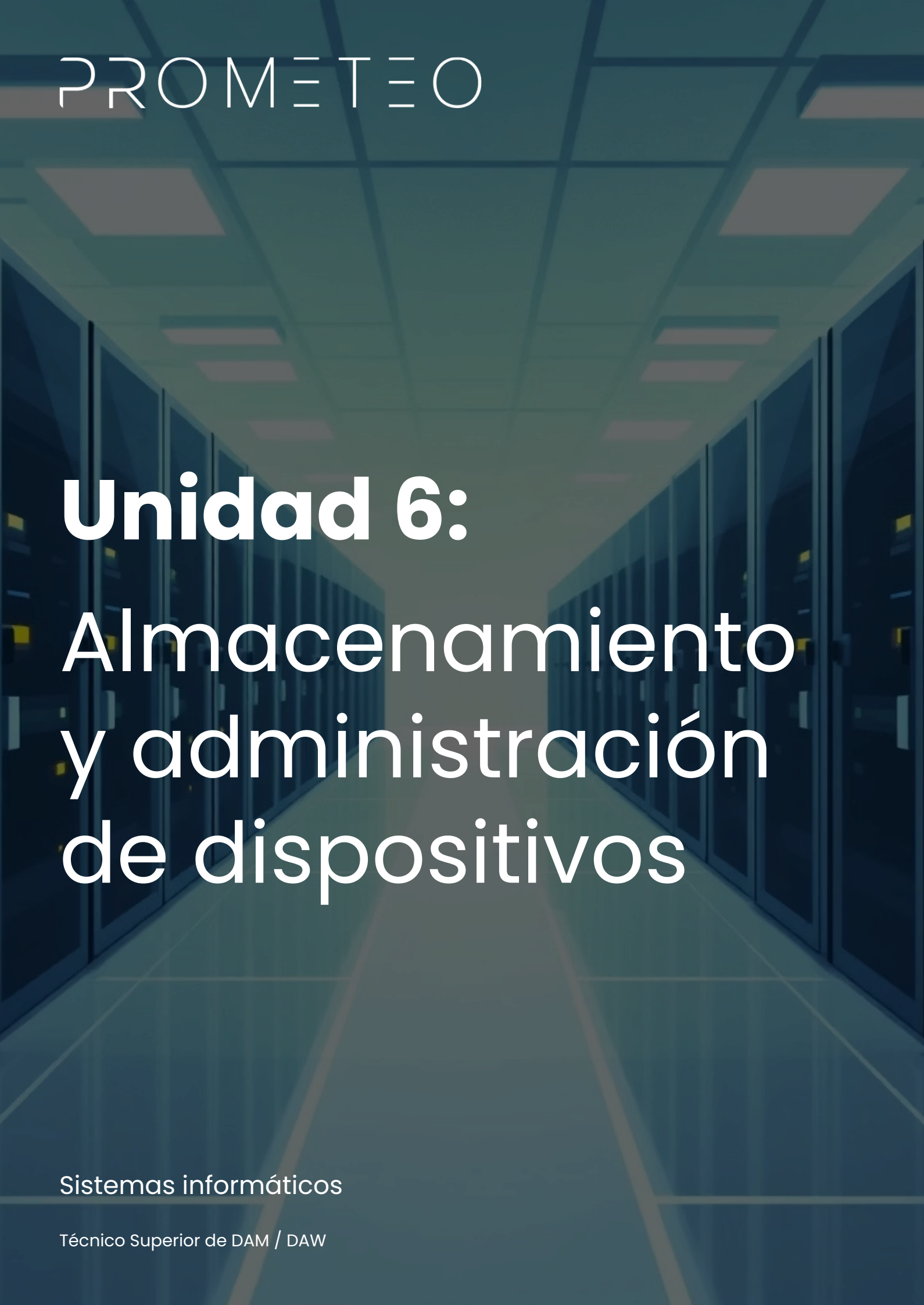
PROMETEO



Unidad 6:

Almacenamiento y administración de dispositivos

Sistemas informáticos

Técnico Superior de DAM / DAW

Sesión 20 – RAID: niveles 0,1,5,10 y uso en servidores

Qué es RAID y por qué es tan importante en servidores

RAID (Redundant Array of Independent Disks) es una forma de combinar varios discos físicos para que se comporten como una única unidad lógica. El objetivo principal es uno de estos tres (o una mezcla): más rendimiento, más seguridad de los datos (redundancia) o un equilibrio entre ambas cosas.

En un servidor, un único disco duro es un punto débil clarísimo: si falla, el servicio se cae y puedes perder todos los datos almacenados. RAID nace justo para evitar eso o, al menos, reducir drásticamente el impacto de un fallo de disco.

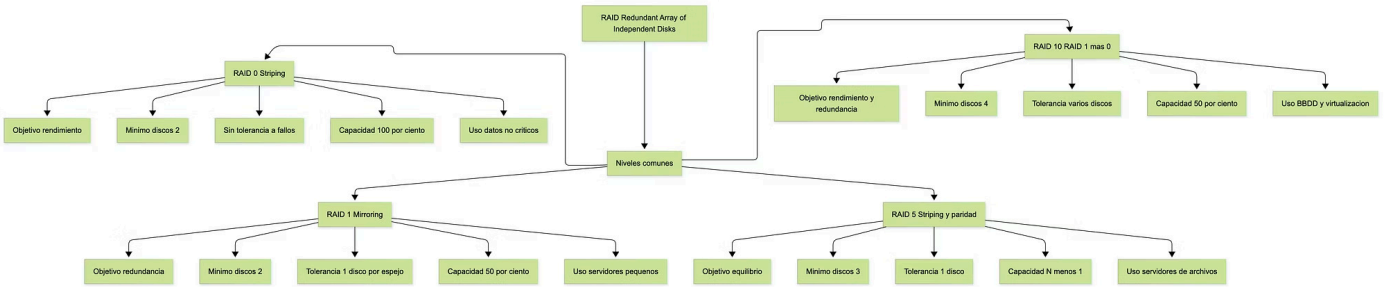
En la práctica, funciona distribuyendo los datos entre los discos de distintas formas:

- **Striping (distribución por bloques):** reparte los datos en "tiras" entre varios discos, lo que aumenta mucho la velocidad de lectura y escritura, porque varios discos trabajan en paralelo.
- **Mirroring (espejo):** copia exacta de la información en dos o más discos; si uno cae, el otro tiene la misma información.
- **Paridad:** se calculan datos adicionales (paridad) que permiten reconstruir la información si un disco falla.

En esta sesión te centras en los niveles más usados en servidores y NAS: RAID 0, RAID 1, RAID 5 y RAID 10.

Esquema Visual: comparativa detallada de RAID 0, 1, 5 y 10

A continuación tienes un diagrama en Mermaid que resume de forma visual los niveles de RAID trabajados, su objetivo principal, capacidad útil, tolerancia a fallos y uso típico en servidores.



