

4

ORGANIZACIÓN Y GESTIÓN DE LA INFORMACIÓN

En este capítulo se estudiará todo lo concerniente a la persistencia de la información en un sistema informático. Se estudiarán los sistemas de archivo de un sistema operativo y cómo implementarlos ya sea con particionamiento clásico, protección RAID, gestión de volúmenes lógicos, etc. Además de estos conceptos se verán las políticas de salvaguarda y de seguridad para que el sistema además de eficiente sea seguro frente a cualquier circunstancia.

4.1 SISTEMAS DE ARCHIVO

El objetivo de un sistema de archivos es el gestionar los ficheros almacenados generalmente en un dispositivo físico como un disco duro, unidad SSD, *pendrive*, etc. El sistema de archivos mantiene unas estructuras internas para mantener organizados los ficheros de forma eficiente y para que el acceso a los mismos sea rápido.

El sistema de archivos es el responsable de gestionar el espacio en los diferentes dispositivos organizando ficheros y directorios en ellos y llevando un control de qué zonas del dispositivo están en uso y cuáles no. Si no se hace una gestión eficiente del espacio se generará fragmentación (es cuando el espacio sin utilizar no está contiguo). La fragmentación provoca una mala gestión del espacio en el dispositivo e incluso una pérdida de eficiencia del sistema cuando se reorganizan los ficheros para eliminarla.

Otra función importante de los sistemas de archivos es el control de acceso a los mismos. El sistema de archivos debe tener mecanismos para permitir o no el acceso a usuarios o grupos de usuarios dependiendo de los derechos que tengan sobre dichos archivos o directorios. Estos mecanismos utilizarán ACL o listas de control de accesos, permisos de ficheros en forma de bits como en Unix, u otro sistema. En ocasiones, los sistemas de archivo además de mecanismos de control de accesos, utilizan la encriptación para cifrar el contenido del fichero en un intento de mejorar la seguridad del sistema.

Los sistemas de archivo también son responsables de mantener la integridad de la información. Deben tener mecanismos para preservar la integridad del sistema de archivos para que en el caso en que pérdidas de conexión, reseteos del equipo, pérdidas de tensión, fallo del dispositivo, cuelgues en los programas, etc., no dejen los datos del archivo o del sistema de archivos corruptos o dañados y se pierda la información.

Existen muchos sistemas de archivos dependiendo de dónde reside la información de los mismos. Por ejemplo:

■ **Sistemas de archivos de disco.** Son los más utilizados. Están pensados para que múltiples procesos accedan a una zona concreta del fichero sin importar la ubicación exacta en el disco. Estos sistemas de ficheros están diseñados para que trabajen de forma eficiente e incluso se puedan anticipar a los datos que los procesos puedan demandar. Los sistemas de archivos más utilizados son FAT, NTFS, EXT, ReiserFS o HFS+. A continuación se verán en detalle los más utilizados:

- **FAT16.** También es conocido como FAT. Permite trabajar con particiones de hasta 2 GB, las unidades de asignación son de 32 KB, el tamaño máximo de archivo es de 2 GB y no distingue entre mayúsculas y minúsculas para nombres de archivo o directorio. Es reconocido por la práctica totalidad de los sistemas operativos.

- **FAT32.** Permite trabajar con archivos de hasta 4 GB y con particiones de más de 2 GB. La unidad de asignación es de 4 KB. El tamaño máximo de partición es de 2 TB. No distingue entre mayúsculas y minúsculas para nombres de archivo o directorio.
 - **NTFS.** Sus volúmenes pueden llegar hasta los 16 EB al igual que el tamaño máximo del archivo, sin embargo la implementación actual es de 256 TB y 16 TB respectivamente. Distingue entre mayúsculas y minúsculas en los nombres de archivo y directorio. El tamaño de la unidad de asignación varía, dependiendo del tamaño de la partición desde los 4 KB a 64 KB.
 - **EXT3.** También conocido como Sistema de Archivos Extendido 3. El tamaño máximo de la partición es de 32 TB y el tamaño máximo de archivo es de 2 TB. Distingue entre mayúsculas y minúsculas para nombres de archivo y directorio. Es propio de sistemas operativos Linux.
 - **EXT4.** También conocido como Sistema de Archivos Extendido 4. Permite particiones de hasta 1 EB y archivos de hasta 16 TB. Distingue entre mayúsculas y minúsculas en los nombres de archivo y directorio. Es utilizado actualmente por muchos sistemas operativos Linux.
 - **HFS+ (*Hierarchical File System Plus*).** También conocido como Sistema Jerárquico de Archivos Extendido. El tamaño máximo de una partición es de 16 EB y el tamaño máximo de archivo es de 8 EB. Es el empleado por los sistemas operativos de Apple.
- **Sistemas de archivos de discos ópticos.** Estos sistemas de archivos son utilizados en CD, DVD y discos Blu-ray. Los más utilizados son ISO 9660 y el UDF (*Universal Disk Format*).
 - **Sistemas de archivo de cintas.** Son sistemas de archivos muy particulares debido a la naturaleza de las cintas. Al ser un sistema de almacenamiento secuencial los accesos aleatorios llevan más tiempo que en los discos tradicionales puesto que implica el rebobinar la cinta para colocar la cabeza lectora sobre el punto exacto donde se va a leer o escribir.
 - **Sistemas de archivo de red.** Los archivos en los sistemas de ficheros en red generalmente están distribuidos en uno o varios puntos de una red local en los que un cliente accede a los ficheros proporcionados por un servidor. Para el acceso a dichos ficheros se necesitarán protocolos como NFS o SMB.

4.1.1 NOMENCLATURA Y CODIFICACIÓN

Generalmente los archivos suelen constar de un nombre y una extensión separadas por un punto (por ejemplo datos.txt). La extensión, que es algo que viene de los tiempos del MS-DOS, suele tener tres caracteres e identifica el contenido del archivo. Por ejemplo un archivo txt suele contener texto mientras que un fichero exe identifica un fichero binario ejecutable. En algunos sistemas de archivos como en Unix, la extensión no es necesaria.

En algunos sistemas la longitud del nombre del archivo no puede sobrepasar un cierto límite y generalmente se impide que formen parte del nombre ciertos caracteres como “*”, “/”, “\”, “:”, “&”, etc.

