Unidad 4

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

Fundamentos de Hardware

4

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

Todos y cada uno de los dispositivos de almacenamiento tienen necesariamente una estructura de particiones para poder funcionar. Se llama partición al espacio físico del dispositivo donde se almacena parte de la información.

Para que pueda haber un almacenamiento estructura es necesario que cada partición cuente con sistema de ficheros independiente.

Tenemos dos tipos principales de particionamiento, el MBR tradicional o el GTP actual de los sistemas UEFI.

4.1.1. El particionamiento MBR

Las siglas *MBR* hacen referencia a *Master Boot Record* y ha sido durante gran parte de la historia de la informática el formato de particiones usado para todos los dispositivos. De hecho, todavía hay algunos dispositivos que tienen este sistema implementado.

El hecho de que al final se haya optado por dejar de usar MBR en la mayoría de los dispositivos es debido a que tiene varias limitaciones:

- **El tamaño máximo de sus particiones es de 2 terabytes.** Cuando se desarrolló este sistema era impensable sobrepasar esa cantidad, pero hoy en día cualquier equipo se puede llenar con más de ese tamaño sin mucha complicación.
- **Solo se pueden crear cuatro particiones primarias.** Por lo general, para gestionar un único sistema no deben de ser necesarias más de 4 particiones, pero si queremos que varios convivan en un mismo dispositivo tendremos un problema, aunque, en caso de necesitar particiones adicionales, se crearían particiones en una partición extendida, Las particiones que se crean dentro de una partición extendida son las llamadas particiones *lógicas*.

Tenemos tres tipos de particiones MBR:

- Partición primaria.
- Partición extendida, Dentro de estas particiones se pueden almacenar particiones lógicas.
- Partición lógica.

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.

¿SABÍAS QUÉ?

Las particiones activas son las que se encuentran marcadas como las particiones que recogen el arranque del sistema, por lo tanto, si no tenemos esta partición activa no se puede iniciar el sistema.

4.1.2. El particionamiento UEFI

El arranque de los sistemas usando UEFI es el más moderno y usado en la actualidad ya que tiene menos limitaciones y varias ventajas.

Las ventajas de UEFI sobre *Legacy BIOS* son:

- El sistema tiene un inicio mucho más rápido
- Las particiones pueden ser de más de 2 TB
- Es más fiable que Legacy BIOS
- La energía y los recursos se gestionan más eficientemente
- Puede que tengamos más de cuatro particiones primarias en cada dispositivo de almacenamiento

Entonces, resumiendo las particiones ahora son *GPT* en vez de MBR porque son más modernas y fiables.

Se utiliza en sistemas con UEFI, es una evolución de la anterior descrita, añade características como la redundancia o la posibilidad de crear hasta 128 particiones con una capacidad total de 8 ZB y no tiene la necesidad de distinguir entre particiones primarias o lógicas.

Imagen 1. Esquema de particiones de un disco duro GPT

Los sistemas UEFI son un camino intermedio entre la BIOS y el propio sistema operativo, lo que nos ofrece un amplio abanico de ventajas debido a su gran flexibilidad.

Por lo general la denominación BIOS hace referencia a sistemas BIOS y UEFI, asumiendo el nombre genérico.

4.1.3. Formateo a alto nivel o formateo lógico

Es común que cuando adquirimos un equipo el sistema de almacenamiento venga ya formateado y no haga falta que se le realice otro formato a no ser que queramos cambiar el sistema de ficheros que venga instalado por defecto. O el sistema de particiones.

Debemos tener muy cuenta lo siguiente: **SI SE FORMATEA UNA UNIDAD DE ALMACENAMIENTO O UNA PARTICIÓN, SE PIERDE TODA LA INFORMACIÓN ALMACENADA.**

Por esto último lo mejores primero separar la unidad en particiones y luego cambiar el sistema de archivos de cada una de las particiones, realizando el llamado **formateo lógico**.

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

- En los dispositivos de Apple: HFS Plus.
- En Microsoft Windows: NTFS.
- En Linux: EXT.
- EL sistema de archivos FAT que se usa en tarjetas SD, pendrives y otros dispositivos extraíbles se puede usar en todos los sistemas operativos, pero en un principio fue desarrollado por Microsoft.

4.1.4. Formateo a bajo nivel o formateo físico

Este tipo de formateo es importante que sepamos que no debe realizarse a no ser que sea estrictamente necesario porque un disco duro ya viene de fabrica formateado a bajo nivel y es raro que necesite un nuevo formateo.

Lo que hace el formateo a bajo nivel es leer y escribir todos los bytes de la superficie del disco y así comprueba que estas acciones se pueden realizar sin problema y cuando tengamos bytes defectuosos se marcan como inutilizables.

