Unidad 4

Creación de imágenes de software. Respaldo del software base de un sistema

Fundamentos de Hardware

Índice

Introducción

Cualquier técnico medianamente competente de microinformática debe de saber en mayor o menor medida manejar herramientas de clonación, *backup* y RAID,

En esta unidad nos centraremos en cómo proteger nuestro sistema frente a problemas que no sean ataques, como un fallo físico del equipo o una desgracia.

Algunas amenazas y sus posibles soluciones		
Clonación	**Backup**	**RAID**
Desgracia	Desgracia	Borrado accidental
Borrado accidental	Borrado accidental	Fallo en una unidad de almacenamiento
Fallo del software		

Este es posiblemente una de las unidades más importantes de todo el temario puesto que vamos a tratar varias de las herramientas de mayor importancia para un técnico de soporte.

Al finalizar esta unidad

- Sabremos como mantener un sistema de manera que funcione con seguridad frente a fallos y desgracias.
- Seremos capaces de manejar las copias de seguridad, las clonaciones y los sistemas RAID.
- Entenderemos los conceptos en profundidad.
- Comprenderemos para qué sirve el particionamiento y como se realiza.
- Aplicaremos las ventajas de los nuevos sistemas UEFI.
- Conoceremos la diferencia entre el formateo físico y lógico.

4.1. El arranque

Para que un sistema informático pueda iniciar correctamente, es necesario que el dispositivo de almacenamiento disponga de una estructura adecuada de particionado y un sistema de archivos funcional. Este proceso implica aspectos tanto físicos como lógicos, fundamentales en la instalación y gestión de sistemas operativos.

El proceso de **particionado** permite dividir un dispositivo de almacenamiento (como un disco duro o SSD) en áreas independientes llamadas **particiones**, que se gestionan como unidades separadas. Cada partición debe contar con un **sistema de archivos** que permita organizar y estructurar la información contenida.

- **MBR (Master Boot Record),** tradicionalmente utilizado en sistemas antiguos.
- **GPT (GUID Partition Table),** utilizando predominantemente en sistemas actuales con firmware UEFI.

4.1.1. El particionamiento MBR

El sistema MBR ha sido el estándar en la gestión de particiones durante muchos años. Aunque aún está presente en algunos sistemas, su uso ha disminuido debido a limitaciones técnicas importantes, entre las que destacan:

- **Limitaciones de capacidad:** cada partición tiene un tamaño máximo de **2 terabytes (TB)**. Por ejemplo, un disco duro de 3TB no podría gestionarse íntegramente con MBR.
- **Número limitado de particiones primarias:** únicamente se permiten hasta **cuatro particiones primarias**. Para superar esta limitación, se crea una partición extendida que puede contener múltiples particiones lógicas. Por ejemplo, en un mismo disco podemos tener una partición primaria para Windows, otra primaria para Linux y una partición extendida que contenga múltiples particiones lógicas destinadas a almacenamiento adicional para ambos sistemas.

Tenemos tres tipos de particiones MBR:

- **Partición primaria:** contiene un sistema operativo o datos. Puede marcarse como activa para permitir el arranque.
- **Partición extendida,** contenedor que permite superar la limitación de 4 particiones. Solo puede existir una por disco.
- **Partición lógica:** se crean dentro de una extendida. Se usan para almacenar datos o incluso instalar sistemas operativos secundarios.

NOTA

Para que un equipo arranque correctamente desde un disco MBR, es necesario que una de las particiones esté **marcada como activa,** conteniendo el **sector de arranque.**

Para realizar el particionamiento MBR tenemos que seguir cuatro reglas básicas:

1. Un dispositivo solo puede tener una o ninguna partición extendida.
2. Una partición extendida puede tener varias o ninguna partición lógica, no hay límites para estas.
3. En una misma unidad de almacenamiento puede haber cuatro particiones primarias como máximo.
4. Si tenemos una partición extendida solo podremos tener entonces 3 particiones primarias.

4.1.2. El particionamiento GPT y UEFI

La utilización del sistema UEFI (**Unified Extensible Fimware Interface**) junto con GPT ha revolucionado la gestión de particiones debido a sus múltiples ventajas frente a MBR, destacando especialmente:

- **Arranque más rápido del sistema operativo:** gestión optimizada de los recursos durante el inicio.
- **Superación del límite de 2 TB:** permite manejar discos duros con capacidad muy superior, hasta 8 ZB (zettabytes).
- **Mayor fiabilidad y robustez:** incluye mecanismos avanzados de redundancia y recuperación ante fallos.
- **Mejor gestión de energía y recursos del sistema:** eficiencia energética mejorada.
- **Mayor número de particiones:** permite hasta 128 particiones primarias, sin distinción entre primarias o lógicas.

Es importante aclarar que UEFI actúa como interfaz moderna entre el hardware y el sistema operativo, ofreciendo una flexibilidad y capacidad muy superiores al BIOS tradicional (Legacy BIOS). No obstante, el término "BIOS" aún es empleado frecuentemente de forma genérica para referirse tanto a sistemas BIOS como UEFI.

Imagen 1. Esquema de particiones de un disco duro GPT

Diferencias entre BIOS y UEFI

Diferencias entre BIOS y UEFI		
Característica	**BIOS (Legacy)**	**UEFI**
Interfaz	Texto básico (modo real)	Gráfica o textual avanzada
Tamaño de disco soportado	Hasta 2 TB (MBR)	Más de 2 TB (GPT)
Número de particiones	Hasta 4 primarias (o 3+extendida)	Hasta 128
Seguridad	Sin protección avanzada	Soporta **Secure Boot**
Velocidad de arranque	Menor	Mayor

4.1.3. Formateo lógico (formateo de alto nivel)

El formateo lógico es el proceso mediante el cual se establece el sistema de archivos en una partición previamente creada. Habitualmente, cuando se adquiere un equipo nuevo, el dispositivo de almacenamiento ya viene formateado; sin embargo, el formateo lógico es necesario cuando se requiere cambiar el sistema de archivos o redefinir las particiones existentes.

Advertencia importante

Al realizar un formateo lógico, se elimina completamente la información existente en la partición afectada. Por ello, es crucial realizar una copia de seguridad previa si existen datos importantes.

Los sistemas de archivos que más se usan son los siguientes:

Sistema de archivos	Sistema operativo	Características principales
NTFS	Windows	Soporte de permisos, compresión, cifrado
HFS+/APFS	macOS	Rendimiento y fiabilidad en macOS
EXT4	Linux	Estabilidad, soporte de volúmenes grandes
FAT32 / exFAT	Todos (dispositivos extraíbles)	Compatible con múltiples sistemas, limitado en funciones

4.1.4. Formateo físico (formateo de bajo nivel)

El **formateo físico** actúa directamente sobre la estructura interna del disco. Recorre sector por sector, detectando errores y reorganizando la superficie del disco.

Características:

- Reasigna sectores defectuosos como no utilizables.
- Puede prolongar la vida útil del dispositivo en caso de fallos puntuales.
- Suele realizarse con herramientas especializadas a nivel de fabricante.