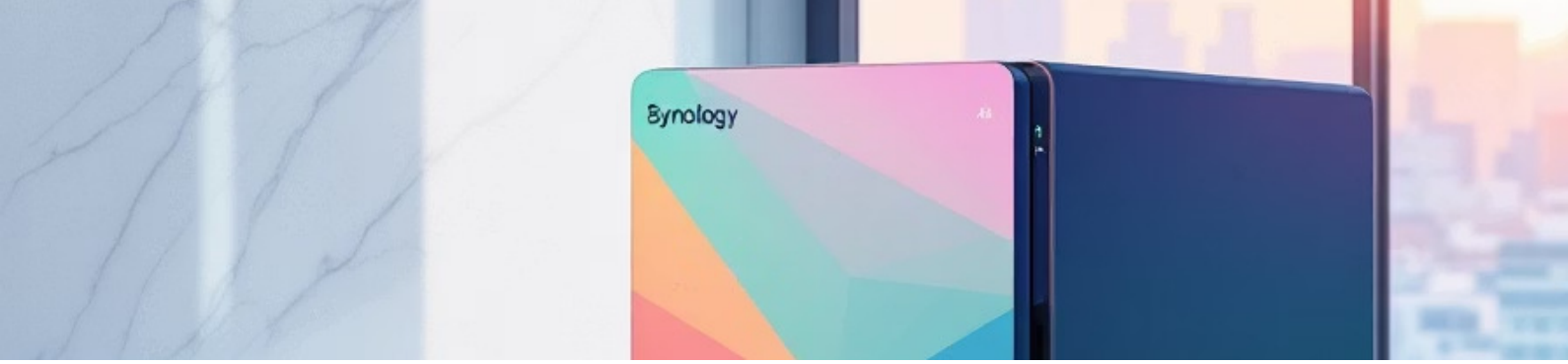
Cómo leer el esquema:

- El nodo **A (RAID)** es el concepto general.
- Desde **B** se despliegan los cuatro niveles que debes dominar: RAID 0, 1, 5 y 10.
- Cada nivel se descompone en cinco nodos:
  - **Objetivo principal**: rendimiento, redundancia, equilibrio o combinación.
  - **Mínimo de discos** necesarios para montar el array.
  - **Tolerancia a fallos**: cuántos discos pueden fallar sin perder datos.
  - **Capacidad útil**: qué porcentaje de la suma total de discos realmente puedes usar para datos.

Uso típico en servidores: en qué tipo de carga o entorno tiene más sentido.

Cómo decidir rápidamente:

- Solo rendimiento y datos no críticos → RAID 0
- Pocos discos y prioridad absoluta a la sencillez de la redundancia → RAID 1
- NAS de pyme que busca equilibrio entre coste y protección → RAID 5
- Servidor de base de datos o virtualización muy crítico → probablemente RAID 10



Caso de Estudio: Synology en una pyme con NAS en RAID 5

Contexto

Imagina una pequeña agencia de diseño en Barcelona con 20 empleados. Durante años han trabajado guardando los proyectos en discos USB individuales y en los propios PCs de los diseñadores. El resultado:

- Archivos duplicados por todas partes
- Pérdida de trabajos cuando fallaba un disco externo
- Dificultad para colaborar porque cada uno tenía una versión distinta

El gerente decide invertir en un NAS de Synology con 4 bahías para centralizar los archivos y proteger el trabajo del equipo. Sin embargo, nadie en la empresa es administrador de sistemas: necesitan algo potente, pero sencillo de gestionar.

Estrategia: implantación de RAID con Synology DSM

Elección del hardware

- NAS Synology de 4 bahías
- 4 discos duros de 4 TB diseñados para NAS

Diseño del RAID

- Objetivo principal: equilibrio entre capacidad, rendimiento y redundancia
- Opción elegida: RAID 5 (o SHR, la variante híbrida de Synology basada en los mismos principios)
- Capacidad resultante aproximada: 4 discos × 4 TB = 16 TB brutos. Capacidad útil en RAID 5 ≈ 3 discos (N-1) → unos 12 TB utilizables

Configuración en DSM

- Desde el asistente gráfico, el administrador selecciona los discos y el tipo de RAID
- DSM se encarga de: crear automáticamente el volumen en RAID 5, formatear con el sistema de archivos adecuado, activar la monitorización S.M.A.R.T. de los discos
- Se configuran carpetas compartidas para cada equipo con permisos diferenciados

Resultado: impacto medible

- **Disponibilidad:** un año después, uno de los discos falla. El NAS envía un aviso por email. El sistema sigue funcionando en estado degradado. Se sustituye el disco defectuoso y el RAID se reconstruye sin pérdida de datos
- **Seguridad:** Zero pérdidas de proyectos por fallo de disco en todo el año
- **Productividad:** Los tiempos de apertura de proyectos pesados mejoran gracias al paralelismo de discos

Herramientas y Consejos para trabajar con RAID en servidores

Elige bien entre RAID por hardware y RAID por software

RAID por hardware: Usa una controladora dedicada (por ejemplo, tarjetas Dell PERC, HPE Smart Array). Ventajas: mejor rendimiento, descarga trabajo de la CPU. Ideal para servidores físicos en producción.

RAID por software: Se gestiona desde el sistema operativo (Linux: mdadm, LVM; Windows Server: Storage Spaces; NAS: DSM en Synology). Ventajas: más barato, muy flexible.

RAID no es un backup: diseña siempre una estrategia de copias

RAID solo te protege del fallo físico de uno (o varios) discos, nada más. No te protege de: borrados accidentales, ransomware que cifra tus archivos, incendios, inundaciones o robos del servidor/NAS.

Combina RAID con copias locales en otro dispositivo y copias externas (en la nube o en otra ubicación física).

Monitoriza el estado de los discos y del array RAID

Activa alertas de: sectores reasignados o errores S.M.A.R.T., estado "degradado" del volumen.

Herramientas útiles: En NAS: panel de DSM (Synology) o QTS (QNAP). En servidores: Linux: smartctl, mdadm --detail; Windows: herramientas del fabricante de la controladora.

Objetivo: no enterarte del problema cuando ya es tarde, sino cuando todavía puedes actuar con calma.