4.2. Clonación de equipos

La clonación de un equipo se trata de la clonación de su información, de sus discos duros o unidades de almacenamiento. Cada unidad debe de formarse de distintas particiones entre las que estarán las de arranque y las del sistema, sin lugar a duda.

Cuando usemos una herramienta de clonación, esta se puede usar para clonar el disco al completo o para clonar solo una o algunas particiones del disco. La diferencia de estas dos clonaciones es bastante fácil de intuir, si clonamos un disco de uno entero a otro los discos serán exactamente iguales, mientras que si se hace la clonación por particiones el cargador de arranque del disco original podría no clonarse.

NOTA

Según lo descrito anteriormente quedaría de tal forma:

- Si queremos clonar un equipo con un sistema no instalado se puede o copiar el disco o las particiones.
- Si el disco sí tiene un sistema instalado deberíamos de clonar el disco al completo .

Además, tenemos otros dos tipos distintos de clonación, la clonación directa, donde se transfiere la información directamente de un disco duro a otro o la clonación por imagen.

En este último tipo de clonación tenemos la base de que se crea una imagen del sistema similar a la que se usa para la instalación de un sistema, un **.iso**, pero en este caso es una réplica exacta de nuestro sistema.

Esto se traduce en que cuando se haga la instalación, una vez terminada, el nuevo sistema será idéntico al anterior.

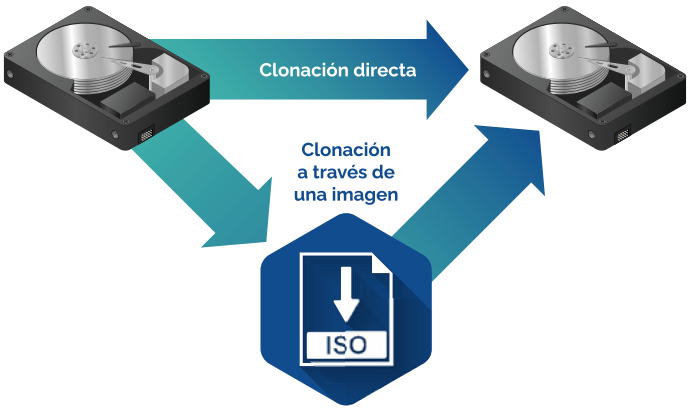

Imagen 2. Diferentes tipos de clonación.

4.2.1. Herramientas de clonación y creación de USB arrancables

A la hora de realizar una clonación tenemos varios modos para hacerlo. Muchas utilidades muy buenas son de pago, pero nos vamos a centrar nosotros en una que es de código abierto y además es de las más utilizadas, esta es Clonezilla.

Secure Boot

Con el nacimiento de Windows 8, los sistemas de Microsoft decidieron que se debía apostar por la seguridad al intentar deshabilitar la opción de que se pudiera instalar un software sin firmar o que no esté certificado por el fabricante dado que se podía estropear el arranque del sistema.

Lo que se decidió entonces es crear **Secure Boot** o arranque seguro, que realmente lo que hace es que no permite la instalación de otro sistema que no sea Windows.

Para poder desactivar el Secure Boot debemos de hacer lo siguiente desde el panel de control de la BIOS (son dos opciones que dependerán del fabricante de la BIOS): Tenemos dos opciones:

- Se desactiva solamente Secure Boot.
- Se desactiva el arranque UEFI.

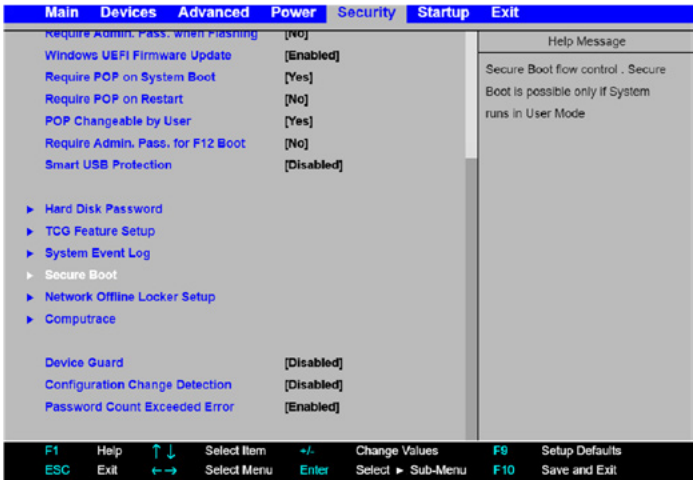

Imagen 3. Desactivar Secure Boot.

Desactivando Secure Boot conseguimos lo que queríamos, que era que se pueda instalar cualquier otro sistema en el mismo equipo.

