



# INICIO GRABACIÓN



**SANJOSÉ**  
FUNDACIÓN DE EDUCACIÓN SUPERIOR



## **SEGURIDAD PASIVA**


un auditor informático es visto como un profesional altamente capacitado independiente que evalúa la eficiencia de un sistema con el objetivo principal de detectar fallas que deben ser solucionadas



# UBICACIÓN DEL CPD



Las empresas colocan los equipos de usuario cerca del usuario (un ordenador sobre su mesa, un portátil que se lleva a casa); pero los servidores están todos juntos en una misma sala: Esa sala tiene varios nombres: CPD (centro de proceso de datos), centro de cálculo, DataCenter, sala fría, «pecera», etc: Centralizando se consigue:

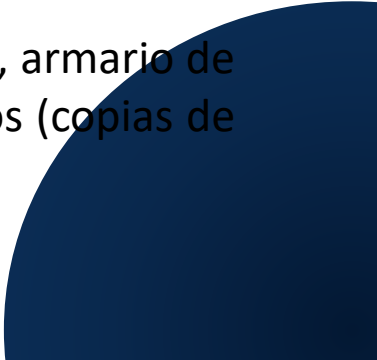
- Ahorrar en costes de protección y mantenimiento. No necesitan duplicar la vigilancia, la refrigeración, etc:
  - Optimizar las comunicaciones entre servidores. Al estar unos cerca de otros no necesitan utilizar
  - Aprovechar mejor los recursos humanos del departamento de informática. No tienen que desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc:
- 



# UBICACIÓN DEL CPD



Tan importante como tomar medidas para proteger los equipos es tener en cuenta qué hacer cuando esas medidas fallan: Todas las empresas deben tener documentado un plan de recuperación ante desastres, donde se describa con el máximo detalle (en una crisis no hay tiempo para reflexionar) qué hacer ante una caída de cualquiera de los servicios que presta el CPD: Este plan debe ser actualizado cuando se efectúe un cambio en el CPD (nuevo servicio, nuevo equipo): El plan debe incluir:

- Hardware. Qué modelos de máquinas tenemos instalados (tanto servidores como equipamiento de red), qué modelos alternativos podemos utilizar y cómo se instalaran (conexiones, configuración):
  - Software. Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración (permisos, usuarios, etc):
  - Datos. Qué sistemas de almacenamiento utilizamos (discos locales, armario de discos), con qué configuración y cómo se hace el respaldo de datos (copias de seguridad):
- 



# PROTECCION



La informática es vital para la empresa: si los servidores se paran, la empresa se para. Sucede en todos los sectores: en una empresa de telefonía, en una compañía aérea, en unos grandes almacenes...

El CPD debe estar protegido al máximo:

- Elegiremos un edificio en una zona con **baja probabilidad de accidentes naturales** (terremotos, ciclones, inundaciones).
- También evitaremos la proximidad de ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.
- Evitaremos ubicaciones donde los edificios vecinos al nuestro pertenezcan a empresas dedicadas a **actividades potencialmente peligrosas**: gases inflamables, explosivos, etc.
- Preferentemente **seleccionaremos las primeras plantas del edificio**.
  - La planta baja está expuesta a sabotajes desde el exterior (impacto de vehículos, asaltos, etc.).
  - Las plantas subterráneas serían las primeras afectadas por una inundación.
  - Las plantas superiores están expuestas a un accidente aéreo y, en caso de incendio iniciado en plantas inferiores, es seguro que nos afectará.





# PROTECCION



- Se recomienda que el edificio tenga **dos accesos y por calles diferentes**. Así siempre podremos entrar en caso de que una entrada quede inaccesible (obras, incidente, etc.).
- Es recomendable **evitar señalar la ubicación del CPD** para dificultar su localización a posibles atacantes. La lista de empleados que entran a esa sala es muy reducida y saben perfectamente dónde está.
- **Los pasillos que llevan hasta el CPD deben ser anchos** porque algunos equipos son bastante voluminosos. Incluso conviene dotarlo de un muelle de descarga.
- **El acceso a la sala debe estar muy controlado**. Los servidores solo interesan al personal del CPD.
- En las paredes de la sala se deberá **utilizar pintura plástica** porque facilita su limpieza y se evita la generación de polvo.
- En la sala se **utilizará falso suelo y falso techo** (Fig. 3.1) porque facilita la distribución del cableado (para electricidad y comunicaciones) y la ventilación.
- **La altura de la sala será elevada** tanto para permitir el despliegue de falso suelo y falso techo como para acumular muchos equipos en vertical (Fig. 3.1), porque el espacio de esta sala es muy valioso.
- En empresas de alta seguridad, la sala del CPD se recubre con un **cofre de hormigón** para protegerla de intrusiones desde el exterior.
- Instalaremos **equipos de detección de humos y sistemas automáticos de extinción de incendios**, como los elementos del techo de la Figura 3.1.
- El mobiliario de la sala debe utilizar **materiales ignífugos**.

# PROTECCION




<http://goo.gl/Xt9hC>



# AISLAMIENTO



Las máquinas que situamos en el CPD utilizan circuitos electrónicos. Por tanto, hay que protegerlas ante:

- **Temperatura.** Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.
  - **Humedad.** No solo el agua, también un alto porcentaje de humedad en el ambiente puede dañarnos. Para evitarlo utilizaremos deshumidificadores.
  - **Interferencias electromagnéticas.** El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad, sean nuestros o de alguna empresa vecina.
  - **Ruido.** Los ventiladores de las máquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento
- 