Planifica la escalabilidad desde el principio

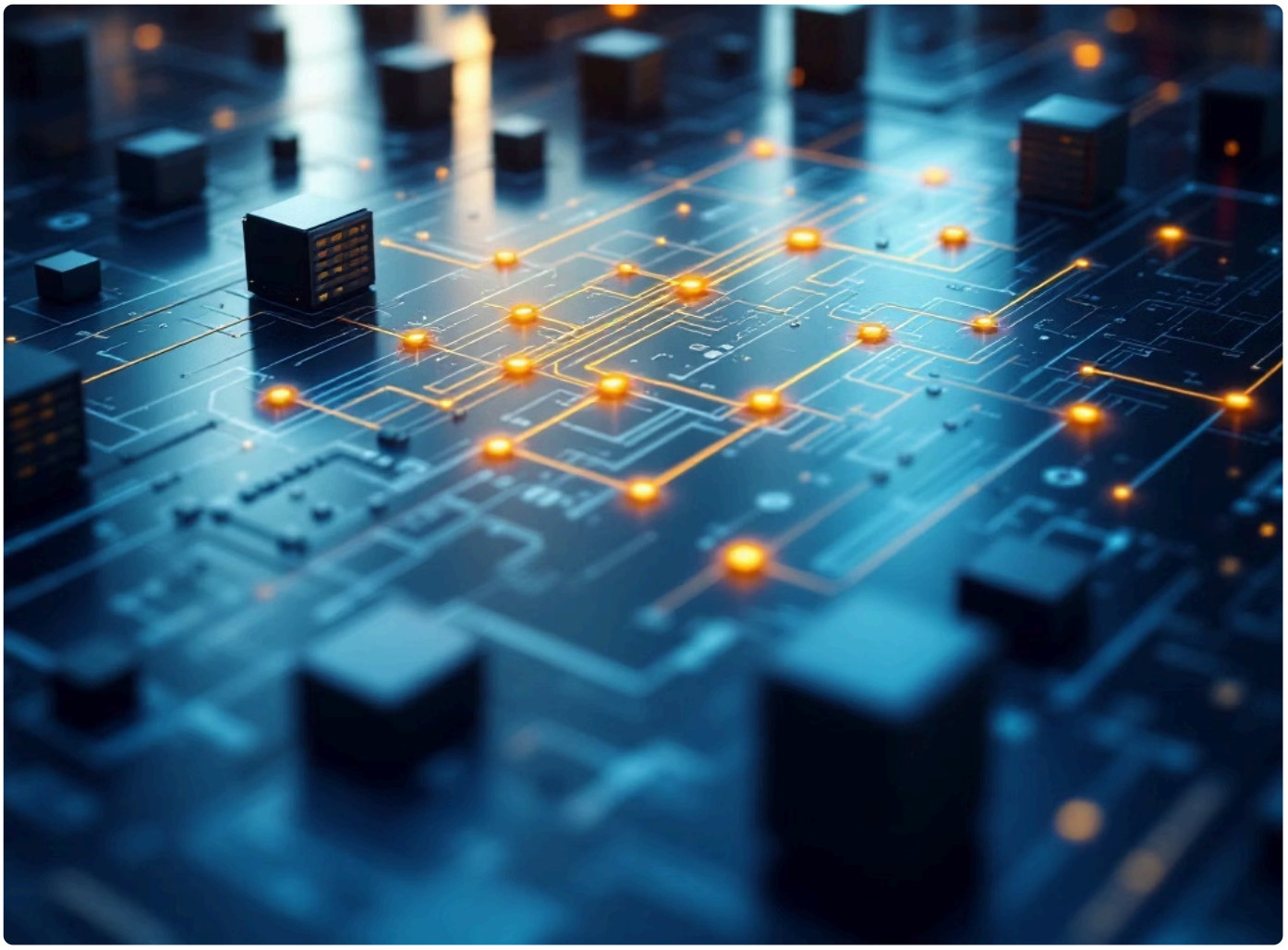
Piensa cuántos discos podrás añadir en el futuro. Ejemplo: Si montas un servidor con solo 2 bahías y RAID 1, para crecer tendrás que sustituir discos por otros más grandes. Con 4 bahías, podrías pasar de un RAID 1 a un RAID 5 o RAID 10 sin cambiar de chasis.

En entornos reales, la necesidad de espacio casi siempre crece más rápido de lo que se pensaba.

Documenta tu configuración

Deja por escrito: tipo de RAID, número y modelo de discos, procedimiento de sustitución y reconstrucción.

Esto te ahorra muchos sustos cuando haya que intervenir deprisa (por ejemplo, si un técnico de guardia tiene que cambiar un disco a las 3 de la mañana).



Mitos y Realidades sobre RAID en servidores

❌ Mito: "Con RAID 1, si un disco falla, puedo seguir trabajando sin problemas."

→ **FALSO.** Aunque es verdad que el sistema puede seguir funcionando si se rompe uno de los discos, entras en lo que se llama un estado degradado. En ese momento: Ya no tienes redundancia: si falla el segundo disco antes de reconstruir el array, pierdes todos los datos. El rendimiento puede empeorar durante la reconstrucción.

La realidad profesional es que, en cuanto un disco de un RAID 1 (o de cualquier RAID) falla, tu prioridad debe ser reemplazarlo y reconstruir el array cuanto antes. Seguir trabajando "como si nada" es jugar con fuego.

❌ Mito: "RAID 5 es la mejor opción para todo."

→ **FALSO.** RAID 5 fue durante años el estándar en muchos servidores y NAS por su buen equilibrio entre capacidad, rendimiento y redundancia. Pero con los discos actuales de gran tamaño, tiene limitaciones importantes: Los tiempos de reconstrucción tras un fallo pueden ser de muchas horas o incluso días.

Por ese motivo, en muchos entornos profesionales se prefiere hoy: RAID 6 (tolerancia a fallo de 2 discos) para grandes volúmenes. RAID 10 para cargas de alta E/S (bases de datos, virtualización).

La realidad es que no existe un "RAID perfecto" para todo. Debes valorar tamaño de discos, tipo de carga, presupuesto y criticidad de los datos antes de elegir.

Resumen final

- RAID combina varios discos físicos en una unidad lógica para mejorar rendimiento, redundancia o ambas cosas
- RAID 0 = solo rendimiento, sin protección; RAID 1 = espejo con alta redundancia, mitad de capacidad útil
- RAID 5 ofrece equilibrio (N-1 discos útiles, tolera 1 fallo); RAID 10 combina striping + mirroring para máximo rendimiento y seguridad a costa de capacidad
- RAID no es un backup: necesitas igualmente una estrategia de copias de seguridad externa y probada

Sesión 21 – Backups locales y en la nube (rsync, Veeam, snapshot, OneDrive/Google Drive)

Por qué una buena estrategia de backup te salva la vida profesional

Tarde o temprano algo va a fallar: un disco duro muere, alguien borra una carpeta "sin querer", un ransomware cifra el servidor o simplemente se rompe el portátil justo antes de una entrega importante. La pregunta no es si pasará, sino cuándo. Y ahí es donde entra tu estrategia de backup.

Un backup es una o varias copias de tus datos que se guardan en otro lugar distinto al original, con el objetivo de poder restaurarlos cuando algo sale mal. La idea parece simple, pero en el mundo profesional hay muchos matices:

Backups locales:

Se guardan en un dispositivo físico que tú controlas: un disco duro externo, otro servidor, un NAS, etc.

- **Ventajas:** muy rápidos para hacer copias y restaurar; no dependen de tu conexión a Internet
- **Inconvenientes:** si tienes un incendio, robo o inundación, es posible que el backup local también desaparezca

Backups en la nube:

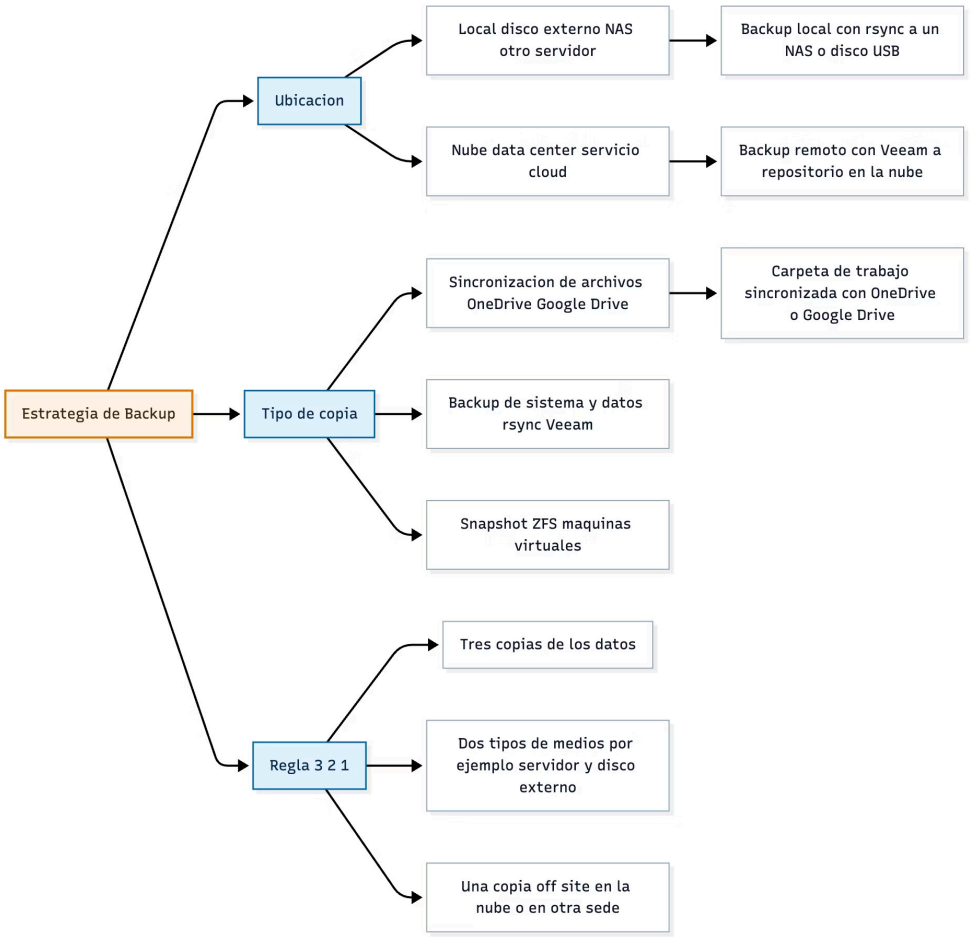
Se almacenan en servidores remotos (data centers) de un proveedor externo.