NOTA

El formateo físico **solo debe usarse en casos críticos,** ya que puede reducir la vida útil del dispositivo. Actualmente, los discos modernos ya vienen preformateados de fábrica y no requieren este tipo de proceso en condiciones normales

4.2. Clonación de equipos

La clonación de equipos es un procedimiento técnico mediante el cual se realiza una **copia exacta** de la información contenida en **unidades de almacenamiento** (como discos duros o unidades de estado sólido SSD). Esta copia incluye tanto los **datos almacenados** como las **estructuras internas del sistema**, incluyendo tablas de particiones, configuraciones del sistema operativo y programas instalados.

Enfoques de clonación

Existen dos enfoques fundamentales:

- **Clonación completa de discos:** se copia la información del disco de origen en su totalidad a un disco de destino, generando una réplica exacta.
- **Clonación parcial (por particiones):** solo se copian particiones específicas. En este caso, es fundamental incluir la partición de arranque (*boot*) si se desea que el nuevo disco sea capaz de iniciar el sistema operativo.

NOTA

Durante cualquier proceso de clonación, es fundamental realizar una **copia de seguridad previa** de los datos críticos, ya que el contenido del disco o partición de destino será sobrescrito de forma irreversible.

Aplicaciones de la clonación

Este procedimiento puede aplicarse en diversos contextos, entre los que destacan:

- **Despliegue masivo de equipos:** útil en empresas o centros educativos donde se requiere instalar la misma configuración de software en múltiples dispositivos.
- **Sustitución o actualización de almacenamiento:** al cambiar un disco defectuoso o sustituir un disco duro mecánico por un SSD para mejorar el rendimiento.
- **Copias de seguridad avanzadas:** permite conservar imágenes completas del sistema para restaurarlas rápidamente en caso de fallo grave.

EJEMPLO

Si clonamos un disco mediante una imagen creada con una herramienta de clonación, podemos restaurar esa imagen en otro disco y obtener un sistema idéntico al original, incluyendo configuraciones, programas instalados y datos.

Tipos de clonación según el método de transferencia

Se pueden distinguir dos modalidades técnicas:

- **Clonación directa (disk to disk):** se copian los datos directamente desde el disco origen al disco destino, ambos conectados simultáneamente al mismo equipo. Por ejemplo, conectar dos discos mediante interfaces SATA o USB para transferir la información directamente.
- **Clonación por imagen (disk to image):** se crea un archivo imagen comprimido (.iso, .img) que contiene toda la información del disco original. Esta imagen puede restaurarse posteriormente en uno o varios discos distintos. Por ejemplo, se puede generar una imagen de un sistema configurado con software específico y restaurarla en múltiples ordenadores.

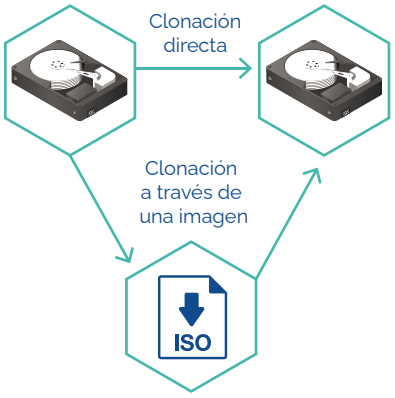

Imagen 2. Diferentes tipos de clonación.

4.2.1. Herramientas de clonación y creación de USB arrancables

A la hora de realizar una clonación, existen diversas herramientas disponibles. Muchas de estas herramientas de clonación son de pago, pero nos centraremos en una opción de código abierto y ampliamente utilizada llamada *Clonezilla*.

Secure Boot

Con el lanzamiento de Windows 8, Microsoft decidió apostar por la seguridad e implementó la función de Secure Boot o arranque seguro. Esta función evita la instalación de software no firmado o no certificado por el fabricante, con el objetivo de proteger el sistema contra posibles daños en el arranque.

Para desactivar el Secure Boot, debemos seguir los siguientes pasos desde el panel de control de la BIOS (los pasos pueden variar según el fabricante de la BIOS):

- Desactivar únicamente el Secure Boot.
- Desactivar el arranque UEFI.

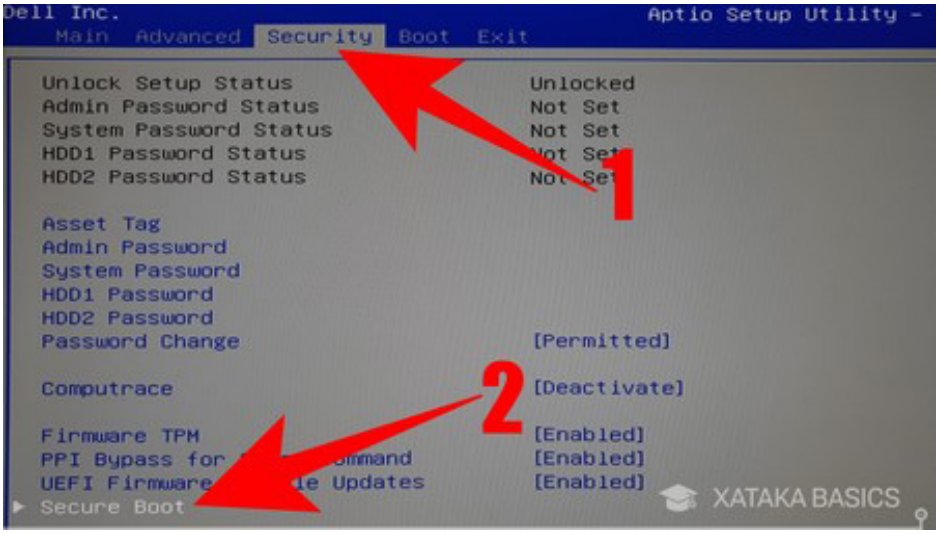

Imagen 3. Desactivar Secure Boot.

IMPORTANTE

Desactivar el Secure Boot nos permite instalar otros sistemas en el equipo, ya que no restringe la instalación únicamente a Windows.

Fast Boot

En la mayoría de los sistemas Windows modernos, se encuentra activada la opción de Fast Boot o Inicio rápido para mejorar el rendimiento del sistema operativo. Sin embargo, esta función puede impedir el inicio de otros sistemas operativos, ya que el sistema se inicia rápidamente y se dirige directamente a Windows.

Para desactivar Fast Boot, debemos seguir estos pasos:

1. Acceder al 'Panel de Control'.
2. Buscar y seleccionar 'Opciones de energía'.

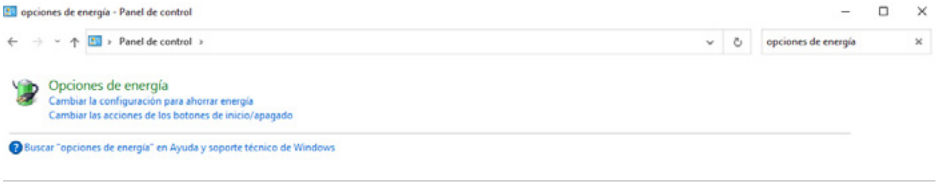

Imagen 4. Desactivación de Fast Boot 1.

1. Dentro de 'Opciones de Energía', tendremos en el margen derecho la opción 'Elegir el comportamiento de los botones de inicio/apagado', la seleccionamos.