Fast Boot

En casi todos los sistemas Windows modernos viene aplicada la opción de Fast Boot o Inicio rápido para ganar en rendimiento en Windows.

Esta implementación es bastante buena, pero al iniciarse el sistema tan rápido no se podrá iniciar otro sistema en conjunto porque directamente entrará en Windows.

Para desactivarlo debemos de hacer lo siguiente:

1. Nos dirigimos al 'Panel de Control'.
2. Dentro del Panel de Control buscamos 'Opciones de energía y entramos en estas'.

Imagen 4. Desactivación de Fast Boot 1.

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

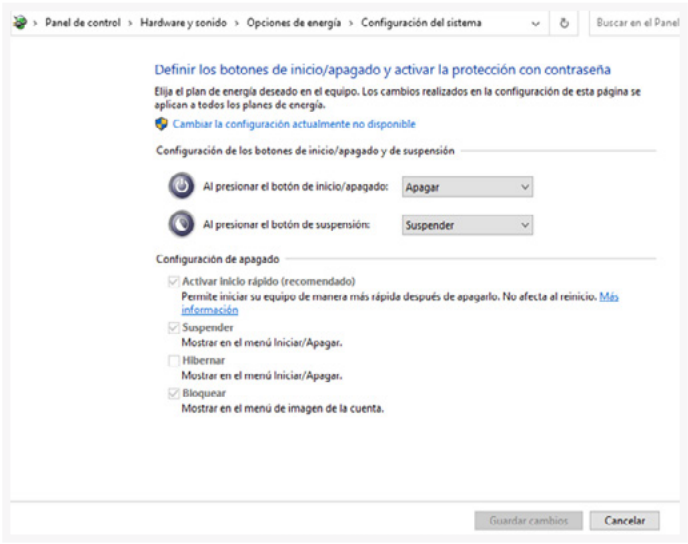

Imagen 5. Desactivación de Fast Boot 2.

4. 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.

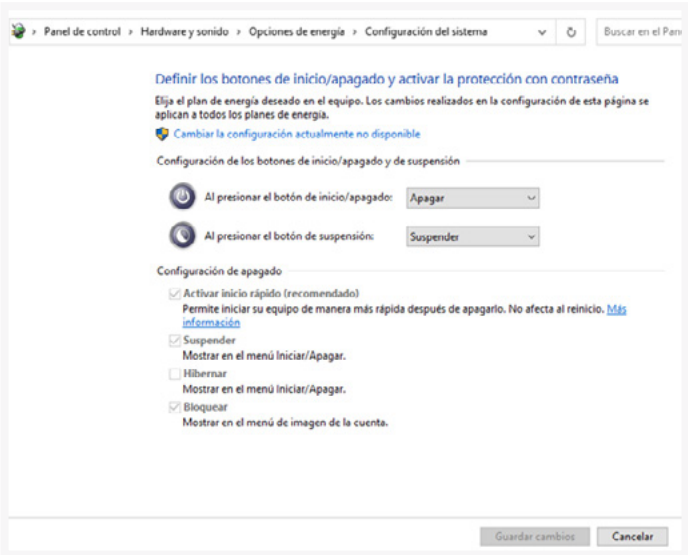

Imagen 6. Desactivación de Fast Boot 3.

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.

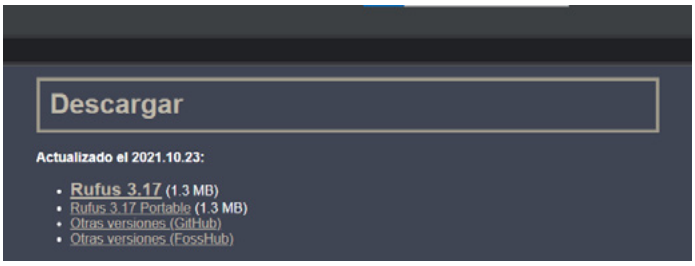

Imagen 7. Instalación de Rufus.