Ejemplos de uso: Sincronización y trabajo diario: OneDrive, Google Drive, Dropbox. Backups de sistemas completos y servidores: herramientas como Veeam, Acronis, etc.

- **Ventajas:** ideales para tener una copia off-site (fuera de tu ubicación física)
- **Inconvenientes:** dependen de tu conexión a Internet, y el coste crece con el volumen de datos

Una idea esencial que debes grabarte es la **regla 3-2-1:** Tener al menos 3 copias de los datos, en 2 tipos de soportes diferentes, con 1 copia fuera de la ubicación principal (off-site).

Esquema Visual: mapa completo de tu estrategia de backup



Cómo interpretar el esquema:

- Desde **Estrategia de Backup (A)** salen tres ejes:
  a. **Ubicación**:
     - **Local (C)**: discos externos, NAS, otros servidores en la misma oficina.
     - **Nube (D)**: copias alojadas en un data center remoto.
  b. **Tipo de copia**:
     - **Sincronización (F)**: para trabajo diario y colaboración (ej. Google Drive), pero cuidado, porque *no es* un backup real.
     - **Backup de sistema y datos (G)**: copias pensadas para restaurar máquinas enteras, carpetas críticas o bases de datos (rsync, Veeam).
     - **Snapshots (H)**: puntos de restauración rápida, ideales antes de una actualización o cambio de configuración delicado.
  c. **Regla 3-2-1 (I)**: te obliga a pensar en redundancia, diversidad de soportes y ubicación off-site.
     Debes ser capaz de coger este esquema y adaptarlo a cualquier entorno: desde tu propio portátil hasta un pequeño servidor de una pyme.

Caso de Estudio: una asesoría que se salva gracias a Veeam y a la regla 3-2-1

Contexto

Una asesoría fiscal y laboral con 15 empleados gestiona nóminas, impuestos y contabilidad de más de 200 clientes. Toda su información está centralizada en:

- Un servidor de ficheros con la documentación de clientes
- Un servidor de virtualización con varias máquinas virtuales de aplicaciones (software de nóminas, contabilidad, gestión interna)

Durante años, hacían "backups" copiando algunas carpetas críticas a un disco USB que el responsable de IT conectaba de vez en cuando. Nadie comprobaba si esas copias se podían restaurar correctamente.

Problema

Un día, el servidor de virtualización sufre un ataque de ransomware: todas las máquinas virtuales quedan cifradas. Los archivos compartidos del servidor de ficheros también. El negocio está parado. Para colmo: El disco USB de "backup" llevaba semanas sin actualizarse. Además, algunas carpetas cifradas se habían copiado al disco, por lo que el "backup" también estaba contaminado.

Estrategia implantada

Backup local con Veeam

Se instala Veeam Backup & Replication en un servidor dedicado. Se configuran trabajos de backup diarios de todas las máquinas virtuales (entorno VMware/Hyper-V): Copias incrementales durante la semana. Copia completa el fin de semana. El repositorio principal de backup se sitúa en un NAS local con discos en RAID.

Copia off-site en la nube

Veeam replica automáticamente las copias más recientes a un repositorio en la nube del proveedor. Se cumple así la parte de "1 copia off-site" de la regla 3-2-1.

Backups de ficheros con rsync

Además, se configura un servidor Linux que ejecuta rsync cada noche para copiar las carpetas de trabajo a otro almacenamiento local. De este modo, si hay un problema puntual en el NAS de backup, sigue existiendo otra copia adicional de los ficheros más críticos.

Pruebas de restauración periódicas

Una vez al mes, IT restaura una máquina virtual entera en un entorno de pruebas a partir de las copias de Veeam. También se restauran carpetas concretas desde el backup de rsync. Se documenta el tiempo real necesario de recuperación (RTO).

Resultado

Un año después, uno de los discos del servidor de virtualización falla. Aunque no hay ransomware esta vez, varias máquinas quedan inestables. Gracias a la nueva estrategia: Se restauran todas las VMs afectadas desde Veeam en pocas horas. No se pierde información sensible de ningún cliente. El negocio puede retomar la actividad en el mismo día.

Herramientas y Consejos para tu futuro profesional

Aplica siempre la regla 3-2-1 en cualquier entorno

3 copias: datos originales + 2 copias adicionales. 2 tipos de medios: por ejemplo, servidor + NAS, o disco interno + disco USB. 1 copia off-site: en otro edificio, en la nube o en un data center.

Este principio es válido para: Tu propio portátil. Un pequeño servidor de una pyme. Un entorno virtualizado en un centro de datos.

Domina rsync si trabajas con Linux

rsync es una navaja suiza para backups: Copia solo los cambios (incremental). Puede trabajar a través de la red (por ejemplo, mediante SSH). Permite excluir carpetas temporales o ficheros poco relevantes.

Ejemplo típico: Copiar /home/proyectos a un NAS cada noche: rsync -av --delete /home/proyectos/ backupnas:/backups/proyectos/

Usa herramientas de backup profesionales en servidores: Veeam, por ejemplo

Veeam destaca en: Backups de máquinas virtuales (VMware, Hyper-V). Integración con nubes públicas y repositorios remotos. Restauración granular (un archivo, una VM, un volumen completo).

Aunque no vayas a ser administrador de sistemas, entender qué es un job de backup, un repositorio o una política de retención te ayudará a hablar el mismo idioma que el equipo de IT.

Entiende la diferencia entre sincronización y backup

OneDrive, Google Drive o Dropbox son herramientas fantásticas para: Mantener una carpeta actualizada en varios dispositivos. Colaborar con otras personas en tiempo real.

Pero su función principal es sincronizar, no asegurar versiones históricas a largo plazo. ¿Qué implica esto? Que si borras un archivo o se cifra por un ransomware, ese cambio suele propagarse a todos los dispositivos y a la nube.

Prueba tus backups: un backup no probado es un backup que no existe

Marca en calendario revisiones periódicas para: Restaurar uno o varios archivos. Levantar una máquina virtual o un sistema completo en entorno de pruebas. Documenta: Cuánto tardas. Si los datos están íntegros.

De cara a una auditoría o a la dirección de la empresa, poder decir "hemos probado la restauración hace 10 días" tiene muchísimo peso.

Mitos y Realidades

❌ Mito: "Sincronizar mis archivos con Dropbox/Google Drive es lo mismo que tener un backup."