En cuanto a la **codificación** de los archivos existen distintos sistemas para codificar la información en un archivo. A continuación se describen los más utilizados:

- **ASCII.** El código ASCII ha sido durante mucho tiempo el más empleado. Inicialmente era un código que utilizaba 7 bits para representar texto, lo que significaba que era capaz de codificar 127 caracteres. Por ejemplo el número 65 (1000001 en binario) se utiliza para representar la “A”. Poco después surgió un problema: este

código es suficiente para los caracteres de la lengua inglesa, pero no para otras lenguas. Entonces se añadió el octavo bit para representar otros 128 caracteres que son distintos según idiomas (Europa Occidental usa unos códigos que no utiliza Europa Oriental), llamándose así ASCII Extendido.

- **Unicode.** Unicode es una ampliación del código ASCII que puede utilizar hasta 4 *bytes* (32 bits) para representar cada carácter, con lo que es capaz de codificar cualquier símbolo en cualquier lengua del planeta utilizando el mismo conjunto de códigos.
- **UTF-8.** Es un formato que es capaz de representar cualquier carácter Unicode y que al incluir la especificación US-ASCII de 7 bits puede codificar cualquier información ASCII sin cambios. Se suele utilizar también mucho en la codificación de páginas web y *email*. Tiene ventajas al ahorrar espacio de almacenamiento en textos con caracteres latinos.
- **Binario.** Se utilizan los ficheros binarios para almacenar información de cualquier tipo. En binario se pueden almacenar textos, imágenes, sonido, vídeo, datos, etc. Generalmente los ficheros binarios suelen contener una cabecera en la que hay una serie de datos o información para poder interpretar el resto del fichero. Si el fichero carece de esta cabecera se denomina archivo binario plano.

4.1.2 JERARQUÍAS DE ALMACENAMIENTO

Según las características de las memorias y los propósitos para los cuales han sido desarrolladas, los medios de almacenamiento se pueden clasificar de forma jerárquica en distintos niveles. A esta clasificación se la ha denominado “jerarquía de memorias”.



Figura 4.1. Jerarquía de memorias

- **Nivel 0: Registros.** Los registros son memorias muy veloces pero con poca capacidad, los cuales están integrados en el procesador. Estos registros almacenan datos transitorios utilizados por el procesador, generalmente resultados de operaciones matemáticas. Los valores muy utilizados también son objeto de almacenar en registros del procesador.
- **Nivel 1: Memoria caché.** La memoria caché es una memoria intermedia que se coloca entre un elemento rápido y otro más lento del equipo. Generalmente cuando se habla de memoria caché nos referimos a la memoria existente entre la memoria principal y el procesador. El objetivo de esta memoria es almacenar copia de datos situados en memoria principal los cuales o son muy utilizados o se prevé que van a ser utilizados en un futuro. Generalmente cuando se accede a un dato, este se coloca en la memoria caché. La segunda vez que se acceda a dicho dato no hará falta acceder a la memoria principal puesto que el dato ya lo tenemos en la caché.

El procesador, antes de escribir o leer de memoria siempre va a mirar en la memoria caché por si una copia del dato está en ella. Si el dato está en caché las operaciones se realizan mucho más rápido puesto que la memoria caché es mucho más rápida que la memoria principal.

La caché generalmente utiliza tecnología SRAM (*static RAM*) la cual es más rápida que la tecnología utilizada en la memoria principal.

En los discos duros también hay una memoria caché que funciona de modo análogo a la caché situada entre la RAM y el procesador. Esta memoria caché no utiliza SRAM, la cual es muy cara, utiliza la misma tecnología que en la memoria RAM tradicional.

- **Nivel 2: Memoria RAM o principal.** La memoria RAM es la insertada en el *slot* de la placa base. Está presente en muchos elementos internos del equipo y es mucho más rápida que la memoria secundaria o disco duro. Posteriormente se estudiará la memoria RAM en profundidad.
- **Nivel 3: Disco duro.** Este nivel se suele denominar almacenamiento secundario. En este nivel se incluye el mecanismo de memoria virtual el cual utiliza espacio en disco para gestionar la memoria.
- **Nivel 4: Almacenamiento externo en redes.** El almacenamiento en red se está popularizando mucho dado que el crecimiento y mejora de las redes en cuanto a velocidad y prestaciones lo hace posible. Actualmente las necesidades con respecto a la información son que sea accesible desde cualquier dispositivo y cualquier lugar, lo que implica que tengamos que almacenar los datos en la red.

Los sistemas más populares y generalmente más económicos que se han estado utilizando desde hace tiempo son los NAS (*Network Attached Storage*). En estos sistemas los datos residen en un servidor el cual los comparte con el resto de la red (casi siempre TCP/IP). Muchas veces se denomina NAS a un equipo servidor (ordenador convencional) con un sistema operativo Linux o Windows®. No obstante, los auténticos NAS son dispositivos dedicados específicamente diseñados a tal fin. Entre los protocolos más utilizados por los NAS están el NFS y el CIFS (de Microsoft®).

Últimamente se está popularizando mucho el almacenamiento en la nube. Con el almacenamiento en la nube lo que se hace es almacenar nuestros datos en un servidor externo de Internet con lo cual se puede recuperar dicha información con cualquier dispositivo o compartirla con otras personas.

Quizás la aplicación más utilizada de almacenamiento en la nube actualmente es Dropbox. La instalación y utilización de Dropbox es sumamente sencilla e intuitiva. La aplicación funciona para las plataformas más usuales (Linux, Windows®, Android, Mac OS X®, iPhone, iPad® o Blackberry®). Una vez instalado Dropbox se crea una carpeta en la cual se pueden almacenar documentos los cuales estarán en la nube sincronizándose también en local, pudiendo ser utilizados por otros usuarios o dispositivos. Además de Dropbox existen muchas otras aplicaciones similares como Box, Ubuntu One, iDrive, SOS Online *Backup*, Zumo drive, ADrive, etc.

4.1.2 MIGRACIONES Y ARCHIVADO DE DATOS

Las migraciones de datos se realizan cuando hay que traspasar datos de un sistema a otro. Cada migración es un mundo y por ello hay que planear de una forma concienzuda la misma. Generalmente las migraciones de datos se hacen entre una base de datos de un sistema y la base de datos de otro sistema.

Existen muchos tipos de migraciones de datos. Algunos tipos de migraciones son los siguientes:

- **Traslado del sistema a otra máquina más potente** con el mismo gestor de base de datos. En ese caso las mismas herramientas de *backup* y restauración o exportación e importación del propio gestor de bases de datos pueden servir para realizar la migración.
- **Migración por upgrade o mejora de la base de datos.** En ocasiones se migra de una base de datos en Access o ficheros ASCII a una base de datos de más entidad como Oracle, Informix, MySQL, SQLServer, etc. En ese caso la migración implica el tener que crear una nueva base de datos con los requisitos de la base de datos previa. Para ello, habrá que realizar un análisis a fondo del sistema previo antes de la migración.
- **Migración entre distintos gestores de bases de datos.** En este caso puede ser de bastante utilidad estudiar a fondo el esquema de la base de datos origen. Si se puede disponer de ambos gestores de bases de datos, se pueden realizar todo tipo de pruebas de verificación de una forma sencilla antes de poner el nuevo sistema en producción.

