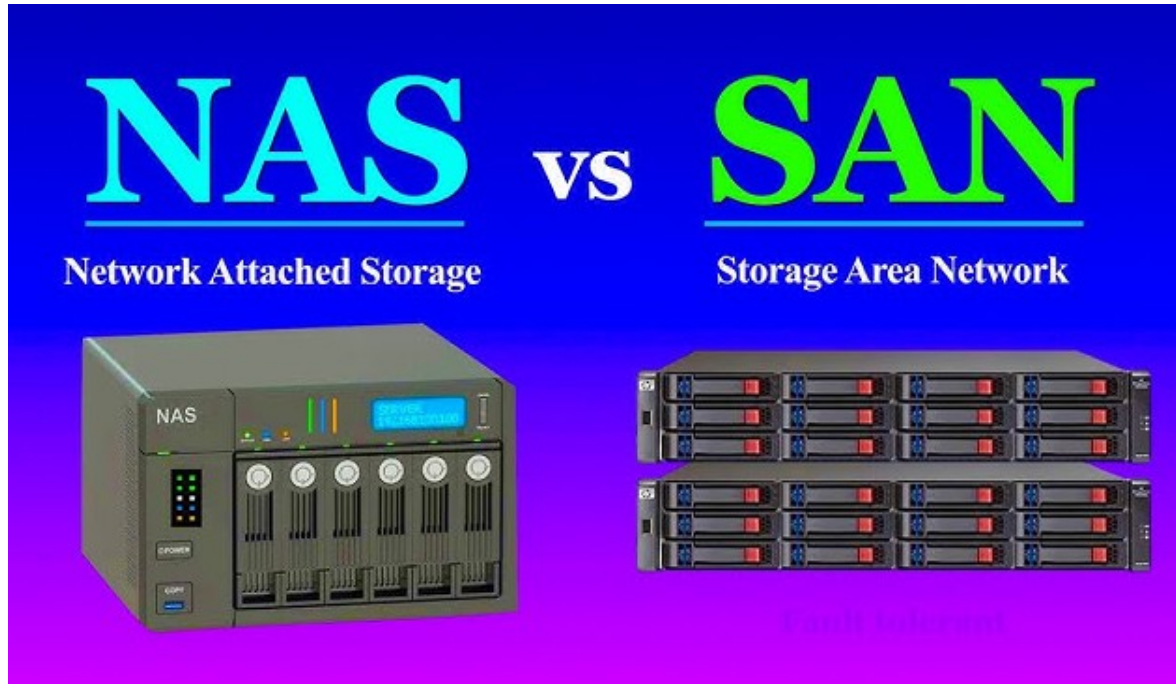
16 – Clasificación de sistemas de almacenamiento

- Los sistemas de almacenamiento se clasifican según su capacidad, rendimiento y tipo de conexión. Existen soluciones internas (HDD, SSD) y externas (NAS, SAN, cintas, USB). En entornos empresariales, se priorizan aquellos que permiten compartir datos en red, como NAS.

CE2.1 – Tipos de almacenamiento

17 – NAS y su función

- Un NAS (Network Attached Storage) es un dispositivo que se conecta a la red y permite acceder, compartir y gestionar archivos desde distintos equipos. Es ideal para entornos colaborativos y copias centralizadas. Se configura con permisos por usuario y carpetas compartidas.
- Por tanto, permite almacenar archivos en red.



CE2.1 – Tipos de almacenamiento

18 – Ventajas del almacenamiento conectado a red

- Centralización de archivos
- Acceso desde distintos dispositivos
- Permisos controlados por usuario
- Copias de seguridad automatizadas
- Esto convierte al NAS en una solución asequible y eficiente para pequeñas y medianas empresas.


CE2.2 – Protección de datos con RAID

19 – ¿Qué es RAID?

- RAID (Redundant Array of Independent Disks, Conjunto Redundante de Discos Independientes) es una tecnología que combina varios discos duros para mejorar rendimiento, tolerancia a fallos o ambos. Existen varios niveles, como RAID 0, RAID 1, RAID 5 y RAID 6.