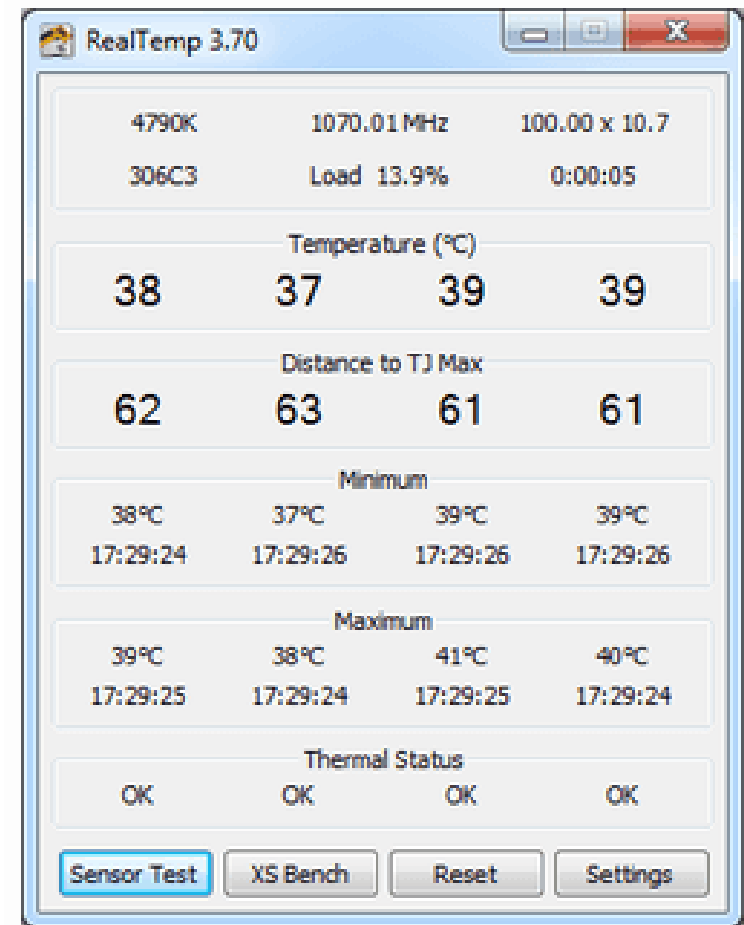


# CONTROL DE TEMPERATURA EN WIN



1. El ordenador tiene varios sensores de temperatura: en la CPU, en la tarjeta gráfica, en el disco duro, etc. El principal es el de la CPU, porque es la parte crítica del sistema que funciona a más velocidad, lo cual genera mucho calor. Por eso la CPU siempre dispone de ventilación especial (disipador más ventilador).
2. Podemos conocer la temperatura instalando alguna utilidad software, como RealTemp. En la Figura 3.2 tenemos la ventana principal de la herramienta. Por desgracia, estas herramientas no funcionan bien en todos los equipos porque dependen mucho del API (Application Programming Interface) ofrecido por el fabricante de la CPU, la tarjeta gráfica, la placa base, etc. Es decir, el sensor está, pero no siempre resulta fácil que cualquier software lo consulte.

<https://www.techpowerup.com/download/techpowerup-real-temp/>



# CONTROL DE TEMPERATURA EN WIN



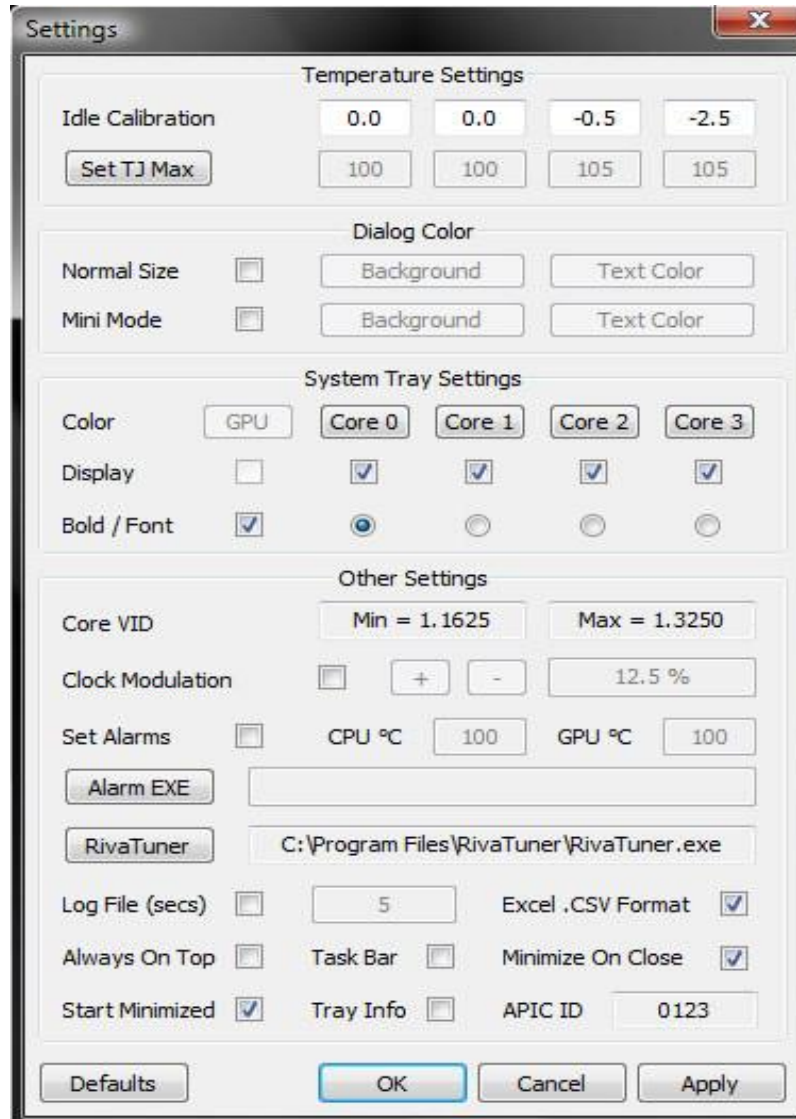
La primera parte de la ventana muestra el tipo de CPU y la velocidad actual (en Mhz), así como la carga del sistema operativo (Load: una alta carga supone que la CPU trabaja más y genera más calor). Debajo tiene la temperatura de la CPU. En este caso ofrece dos valores porque es un procesador de doble núcleo. La siguiente fila es la diferencia con el máximo que admitimos (este valor lo podemos configurar), es decir: cuántos grados más se puede calentar antes de que sea importante. Finalmente, hay dos filas donde aparecen los valores mínimo y máximo que ha registrado la herramienta desde que está arrancada. Esto nos sirve para comprobar si la máquina está siempre trabajando al mismo ritmo o tiene altibajos.

Esta misma información está disponible en la barra de tareas (Fig. 3.5).