Algunas cuestiones a tener en cuenta al hacer una migración son las siguientes:

- **Antes.** Analizar a fondo los datos de origen y analizar el nuevo sistema, más si cabe si alguno de los sistemas que se va a migrar está en producción y los datos no son estáticos.
- **Durante.** Convertir o adaptar tipos de datos verificando que los valores que se vayan a grabar en la nueva base de datos son los que se necesitan. Cuidado con los espacios en blanco, tabuladores o caracteres extraños que puedan aparecer por culpa de la migración. En ocasiones hay que deshabilitar *triggers* o también restricciones que puedan impedir el correcto proceso de migración.
- **Después.** Realizar pruebas para verificar que la totalidad de registros en origen se ha copiado en el sistema destino. Estas pruebas tienen que estar previstas de antemano. Generalmente estas pruebas consisten en su mayor parte en conteos de registros en origen y destino. Hay que prever mecanismos de vuelta atrás o de emergencia por si la migración no concluye de forma exitosa.

Sobre el archivado de datos, decir que hay que tener mucho cuidado con los *backups* puesto que uno de los mayores errores de seguridad se cometen cuando se descuida su correcta custodia. En ocasiones acceder al fichero y enviarlo por Internet mediante correo electrónico u otro sistema es una práctica fácil y común.

Además, el concepto de archivado implica el almacenar datos que no sean actuales o no se van a utilizar de forma habitual (por ejemplo las facturas de dos años hacia atrás). Lo más normal es que para este tipo de prácticas se utilice un software de archivado de datos más que un software de *backup*. Aunque parecen diferentes no son lo mismo. El software de archivado de datos está específicamente diseñado tanto para archivar datos como para recuperar datos según unos criterios determinados.

Existen muchos software en el mercado de archivado de datos. Algunos son StorNext FX™, Autonomy Zantaz™, Iron Mountain™, Mimosa™, NearPoint™ o Enterprise Vault™ entre otros.

4.2 VOLÚMENES LÓGICOS Y FÍSICOS

En este apartado se estudia todo lo concerniente al almacenamiento físico de un sistema operativo. Se comenzará estudiando el particionamiento para luego ver conceptos interesantes como la gestión de volúmenes lógicos o los sistemas RAID.

4.2.1 PARTICIONAMIENTO

Prácticamente todos los discos incluso los dispositivos con memoria *flash* se pueden particionar.

Existen tres tipos de particiones principales:

- **Primaria.** Suelen utilizarse para instalar los sistemas operativos aunque también los sistemas operativos pueden instalarse en una partición lógica. Como mucho un disco puede tener hasta 4 particiones primarias.
- **Extendida.** Las particiones extendidas pueden albergar particiones lógicas.
- **Lógica.** Son particiones “secundarias” por así decirlo. Su finalidad en muchas ocasiones es almacenar información.

Las particiones extendidas son necesarias, porque si no un disco solamente podría tener 4 particiones.

En el particionamiento se siguen una serie de reglas y limitaciones que se van a ver a continuación:

- **Regla 1:** un disco solo puede tener hasta 4 particiones primarias.
- **Regla 2:** las particiones extendidas cuentan como si fueran particiones primarias.
- **Regla 3:** no puede existir más de una partición extendida.
- **Regla 4:** dentro de una partición extendida pueden existir una o varias particiones lógicas.

PRÁCTICA 4.1



Pregunta: ¿Puedo tener un disco con 2 particiones primarias y 2 extendidas?

Respuesta: No, según la regla 3 no puede existir más de una partición extendida.

Pregunta: ¿Puedo tener un disco con 2 particiones primarias y 5 lógicas?

Respuesta: No, puesto que no existe ninguna partición extendida.

Pregunta: ¿Puedo tener en un disco 3 particiones primarias, 1 partición extendida y 4 particiones lógicas?

Respuesta: Sí, siempre que las particiones lógicas estén dentro de la partición extendida.

Pregunta: ¿Puedo tener en un disco 7 sistemas de archivos diferentes o repetidos?

Respuesta: Sí. El disco anterior podría tener todos esos sistemas.

Para particionar o modificar las particiones de un disco es preciso utilizar una herramienta de particionado. En sistemas Linux, GParted es una de las herramientas más utilizadas.

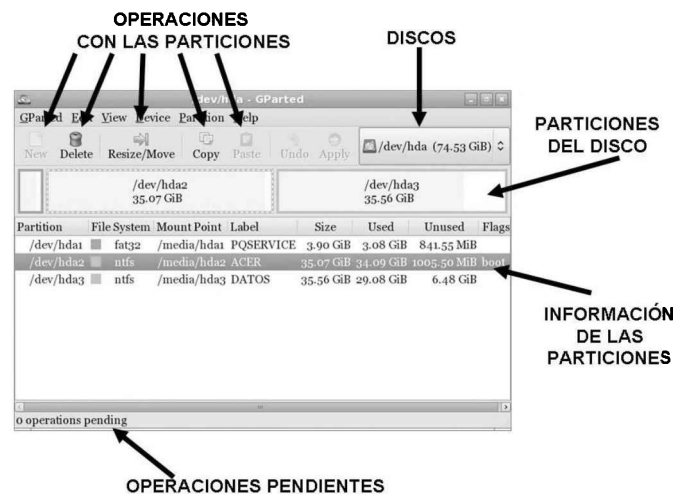


Figura 4.2. Utilidad de particionamiento GParted

4.2.1.1 Las particiones activas

Las particiones primarias son las utilizadas para instalar los sistemas operativos. Si un equipo no tiene ninguna partición activa, al arrancar dará un fallo. El sistema operativo de la partición activa será el que se cargue al arrancar desde el disco duro.

4.2.1.2 El sector de arranque

Un disco se compone de un sector de arranque y una serie de particiones y opcionalmente espacio sin particionar.

El sector de arranque es el primer sector del disco (cabeza 0, cilindro 0 y sector 1). Dentro de él está la tabla de particiones y el Master Boot o gestor de arranque. Este programa lee la tabla de particiones y cede el control al sector de arranque de la partición activa. Como se ha dicho antes si no hay partición activa, el equipo da un error al arrancar.