→ **FALSO.** Aunque servicios como Dropbox, OneDrive o Google Drive puedan tener funciones de historial de versiones o papelera, su objetivo principal es la sincronización. Eso significa que: Si borras un archivo en tu carpeta sincronizada, se borrará también en la nube y en el resto de dispositivos. Si un malware cifra tus archivos locales, la versión cifrada puede sincronizarse y sobreescribir la copia buena en la nube.

La realidad es que una solución de backup profesional (Veeam, soluciones de backup en NAS, herramientas específicas de servidor) mantiene versiones históricas, permite restaurar puntos concretos en el tiempo y está diseñada justo para escenarios de desastre.

❌ Mito: "Los snapshots de una máquina virtual son suficientes como backup."

→ **FALSO.** Un snapshot es una "foto" rápida del estado de una máquina virtual o de un sistema de archivos en un instante. Son muy útiles para: Probar una actualización de software. Hacer cambios de configuración arriesgados. Poder deshacerte de cambios recientes que han roto algo.

Pero dependen completamente de los archivos de disco originales: Si el almacenamiento donde viven esos discos se corrompe, se borra o sufre un desastre físico, todos los snapshots se pierden con él.

La realidad es que los snapshots son una herramienta de recuperación rápida a corto plazo, no una estrategia de copia de seguridad completa.

Resumen final

- Una estrategia de backup combina ubicación (local y nube), tipo de copia (sincronización, backup completo, snapshot) y la regla 3-2-1
- rsync es clave para backups incrementales en Linux; Veeam es referencia en entornos de servidores y virtualización
- Sincronizar con OneDrive/Google Drive no equivale a tener un backup real; los snapshots tampoco sustituyen a una copia de seguridad completa
- Un backup solo es confiable si se prueba periódicamente su restauración

Sesión 22 – Virtualización: VMware, VirtualBox, Hyper-V, Proxmox

Qué es la virtualización y por qué es clave en cualquier infraestructura moderna

La virtualización es una de las tecnologías más influyentes del mundo IT. Gracias a ella, puedes ejecutar varios sistemas operativos —cada uno con su CPU, RAM y disco virtuales— dentro de un único servidor físico. Cada uno de estos sistemas virtualizados se llama máquina virtual (VM). Esta capa de abstracción te permite usar el hardware de forma más eficiente, aislar servicios y escalar infraestructuras sin multiplicar el número de servidores físicos.

En el centro de la virtualización está el hipervisor, un componente que actúa como intermediario entre el hardware físico y las máquinas virtuales. Su trabajo es asignar recursos (CPU, memoria, almacenamiento, red) y garantizar que cada VM esté aislada y funcione como si fuese un ordenador independiente.

Hipervisores de Tipo 2 (o alojados)

Se instalan como un programa normal dentro de un sistema operativo existente (Windows, macOS o Linux).

- **Ejemplos:** Oracle VirtualBox, VMware Workstation / VMware Fusion
- **Ideales para:** Estudiantes, laboratorios de pruebas, desarrolladores
- **Ventajas:** simplicidad y compatibilidad
- **Inconveniente:** el rendimiento depende del sistema operativo anfitrión

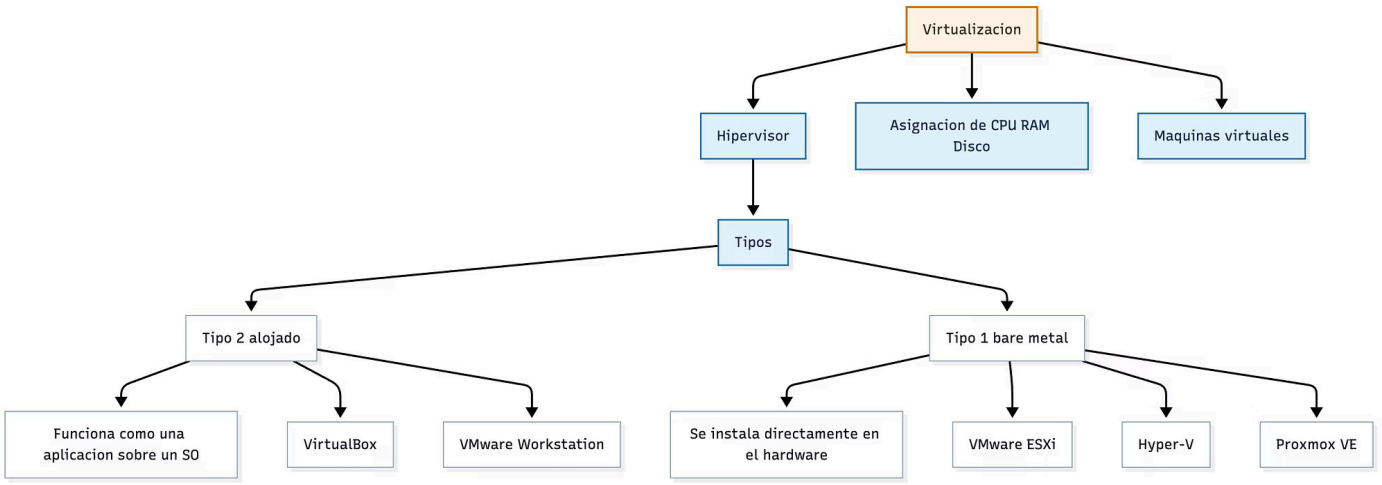
Hipervisores de Tipo 1 (o bare metal)

Se instalan directamente sobre el hardware, sin sistema operativo intermedio.

- **Ejemplos:** VMware ESXi, Microsoft Hyper-V Server, Proxmox VE
- **Ventajas:** Rendimiento casi nativo, gestión avanzada de recursos, alta disponibilidad, réplicas, migraciones en caliente
- **Uso:** Base de cualquier infraestructura profesional

¿Por qué las empresas usan virtualización? **Ahorro de costes:** en vez de tener 10 servidores físicos, puedes tener 1 o 2 hosts potentes con muchas VMs. **Escalabilidad:** crear una nueva VM lleva segundos; adquirir hardware lleva semanas. **Aislamiento:** si una VM falla, no afecta al resto. **Continuidad de negocio:** muchas plataformas permiten mover VMs entre hosts sin apagarlas (vMotion en VMware, Live Migration en Hyper-V).

Esquema Visual: arquitectura de la virtualización y tipos de hipervisores



Cómo leerlo:

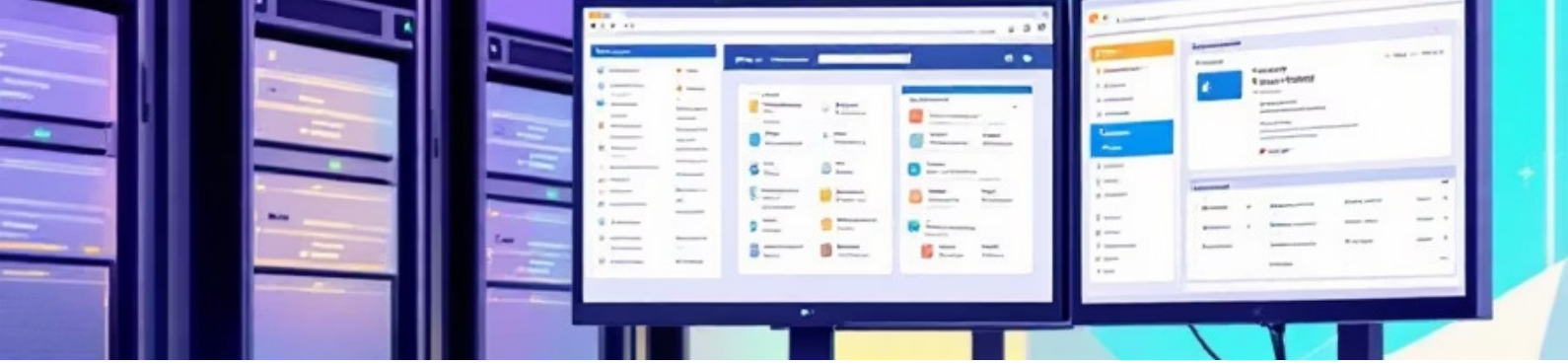
- El bloque A representa la idea general de virtualización.