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

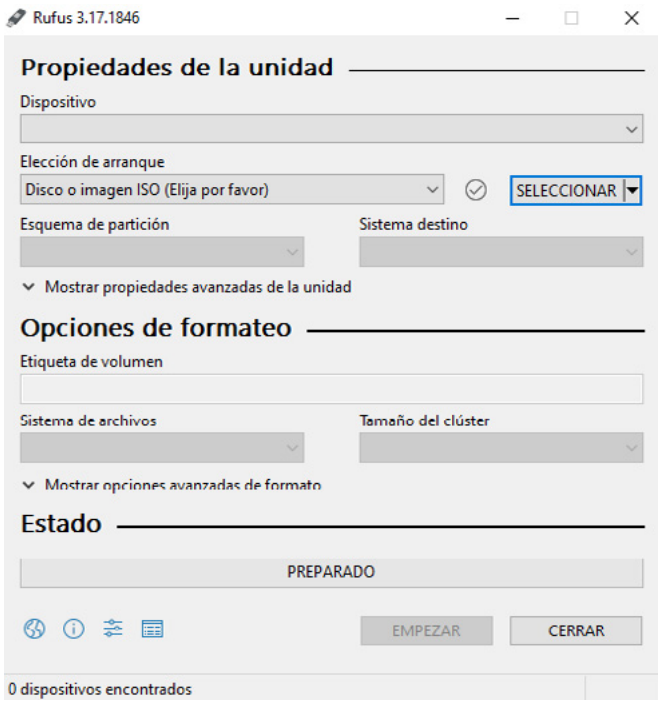

Imagen 8. Rufus.

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.

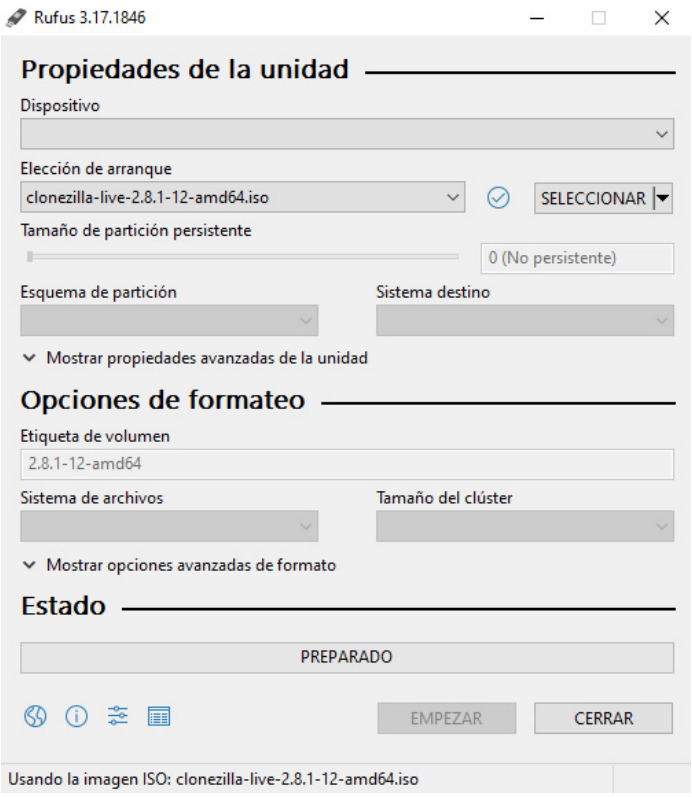

Imagen 9. Rufus con una imagen de Clonezilla.

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.

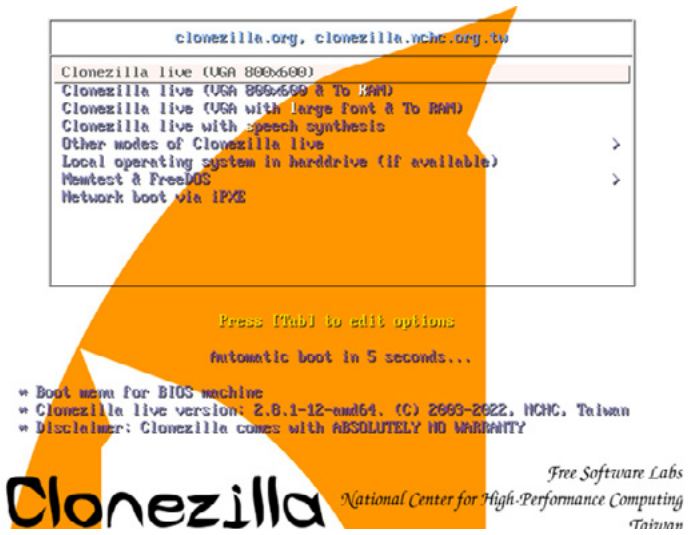

Imagen 10. Clonación con Clonezilla 1.

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.

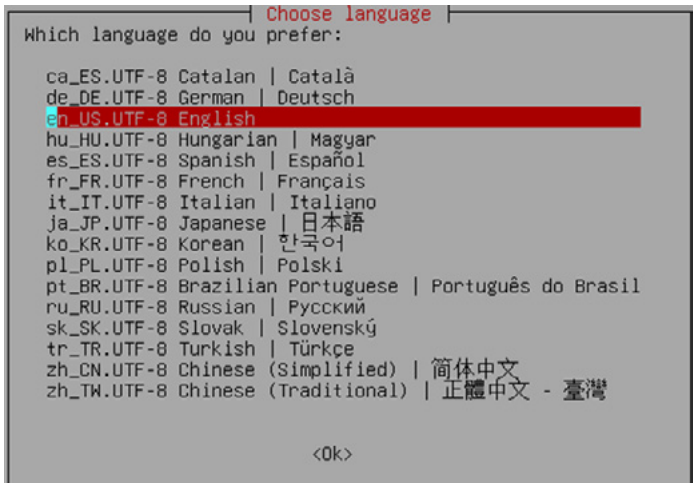

Imagen 11. Clonación con Clonezilla 2.