20 – Niveles RAID comunes

- RAID 0: mejora el rendimiento pero no ofrece redundancia
-  RAID 1: copia idéntica en dos discos (espejo)
- RAID 5: distribuye paridad para tolerancia a fallos con mejor uso de espacio
- RAID 6: similar a RAID 5 pero tolera la caída de 2 discos

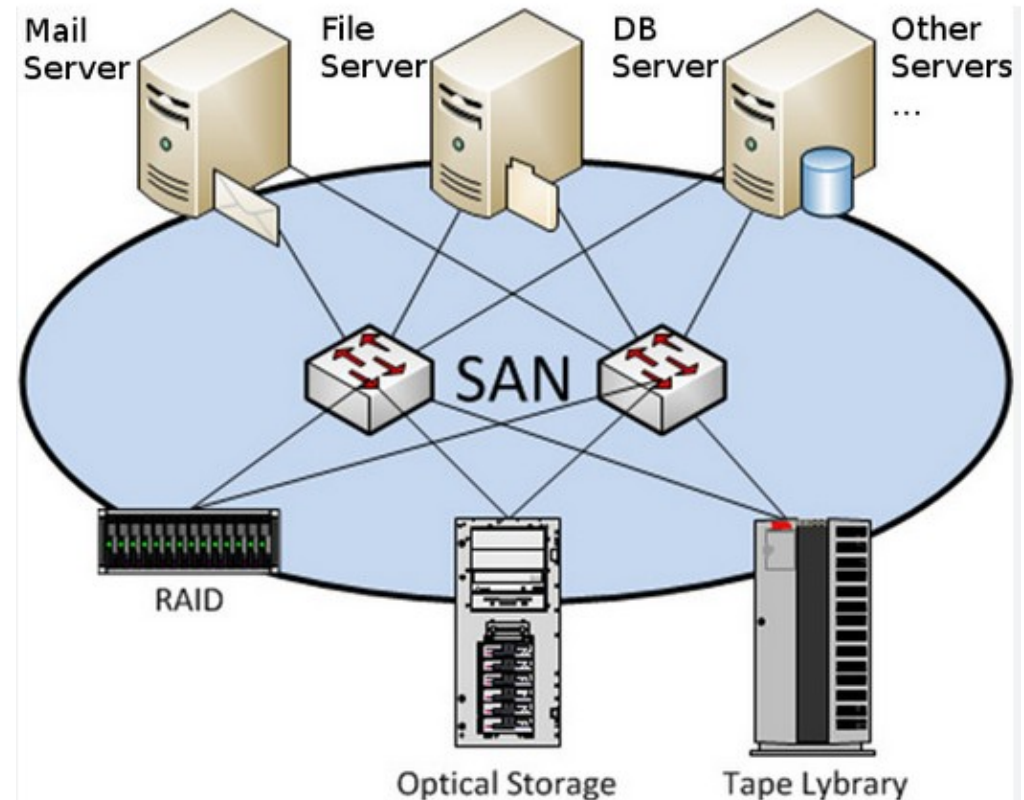
21 – Controladoras RAID: hardware vs software

- Las soluciones RAID pueden ser por software (configuradas por el sistema operativo) o por hardware (mediante controladoras dedicadas). Las controladoras hardware ofrecen mayor rendimiento y son independientes del sistema operativo.

CE2.3 – Estructura física y SAN

22 – ¿Qué es una SAN?

- Una SAN (Storage Area Network, área de almacenamiento en red) es una red de alta velocidad dedicada al almacenamiento. Es decir, red especializada para conectar servidores dedicados al almacenamiento. A diferencia de NAS, no usa protocolos de archivos compartidos sino de bloques, lo que permite mayor rendimiento.