- El bloque B muestra el rol del hipervisor como pieza central.

- El nodo C lo divide en **Tipo 2** (VirtualBox, VMware Workstation) y **Tipo 1** (ESXi, Hyper-V, Proxmox).

- Las flechas finales indican que la virtualización consiste en asignar recursos y ejecutar VMs aisladas.

Este esquema es útil para que diferencies **dónde** se instala cada hipervisor y qué casos de uso tiene.



Caso de Estudio: VMware vSphere como estándar en centros de datos

Contexto

Una empresa tecnológica con 200 empleados tiene más de 50 servicios: bases de datos, servidores web, aplicaciones internas, ERP, sistemas de tickets, repositorios de código, etc. Antes de virtualizar, cada aplicación estaba en un servidor físico independiente. Esto provocaba:

- Alto consumo energético
- Servidores infrautilizados
- Dificultad para escalar
- Tiempo de inactividad elevado en mantenimientos

La empresa decide migrar toda su infraestructura a VMware vSphere, la plataforma de virtualización empresarial líder del mercado.

Estrategia y ejecución

Instalación de VMware ESXi

Se compran 3 hosts físicos potentes. Se instala ESXi directamente en el hardware de cada uno.

Gestión centralizada con vCenter

Desde vCenter pueden: Crear, clonar y mover máquinas virtuales. Asignar CPU, memoria y almacenamiento dinámicamente. Monitorizar rendimiento.

Función estrella: vMotion

Permite mover una VM de un host a otro sin detenerla. Esto permite hacer mantenimiento de hardware sin parar los servicios.

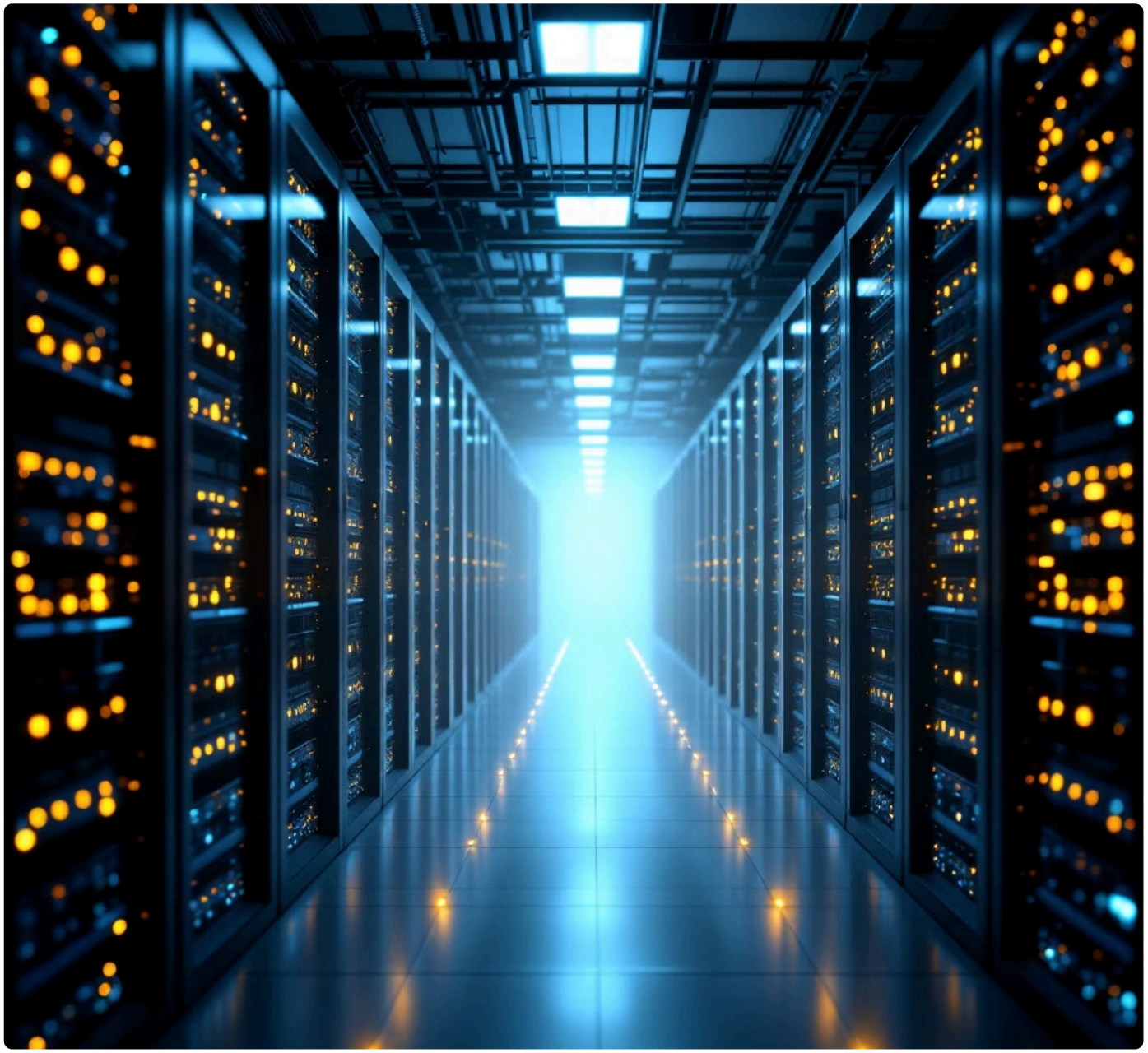
Alta disponibilidad

Si un host cae, las VMs se levantan automáticamente en otro host. Minimiza los tiempos de caída incluso ante fallos físicos.

Resultados

- Reducción del 60% en consumo energético
- Provisionamiento de nuevas máquinas en minutos en lugar de días
- Cero interrupciones por mantenimiento programado
- Mejor control del rendimiento y crecimiento de la infraestructura

VMware se convierte así en el eje central del centro de datos y demuestra por qué sigue siendo el estándar para grandes empresas.



Herramientas y Consejos para gestionar la virtualización

1 Activa la virtualización por hardware en la BIOS

Las CPUs modernas incluyen extensiones que aceleran drásticamente la virtualización: Intel VT-x, AMD-V. Sin esto activado, muchas VMs ni siquiera arrancan.

2 Instala las Guest Additions / VMware Tools

Dentro de cada máquina virtual debes instalar un paquete de herramientas que mejora: Rendimiento gráfico. Sincronización del reloj. Driver de red optimizado. Integración del portapapeles y del ratón. Resolución automática de pantalla.