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.

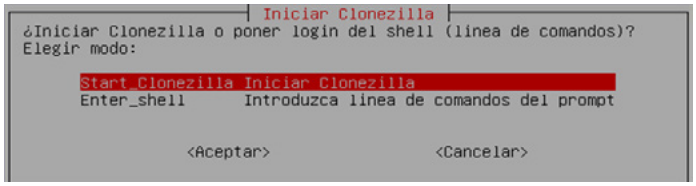

Imagen 12. Clonación con Clonezilla 3.

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.

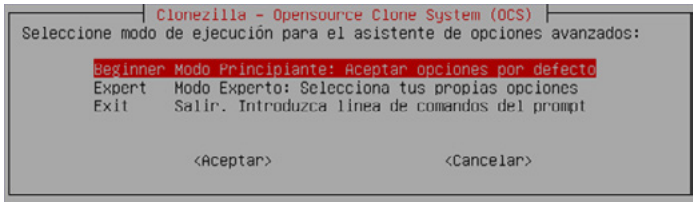

Imagen 13. Clonación con Clonezilla 5.

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.

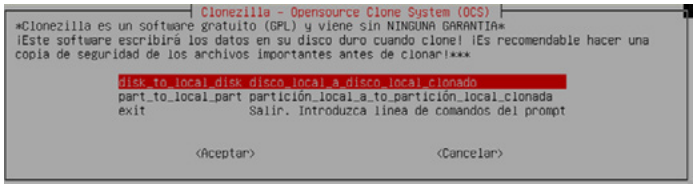

Imagen 14. Clonación con Clonezilla 6.

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.

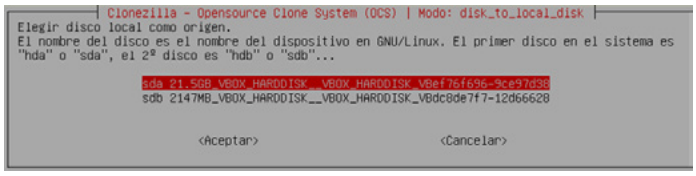

Imagen 15. Clonación con Clonezilla 7.

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

Imagen 16. 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.

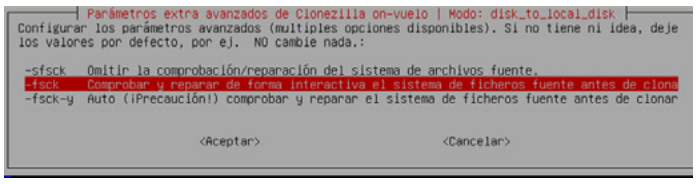

Imagen 17. Clonación con Clonezilla 9.

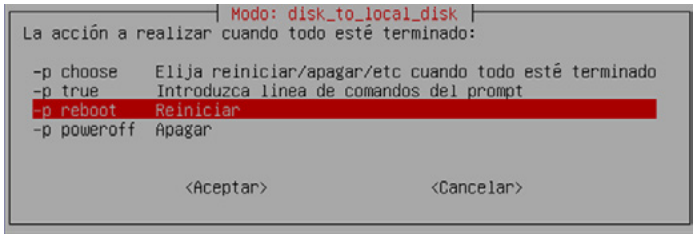

Imagen 18. Clonación con Clonezilla 10.

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.

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.

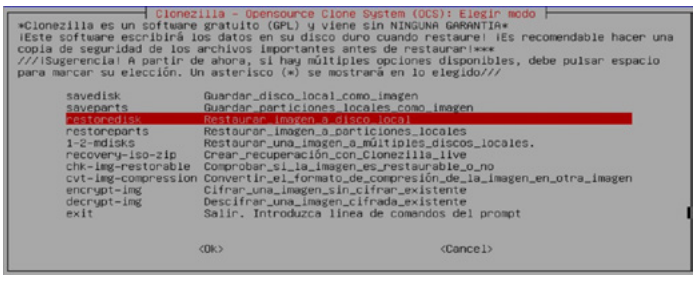

Imagen 19. Restauración de una copia de seguridad con Clonezilla.

4.3. Las copias de seguridad o backups

Las copias de seguridad o *backups* son herramientas que se usan en la informática para respaldar la información de modo que si ocurre un incidente que suponga la perdida de información esta esté replicada en algún sitio y se pueda recuperar.