23 – Tipos de SAN

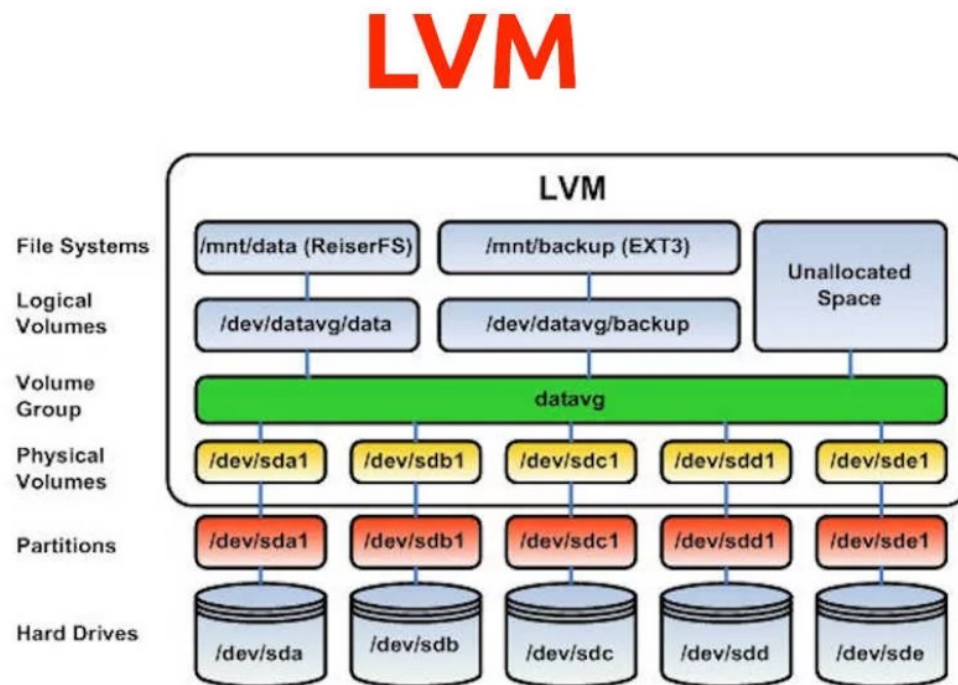
- **iSCSI:** usa la red IP, económica y común
- **Fibre Channel (FC):** alto rendimiento, más costosa
- **FCoE:** combina Fibre Channel sobre redes Ethernet

24 – MBR y particiones

- El MBR (Master Boot Record) es la tabla que indica cómo se divide un disco en particiones. Es esencial para que el sistema pueda identificar los volúmenes. Aunque ha sido reemplazado por GPT en sistemas modernos, sigue siendo muy utilizado.

25 – ¿Qué es LVM?

- LVM (Logical Volume Manager) permite gestionar discos o volúmenes lógicos de forma flexible, agrupándolos y creando volúmenes que se pueden redimensionar o mover sin afectar a los datos. Es muy útil en servidores Linux.



Logical Volume Manager

26 – Ventajas de LVM

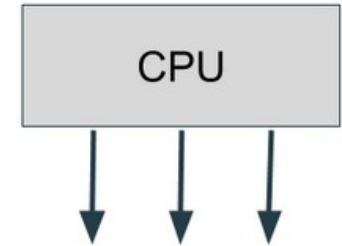
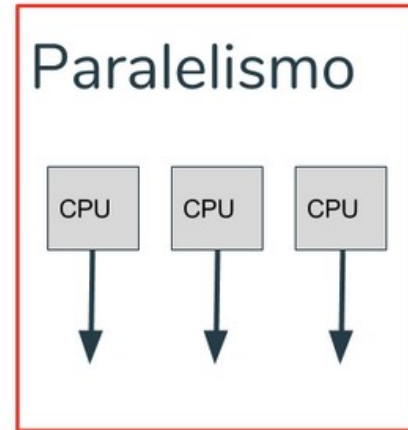
- Redimensionar volúmenes “en caliente”
- Añadir nuevos discos fácilmente
- Crear instantáneas (snapshots)
- Mejor administración en entornos complejos

27 – Aplicación práctica

- Con LVM, un administrador puede ampliar una partición /datos al añadir un nuevo disco, sin necesidad de formatear ni interrumpir el servicio. Esta capacidad hace que LVM sea ideal en entornos de producción.

28 – ¿Qué es el acceso en paralelo?

- El acceso en paralelo a volúmenes físicos permite que múltiples procesos lean o escriban datos simultáneamente desde diferentes unidades, mejorando el rendimiento general del sistema y reduciendo cuellos de botella.



CE2.5 – Acceso en paralelo a volúmenes

29 – Casos de uso

- Servidores con muchas peticiones simultáneas
- Bases de datos de alto tráfico
- Equipos con múltiples discos trabajando como un solo volumen lógico

30 – Medición del impacto

- Las herramientas de monitorización del sistema operativo (como iostat, top, vmstat) permiten observar cómo se reparten las lecturas/escrituras. El balanceo entre discos mejora la velocidad de respuesta del sistema.