3 Explora Proxmox como plataforma profesional y gratuita

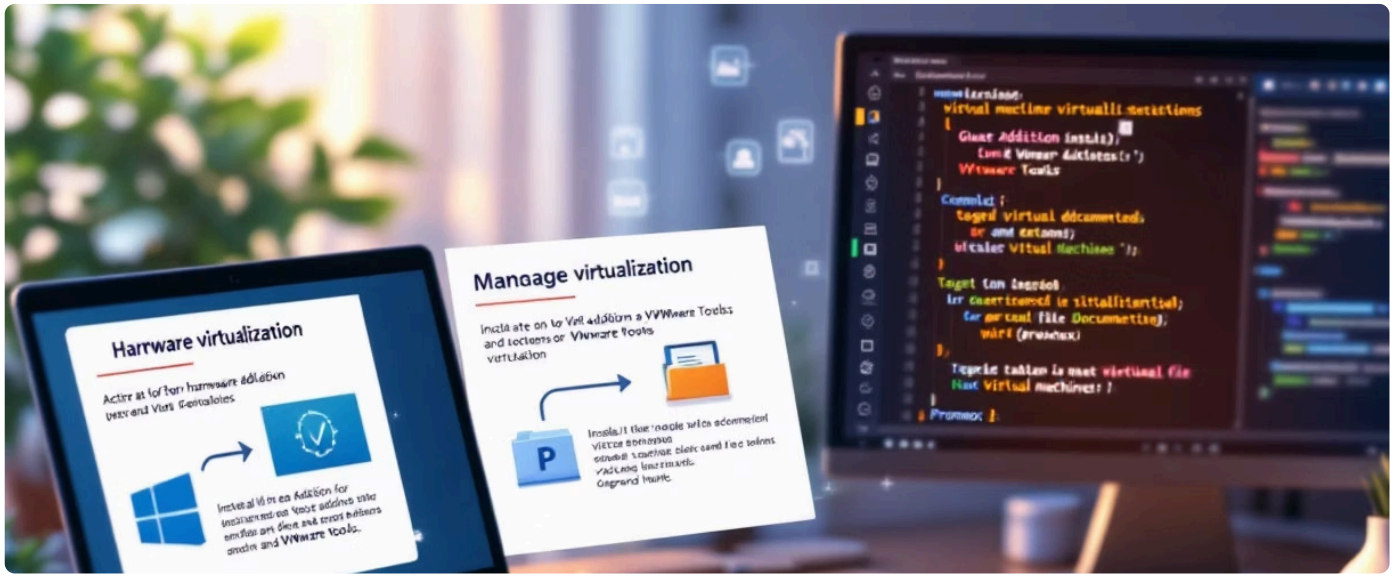
Proxmox VE es muy popular en pymes, laboratorios y sysadmins independientes. Ofrece: KVM para virtualización completa. LXC para contenedores ligeros. ZFS integrado. Backups, snapshots y clústeres. Es una alternativa sólida a VMware con coste cero.

4 Snapshot no es backup

Antes de hacer cambios importantes, crea un snapshot. Pero no lo uses como sustituto de una copia de seguridad real (lo verás en detalle en la sesión 21).

5 Etiqueta y documenta tus VMs

Pon nombres claros a las máquinas virtuales. Documenta: Sistema operativo. Función del servidor. Recursos asignados. Backups asociados. Esto es fundamental cuando gestionas decenas de VMs.



Mitos y Realidades

❌ Mito: "Las máquinas virtuales son muy lentas."

→ **FALSO.** Con hipervisores modernos y virtualización asistida por hardware, el rendimiento de una VM se acerca muchísimo al servidor físico. La diferencia suele ser menor al 5%. Dónde sí hay impacto: VMs con mucho uso de disco si el almacenamiento no es rápido. Hipervisores tipo 2, que dependen del sistema operativo anfitrión.

En servidores profesionales (Tipo 1), la virtualización no es un cuello de botella para la mayoría de las cargas.

❌ Mito: "Si una VM se infecta con un virus, infectará al servidor físico."

→ **FALSO.** Uno de los mayores beneficios de la virtualización es el aislamiento. Las VMs funcionan como si estuvieran dentro de una "caja de arena".

Un virus dentro de una VM no puede "saltar" al host a menos que exista una vulnerabilidad grave en el hipervisor (casos extremadamente raros). Esto permite ejecutar software sospechoso sin comprometer la máquina principal.

En el mundo real, la virtualización es una herramienta clave en laboratorios de malware precisamente por ese aislamiento.

Resumen final

- La virtualización permite ejecutar múltiples sistemas operativos dentro de un mismo host físico mediante máquinas virtuales
- El hipervisor es clave: Tipo 1: se instala directamente en el hardware (ESXi, Hyper-V, Proxmox). Tipo 2: funciona como una aplicación sobre un SO (VirtualBox, VMware Workstation)
- Las VMs ofrecen aislamiento, flexibilidad y un uso eficiente del hardware
- VMware es la plataforma de referencia en entornos empresariales por funciones como vMotion y alta disponibilidad
- Activar virtualización por hardware (VT-x / AMD-V) y usar Guest Additions/VMware Tools mejora muchísimo el rendimiento

Sesión 23 – Contenedores con Docker: conceptos y práctica

Qué son los contenedores y por qué han transformado el desarrollo moderno

Durante años, los equipos de desarrollo se enfrentaban al clásico problema: "En mi ordenador funciona". Una aplicación podía ejecutarse perfectamente en el portátil del desarrollador, pero fallar al desplegarse en producción porque la versión de Python no coincidía, faltaba una librería o el sistema operativo era diferente. Los contenedores nacen precisamente para eliminar este caos.

Un contenedor es una forma de virtualización ligera que empaqueta una aplicación junto con todo lo que necesita para funcionar: dependencias, configuraciones, binarios y librerías. La gran diferencia respecto a una máquina virtual es que los contenedores no incluyen un sistema operativo completo, sino que comparten el kernel del sistema anfitrión. Esto los hace extremadamente ligeros, rápidos de iniciar y muy eficientes.

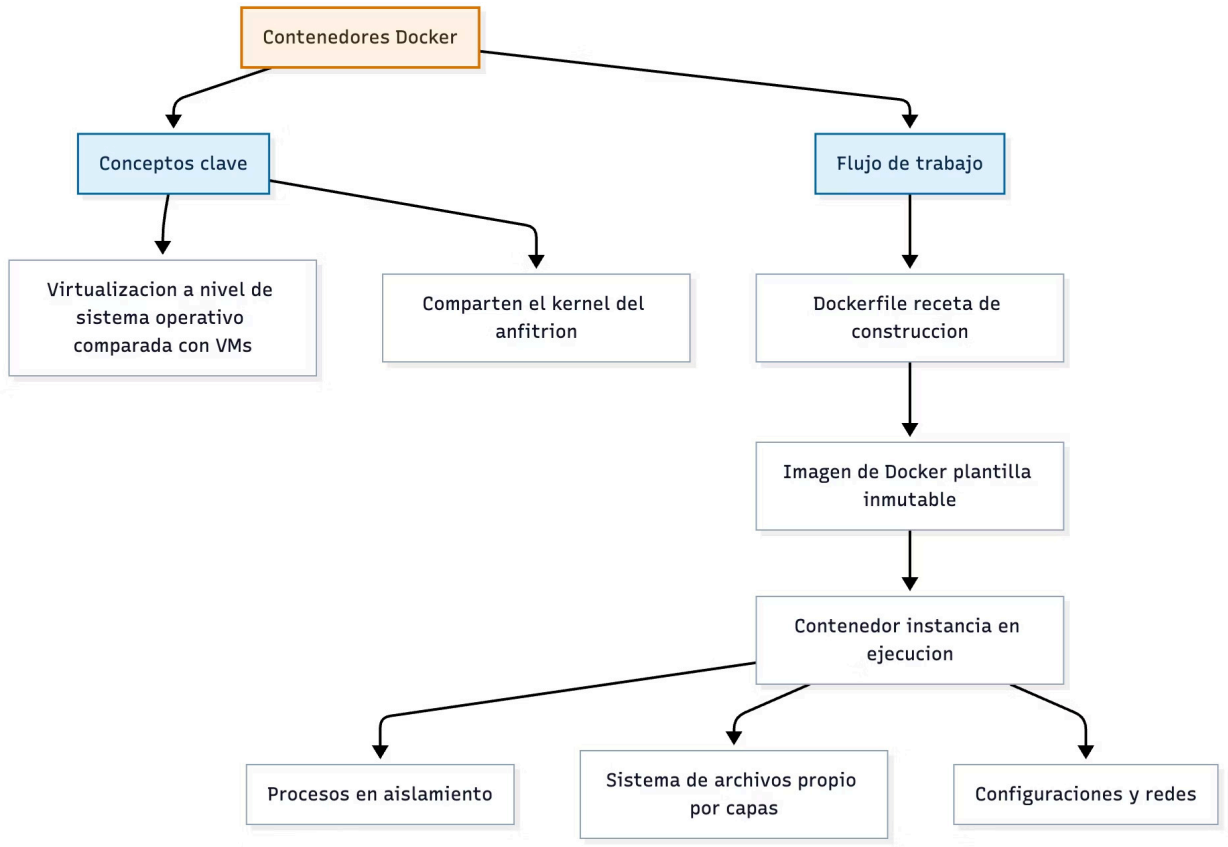
Kernel	Comparte el kernel del host	Tiene su propio kernel
Peso	Muy ligero	Pesado (varios GB)
Tiempo de arranque	Milisegundos	Decenas de segundos/minutos
Casos de uso	Microservicios, despliegues rápidos, CI/CD	Virtualización completa, sistemas independientes