Cuando se hace una restauración de una copia de seguridad esto implica que se recupera toda la información contenida en la copia.

4.3.1. Tipos de copias de seguridad

Hay veces en las que no es posible realizar copias de seguridad completas de toda la información almacenada, ya sea por falta de recursos o porque no es lo deseado y por eso tenemos tres tipos de copias de seguridad:

- **Completas o totales:** este tipo de copias almacenan en el backup toda la información que albergamos. Además, activan el atributo o flag de modificado para todos los archivos.
- **Incrementales:** en este tipo de copias solo se copia lo que ha sido cambiado o modificar y desactivan el flag de modificar de los archivos que se copian.
- **Diferenciales:** solo se copian los archivos modificados.

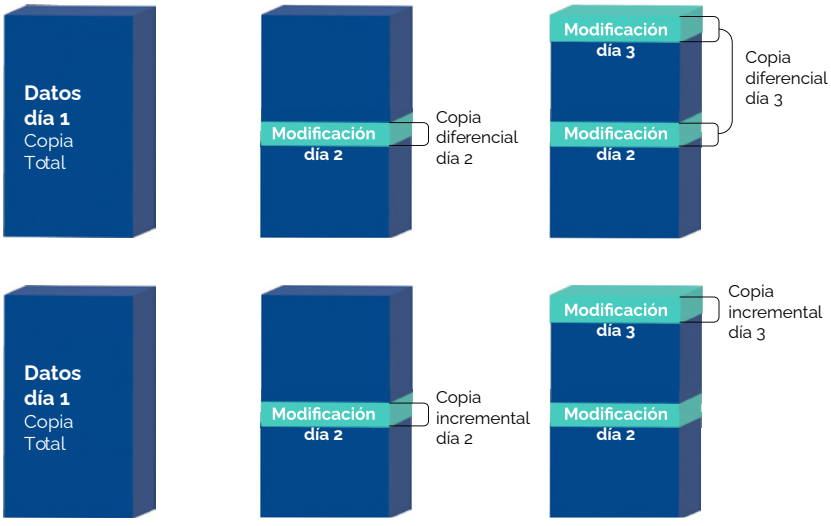

Imagen 20. Tipos de copia de seguridad.

NOTA

La diferencial real entre una copia de seguridad incremental y una diferencial es que en la segunda nunca se desactiva el flag de modificado.

Es conveniente que las copias de seguridad no se espacien mucho en el tiempo, porque si por ejemplo realizamos una copia el lunes y los datos los perdemos jueves, los de martes y miércoles no se podrán recuperar.

4.3.2. Restauración de los backups

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

- **Paso 1.** Se restaura la última copia de seguridad total.
- **Paso 2.** Si tenemos copias de seguridad incrementales se restauran de la más antigua a la más moderna siempre que sean posteriores a la copia de seguridad total.
- **Paso 3.** Si tenemos copias de seguridad diferenciales y no haya ninguna total o incremental posterior, se restaura la más moderna de estas.

4.3.3. Consejos a la hora de realizar copias de seguridad

A la hora de realizar copias de seguridad debemos de tener en cuenta los siguientes aspectos de manera fundamental:

- **Orden y claridad:** el nombre que le pongamos a la copia debe de ofrecernos una buena descripción de que contiene y de cuando es la copia.
- **Comprobación de las copias:** debemos de comprobar habitualmente si las copias de seguridad se realizan y si se encuentran en buen estado.
- **Localización:** debemos de intentar que las copias se almacenen en un lugar distinto al de la realización, porque en caso de fallo físico perderíamos ambas informaciones.
- **Automatización:** es conveniente que esta tarea se automatice para ahorrar costes.
- **Calendario:** todos los *backups* deben de estar planificados además de su tipo.
- **Simulacros:** es conveniente que se realicen simulacros de perdida de datos para poder comprobar que la restauración funcionaria.
- **Protección:** los *backups* deben de tener una protección igual a la del sistema cuando no superior para evitar ataques y filtraciones.

4.4. RAID

RAID significa Redundant Array of Independent Disks o conjunto redundante de discos independientes. Esto quiere decir que cogeremos dos o más discos duros por lo general de manera redundante para que el proceso de lectura de memoria sea más eficiente al mismo tiempo que protegemos al sistema frente a los posibles fallos de alguno de los discos.

Cuando nos referimos a redundancia normalmente estaremos hablando de una seguridad de los datos mayor porque al implementar casi todos los tipos de RAID, menos el RAID 0, que veremos más adelante, tenemos una garantía de que, si un disco cae, otro hará su labor para que nuestro sistema siga en funcionamiento. Si no tenemos un RAID implementado, la caída de un disco significa la caída del sistema (casi siempre).