CE2.6 – Cintas y cartuchos

31 – Almacenamiento en cinta

- Las cintas magnéticas se siguen usando para copias de seguridad a largo plazo por su bajo coste por GB, alta capacidad y duración. No están pensadas para acceso frecuente, sino para archivo. Los HDD suelen dar problemas a largo plazo con sus partes mecánicas (en menor medida por su componente magnético) y los SSD tienen como principal inconveniente su caducidad para reescrituras y su enorme coste por GB.



32 – Tipos de cintas

- **Ejemplos comunes:**
 - LTO (Linear Tape-Open)
 - DAT (Digital Audio Tape)
 - T10000, SDLT
- **Se clasifican por tipo de soporte, gestión (manual o automática), y compatibilidad.**

33 – Aplicaciones y ventajas

- Almacenamiento offline seguro
- Protección contra ransomware (desconexión física)
- Bajo coste a gran escala
- Por ello, siguen siendo clave en políticas de respaldo institucionales.

34 – Volúmenes espejados y tolerancia a fallos

- El espejado de volúmenes consiste en mantener dos copias exactas en tiempo real. Si un disco falla, el sistema sigue funcionando con la réplica, mejorando la disponibilidad del servicio.

CE2.7 – Técnicas avanzadas: espejado, balanceo, análisis

35 – Balanceo de accesos y rendimiento

- El balanceo de accesos distribuye la carga de trabajo entre varios volúmenes físicos, permitiendo mayor rendimiento y evitando saturaciones. Este enfoque es común en almacenamiento en red con múltiples discos.

36 – Monitorización y análisis

- Herramientas como Nagios, Zabbix, Grafana o iostat permiten visualizar el estado del almacenamiento, detectar cuellos de botella, prever fallos y ajustar políticas de migración y replicación.

CE3.1 – Políticas de seguridad y recuperación del servicio

37 – Políticas de seguridad y continuidad

- Las políticas de seguridad definen las normas para proteger la información y garantizar la continuidad del servicio. Incluyen medidas para prevenir pérdidas, accesos no autorizados, y asegurar que, en caso de fallo, los sistemas puedan recuperarse en un tiempo razonable.

CE3.1 – Políticas de seguridad y recuperación del servicio

38 – Plan de continuidad de negocio: RTO y RPO

- **RTO (Recovery Time Objective):** Tiempo máximo aceptable de inactividad.
- **RPO (Recovery Point Objective):** Cantidad máxima de datos que pueden perderse (en minutos u horas).
- Un plan adecuado define qué sistemas son críticos, cómo recuperarlos y qué copias usar.

CE3.1 – Políticas de seguridad y recuperación del servicio

39 – Alta disponibilidad y recuperación

- **Sistemas con alta disponibilidad (clústeres, balanceadores, etc.) reducen el impacto de fallos y garantizan un tiempo de inactividad mínimo. La integración con copias de seguridad y tolerancia a fallos permite una rápida recuperación.**

CE3.2 – Tipos de copias de seguridad y salvaguarda

40 – Tipos de copias: completas, incrementales y diferenciales

- **Completa:** Copia todo, ocupa más espacio
- **Incremental:** Copia solo los cambios desde la última copia (menos espacio, más rápida)
- **Diferencial:** Copia los cambios desde la última copia completa

Cada una se usa según el plan de respaldo y el RPO/RTO deseado.

CE3.2 – Tipos de copias de seguridad y salvaguarda

41 – Salvaguarda física y lógica

- Física: Dispositivos externos (cintas, discos, NAS)
- Lógica: Software de respaldo, snapshots, imágenes del sistema
- También pueden clasificarse por nivel: bloque (más eficiente) o fichero (más simple).