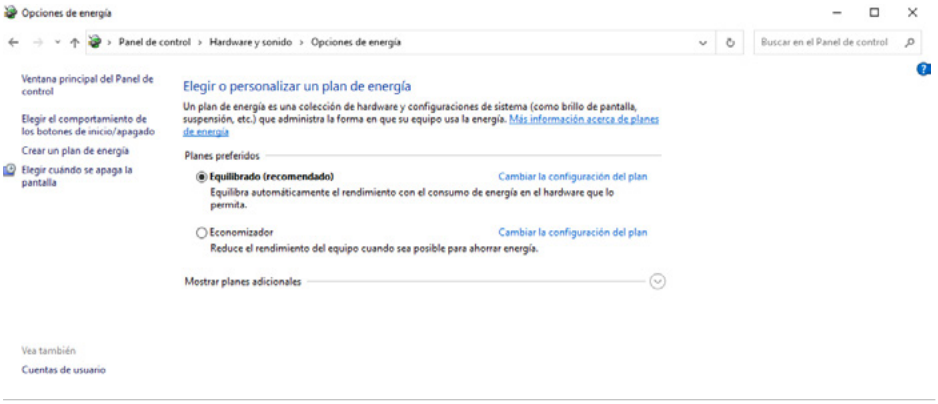

Imagen 5. Desactivación de Fast Boot 2.

2. Como podremos ver, nos aparecerá la opción para cambiar las características y más abajo tendremos la opción de *Fast Boot* habilitada, la deshabilitamos y ya podríamos iniciar la BIOS sin problema u otro sistema operativo.

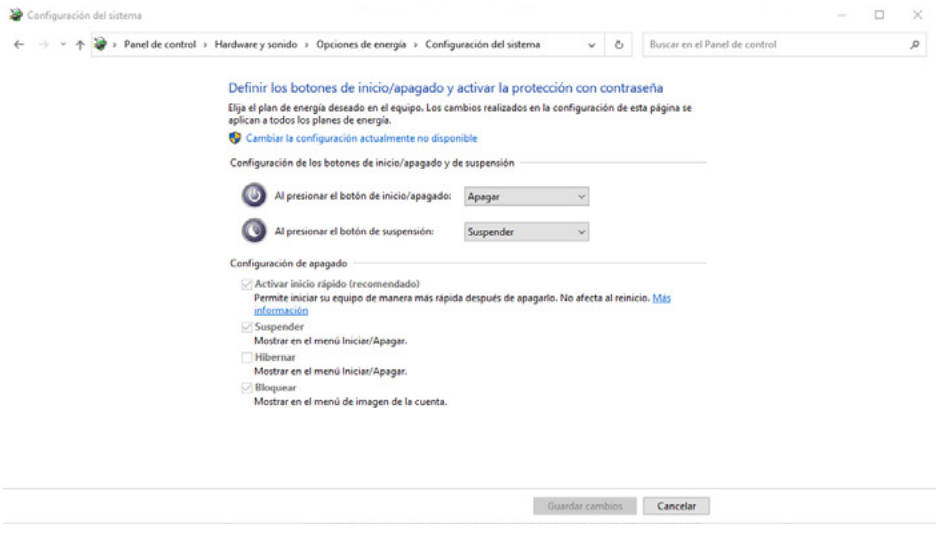

Imagen 6. Desactivación de Fast Boot 3.

4.2.2. Creación de un USB arrancable con Rufus

Para poder hacer que un USB sea *booteable*, es decir, pueda funcionar como arranque de un equipo, debemos de insertarle una imagen de un sistema o de un inicio con alguna aplicación externa especial para este cometido.

En este caso vamos a usar Rufus.

Instalación de Rufus

1. Lo primero que vamos a hacer es dirigirnos al navegador Web y descargar la última versión de *Rufus*, en este caso es la 3.17.

Imagen 7. Instalación de Rufus.

2. Una vez descargado es un ejecutable que se inicia al momento con privilegios de Administrador. Su aspecto es el siguiente:

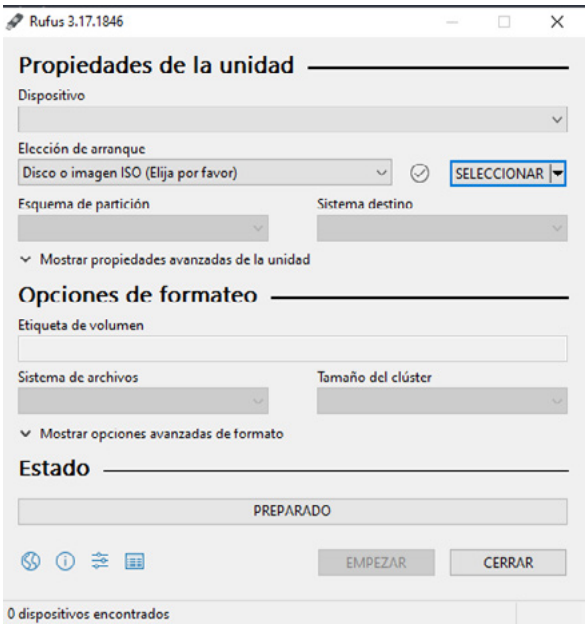

Imagen 8. Rufus.

Creación de la imagen de Rufus

Una vez que tenemos Rufus instalado tendremos que seleccionar la imagen y el dispositivo donde se va a crear la ISO.

Cuando esto haya terminado se nos marcará como completado y se podrá usar el USB arrancable.

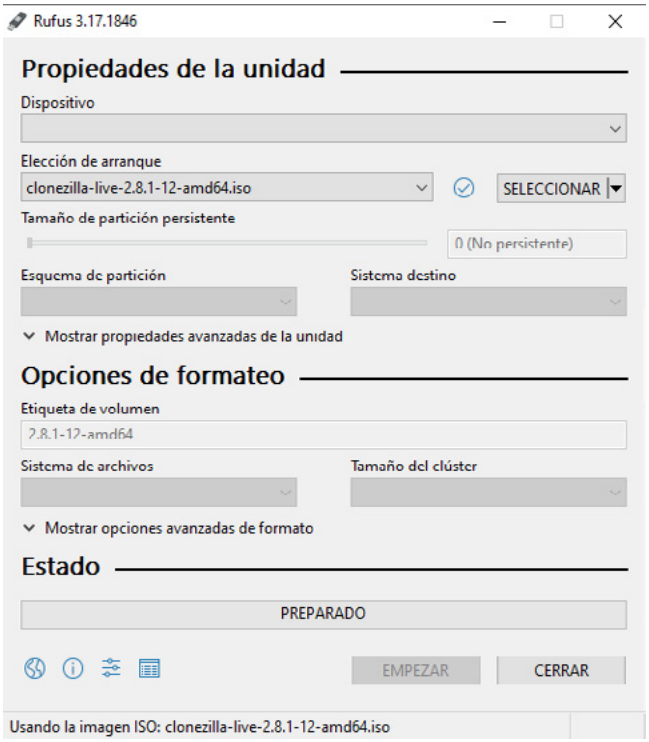

Imagen 9. Rufus con una imagen de Clonezilla.

4.2.3. Arrancar Clonezilla desde el USB

Una vez que tenemos ya el USB preparado, vamos a pasar a ejecutar el USB con *Clonezilla*.

Clonezilla es un software usado para realizar clonaciones de unidades de almacenamiento, como hemos dicho anteriormente.

Lo primero que vemos nada más arrancar el *software* es la opción de que entorno de *Clonezilla* se quiere usar.