3. Pulsando en *Settings* accedemos a la configuración (Fig. 3.3). Si nuestra tarjeta gráfica es ATI o Nvidia, podemos activar la casilla correspondiente para disponer de su temperatura. Para verla activaremos su casilla en la zona central bajo GPU (Graphics Processing Unit, el procesador gráfico).

# CONTROL DE TEMPERATURA EN WIN



The screenshot shows the RivaTuner Settings window, which is used for monitoring and controlling system temperatures. The window is divided into several sections:

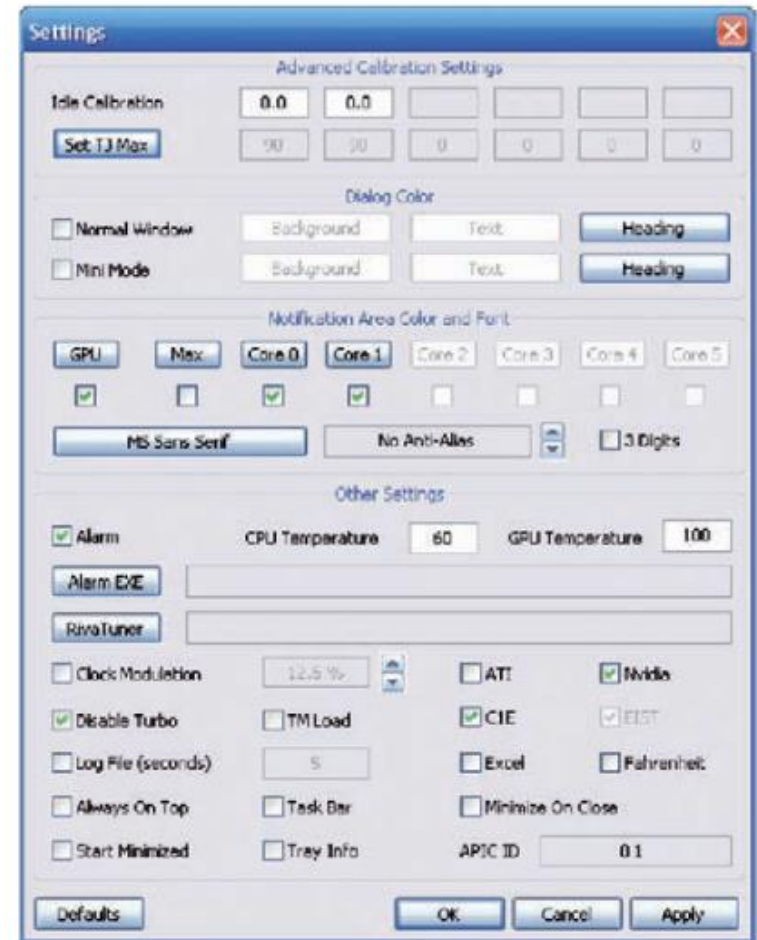
- Temperature Settings:** Includes fields for Idle Calibration (0.0, 0.0, -0.5, -2.5) and a Set TJ Max button. Below it are fields for 100, 100, 105, and 105.
- Dialog Color:** Includes checkboxes for Normal Size and Mini Mode, and buttons for Background and Text Color.
- System Tray Settings:** Includes a Color dropdown (GPU, Core 0, Core 1, Core 2, Core 3), Display checkboxes, and Bold / Font checkboxes.
- Other Settings:** Includes Core VID (Min = 1.1625, Max = 1.3250), Clock Modulation (+, -, 12.5 %), Set Alarms (CPU °C, GPU °C), Alarm EXE, RivaTuner, Log File (secs), Always On Top, Start Minimized, Task Bar, Tray Info, APIC ID, and Minimize On Close.

Buttons at the bottom include Defaults, OK, Cancel, and Apply.

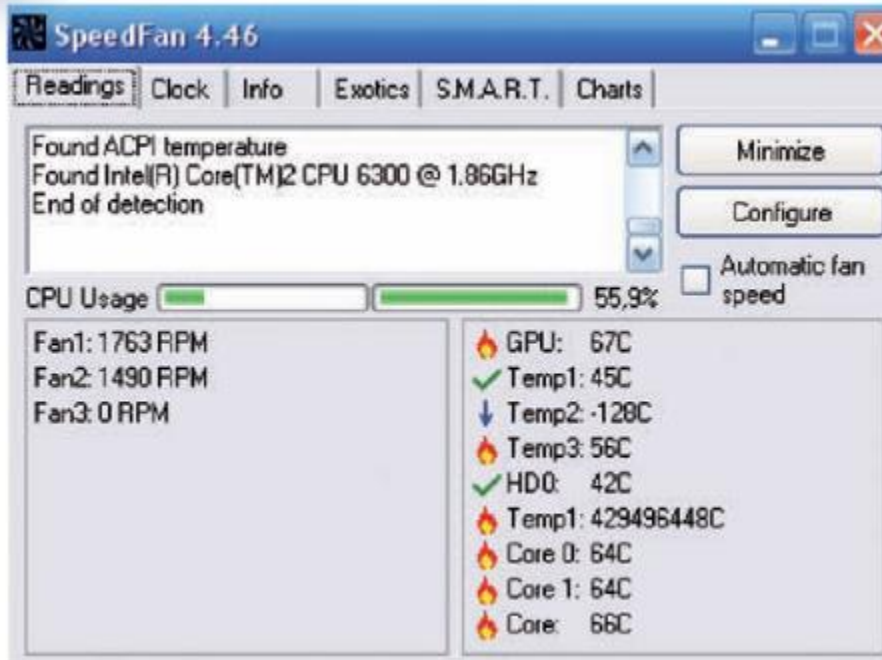
# CONTROL DE TEMPERATURA EN WIN



6. Finalmente, esta herramienta incorpora un mecanismo de aviso de sobrecalentamiento. En la ventana de configuración activaremos la casilla *Alarm* (Fig. 3.6). A la derecha podemos asignar valores para la temperatura de CPU y GPU. Si se superan, oiremos una sirena. También podemos ejecutar un programa cualquiera (enviar un correo, registrar un evento, avisar a un sistema de monitorización como los que veremos en la Unidad 5): basta elegirlo pulsando en *Alarm EXE*. En el ejemplo, como la temperatura de la CPU estaba por encima de 60, poniendo un valor de 60 y pulsando *Apply* se activa la alarma.
7. Algunas utilidades, además de la temperatura, saben cómo hablar con la placa base para obtener la velocidad de los ventiladores. Por ejemplo, SpeedFan. En la Figura 3.7 vemos que aparece la velocidad en RPM (revoluciones por minuto) de los ventiladores Fan1 y Fan2 (mirando en el manual de la placa, uno corresponde a la CPU y el otro, al chipset). Hay un tercero, Fan3, que no está siendo utilizado. Si la velocidad de Fan1 o Fan2 baja repentinamente, debemos averiguar qué pasa, porque en poco tiempo subirá la temperatura.