CE3.2 – Tipos de copias de seguridad y salvaguarda

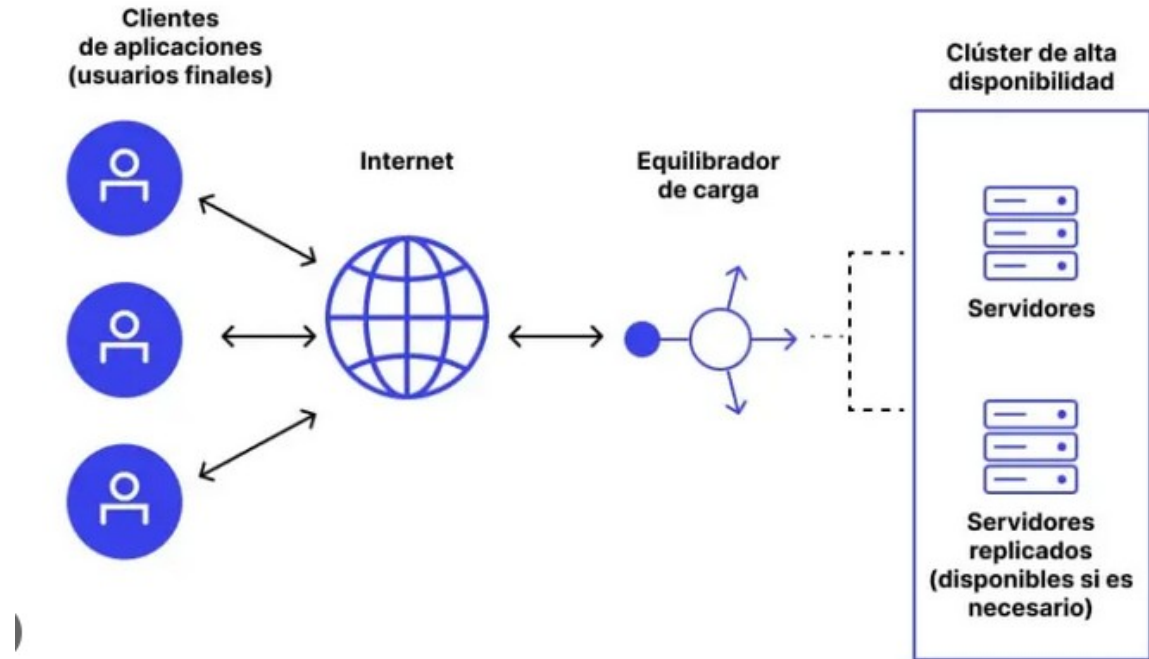
42 – Calendarización de copias

- Las copias pueden programarse en intervalos regulares: diaria, semanal o mensual. También pueden activarse ante eventos. Automatizar esta tarea garantiza la protección de los datos y reduce errores humanos.

CE3.3 – Alta disponibilidad y arquitecturas tolerantes a fallos

43 – Concepto de alta disponibilidad

- Un sistema con alta disponibilidad está diseñado para funcionar de forma continua, incluso ante fallos. Esto se consigue con redundancia, monitoreo y sistemas tolerantes a errores. Reduce de manera efectiva el tiempo de inactividad en caso de fallos de cualquier tipo.



CE3.3 – Alta disponibilidad y arquitecturas tolerantes a fallos

44 – Cluster, grid y balanceo de carga

- **Clúster:** varios equipos que actúan como uno, conmutación ante fallo
- **Grid:** recursos distribuidos conectados por red
- **Balanceo de carga:** distribuye peticiones entre varios servidores para mejorar rendimiento

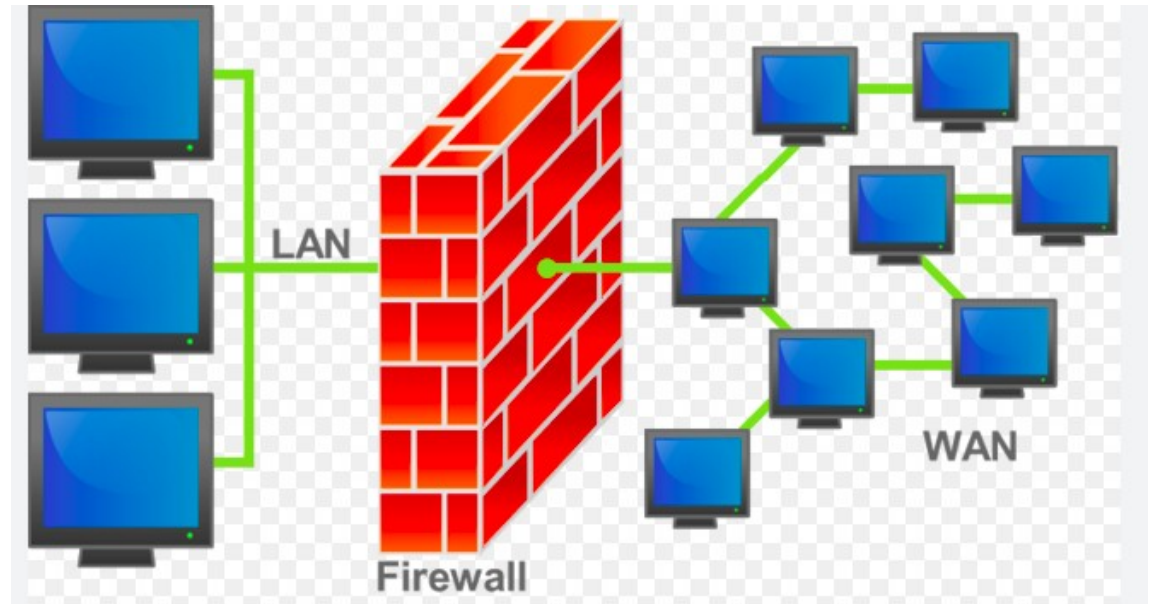
CE3.3 – Alta disponibilidad y arquitecturas tolerantes a fallos