ESTRUCTURA DEL MASTER BOOT RECORD

446 Bytes – Código máquina (gestor de arranque o Boot manager)
64 Bytes – Tabla de particiones
2 Bytes – Firma de unidad arrancable ("055AAh" en hexadecimal)

Primer sector físico del disco. Tamaño 512 Bytes

Figura 4.3. Estructura del MBR

El sector de arranque tiene 512 bytes ($446 + 64 + 2 = 512$) como se puede observar en la figura anterior.

4.1.2 SISTEMAS NAS Y SAN

Los servidores de almacenamiento masivo suelen emplearse en redes de área de almacenamiento concebidas para conectar servidores y arrays de discos. Existen distintas tecnologías para dar soporte a este tipo de redes como veremos a continuación.

Los Sistemas de Almacenamiento son fundamentales en los sistemas informáticos ya que serán los encargados de dar soporte a toda la información con la que trabajan. Existen diferentes tecnologías de almacenamiento entre las que destaca **NAS**.

4.2.2.1 Los sistemas NAS

El servidor NAS (*Network Attached Storage*) es un tipo de servidor de almacenamiento que da servicio a través de una red mediante el uso de protocolos estándar de comunicaciones como TCP/IP.

Es un modelo válido y necesario para sistemas que impliquen crecimiento y tamaño (escalabilidad).

Requieren altas prestaciones en accesos a disco y comunicaciones de red.

Emplean array de discos o *disk array*, conectados a la red de forma que todos los datos del sistema están asociados al dispositivo NAS y pasan por el mismo, constituyendo un punto sensible a fallos. Son también sistemas de alta disponibilidad.

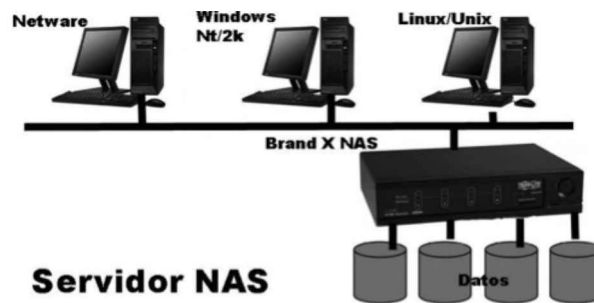


Figura 4.4. Servidor NAS

Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Normalmente, estos dispositivos están dispuestos en **RAID** (*Redundant Arrays of Independent Disks*).

NAS es muy útil para proporcionar el almacenamiento centralizado a ordenadores clientes en entornos con grandes cantidades de datos.

NAS puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web para proveer servicios de almacenamiento. El crecimiento del mercado potencial para NAS es el mercado de consumo donde existen grandes cantidades de datos multimedia.

El precio de las aplicaciones NAS ha bajado en los últimos años, ofreciendo redes de almacenamiento flexibles para el consumidor doméstico con costos menores de lo normal, con discos externos USB.

4.2.2.2 Los sistemas SAN

Los servidores SAN (*Storage Area Network*) son servidores de almacenamiento que dan servicio a través de una red y emplean acceso a través de fibra óptica no admitiendo enrutamientos.

Se emplean en sistemas de prestaciones muy elevadas, con alta velocidad de datos y crecimiento casi ilimitado (hasta 16 millones de dispositivos) y en acceso a discos y comunicaciones. Además permiten una escalabilidad y crecimiento más sencillos que en NAS pero más caros. Admiten grandes distancias de hasta 10 Km entre equipos.

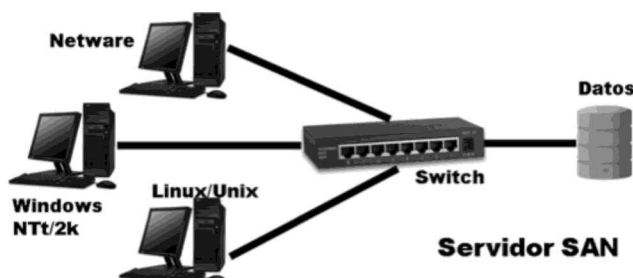


Figura 4.5. Servidor SAN

4.2.2.3 Gestión de volúmenes lógicos

La gestión de volúmenes lógicos es una solución para virtualizar el almacenamiento. Con la gestión de volúmenes lógicos se cambia el sistema tradicional de discos y particiones a una estructura más flexible.



Linux ofrece un gestor de volúmenes lógicos llamado Logical Volume Manager (LVM). LVM fue escrito originalmente por Heinz Mauelshagen en 1998 y ofrece las características típicas de cualquier gestor de volúmenes lógicos.

Antes de comenzar a ver la gestión de volúmenes lógicos hay que tener claros ciertos conceptos:

- **Número de unidad lógica o LUN (Logical Unit Number).** Un LUN es un número que identifica una unidad lógica utilizado por el protocolo SCSI. Generalmente suele utilizarse para referirse a un disco lógico creado en un SAN aunque también se utiliza en unidades de cinta.
- **Volumen físico (VF) o Physical Volume (PV).** Un volumen físico puede ser un disco, una partición de un disco, un LUN, un dispositivo RAID (ya sea por software o por hardware). En grandes servidores no es raro ver volúmenes físicos como un grupo de discos conectados a una tarjeta controladora en RAID, ya sea para aumentar el rendimiento, para aumentar la seguridad o para ambas cosas. Generalmente en servidores no suelen utilizar RAID software sino RAID hardware.

- **Área física (AF) o Physical Extent (PE).** Un volumen físico está dividido en áreas físicas. Generalmente todas estas áreas físicas tienen el mismo tamaño aunque en algunos sistemas el tamaño puede ser variable.
- **Área lógica (AL) o Logical Extent (LE).** Un área lógica generalmente se corresponde con un área física. En el caso en que un área lógica se corresponda con varias áreas físicas de distintos volúmenes físicos se está creando una especie de redundancia.

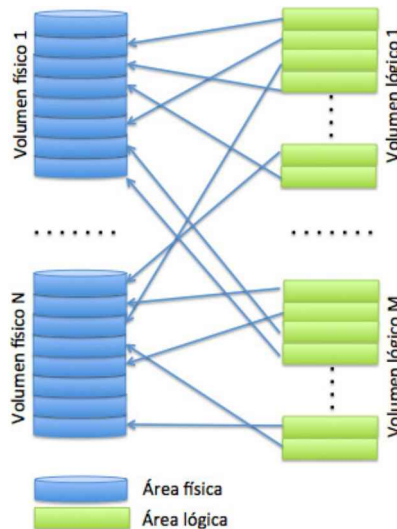


Figura 4.6. Relación entre volúmenes físicos y lógicos



Mapeo entre áreas físicas y lógicas

Generalmente el mapeo es uno a uno, esto quiere decir que un área física se corresponde a un área lógica. Con *mirroring* o RAID en espejo un área lógica se corresponderá con dos o más áreas físicas de discos separados. De esta forma, un grupo de áreas físicas puede corresponderse a un grupo de discos en RAID 1.