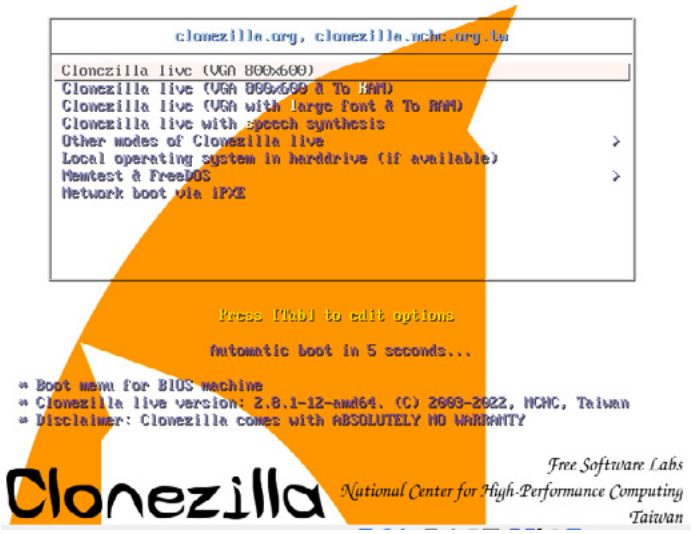

Imagen 10. Clonación con Clonezilla 1.

En las siguientes pantallas se nos pedirá cuando arranque, que idioma y distribución de teclado queremos usar. Lógicamente debemos de seleccionar el idioma que prefiramos y que mejor entendamos.

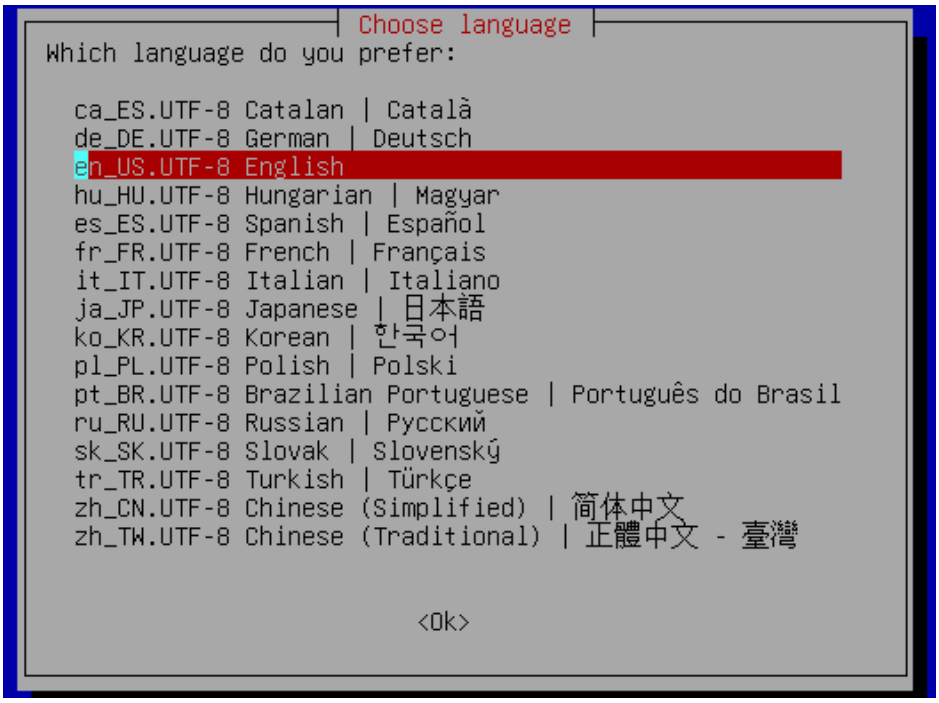

Imagen 11. Clonación con Clonezilla 2.

Elegimos la opción de teclado por defecto de manera normal porque va asociada al lenguaje, y ahora se nos presenta la opción de iniciar *Clonezilla* o de ejecutar un *Shell* de comandos, deberíamos de elegir la primera.

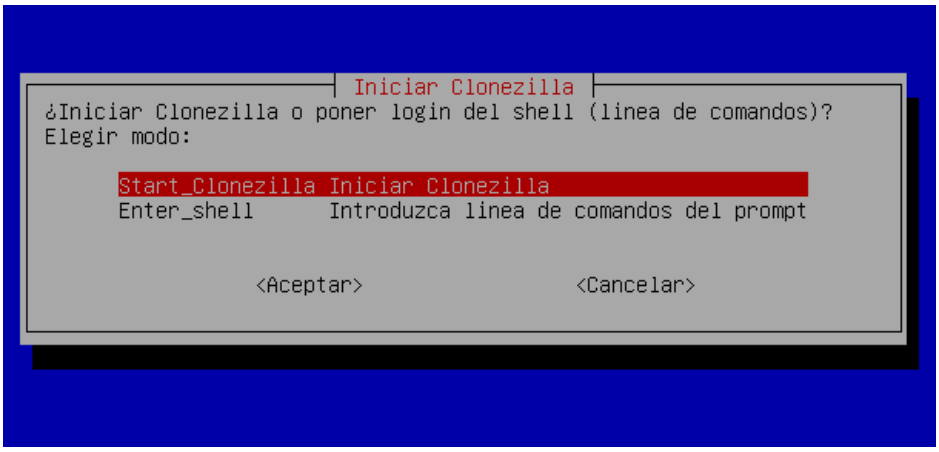

Imagen 12. Clonación con Clonezilla 3

Una vez realizado todo lo anterior, se nos presentará el modo de uso que queremos seleccionar, y nos tenemos que fijar en las dos primeras opciones:

- **Device-image.** Dispositivo-imagen, se creará una imagen del disco.
- **Device-device.** Dispositivo-dispositivo, se clona la información de un disco a otro.

Si lo que queremos es realizar una clonación puntual lo mejor será elegir la segunda opción, pero si esta copia queremos almacenarla para varios equipos, deberíamos de elegir la primera y conservar la imagen creada.

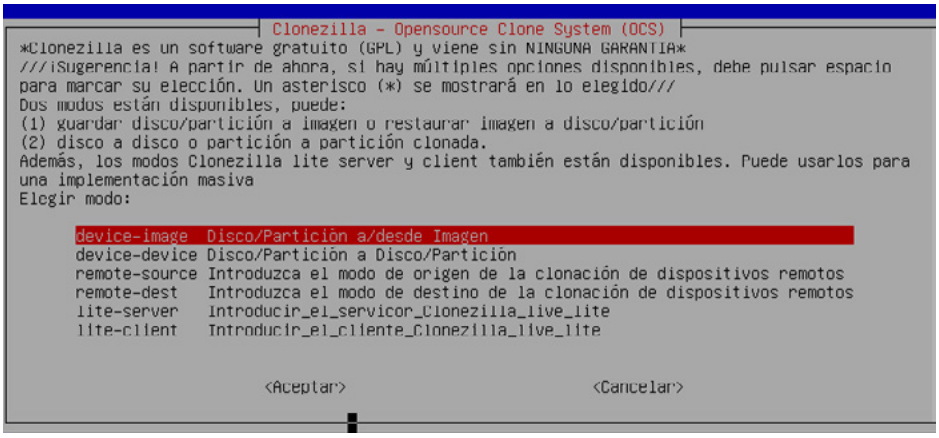

Imagen 13. Clonación con Clonezilla 4.