45 – Ejemplos prácticos

- Una web crítica puede estar distribuida en varios servidores balanceados y sincronizados por clúster. Si uno cae, los otros continúan. Esto mejora la resiliencia y el tiempo de actividad.

46 – Cortafuegos (firewall)

- Un cortafuegos filtra el tráfico de red según reglas definidas. Puede bloquear accesos no autorizados, limitar puertos abiertos y registrar intentos sospechosos. Puede ser software (Windows Firewall, ufw en Linux) o hardware (appliance dedicado).



47 – Antivirus y proxys

- **Antivirus:** detecta, bloquea o elimina software malicioso
- **Proxy:** intermedia entre un cliente y el servidor, permitiendo control, filtrado y cacheo de contenidos
- Su correcta configuración es clave en la protección de redes y usuarios.

48 – Integración en la arquitectura de red

Un sistema seguro incluye:

- Firewall perimetral
- Antivirus actualizado
- Proxy para navegación segura
- Segmentación de red interna
- Registro de eventos para auditoría

Esto forma una defensa en profundidad frente a amenazas.

49 – Accesos restringidos por usuario

Los sistemas deben garantizar que cada usuario acceda solo a la información que necesita. Esto se gestiona mediante permisos, grupos, políticas y listas de control de acceso (ACL). Cada recurso puede tener propietario y reglas específicas.

50 – Identificador único y SSO

Un identificador único de usuario permite rastrear y auditar acciones. El sistema SSO (Single Sign-On) permite que un usuario acceda a múltiples servicios con una única autenticación, reduciendo errores y mejorando la experiencia sin sacrificar seguridad.












51 – Auditorías de seguridad

Las auditorías de seguridad revisan accesos, cambios, errores y fallos del sistema. Estas pueden ser automáticas (mediante registros y alertas) o periódicas (revisiones manuales). Son esenciales para cumplir normativas como la LOPD o el RGPD.

Diferencias NAS / SAN

- Archivos / Bloques
- Archivos Generales / Datos críticos
- LAN / SAN
- Sencillo / Complejo
- Coste bajo / Coste alto

Característica	NAS (Network Attached Storage)	SAN (Storage Area Network)
 Tipo de acceso	Basado en archivos	Basado en bloques
 Protocolo típico	SMB/CIFS (Windows), NFS (Linux)	iSCSI, Fibre Channel, FCoE
 Uso habitual	Compartir archivos en red (documentos, multimedia, backups)	Aplicaciones críticas (bases de datos, virtualización, servidores)
 Accesible como...	Unidad de red o carpeta compartida	Disco duro local (bloque sin sistema de archivos)
 Tipo de red	Red LAN estándar (Ethernet)	Red dedicada (SAN fabric) o Ethernet especializado (iSCSI)
 Gestión de archivos	El propio NAS gestiona el sistema de archivos	El servidor gestiona el sistema de archivos
 Complejidad	Baja (plug & play)	Alta (requiere configuración avanzada y red dedicada)
 Coste	Menor	Mayor (por hardware y red dedicada)
 Ejemplo de uso	Compartir carpetas en una oficina	Almacenar discos virtuales de máquinas VMware o bases de datos