- **Volumen lógico (VL) o Logical volume (LV).** Un volumen lógico es un grupo de áreas lógicas. Estos volúmenes lógicos funcionan como una partición de un disco duro. Se pueden montar sistemas de archivos en ellos o utilizarlos como partición de *swap*. Cada volumen lógico representa un espacio consecutivo de almacenamiento (aunque físicamente no esté contiguo).
- **Grupo de volúmenes (GV) o Volume Group (VG).** Se trata de un grupo de varios volúmenes físicos que se corresponden con un conjunto de áreas físicas, áreas lógicas y volúmenes lógicos. Estos siempre pertenecen a un conjunto de volúmenes y no pueden intercambiarse entre distintos grupos de volúmenes si existieran. Los conjuntos de volúmenes se utilizan para realizar gestiones administrativas independientes sobre ellos como ponerlos *online* u *offline*.

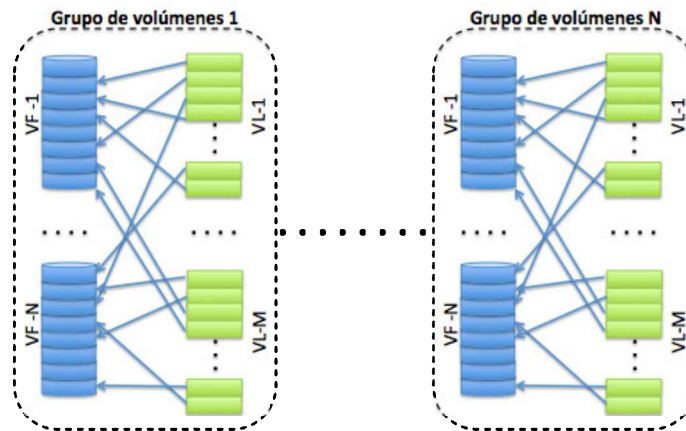


Figura 4.7. Conjunto de grupos de volúmenes



Crecimiento de volúmenes lógicos

Los volúmenes lógicos pueden agrandarse y encogerse cogiendo más áreas físicas o dejándolas en el grupo de áreas físicas no asignadas. Al no tener que estar las áreas físicas contiguas, un volumen lógico no tiene que moverse ni nada por el estilo.

Cuando se modifica el tamaño de un volumen lógico hay que cambiar también el tamaño del sistema de ficheros que reside sobre él. Existen sistemas de ficheros que pueden ajustarse on-the-fly como el ext3 y ext4 y de esa manera no se interrumpen los procesos que están almacenados en él.

- **Instantáneas o snapshots.** Las instantáneas lo que hacen es tomar como una fotografía de un volumen lógico en un momento dado. Haciendo un *snapshot* lo que se obtiene es una réplica del volumen lógico. Las instantáneas son muy útiles cuando se quiere hacer por ejemplo una actualización de un sistema operativo o un *backup* de una base de datos. Si se quiere hacer una actualización de un sistema operativo se toma una instantánea, se monta y se prueba la nueva actualización. Si no gusta el resultado se desmonta y se vuelve a montar el volumen lógico original. En versiones anteriores de LVM, las instantáneas eran solamente de lectura, actualmente las instantáneas son de lectura/escritura.

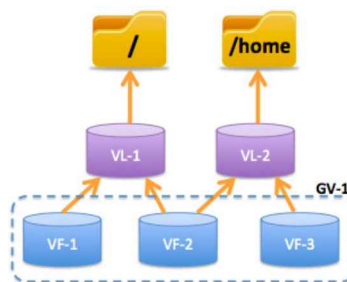


Figura 4.8. Configuración de un gestor de volúmenes lógicos

El montaje de un gestor de volúmenes lógicos no es un procedimiento muy complejo, simplemente basta con seguir los siguientes pasos:

- Primero se borran las tablas de particiones y se inicializan las particiones de los discos a utilizar. De esa manera se crean los volúmenes físicos (VF).
- Una vez creados los volúmenes físicos se crea el grupo de volúmenes (GV) que contendrá los volúmenes físicos inicializados anteriormente.
- El siguiente paso es crear los volúmenes lógicos, para ello se incluirán en los volúmenes lógicos el grupo de volúmenes o los volúmenes físicos que sean requeridos.
- Por último, habrá que crear un sistema de ficheros sobre el volumen lógico y montarlo para que esté disponible.

4.2.3 ACCESO PARALELO

En un sistema operativo multitarea generalmente existen muchos procesos ejecutándose al mismo tiempo. Eso implica que la probabilidad de que un fichero sea accedido por varios procesos es alta. Si todos los procesos se coordinasen a la hora de acceder a un mismo fichero no habría problemas pero como se sabe que esto no existe, el sistema operativo debe crear mecanismos para permitir un uso eficiente en el acceso a los ficheros.

Imaginemos por qué es importante la coordinación en el acceso concurrente a ficheros:

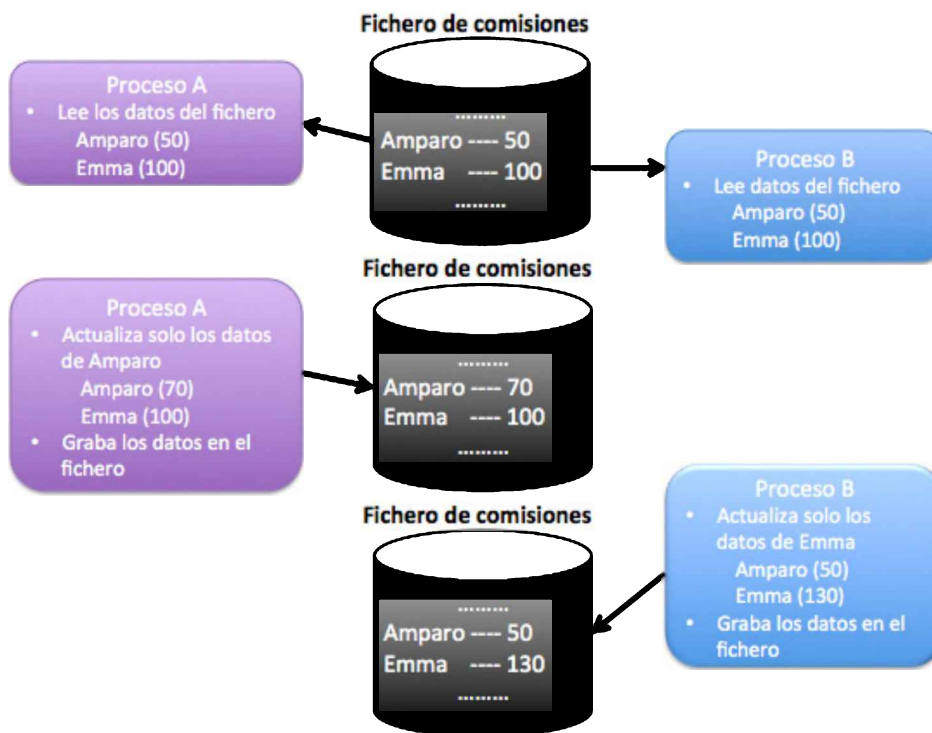


Figura 4.9. Problema del acceso concurrente a ficheros

Imaginemos que en una compañía existe un sistema de incentivos según el volumen de ventas que hagan sus comerciales. Al comienzo del día Amparo lleva ganados 50 euros en comisiones y Emma 100. Amparo realiza una venta y existe un proceso en el sistema para actualizar sus comisiones (ha ganado 20 euros más en comisiones) mientras que en ese mismo instante Emma realiza otra venta y automáticamente incrementa sus comisiones en 30 euros. Se lanzan dos procesos de actualización de comisiones de tal manera que el primero actualiza los datos de Amparo mientras que el segundo actualiza los datos de Emma.

Al terminar el segundo proceso, se observa que los datos de Amparo no quedan actualizados puesto que el proceso B trataba con unos datos del fichero no actualizados y por lo tanto una persona perdería su comisión.

Una solución a todo puede ser implementar bloqueos en el acceso a los ficheros. El proceso A como va a actualizar los datos del fichero de comisiones tendrá que bloquear el fichero en exclusiva a la vez que procede a hacer la actualización de las comisiones de Amparo. Mientras tanto, el proceso B espera a que el proceso A desbloquee el fichero y una vez ocurrido esto actualizar los datos de Emma.

Los sistemas operativos tienen distintos mecanismos para proteger los datos en el acceso simultáneo a ficheros como pueden ser:

- Utilizar bloqueos para todo el fichero o partes de un fichero. Estos bloqueos pueden ser meramente informativos (como sucede en Unix o Mac OS®) o ser forzosos (como ocurre en Windows®).
- Deshabilitar la escritura, borrado o actualización de ficheros.
- Utilizar mecanismos de control de accesos para que no todos los usuarios del sistema puedan hacer cualquier operación sobre el fichero.
- Utilización de ficheros de bloqueo. En ocasiones, aplicaciones y programas utilizan ficheros de bloqueo para el control de acceso a recursos (generalmente ficheros con extensión *lock*). Cuando un proceso va a acceder a algún recurso u archivo, crea un fichero de bloqueo para avisar al resto de procesos de que ese recurso está siendo utilizado y lo borra cuando deja de utilizarlo.

4.2.3.1 ¿Puede realizarse un backup mientras se están haciendo accesos concurrentes a ficheros?

Igual que en las bases de datos existen los *snapshots* o fotografías del estado de unos datos en un momento determinado, algunos sistemas operativos ofrecen un mecanismo de *snapshot* de volumen. Esto quiere decir que el sistema operativo realiza como una especie de fotografía de los ficheros del volumen en un momento determinado, para que en el *backup* no se vayan grabando las actualizaciones de ficheros realizadas mientras que dure el *backup*.

4.2.4 PROTECCIÓN RAID

RAID es una tecnología que generalmente consiste en duplicar la información de un sistema en varios discos con el objetivo de que en el caso de fallo de uno de ellos, el sistema pueda seguir funcionando sin pérdida de información.

4.2.4.1 ¿Qué es la tecnología RAID?

RAID significa *Redundant Array of Inexpensive Disks* (matriz redundante de discos económicos). Es una matriz de discos compuesta de dos o más discos, los cuales no tienen por qué ser caros (podemos utilizar la tecnología SATA), y organizados de una forma “redundante”, lo cual indica que la información está repetida de alguna forma.

La repetición de esta información lo que implica es seguridad. Seguridad de que, en caso de que se estropee algún disco, la información no se pierda, pues está repetida. En el caso de fallo, el sistema puede seguir funcionando (en caso de que esté replicado por completo), cosa que no ocurre en un sistema en el que la información no esté repetida.

Los sistemas RAID se pueden implementar mediante:

- **Software:** es el sistema más económico, pero el menos eficiente. Normalmente se suele utilizar RAID para salvaguardar solamente los datos. El establecer RAID por software para salvaguardar el sistema operativo, por regla general, ralentiza mucho el sistema y los administradores no suelen optar por esta opción. No todos los sistemas operativos soportan RAID (Linux sí lo soporta y Windows Server® también).
- **Hardware:** es la forma más lógica de implementar RAID. De siempre se ha venido utilizando una tarjeta controladora conectada mediante un bus SCSI a discos SCSI con prestaciones mucho más altas que los discos normales (10.000-15.000 RPM frente a las 7.200 de los discos de un equipo de sobremesa), aunque actualmente existen controladoras integradas en las placas base que permiten realizar los métodos RAID más comunes con discos SATA, lo cual se convierte en algo más fácil de configurar y más económico.

Tipo de RAID	Ventajas	Limitaciones
RAID por software.	Bajo coste. Solo se requiere un sistema operativo correctamente configurado.	Mucho menos eficiente que el RAID por hardware. Bajo rendimiento del sistema.
RAID por hardware.	Más eficiente que el RAID por software. Menos carga de trabajo para el microprocesador.	Más costoso, aunque con una placa base que incorpore RAID los costes se reducen bastante (y también el rendimiento si es fake-RAID).

Tabla 4.1. Ventajas y limitaciones de los tipos de RAID software y hardware

4.2.4.2 RAID como complemento o no de las copias de seguridad

El administrador o responsable de sistemas que piense que RAID sustituye por completo las copias de seguridad está bastante equivocado.

RAID nos da la tranquilidad de que, ante cualquier fallo hardware, se puede recuperar el sistema de una manera ágil y rápida. De todas formas no previene sobre un borrado accidental de los datos, una corrupción de ficheros u otra desgracia parecida.

Por lo tanto, se deberán realizar copias de seguridad tanto si se utiliza RAID como si no se utiliza. RAID lo que da al administrador es una seguridad mayor ante cualquier posible fallo del hardware y la certeza de que el sistema puede seguir funcionando en menos tiempo.