Hay dos tipos de implementación de RAID:

- **Por software.** Es el tipo más económico pero el más lento. Este tipo de RAID no se suele implementar tanto debido a que su eficiencia pierde mucho y se nota a la hora de trabajar con ellos, Una ventaja es que hay varios sistemas como Windows Server que llevan implementada una opción de soporte RAID.
- **Por hardware.** Es la opción más cara pero la mejor en cuanto a eficiencia nos referimos y por eso es el más usado. Para crearlos se usa una controladora RAID ya que son fáciles de configurar y gestionar.

NOTA

Hay algunas placas base muy baratas que implementan RAID por software con un rendimiento muy malo, ralentizando el funcionamiento en gran medida. Estos son los llamados fake RAID y no está recomendado que se usen en entornos profesionales.

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

Este tipo de RAID también se denomina striping y no usa ningún mecanismo de seguridad.

La información almacenada en los discos se divide en bloques y se reparte entre los discos que formen el RAID, generalmente 2.

Este tipo de RAID, es decir, este stripe se usa realmente para que el aumento en la lectura y en la escritura de un sistema aumente porque la información está repartida en varios discos.

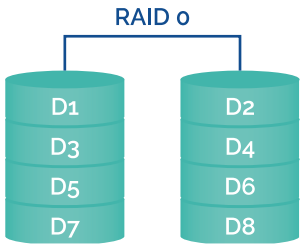

Imagen 21. Esquema de RAID 0.

4.4.2. RAID 1

Al RAID 1 también se le puede llamar mirroring o discos en espejo. Este tipo de RAID se suele componer de dos discos donde la información se encuentra replicada, es decir, ambos discos tienen la misma información. Este tipo de RAID sí que nos previene de un fallo de hardware, porque si uno de los discos falla la información se encuentra alojada en el otro.

El problema de esta implementación es que sufre de overload o sobrecarga, que viene dada porque solo se aprovecha la mitad de espacio del sistema, ya que se ocupa el doble por cada archivo que contengamos debido a la replicación.

Imagen 22. Esquema de RAID 1.

NOTA

Cuando configuremos un RAID 1 deberíamos de hacerlo con discos totalmente iguales, ya que, si por ejemplo uno de los dos tiene menos velocidad o almacenamiento, solo se podrán usar las prestaciones menores.

Otra de las ventajas que otorga un RAID en espejo es que la velocidad de lectura aumenta, porque se puede leer la información de ambos discos de manera simultánea. Por otro lado, la escritura permanecerá constante.

NOTA

Nos referimos a paridad como la información adicional que se escribe en un conjunto de discos con el propósito de que, si alguno falla, se pueda recuperar la información ya que se encuentra recogida en alguno de los otros discos.

Cuando se reemplace el disco afectado y el RAID esté reestablecido, la paridad se calcula de nuevo.

4.4.3. RAID 5

El RAID 5 se trata de un sistema redundante en el que la paridad que se conseguía en el apartado anterior se reparte por todos los discos del stripe. Para poder conseguir este tipo de RAID es necesario mínimo que haya 3 discos.

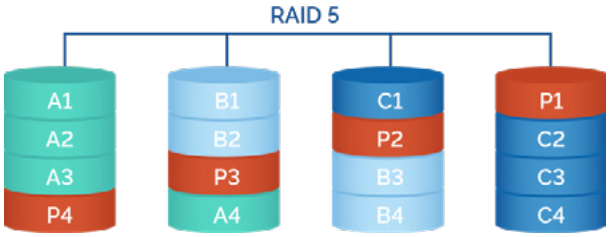

Imagen 23. Esquema de RAID 5.

NOTA

Como podemos observar, del RAID 1 pasamos directamente al RAID5, esto es porque los RAID 2, 3 y 4 no se usan debido a que pierden mucho en costes, protección y rendimiento.

Como la información se encuentra distribuida entre todos los discos, se aumenta la tasa de escritura porque hay que escribir menos información en cada uno de los discos.

Además, la sobrecarga es menor porque se reduce a un 25% debido a la repartición de la información.

Hay que aclarar que el RAID 5 previene del fallo de un disco, pero en cuanto falle otro ya habría otra pérdida de memoria, aunque no de manera completa.

4.4.4. RAID 6

El RAID 6 funciona del mismo modo que el RAID 5, distribuyendo la información entre todos los discos, pero en este tipo se añade otro bloque de paridad.

La sobrecarga de estos discos es de N-2, lo que hace necesario que haya más discos que en el RAID 5 ya que la sobrecarga es mayor.