NOTA

Clonezilla permite el cifrado de las imágenes del disco para que sean protegidas contra cualquier acceso no deseado.

Si queremos hacer una imagen del sistema en cuestión, este programa nos dará las siguientes opciones de almacenamiento:

- En un disco local.
- En un servidor externo al que se conectará por *SSH*.
- En un servidor *Samba* o algún recurso compartido de Windows.
- En un servidor *NFS*.
- Otras opciones.

Ahora, vamos a imaginar que seleccionamos la opción de crear una clonación de disco a disco, el proceso sería el siguiente:

1. Lo primero que hacemos es seleccionar el modo de ejecución de *Clonezilla*, en nuestro caso vamos a ejecutar el segundo, modo experto.

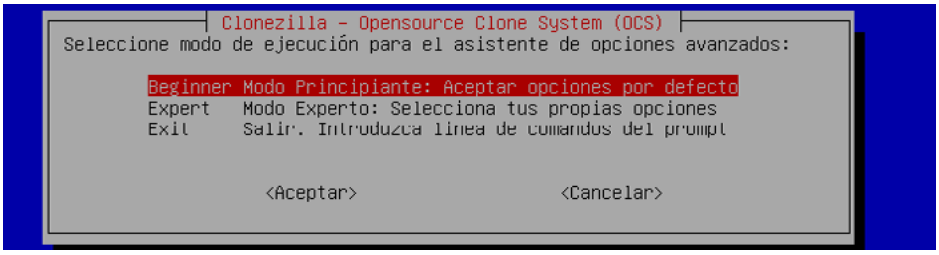

Imagen 14. Clonación con Clonezilla 5

2. El siguiente paso será seleccionar si se hace de un disco local a otro o de una partición en concreto a otra, en nuestro caso seleccionamos los discos completos.

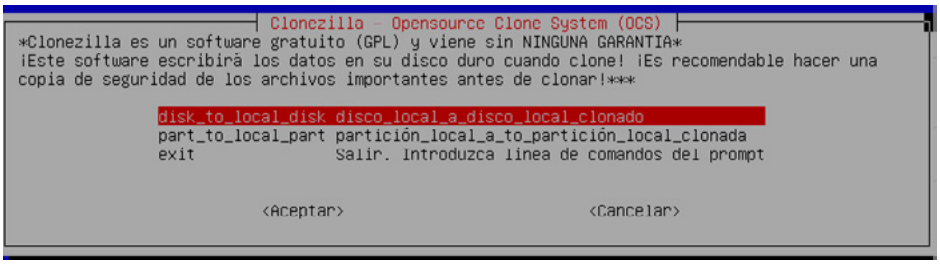

Imagen 15. Clonación con Clonezilla 6.

3. Ahora seleccionamos el disco de origen del que queremos que se haga la copia e inmediatamente después, el disco donde se va a plagiar dicha copia.

Es importante tener en cuenta que:

- Los discos siguen la nomenclatura de *Unix*, *sda, sdb, etc.*
- No se puede realizar una clonación de un disco con mayor tamaño a uno menor, pero sí a la inversa.

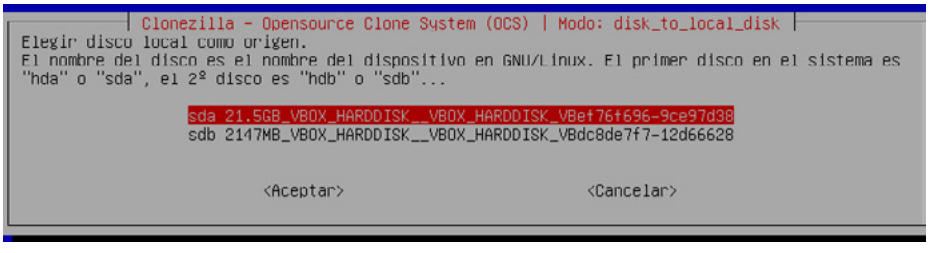

Imagen 16. Clonación con Clonezilla 7

4. Las siguientes opciones sobre el arranque, sistema de archivos, etc., las dejamos por defecto.

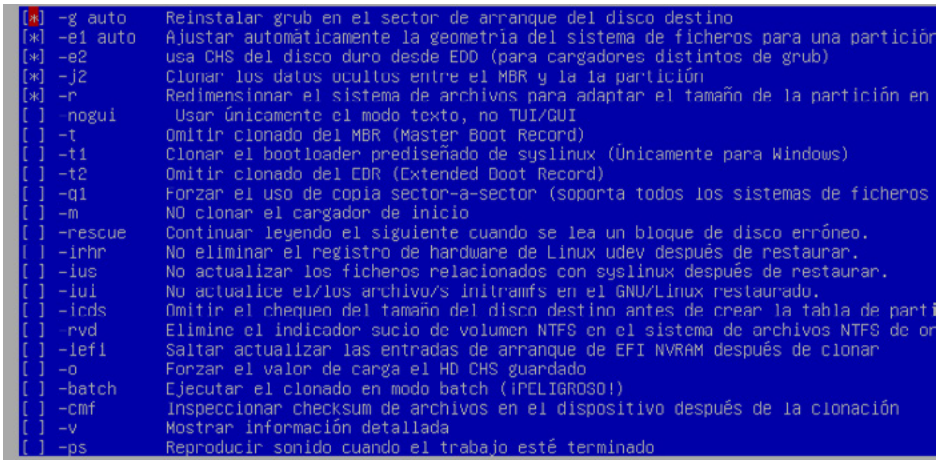

Imagen 17. Clonación con Clonezilla 8.

5. Una vez que casi hemos terminado, se nos presentarán las opciones siguientes:

   » Elegir si revisar o no el sistema de ficheros antes de la clonación y en caso afirmativo, repararlo si se muestra error.

   Se puede hacer de manera interactiva o automática.

   » Seleccionar que hacer una vez completada la clonación.

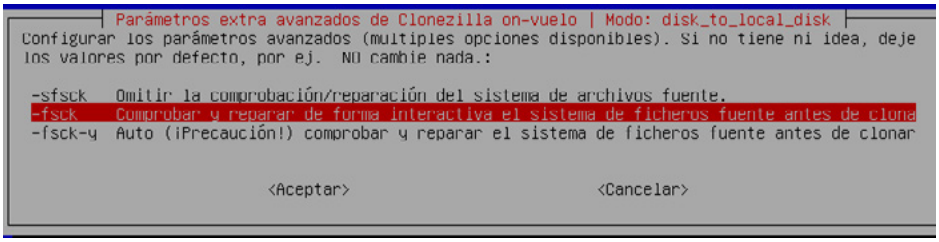

Imagen 18. Clonación con Clonezilla 9

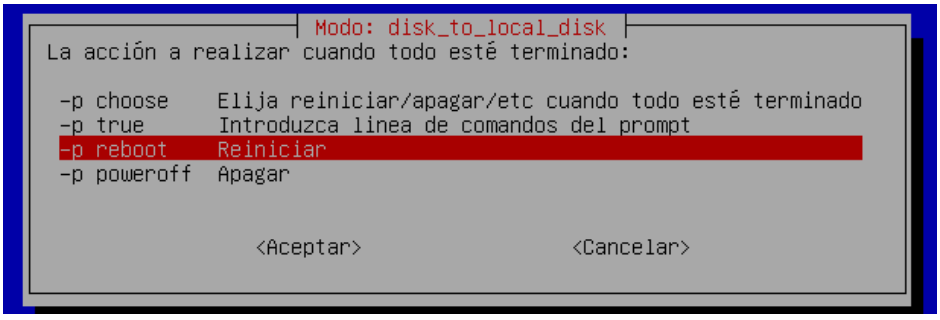

Imagen 18. Clonación con Clonezilla 10

Una vez terminada la configuración previa, empezará la clonación, cuya duración dependerá del tamaño de los datos, de los discos, la velocidad de transmisión, etc.