4.2.4.3 Tipos de RAID

RAID 0 (*striping o duplexing*)

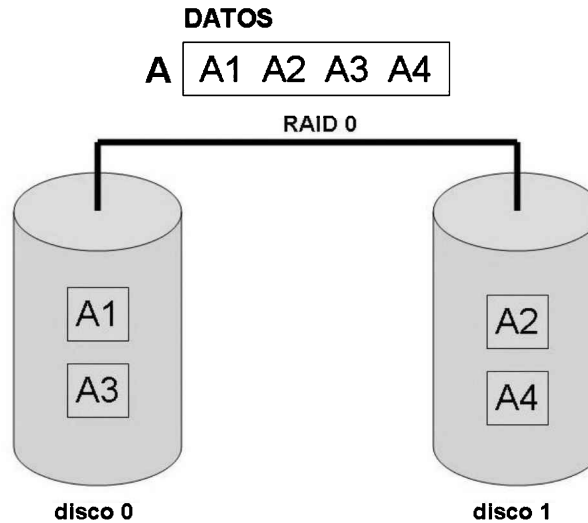


Figura 4.10. Esquema del RAID 0

Striping se puede traducir como entrelazado. En este caso no hay implementado ningún mecanismo de seguridad. La información se reparte en bloques por todos los discos que formen parte del *stripe*.

Se necesitan como mínimo dos discos.

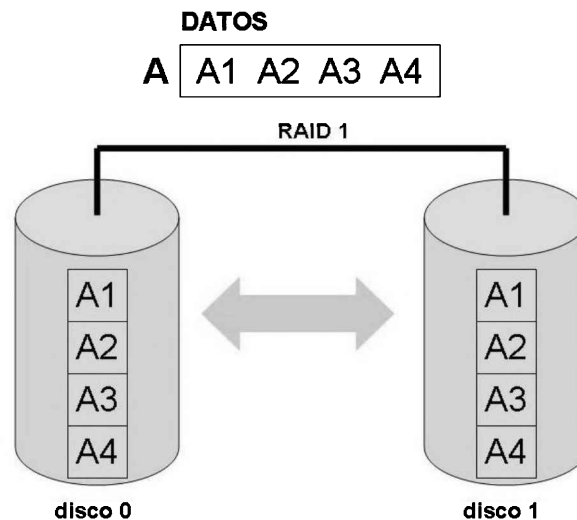
El objetivo es aumentar el rendimiento, pues escribir o leer a la vez en varios discos hace que aumente la velocidad de escritura y lectura.

No es aconsejable utilizar este sistema cuando un fallo en el sistema o una parada prolongada del mismo pueden representar un problema grave.



RECUERDA

La pérdida o error en un disco de RAID 0 implican la pérdida de la información en el sistema. Esta pérdida será definitiva salvo que la información se encuentre en algún *backup*.

RAID 1 (*mirroring*)*Figura 4.11. Esquema RAID 1*

RAID 1 o *mirroring* (discos en espejo) consiste en la duplicidad de los datos. Por cada disco presente en el sistema se tiene otro con la misma información de tal manera que, cuando un disco falla, el sistema puede seguir funcionando dado que la información permanece duplicada.

**RECUERDA**

Se pueden utilizar en RAID 1 discos de diferentes capacidades o velocidades. Al final la pareja de discos tendrá la velocidad del menor y la capacidad del menor. Aunque esto es posible, se aconseja utilizar discos exactamente iguales, de esa forma se evitarán problemas y se maximizará el rendimiento.

La sobrecarga u *overload* del sistema siempre será del 50%. Por cada disco se tendrá un disco extra, por lo tanto el sistema tendrá $2 \times n$ discos.

El rendimiento de lectura aumenta (hasta el doble como máximo) porque pueden leerse varios discos a la vez.

El rendimiento de escritura permanece constante.

RAID 2 (*bit striping + Hamming code*)

Utiliza una división de la información en bits por todos los discos del *stripe* y el código Hamming para la recuperación de errores.

RAID 2 no se utiliza debido a que existen sistemas más avanzados y eficientes como RAID 4 o 5.

RAID 3 (*byte striping* + *paridad*)

Utiliza una división de la información en *bytes* por todos los discos del *stripe* y la paridad para la recuperación de errores.



IMPORTANTE

La paridad

La paridad es una información adicional que se calcula antes de escribir los datos en disco. Si falla algún disco, la información se reconstruye con ayuda de la paridad. En el caso de que el disco que falle sea el de la paridad, la paridad se volverá a recalcular en el disco de repuesto.

La ventaja frente al RAID 2 es que la paridad ocupa menos que el código Hamming.

RAID 3 no se utiliza debido a que existen sistemas más avanzados y eficientes como RAID 4 o 5.

RAID 4 (*striping* + *paridad*)

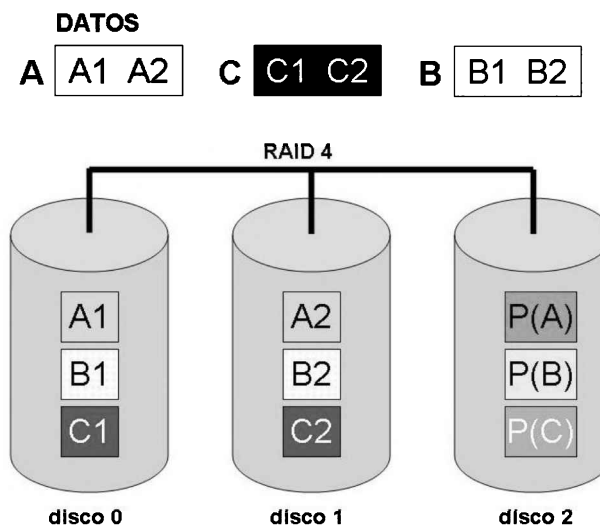


Figura 4.12. Esquema del RAID 4

Igual que RAID 3 pero en vez de distribuir la información por los discos por *bytes*, la distribuye por sectores. La paridad la almacena en un disco del *stripe* aparte de los datos.

Tiene un rendimiento mayor que RAID 2 y 3.

Necesita como mínimo 3 discos (2 para datos y 1 para paridad).

RAID 5 (*striping* + paridad distribuida)

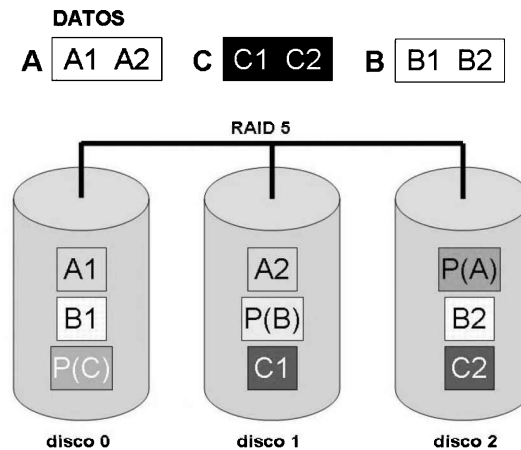


Figura 4.13. Esquema del RAID 5

RAID 5 funciona igual que RAID 4, pero distribuye la paridad por cada uno de los discos del *stripe* o matriz.