Este RAID se aconseja para los sistemas que tienen varios discos porque si tenemos pocos, se vuelve muy ineficiente ya que se destina mucho a la paridad. Por otro lado, si tenemos varios discos, la perdida de almacenamiento se disimulará bastante más.

Como el cálculo de paridad es el doble, pierde tasa de escritura con respecto al RAID 5.

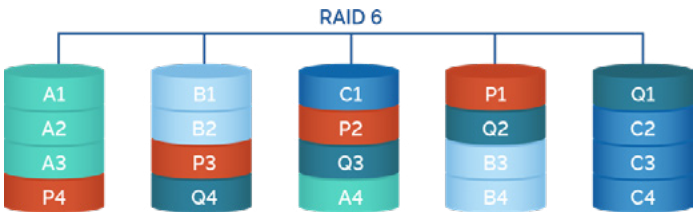

Imagen 24. Esquema de RAID 6.

Este tipo de RAID sí que sobreviviría sin problema al fallo de dos discos.

Resumen de los principales tipos de RAID.			
RAID	Ventajas	Desventajas	Mínimo de discos
RAID 0	Excelente rendimiento.	No ofrece ninguna protección.	2
RAID 1	Buena protección y rendimiento alto.	Sobrecarga alta, del 50%.	2
RAID 5	Económico y rápido.	No hay protección frente a un fallo múltiple en los discos.	3
RAID 6	Puede sobrevivir al fallo de hasta dos discos al mismo tiempo.	Ineficiente si hay pocos discos, su tasa de escritura disminuye.	4

4.4.5. Sistemas RAID anidados

Hay veces en las que por necesidades del sistema se deben implementar dos tipos distintos de RAID al mismo tiempo, y esos son los llamados **sistemas RAID anidados**. Con esto no se pretende nada que no sea la combinación de las características de los RAID para aumentar la seguridad frente a fallos, por eso se deben de juntar solo algunos tipos, que los vamos a ver a continuación.

RAID 0 + 1

En estos RAID lo primero que hacemos es implementar un RAID 0 y después se le aplica un RAID 1, es decir, duplicar en espejo el RAID 0 que se ha creado, primeramente.

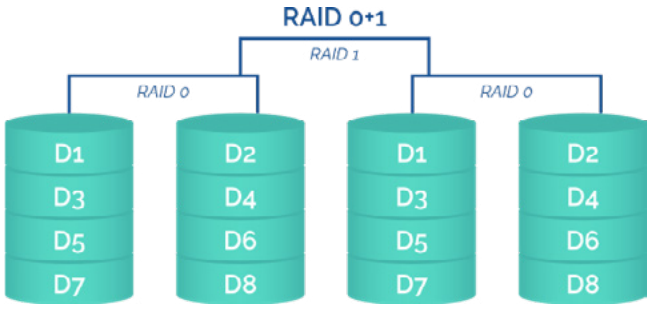

Imagen 25. Esquema de RAID 0 + 1.

Para poder realizar este tipo de RAID se necesitan mínimo 4 discos, dos por cada RAID 0 y mínimo dos RAID 0 conjuntamente para formar el RAID 1. La sobrecarga aquí es realmente la misma que en el RAID 1, del 50%.

RAID 10 o 1 + 0

Este tipo de RAID funciona contrario al anterior, primero se crean dos RAID 1 y juntos se implementa un stripe con ellos.

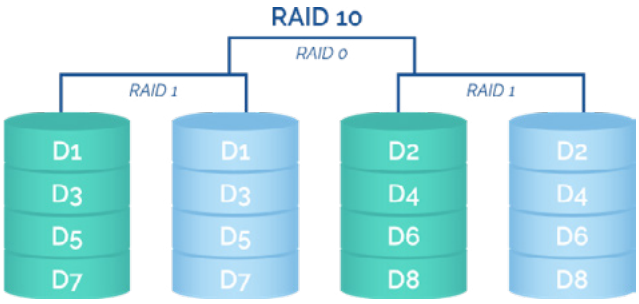

Imagen 26. Esquema de RAID 10.

Como ocurría con el RAID 0 + 1, necesitamos al menos cuatro discos para poder implementarlo, además de que su sobrecarga sigue siendo del 50%.

NOTA

Suele implementarse en mayor medida un RAID 1 + 0 en vez de un RAID 0 + 1, porque supuestamente será más tolerante a fallos porque si fallan dos discos que no se encuentran en el mismo espejo, podríamos seguir funcionando.

RAID 50

Si lo que queremos es no tener una sobrecarga tan alta como en el caso de los dos anteriores, se puede recurrir a los RAID 50, que se basan en crear mínimo dos RAID 5 e implementarlos en un stripe. Su sobrecarga es mucho menor que los anteriores mientras que mantiene una alta protección frente a fallos de hardware.

www.universae.com