Los nombres que se asocian a imágenes o particiones que se crean con *Clonezilla* normalmente siguen un modelo basado en la fecha en la que se realizar la clonación, pero esta opción se podría cambiar.

Así mismo, deberíamos de comprobar después que todo ha salido bien, ya sea con el disco o con las imágenes.

4.2.4. Restauración de una imagen

El proceso de restaurar una imagen consiste en elegir una imagen de un sistema que queramos volcar y realizar la clonación entera en un dispositivo.

IMPORTANTE

Debemos de tener en cuenta que a la hora de elegir el disco es importante prestar especial atención a esto, pues una equivocación podría llevar a la perdida de todos los datos de dichos discos.

Hay que tener en cuenta que este proceso no tiene sentido para las clonaciones de un disco a otro, porque no se crea una imagen que volcar.

Para llevar a cabo este proceso debemos de iniciar de igual modo *Clonezilla* pero ahora seleccionaremos la opción de restauración.

Este proceso es bastante sencillo y no lleva mayor complicación ni mucho tiempo, que dependerá del medio, el tamaño, etc.

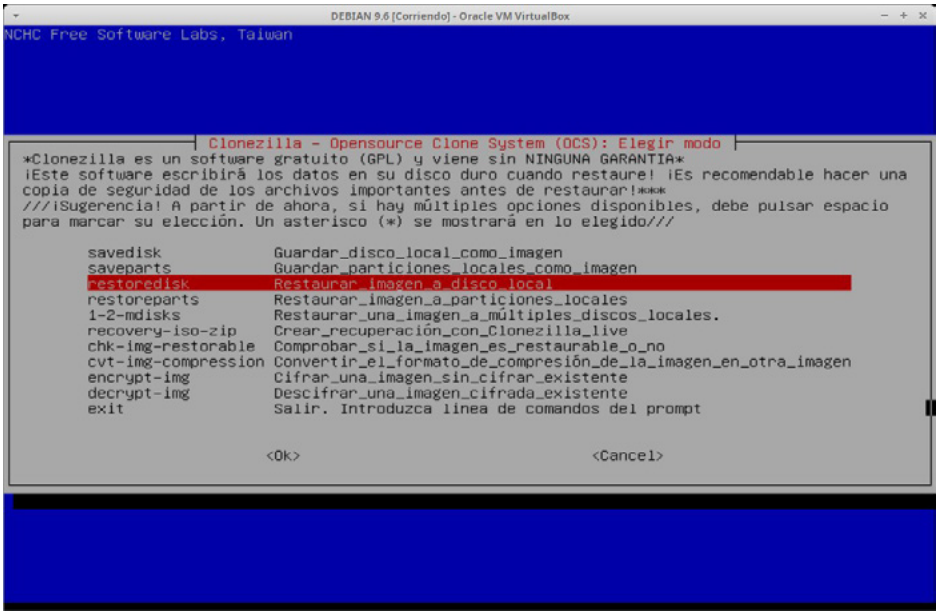

Imagen 19. Restauración de una copia de seguridad con Clonezilla.

4.3. Las copias de seguridad o backups

Las **copias de seguridad**, también conocidas como **backups**, son mecanismos esenciales para la protección de la información digital. Su objetivo principal es **resguardar los datos** de un sistema ante posibles pérdidas causadas por errores humanos, fallos de hardware, ataques de malware o desastres naturales.

Una copia de seguridad permite **restaurar la información** a un estado anterior, minimizando el impacto negativo sobre la continuidad operativa.

4.3.1. Tipos de copias de seguridad

En ocasiones, no es posible realizar copias de seguridad completas de toda la información almacenada, ya sea por limitaciones de recursos o porque no es necesario. Por lo tanto, existen tres tipos de copias de seguridad:

- **Copia completa (o total):** Este tipo de copias almacenan en el backup toda la información que se desea respaldar. Además, **activan** el atributo o flag de "**modificado**" para todos los archivos. Es el método más seguro, pero también el que más espacio y tiempo requiere.
- **Copia incremental:** Solo se respalda **la información modificada** desde la última copia (ya sea completa o incremental). Una vez copiado, el archivo se **marca** como **no modificado** (se desactiva el atributo de "modificado"). Es eficiente en tiempo y almacenamiento, pero la restauración requiere todas las copias incrementales intermedias.
- **Copia diferencial:** Se respaldan todos los archivos **modificados desde la última copia completa**. A diferencia de la copia incremental, **no se desactiva el atributo de modificación**. El tamaño crece con el tiempo, pero la restauración solo necesita la copia completa más reciente y la última copia diferencial.

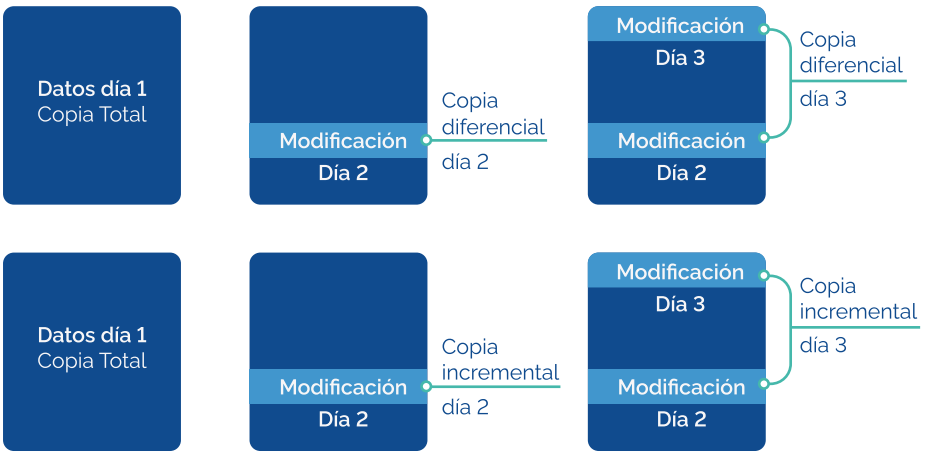

Imagen 20. Tipos de copia de seguridad.

IMPORTANTE

Es recomendable que las copias de seguridad no se realicen con demasiado tiempo de separación entre ellas. Si, por ejemplo, se realiza una copia de seguridad el lunes y se pierden datos el jueves, no será posible recuperar los datos correspondientes al martes y miércoles, ya que no se encuentran en la copia más reciente.

4.3.2. Restauración de los backups

Para restaurar una copia de seguridad solo tenemos que seguir los siguientes tres pasos:

- Paso 1. **Restaurar la última copia completa** disponible.
- Paso 2. Si existen copias **incrementales posteriores**, restaurarlas en **orden cronológico** desde la más antigua hasta la más reciente.
- Paso 3. Si se utilizan copias **diferenciales** y no hay incrementales posteriores, restaurar la **última copia diferencial** disponible.