# CONTROL DE TEMPERATURA EN WIN



8. Un ventilador se puede parar por un fallo interno o por un uso excesivo; pero la causa más frecuente de problemas con los ventiladores es la acumulación de polvo y otras partículas. Por este motivo, conviene abrir la caja del ordenador para limpiarla con un aspirador. Nos centraremos especialmente en los ventiladores y disipadores. Dependiendo del ambiente de la sala, esta tarea se hará una vez al año (oficina) o una vez al mes (ordenador en contacto con el exterior).





# VENTILACION



Los CPD **no suelen tener ventanas**. La ventilación que conseguiríamos con ellas sería mínima para todo el calor que se genera, y el riesgo de intrusiones desde el exterior (o simplemente la lluvia) no es admisible en una instalación de tanta importancia.

La temperatura recomendable en la sala estaría alrededor de los **22 grados**. Las máquinas no lo necesitan, pero hay que pensar que ahí también van a trabajar personas. Para conseguirlo instalaremos **equipos de climatización**. Se suelen instalar por duplicado, para estar cubiertos ante el fallo de uno de los equipos.

En los CPD grandes se adopta la **configuración de pasillos calientes y pasillos fríos** (Fig. 3.8). Las filas de equipos se colocan en bloques formando pasillos, de manera que todos los ventiladores que extraen el calor de la máquina (fuente de alimentación, caja de la CPU) apunten hacia el mismo pasillo. En este pasillo se colocan los extractores de calor del equipo de climatización.

<https://www.youtube.com/watch?v=5MaDIHZYUQk>





# SUMINISTRO ELECTRICO Y COMUNICACIONES

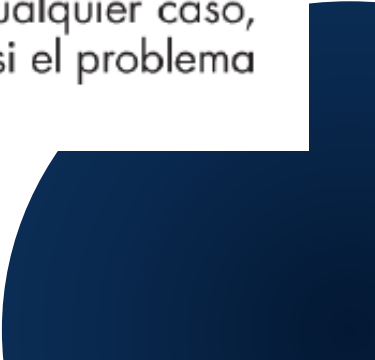


Nuestro CPD no está aislado: necesita ciertos servicios del exterior. Los principales son la alimentación eléctrica y las comunicaciones. En ambos casos **conviene contratar con dos empresas distintas**, de manera que un fallo en una compañía suministradora no nos impida seguir trabajando.

El **suministro eléctrico** del CPD debería estar **separado del que alimenta al resto de la empresa** para evitar que un problema en cualquier despacho de ese edificio afecte a los servidores, porque están siendo utilizados por empleados de otros edificios, incluso por clientes y proveedores.

Para los sistemas críticos, en los que la empresa no puede permitirse ninguna interrupción del servicio, deberemos instalar **generadores eléctricos** alimentados por combustible.

En cuanto a las **comunicaciones**, conviene que el **segundo suministrador utilice una tecnología diferente al primero**. Por ejemplo, si tenemos una conexión ADSL, el segundo no debería ser ADSL también, porque comparten el mismo cable hasta llegar a la central: un fallo en ese cable nos desconectaría de los dos suministradores. En cualquier caso, siempre conviene tener una tercera opción de conexión inalámbrica, por si el problema ocurre en la calle (obras en la acera, etc.).

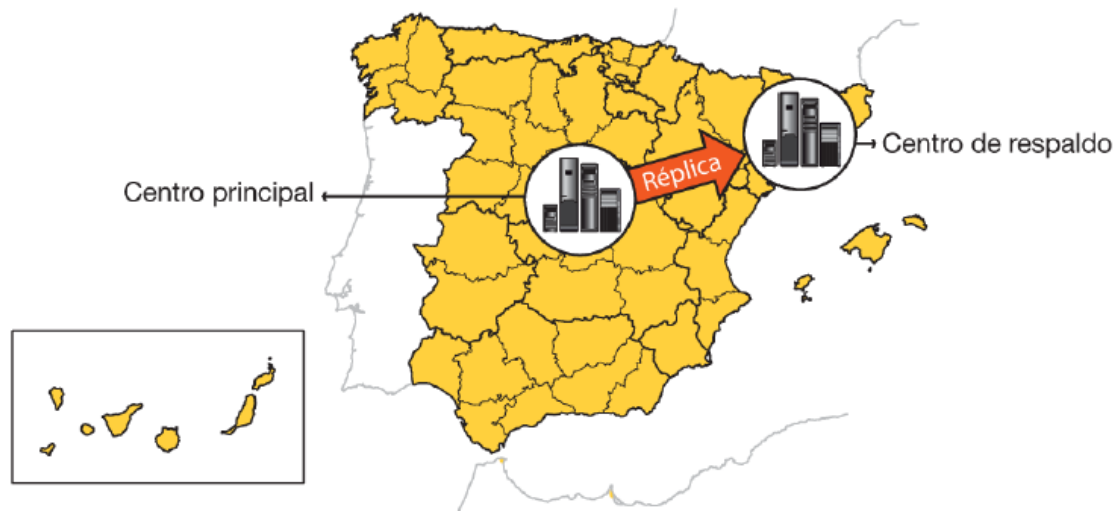


# CENTRO DE RESPALDO



A pesar de tanta protección, debemos pensar en la posibilidad de que ocurra una catástrofe en nuestro CPD y quede inservible (inundación, terremoto, sabotaje). La continuidad de la empresa no puede depender de un **punto único de fallo**; si disponemos de presupuesto suficiente, debemos **instalar un segundo CPD**.