Tiene un rendimiento de escritura mucho mayor al escribir la paridad de forma distribuida.

Se necesitarán como mínimo 3 discos. Con 4 discos el *overload* o sobrecarga es de un 25% (por ejemplo, si tenemos 4 discos de 100 GB cada uno, el tamaño máximo disponible total de datos será de 300 GB).

Sobrevive al fallo de un disco (no al de dos).

Es el RAID más utilizado al ofrecer un mejor equilibrio coste-rendimiento-protección. Dado que RAID 5 es una solución mejorada a los sistemas RAID 2, 3 y 4, es fácil entender por qué estos últimos no se utilizan y prácticamente no se habla de ellos.

Tipo de RAID	N.º mínimo de discos	Ventajas	Limitaciones
RAID 0	2	Rendimiento.	No existe protección de datos.
RAID 1	2	Buena protección de datos y alto rendimiento.	Alto coste. Se necesita duplicar el número de discos ($2 \cdot n$). El <i>overload</i> es elevado, siempre un 50%.
RAID 5	3	Mejor relación rendimiento/precio. Necesita $n+1$ discos con un mínimo de 3 discos. Con 4 discos el <i>overload</i> es solo del 25%, mientras que con RAID 1 sería del 50%.	Escritura más lenta que con RAID 0 o 1, dado que el sistema tiene que calcular la paridad para cada dato que escribe.

Tabla 4.2. Ventajas y limitaciones de los distintos sistemas RAID

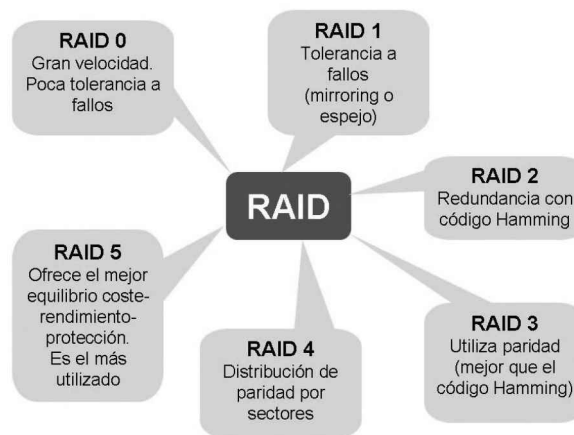


Figura 4.14. Características principales de los distintos tipos de RAID

4.2.4.4 Sistemas RAID anidados

En este caso hay que tener en cuenta el orden en que se enumeran los RAID. RAID 0+1 quiere decir que a un conjunto de discos en RAID 0 se le aplica RAID 1 (*mirroring*).

RAID 0+1

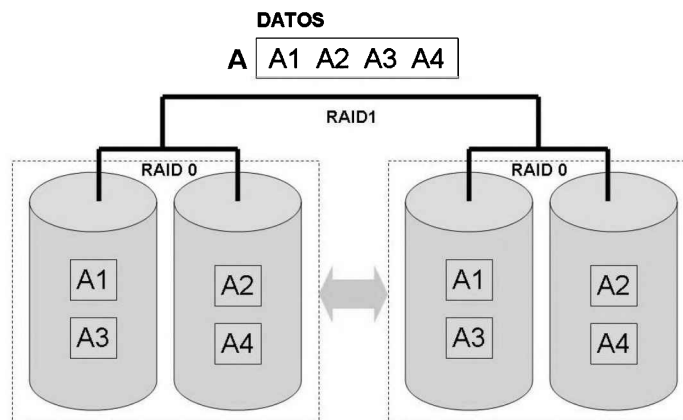


Figura 4.15. Esquema del RAID 0+1

RAID 0+1 corresponde a implementar un *stripe* y duplicarlo en espejo.

Se necesitarán como mínimo 4 discos.

La sobrecarga u *overload* es de un 50%.

RAID 10 (1+0)

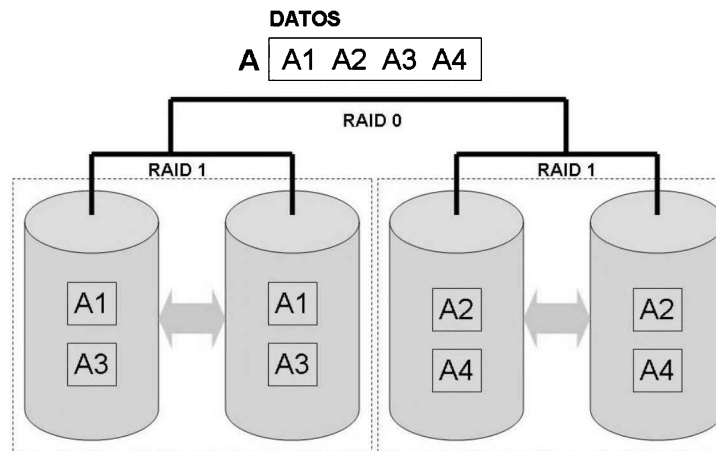


Figura 4.16. Esquema del RAID 10

RAID 10 corresponde a implementar varios espejos y luego realizar con ellos un *stripe*.

Se necesitarán como mínimo 4 discos.

La sobrecarga u *overload* es de un 50%.

Es una configuración más usada que RAID 0+1 puesto que es ligeramente más tolerante a errores. Permite múltiples fallos siempre que se produzcan en un espejo distinto.

Los niveles RAID más utilizados son los siguientes:

- RAID 0, 1 y 10 para equipos normales, *workstations* y servidores pequeños.
- RAID 5 y 50 para grandes servidores. También es común ver RAID 5 en equipos normales o servidores más pequeños.

4.3 POLÍTICAS DE SALVAGUARDA

La supervivencia de una empresa está sujeta a multitud de factores económicos, demográficos, de mercado y otros que son propios de su negocio pero también a otros muchos que son ajenos a esta. Es responsabilidad de la empresa disponer de las medidas que le permitan desarrollar su actividad en condiciones normales ante situaciones adversas.

En grandes empresas suele existir un documento llamado plan de continuidad de negocio, que refleja las capacidades, recursos y procedimientos de la empresa de cara a prevenir los efectos negativos sobre su negocio de riesgos o situaciones externas no controlables