Los contenedores son ideales para arquitecturas modernas basadas en microservicios, donde una aplicación grande se divide en muchas piezas pequeñas, cada una ejecutándose en su propio contenedor.

Docker: el estándar de la industria

Docker es la plataforma más utilizada para crear, ejecutar y distribuir contenedores. Su popularidad se debe a tres ideas clave: **Reproducibilidad:** una app funcionará igual en un portátil, un servidor o la nube. **Portabilidad:** puedes mover contenedores entre sistemas sin cambios. **Escalabilidad:** iniciar cientos de contenedores es trivial comparado con decenas de máquinas virtuales.

Esquema Visual: arquitectura de Docker y flujo de creación de contenedores



Cómo entenderlo:

- Los contenedores se apoyan en la idea de que **no necesitan su propio sistema operativo**, sino que usan el del host.

- El flujo completo siempre empieza por un **Dockerfile**, desde el cual se construye una **imagen**, y de cada imagen puedes lanzar **infinitos contenedores**.

- Cada contenedor tiene su propio sistema de archivos de capas, su configuración, su red y sus procesos aislados del resto.

Este esquema te servirá como mapa mental para cualquier proyecto con Docker.

Caso de Estudio: Docker en Netflix para escalar microservicios globales

Contexto

Netflix gestiona miles de microservicios responsables de recomendaciones, streaming, notificaciones, facturación, perfiles de usuario, medición de calidad de vídeo... La escala es tan enorme que una sola inconsistencia entre entornos podía causar fallos masivos. Antes de Docker, los equipos tenían dificultades para garantizar que un servicio funcionase igual en el portátil del desarrollador, en los servidores de staging y en los de producción.

Estrategia

Netflix adoptó Docker como estándar para empaquetar sus microservicios:

- Estandarización de microservicios

  Cada microservicio se empaqueta como una imagen de Docker. Esto asegura que: Se ejecuta con las mismas versiones de librerías. No depende del sistema operativo del host. Las actualizaciones son predecibles.

- Escalado automático

  Netflix usa plataformas orquestadoras (como Kubernetes) para: Lanzar cientos o miles de contenedores cuando aumenta la demanda (por ejemplo, un estreno global). Apagar contenedores cuando baja el tráfico, reduciendo costes.

- Despliegues controlados

  Cada nueva versión de un microservicio se despliega como una imagen nueva. Si algo falla, se puede volver a la versión anterior en segundos.

Resultados

- Reducción drástica de errores "funciona en mi máquina"
- Escalado elástico para absorber picos de carga
- Despliegues más rápidos y seguros
- Mayor independencia entre equipos, que pueden lanzar nuevas versiones sin afectar a los demás

Este caso refleja el motivo por el que Docker se ha convertido en una tecnología estándar en cualquier empresa que trabaje con microservicios o despliegues distribuidos.

Herramientas y Consejos para trabajar con contenedores

Docker Hub: tu repositorio de imágenes

Es el "GitHub de los contenedores". Aquí encontrarás imágenes oficiales de: Nginx, MySQL / MariaDB, Redis, Python, Node.js, Java..., Ubuntu, Alpine Linux.

Trabajar con imágenes oficiales reduce riesgos de seguridad y aumenta la estabilidad de tus despliegues.

Docker Compose para aplicaciones multicontenedor

Muchísimas aplicaciones modernas necesitan varios servicios: Un backend, Una base de datos, Un servidor web, Un sistema de colas, Un contenedor para tareas en background.

Con Docker Compose puedes definir todo en un único archivo docker-compose.yml y levantarlo con: docker compose up -d. Es esencial para el trabajo profesional.

Usa VS Code con Dev Containers

La extensión Dev Containers te permite desarrollar dentro de un contenedor sin preocuparte por configurar tu sistema operativo. Ventajas: Tu entorno de desarrollo es idéntico al del servidor. Puedes tener múltiples proyectos con versiones distintas de Python, Node, PHP, etc. Elimina conflictos entre librerías del sistema.

Mantén tus imágenes ligeras

Mejor usa: alpine, imágenes slim, multistage builds. Esto acelera descargas, despliegues y reduce superficie de ataque.

Aprende comandos básicos que usarás siempre

docker ps → ver contenedores, docker images → ver imágenes, docker build -t nombre . → construir imagen, docker run -it nombre → ejecutar contenedor, docker logs → ver registros.

Saber estos comandos te permite moverte con soltura en casi cualquier entorno profesional.

Mitos y Realidades

❌ Mito: "Docker es solo para Linux."

→ **FALSO.** Aunque los contenedores se basan en funcionalidades del kernel de Linux, Docker funciona perfectamente en: Windows, macOS, Linux.

En Windows y macOS, Docker usa una pequeña máquina virtual Linux para ejecutar contenedores, pero la experiencia para el usuario es prácticamente idéntica. La realidad es que Docker es multiplataforma, por lo que puedes aprenderlo y utilizarlo sin importar tu sistema operativo.

❌ Mito: "Los contenedores son igual de seguros que las máquinas virtuales."

→ **FALSO.** El aislamiento de una máquina virtual es más fuerte porque: Cada VM tiene su propio kernel. El hipervisor está muy protegido. Un fallo dentro de una VM no afecta a las demás.

Los contenedores comparten el kernel del anfitrión, así que una vulnerabilidad en ese kernel puede afectar a todos los contenedores. En la práctica: Para la mayoría de aplicaciones, los contenedores son suficientemente seguros. Para aplicaciones muy sensibles (banca, defensa), se siguen utilizando VMs o combinaciones de VM + contenedor.

Resumen final

- Los contenedores virtualizan el espacio de usuario, compartiendo el kernel del host
- Docker usa el flujo Dockerfile → Imagen → Contenedor
- Las imágenes empaquetan todo lo necesario para ejecutar una aplicación
- Docker Compose permite gestionar aplicaciones multicontenedor
- Los contenedores son más ligeros que las VMs, pero tienen menor aislamiento