4.3.3. Consejos a la hora de realizar copias de seguridad

Al realizar copias de seguridad, es fundamental tener en cuenta los siguientes aspectos:

- **Orden y claridad:** Asignar nombres descriptivos a las copias de seguridad que indiquen su contenido y fecha.
- **Comprobación de las copias:** Verificar regularmente si las copias de seguridad se realizan correctamente y se encuentran en buen estado.
- **Localización:** Almacenar las copias de seguridad en un lugar distinto al del origen de la información, para evitar la pérdida de ambos en caso de fallo físico.
- **Automatización:** Automatizar la tarea de copias de seguridad para ahorrar costos y garantizar su realización periódica.
- **Calendario:** Planificar y establecer un calendario para las copias de seguridad, incluyendo el tipo de copia y su frecuencia.
- **Simulacros:** Realizar simulacros de pérdida de datos para comprobar la efectividad del proceso de restauración.
- **Protección:** Asegurar que las copias de seguridad tengan un nivel de protección igual o superior al del sistema original, para evitar ataques y filtraciones.

4.4. RAID

RAID significa **Redundant Array of Independent Disks** o **Conjunto Redundante de Discos Independientes**. Consiste en utilizar dos o más discos duros, generalmente de manera redundante, para mejorar el rendimiento de lectura y proporcionar protección contra posibles fallos de los discos.

Cuando hablamos de **redundancia** en RAID, nos referimos a una mayor seguridad de los datos, ya que la implementación de la mayoría de los tipos de RAID (**excepto RAID 0**) garantiza que si un disco falla, otro disco se encargará de mantener el sistema funcionando. Si no se tiene RAID implementado, la caída de un disco generalmente resulta en la caída del sistema.

Existen dos tipos de implementación de RAID:

- **Por software.** Es la opción más económica pero también la más lenta. Este tipo de RAID no se utiliza tanto debido a que su eficiencia se ve comprometida y se nota en el rendimiento. Sin embargo, hay sistemas operativos como Windows Server que ofrecen soporte para RAID por software.
- **Por hardware.** Es la opción más costosa pero la más eficiente en términos de rendimiento, por lo que es la más utilizada. Para crear un RAID por hardware, se utiliza una controladora RAID dedicada, ya que son fáciles de configurar y administrar.

IMPORTANTE

Tener en cuenta que un RAID no reemplaza una copia de seguridad, sino que es una herramienta adicional para brindar mayor seguridad al sistema. Incluso si se implementa un RAID, si uno de los discos falla, deberá ser reemplazado por uno en buen estado.

Hay que tener muy presente que un RAID no es un sustituto a una copia de seguridad, sino otra herramienta más para dotar de mayor seguridad a nuestro sistema. Lógicamente, aunque haya un RAID implementado, si uno de los discos está defectuoso o falla, habrá que cambiarlo por otro en buen estado.

Existen varios tipos de RAID, dependiendo de las prestaciones necesarias se usarán unos u otros. Vamos ahora a citar los tipos de RAID más usados, pero no su implementación, porque la implementación por *software* no es la más usada y por *hardware* realmente dependerá de cada una de las controladoras. Eso sí, es importante saber cómo funciona cada tipo para poder elegir adecuadamente.

4.4.1. RAID 0

RAID 0, también conocido como **striping**, es un tipo de RAID que **no ofrece redundancia ni mecanismos de seguridad**.

En este sistema, la información se **divide en bloques** y se **distribuye entre los discos** del conjunto RAID, normalmente **dos discos**. El objetivo principal es **aumentar la velocidad de lectura y escritura**, ya que los datos se procesan en paralelo.

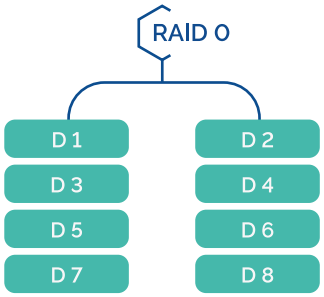

Imagen 21. Esquema de RAID 0.

Sin embargo, es importante tener en cuenta que el RAID 0 **no proporciona ninguna protección contra fallos** de disco. Si uno de los discos falla, se perderá toda la información almacenada en el conjunto RAID. Por esta razón, se recomienda utilizar el RAID 0 únicamente en situaciones donde la **velocidad** de acceso a los datos sea prioritaria y no se requiera una alta fiabilidad o redundancia de los datos.

IMPORTANTE

RAID 0 no se debe utilizar para almacenar datos críticos. Se utiliza, por ejemplo, en tareas de edición de vídeo o diseño gráfico, donde se trabaja con archivos temporales y se necesita mucha velocidad.

4.4.2. RAID 1

RAID 1, también llamado **mirroring** o **discos en espejo**, utiliza **dos discos que almacenan la misma información**. Es decir, **los datos se duplican** en ambos discos.

Este tipo de RAID ofrece **protección frente a fallos de hardware**, ya que, si uno de los discos falla, **los datos permanecen intactos en el otro**.

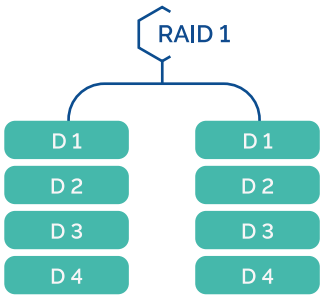

Imagen 22. Esquema de RAID 1.

Una ventaja importante es que **la velocidad de lectura mejora**, ya que **la información puede leerse desde ambos discos al mismo tiempo**. Sin embargo, la **velocidad de escritura no mejora**, ya que los datos deben grabarse en los dos discos.

El principal inconveniente es que **se pierde el 50 % de la capacidad de almacenamiento**, porque **los datos se duplican**.

IMPORTANTE

Se recomienda configurar un RAID 1 con discos completamente iguales, ya que, si uno de los discos tiene una velocidad o capacidad de almacenamiento menor, solo se podrán aprovechar las prestaciones del disco de menor capacidad.

EJEMPLO

RAID 1 es común en **servidores de pequeñas empresas o en ordenadores donde la integridad de los datos es esencial,** como bases de datos o sistemas contables.

4.4.3. RAID 5

RAID 5 combina **rendimiento**, **protección de datos** y **eficiencia de almacenamiento**. Utiliza un **mínimo de tres discos**, en los que se distribuyen tanto **los datos como la información de paridad**.

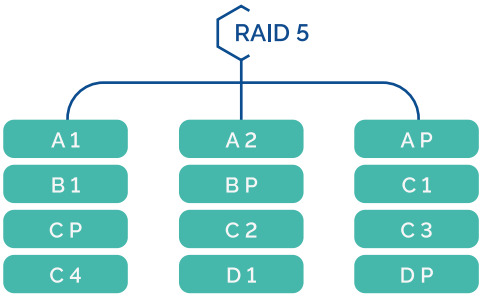

Imagen 23. Esquema de RAID 5.

Gracias a la paridad, si **uno de los discos falla**, el sistema puede **reconstruir la información** usando los datos restantes y la paridad. Además, como los datos se distribuyen, **la velocidad de lectura y escritura mejora**.