Este segundo CPD, también llamado **centro de respaldo** (CR), **ofrece los mismos servicios** del centro principal (CP). Aunque, si la inversión en hardware resulta demasiado elevada, puede limitarse a los servicios principales, o a los mismos servicios pero con menos prestaciones. Por supuesto, **debe estar físicamente alejado del CP**; cuantos más kilómetros entre ambos, mejor (Fig. 3.9).



## SAI / UPS



La corriente eléctrica es vital en cualquier ordenador. Como no podemos confiar en que nunca va a fallar la empresa con la que hemos contratado el suministro eléctrico, tenemos que pensar en alternativas. En esta misma unidad hemos sugerido contratar un **segundo suministrador** o disponer de un **generador propio** (grupo electrógeno). Sin abandonar estas soluciones, en un CPD nunca debe faltar un SAI (**sistema de alimentación ininterrumpida**), en inglés UPS (Uninterruptible Power Supply).

Un SAI es un conjunto de **baterías** que alimentan una instalación eléctrica (en nuestro caso, equipos informáticos). La Figura 3.10 corresponde a la vista trasera de un SAI. Lo enchufamos a la corriente eléctrica por la toma de la izquierda y ofrece cuatro enchufes en la derecha.







## SAI / UPS



En caso de corte de la corriente, los equipos conectados al SAI siguen funcionando porque consiguen electricidad de las baterías. **La capacidad de estas baterías es reducida** depende del SAI elegido y del consumo de los equipos, aunque el mínimo garantizado suele ser diez minutos. Este es el factor más importante a la hora de adquirir un SAI: cuántos vatios consumen los equipos que debe proteger y cuánto tiempo necesitamos que los proteja.

Al igual que ocurría con los equipos de climatización, si el presupuesto lo permite, conviene aplicar redundancia e instalar un **doble juego de equipos SAI**, para estar cubiertos en caso de que uno fallara. Esto es posible porque la mayoría de los servidores vienen con doble fuente de alimentación y conectaríamos una fuente a cada grupo de SAI.

Cuando ocurre un corte de luz, el SAI procede de esta manera:

- Espera unos minutos por si el corte ha sido puntual y el suministro se recupera inmediatamente por sí solo.
- Si no es así, ejecuta una **parada ordenada** de los equipos conectados al SAI. Siempre es mejor solicitar una parada al sistema operativo y las aplicaciones que ejecuta que

Conectar los equipos al SAI tiene otras ventajas:

- Suelen llevar un **estabilizador de corriente** que quita los picos, que también pueden ser muy dañinos.
- En algunos SAI también se incluye una entrada y salida de **cable telefónico** (conectores a la izquierda del ventilador en la Figura 3.10), que sirve para proteger nuestra conexión, porque las comunicaciones por línea telefónica también utilizan corriente eléctrica, luego también estamos expuestos a picos de tensión.



# MANTENIMIENTO SAI / UPS



Las baterías se desgastan con el tiempo y ofrecen cada vez menos rendimiento. El software del SAI nos ayuda en este aspecto:

- Permite lanzar determinados test para comprobar la degradación actual de las baterías. Si no es suficiente para garantizar la parada ordenada de los equipos protegidos, debemos cambiarlas (Fig. 3.17). Para cambiar las baterías acudiremos al personal especializado, porque las baterías utilizan componentes químicos muy peligrosos.
- Incluye operaciones automáticas de descarga controlada, que alargan la vida de las baterías.

Como hemos visto antes, la operación de cambiar las baterías será relativamente sencilla en un SAI de tipo stand-by porque mientras tanto los equipos seguirán alimentados; pero en un SAI on-line perderemos la alimentación, por lo que es necesario detener los equipos. Este aspecto puede ser crítico en una empresa que no pueda permitirse ninguna parada.



The background features a high-five gesture with several hands. Overlaid on this are two large, semi-transparent blue circles and a smaller solid blue circle, creating a modern, abstract design.

# SEGURIDAD PASIVA ALMACENAMIENTO



# ESTRATEGIAS DE ALMACENAMIENTO




Para una empresa, la parte más importante de la informática son los datos: sus datos. Porque:

- El hardware es caro, pero se puede volver a comprar.
- Un informático muy bueno puede despedirse, pero es posible contratar otro.
- Si una máquina no arranca porque se ha corrompido el sistema de ficheros (el típico BSOD), puedes instalar de nuevo el sistema operativo y las aplicaciones desde los CD o DVD originales.

En todos los casos anteriores se recupera la normalidad en un plazo de tiempo razonable.

Sin embargo, los datos de esa empresa son únicos: no se pueden comprar, no se pueden contratar, no hay originales. Si se pierden, no los podemos recuperar (por lo menos, ni fácil ni rápidamente).

Bien, puesto que los datos son tan importantes, hay que esforzarse especialmente en mejorar su integridad y disponibilidad (estos conceptos los aprendimos en la Unidad 1):

- Podemos comprar los mejores discos del mercado en calidad (MTBF) y velocidad; aunque nunca debemos olvidar que son máquinas y pueden fallar (salvo los SSD, todos los discos tienen partes móviles). En un puesto de usuario nos lo podemos permitir (lo cambiamos y listo): en un servidor hemos visto que no.
  - Podemos concentrar los discos en unos servidores especializados en almacenamiento.
  - Podemos replicar la información varias veces y repartirla por ciudades distintas.
  - Podemos contratar el servicio de respaldo de datos a otra empresa, conectados por Internet, para no depender de nuestros equipos y personal.
- 

# ESTRATEGIAS DE ALMACENAMIENTO



- **Crear unidades más rápidas.** Si tenemos dos discos de 500 GB y configuramos el sistema para que, en cada fichero, los bloques pares se escriban en un disco y los impares en otro, después podremos hacer lecturas y escrituras en paralelo (en el mejor caso, ahorramos la mitad de tiempo). Con un único disco de 1 TB tenemos la misma capacidad, pero cada lectura o escritura debe esperar que termine la operación anterior. La diferencia es más notable si ponemos tres discos, cuatro, etc.
- **Crear unidades más fiables.** Si configuramos los dos discos anteriores para que, en cada fichero, los bloques se escriban a la vez en ambos discos, podemos estar tranquilos porque, si falla un disco, los datos estarán a salvo en el otro.