La **sobrecarga de espacio** es baja: se pierde aproximadamente **el 25 % de la capacidad total** (en un sistema con 4 discos, se pierde el espacio equivalente a uno).

IMPORTANTE

RAID 5 solo puede tolerar el fallo de un disco. Si falla un segundo disco antes de completar la reconstrucción, se pierden los datos.

EJEMPLO

RAID 5 es muy utilizado en **servidores corporativos, sistemas de almacenamiento en red (NAS)** y entornos donde se necesita un **equilibrio entre seguridad, rendimiento y capacidad.**

4.4.4. RAID 6

RAID 6 es una evolución de RAID 5. También **distribuye los datos y la paridad** entre los discos, pero añade un **segundo bloque de paridad**, lo que permite **resistir el fallo de dos discos al mismo tiempo**.

Se necesita un **mínimo de cuatro discos**, y la **capacidad útil es igual al total menos dos discos** (N–2). Esto implica una mayor **sobrecarga de almacenamiento**, especialmente si se usan pocos discos.

Otra diferencia clave es que, al calcular dos bloques de paridad, **la velocidad de escritura es menor que en RAID 5**.

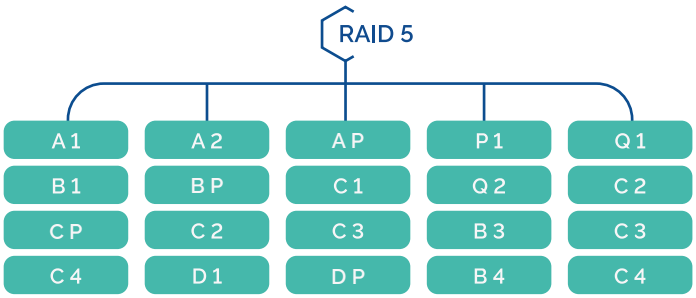

Imagen 24. Esquema de RAID 6.

RAID 6 es habitual en empresas con sistemas de alta disponibilidad, como servidores de bases de datos, servidores web o infraestructuras de nube privada.

IMPORTANTE

RAID 6 ofrece un nivel superior de seguridad, ideal para entornos donde la pérdida de datos no es una opción, como centros de datos o sistemas críticos.

EJEMPLO

RAID 6 es habitual en empresas con sistemas de alta disponibilidad, como servidores de bases de datos, servidores web o infraestructuras de nube privada.

Resumen de los principales tipos de RAID.			
	Ventajas	Desventajas	Mínimo de discos
RAID 0	Aumenta el rendimiento de lectura y escritura	No ofrece redundancia de datos.	2
	Utiliza todo el espacio de almacenamiento de los discos	Si falla un disco, se pierde toda la información	
	Bajo coste		
RAID 1	Proporciona redundancia y protección de datos.	Duplicación de espacio de almacenamiento	2
	Mayor disponibilidad y recuperación ante fallos	No mejora la velocidad de escritura	
RAID 5	Ofrece redundancia y protección de datos.	Se pierde el espacio equivalente a un disco por la paridad.	3
	Mayor tolerancia a fallos de un disco	Menor rendimiento de escritura que RAID 0.	
RAID 6	Mayor nivel de redundancia y protección de datos.	Mayor sobrecarga de almacenamiento.	4
	Tolerancia al fallo de dos discos	Rendimiento de escritura inferior a RAID 5.	

4.4.5. Sistemas RAID anidados

En algunos casos, es necesario combinar **dos tipos diferentes** de RAID para cumplir con las exigencias de rendimiento y protección de datos. A estos sistemas se les llama RAID anidados o RAID híbridos. El objetivo es **aprovechar las ventajas de cada tipo de RAID**, mejorando tanto la **seguridad ante fallos** como el **rendimiento general**.

A continuación, se presentan los sistemas RAID anidados más comunes:

RAID 0 + 1

En este tipo de RAID, primero se implementa un RAID 0 y luego se aplica un RAID 1 a este conjunto RAID 0 inicial. Es decir, se duplica en espejo el RAID 0 creado previamente.

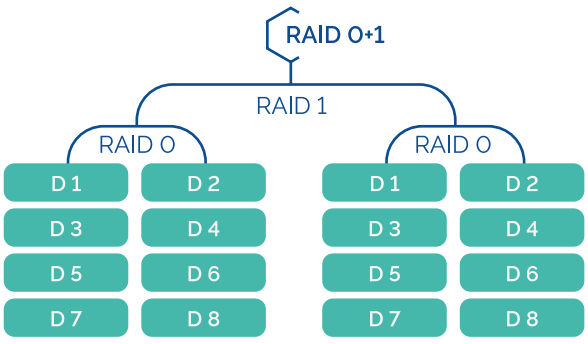

Imagen 25. Esquema de RAID 0 + 1.

Para implementar **RAID 0+1** se necesitan al menos **4 discos**: 2 para el RAID 0 inicial y 2 para duplicar ese conjunto. La **sobrecarga** en capacidad es del **50 %**, como en el RAID 1.

RAID 10 o 1 + 0

Este sistema funciona de forma **inversa al RAID 0+1**. Primero se crean **dos conjuntos RAID 1**, y luego se aplica un **RAID 0** (striping) entre ellos. De este modo, se logra tanto **redundancia** como **mayor velocidad**.

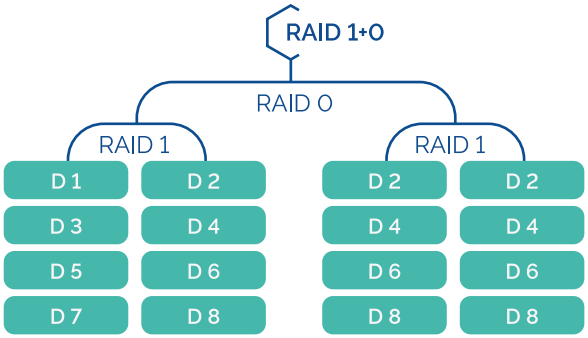

Imagen 26. Esquema de RAID 10.

Para implementar **RAID 10** también se requieren al menos **4 discos**: 2 para cada conjunto RAID 1. La **sobrecarga** sigue siendo del **50 %**, ya que los datos se duplican.

IMPORTANTE

RAID 10 ofrece mayor tolerancia a fallos que RAID 0+1.

Si fallan dos discos que no pertenecen al mismo espejo, el sistema puede seguir funcionando. En cambio, en RAID 0+1, si falla un disco en cada subconjunto, se pierde toda la información.

RAID 50

Para obtener **una mayor capacidad útil y menor sobrecarga** que en los sistemas anteriores, puede usarse **RAID 50**. En este caso, se crean **dos o más conjuntos RAID 5**, y luego se combinan mediante un **RAID 0** (striping).

RAID 50 mejora el rendimiento de escritura frente a RAID 5 individual y **mantiene tolerancia a fallos** (un disco por conjunto RAID 5 puede fallar sin pérdida de datos).

IMPORTANTE

Los sistemas **RAID anidados requieren planificación y configuración cuidadosa.** Antes de su implementación, deben evaluarse:

- Las **necesidades de rendimiento,**
- La **capacidad de almacenamiento disponible,**
- El **nivel de tolerancia a fallos necesario,** y
- El **presupuesto**, ya que estas soluciones requieren **más discos** y, en muchos casos, **controladoras especializadas.**

www.universae.com