Pues una de las tecnologías que lo consigue se llama RAID. Hay varios niveles de RAID. Los más importantes son:

- **RAID 0.** Agrupamos discos para tener un disco más grande, incluso más rápido. Desde ese momento, los bloques que lleguen al disco RAID 0 se escribirán en alguno de los discos del grupo. Por supuesto, para el usuario este proceso es transparente: él solo ve un disco de 1 TB donde antes había dos discos de 500 GB. En el RAID 0 podemos elegir entre spanning y striping (que es lo más común). En cualquier caso, si falla uno de los discos, lo perdemos todo.
- **RAID 1.** Se le suele llamar **mirror** o **espejo**. Agrupamos discos por parejas, de manera que cada bloque que llegue al disco RAID 1 se escribirá en los dos discos a la vez. Si falla uno de los discos, no perdemos la información, porque estará en el otro. A cambio, sacrificamos la mitad de la capacidad (el usuario ha conectado dos discos de 500 GB y solo tiene disponibles 500 GB, en lugar de 1 TB) y no ganamos rendimiento.

# ESTRATEGIAS DE ALMACENAMIENTO



- **RAID 5.** Hemos visto que el RAID 0 es más rápido que cada uno de los discos, pero tan seguro como cualquiera de ellos. El RAID 1 es más seguro que los discos por separado, pero con el mismo rendimiento. El RAID 5 consigue ambas cosas aplicando dos mecanismos:
  - Para cada dato que el sistema quiere almacenar en el RAID, este aplica un procedimiento matemático (en general, la paridad) para obtener información complementaria a ese dato, de tal manera que se puede recuperar el dato en caso de perder cualquier disco (sea disco de datos o paridad).
  - Una vez obtenida la paridad, se hace striping para repartir el dato y su paridad por los discos conectados al RAID.

**RAID** (Redundant Array of Independent Disks). Es un grupo de discos configurados para trabajar en conjunto, con el fin de lograr más rendimiento, más fiabilidad o ambas cosas.

**Spanning.** Los bloques se escriben en el primer disco hasta que lo llenan; entonces pasan al siguiente, y así sucesivamente. Por tanto, la lectura o escritura de cada bloque tiene que esperar hasta que el disco haya terminado la anterior.

**Striping.** Los bloques se escriben cada vez en un disco distinto. Es más rápido que el spanning porque hace trabajar a todos los discos a la vez.



# Tipos de RAID



Por tanto, necesitamos un disco más para almacenar la paridad. Por ejemplo, si queremos una capacidad de 1 TB, necesitamos tres discos de 500 GB (o cinco discos de 250 GB).

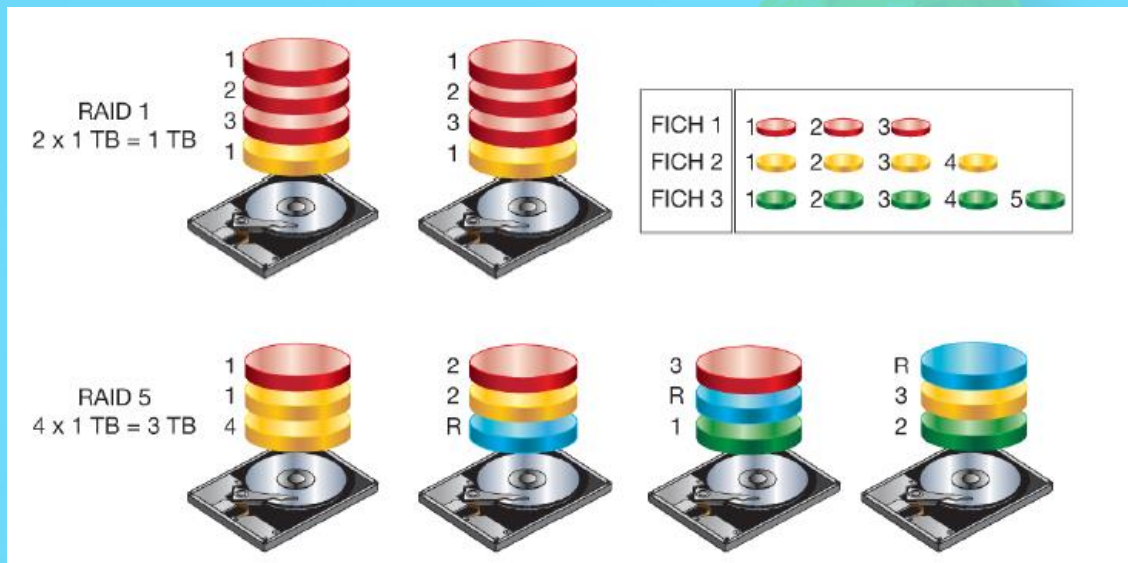
Gracias al striping hemos conseguido mejor rendimiento que el disco individual, y gracias a la paridad estamos más seguros que en RAID 0. A cambio, sacrificamos la capacidad de un disco (aunque cuantos más discos, menos porcentaje de capacidad perdida).

Estamos viendo que el RAID para el sistema operativo es una especie de disco «virtual», que está organizado en stripes (bandas, filas). Al igual que el tamaño del bloque en los discos «físicos» (512 bytes, 4 096 bytes) y el tamaño del bloque del sistema de ficheros (4 096 bytes en NTFS), en el RAID es importante el tamaño de stripe. El valor recomendado es 64 KB.

Veamos un ejemplo (Fig. 4.2). Tenemos tres ficheros y queremos almacenarlos en un RAID donde, por simplificar, el tamaño de stripe es el mismo que el tamaño de bloque del sistema operativo.



# Tipos de RAID




El primer fichero ocupa tres bloques; el segundo, cuatro, y el tercero, cinco. Todos los discos son de 1 TB.

- Si tenemos cuatro discos y los configuramos en RAID 0, los bloques de los ficheros se reparten por los cuatro discos. La capacidad total es de 4 TB, y los bloques de un fichero se pueden recuperar simultáneamente por varios discos.
- Si ponemos dos discos en RAID 1, los bloques de los ficheros se copian en los dos. La capacidad total es de 1 TB.
- Si ponemos los cuatro discos en RAID 5, los bloques de los ficheros se reparten por los cuatro discos, pero hay que incluir un bloque R que representa la redundancia (la paridad). La paridad se calcula para cada fila (el stripe que hemos visto). Este bloque no se usa durante la lectura (salvo fallo de un disco), pero sí durante la escritura, porque hay que actualizarlo. Los bloques R no se dejan en el mismo disco para evitar



# ALMACENAMIENTO EN RED: SAN Y SAN



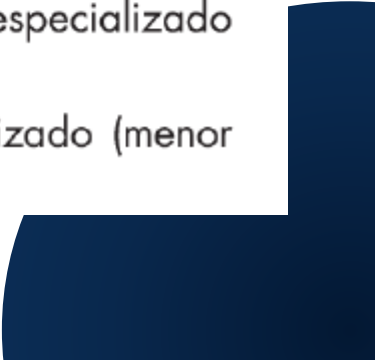
Hemos visto que podemos mejorar el rendimiento y la fiabilidad del almacenamiento de un ordenador conectando varios discos y configurándolos en RAID.

Pero en las empresas se suele trabajar en equipo, compartiendo ficheros entre varios ordenadores. Tenemos que pensar cómo compartir ficheros y cómo hacerlo con seguridad (quién puede leer esos ficheros y quién puede modificarlos, borrarlos o incluir nuevos).

Aunque en el caso práctico 4 veremos cómo se hace en un ordenador de un puesto de trabajo, no es la solución más recomendable porque:

- Hacer de servidor de ficheros afectará al rendimiento de sus aplicaciones (Office, Chrome), y viceversa.
- Estaríamos pendientes de si la otra persona lo ha apagado al salir de la oficina (y puede que estemos en edificios diferentes).
- Es un ordenador personal, luego es probable que no disponga de RAID ni copias de seguridad.
- Estamos expuestos a que un virus entre en ese ordenador y borre todo.

Por tanto, lo mejor es ponerlo en un servidor dedicado y, a ser posible, especializado en almacenamiento. De esta manera:

- Podemos instalar el software estrictamente necesario y tenerlo actualizado (menor riesgo de infecciones).
- 

# ALMACENAMIENTO EN RED: SAN Y SAN

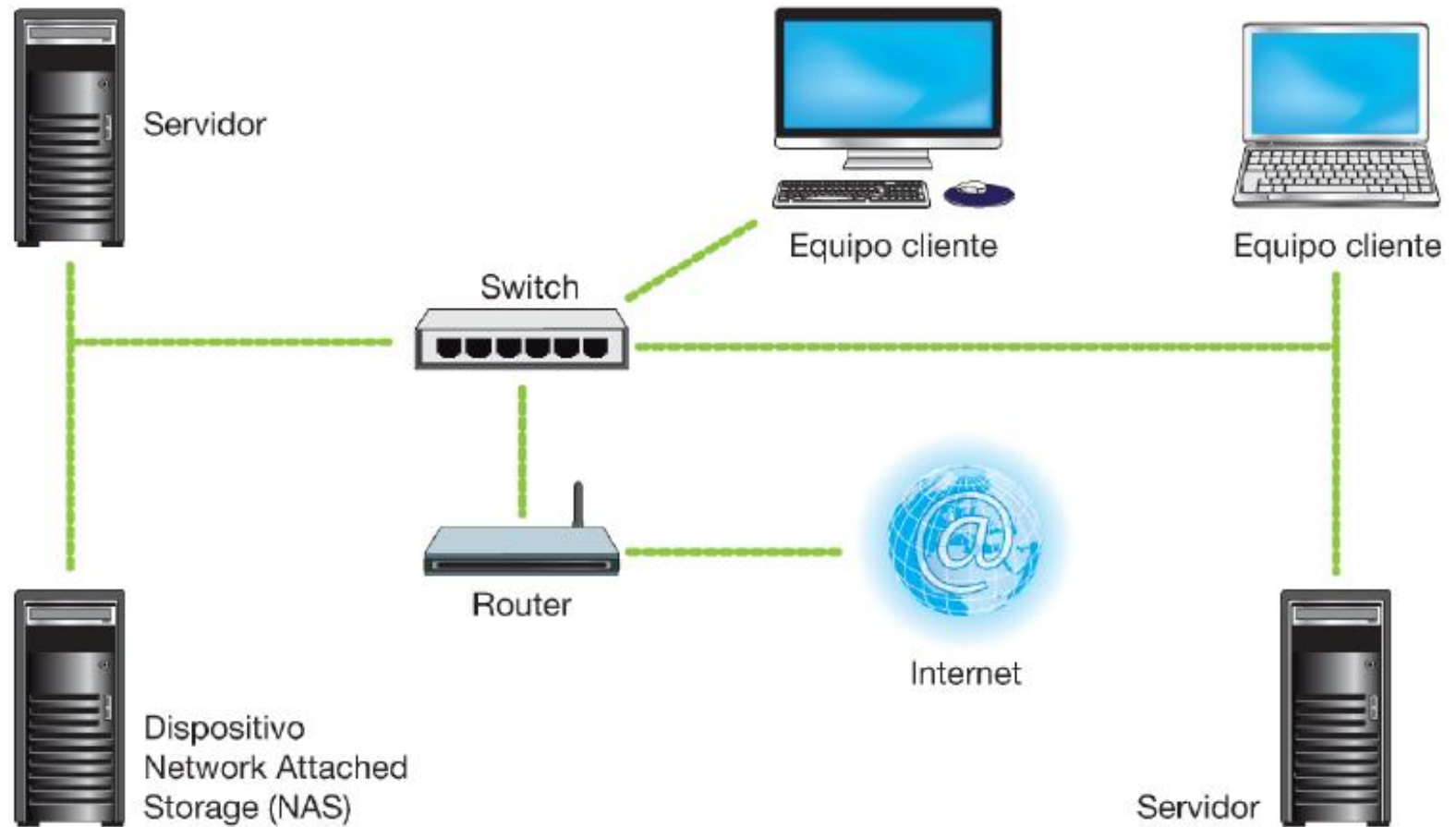


- Estará bajo la supervisión del personal del CPD (centro de proceso de datos), lo que garantiza estar encendido todo el tiempo, formar parte de la política de copias de seguridad de la empresa, detectar cuando el disco está próximo a llenarse, etc.
- Si, además, es un servidor especializado en almacenamiento, dispondrá de hardware suficiente para desplegar configuraciones RAID, una memoria caché de alto rendimiento, etc.

En el caso práctico 4 hemos visto que un equipo de la red ofrece disco a otros equipos conectados a ella. Es lo que se conoce como **NAS** (Network Attached Storage, almacenamiento conectado a la red). En ese esquema tenemos un equipo con almacenamiento local (una carpeta del escritorio, como hemos visto) que desea ofrecerlo a otros equipos de la red. Este equipo servidor ejecutará un determinado software servidor que responde a un determinado protocolo. Aquel equipo que necesite acceder a esa carpeta compartida, ejecutará un software cliente capaz de interactuar con el servidor de acuerdo con el protocolo del servidor (Fig. 4.49). Como la mayoría de los equipos de usuario son Windows, el protocolo más común es CIFS (Common Internet File System), que es una evolución de SMB (Server Message Block). En el caso práctico 5 probaremos distintos servidores CIFS.



# ALMACENAMIENTO EN RED: SAN Y SAN








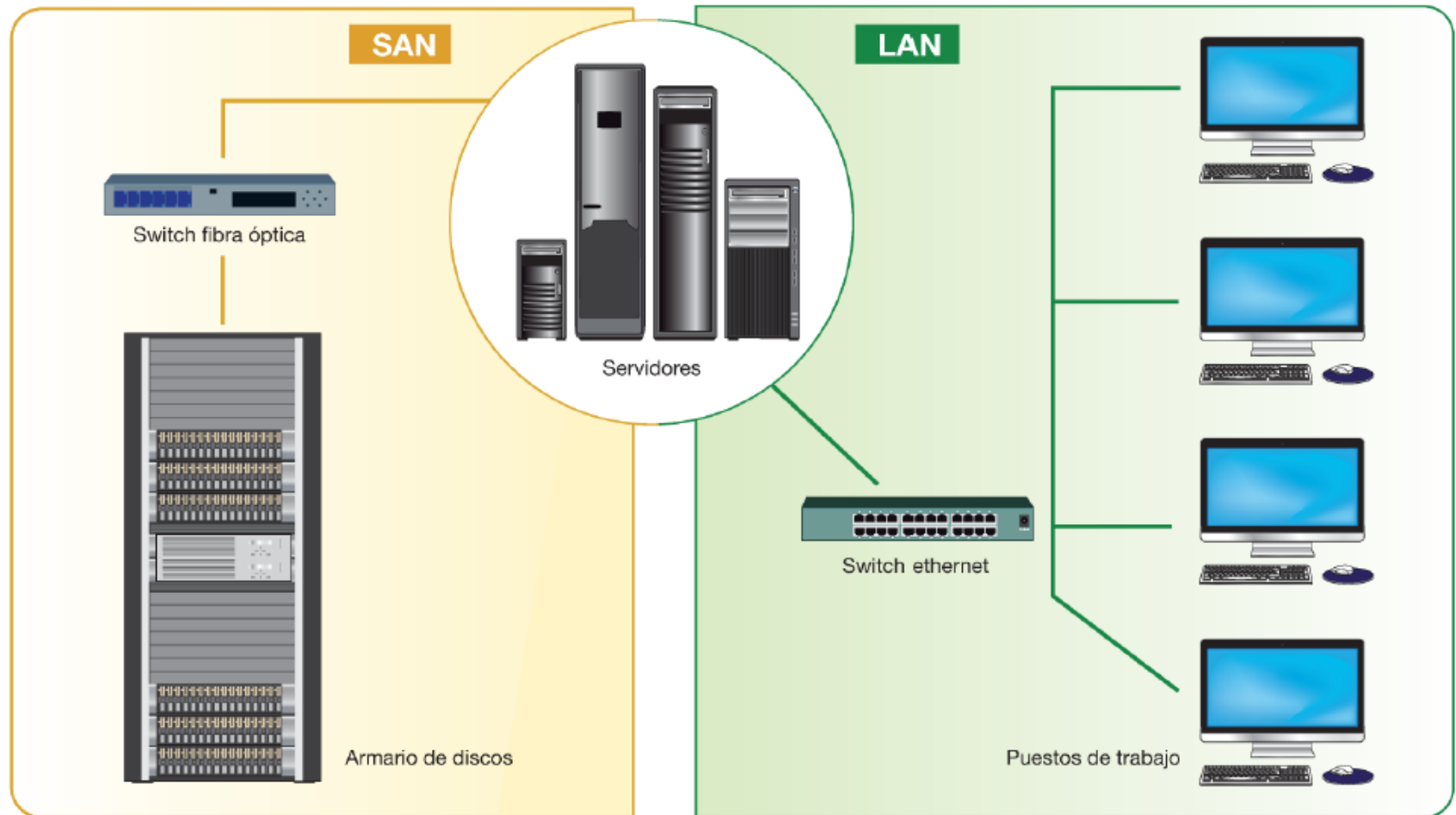
## ALMACENAMIENTO EN RED: SAN Y SAN



En un entorno privado puede ser suficiente con un pequeño equipo que haga de servidor NAS; pero en un entorno empresarial necesitamos mucho más rendimiento y seguridad, por lo que el equipo servidor necesitará potencia de procesamiento, amplia memoria caché, tarjetas de red de alta capacidad y configuraciones RAID. Si otros servidores también lo necesitan, seguramente optaremos por una solución **SAN** (Storage Area Network). En un SAN los discos están en lo que se llama un «armario», donde se realiza la configuración RAID. El armario dispone de cachés de alto rendimiento para reducir los tiempos de operación (Fig. 4.50). Los servidores se conectan al armario mediante conmutadores de fibra óptica (por eso hablamos de network). La configuración de los armarios es flexible: para cada equipo se pueden asignar unos discos concretos y reservarle cierta cantidad de caché. Y cambiarlo cuando sea necesario.



# ALMACENAMIENTO EN RED: SAN Y LAN





FUNDACIÓN DE EDUCACIÓN SUPERIOR

**SAN JOSÉ**

INSTITUCIÓN TECNOLÓGICA

FIN DE  
GRABACIÓN