

1. Explica las diferencias entre los tipos de copias de seguridad: completas, diferenciales e incrementales.

- **Completas:** Realiza la copia de todo el contenido de la carpeta seleccionada.
- **Diferenciales.** Realiza la copia de los ficheros que hayan cambiado desde la última copia completa.
- **Incrementales.** Realiza la copia de los ficheros que hayan cambiado desde la última copia completa o incremental.

Ventajas y desventajas:

Completa: Fácil de restaurar. Necesita más espacio, más tiempo y más ancho de banda (si va a remoto)

Diferencial: Necesita menos espacio y menos tiempo para efectuarse que una completa pero más que una incremental (generalmente). La restauración sólo necesita la última completa y la diferencial.

Incremental: Necesita poco espacio y poco tiempo para efectuarse, pero para la restauración es necesario tener la copia completa previa y todas las diferenciales e incrementales que se hayan hecho desde dicha copia completa.

2. ¿Cuál es el mínimo de discos necesario para configurar un RAID5?

Tres. Para distribuir eficientemente la paridad.

3. Indica cuántos discos pueden fallar, sin que se pierda la capacidad de recuperación de datos, para los siguientes niveles de RAID:

- **RAID0**
- **RAID1**
- **RAID5**
- **RAID0:** Ninguno, no hay redundancia. Se perderían los datos del disco fallido.
- **RAID1:** Uno. Los datos se duplican, por lo que si uno falla, se recuperan del otro.
- **RAID5:** Uno.
 - La información de los bloques de datos perdidos se puede recuperar a partir del bloque de paridad correspondiente a cada bloque perdido (que estará en otro disco) y los restantes bloques de datos relacionados repartidos entre los otros discos.
 - El bloque de paridad que contenía el disco fallido se refiere a datos contenidos en los otros discos, por lo que se podrá calcular de nuevo, recuperando así toda la información.

4. ¿Qué nivel RAID, con posibilidad de recuperar datos ofrece una mejor proporción coste-tamaño final?

RAID5, ya que, para N discos, se obtiene una proporción aproximada de espacio equivalente a N-1 discos para datos y 1 disco para paridad. Por ejemplo, con 4 discos, el equivalente al espacio de 3 de ellos podrá contener datos, y 1 paridad.

5. ¿De qué RAID no se puede recuperar la información si se estropea un disco?

RAID 0, ya que no proporciona redundancia de datos. Los datos se dividen entre los discos, sin duplicación, por lo que si un disco falla, se pierde la información que contiene.

6. Con 4 discos de 2 TB, ¿Con qué configuración RAID se consigue un disco de 6 TB?
RAID 5. Con 4 discos de 2 TB cada uno, RAID 5 utilizará el equivalente a 3 de los discos para datos y el equivalente a 1 para paridad, por lo que el espacio de datos viable será de 6 TB.
7. En un RAID5 de 3 discos, cuya paridad se calcula mediante XOR, calcula el bloque de paridad para los siguientes bloques de datos de 1 byte:

Disco1	Disco2	Disco3
11011000	1110101	10101101
10101100	11111101	1010001
00100000	00110111	00010111
00111100	00011111	00100011

Calculadoras XOR online, para comprobar resultados:

<https://xor.pw/#>

<https://www.compseclib.com/calculate/binaryxor?variation=default>

8. En un RAID5 de 4 discos, cuya paridad se calcula mediante XOR, calcula el bloque de paridad para los siguientes bloques de datos de 1 byte:

Disco1	Disco2	Disco3	Disco4
11100011	10110011	01101011	00111011
10101010	11100110	10000001	11001101
11100011	01111100	01110110	11101001
00000000	11111111	10101010	01010101

Calculadora XOR de n operandos, para comprobar resultados:

<https://toolslick.com/math/bitwise/xor-calculator>

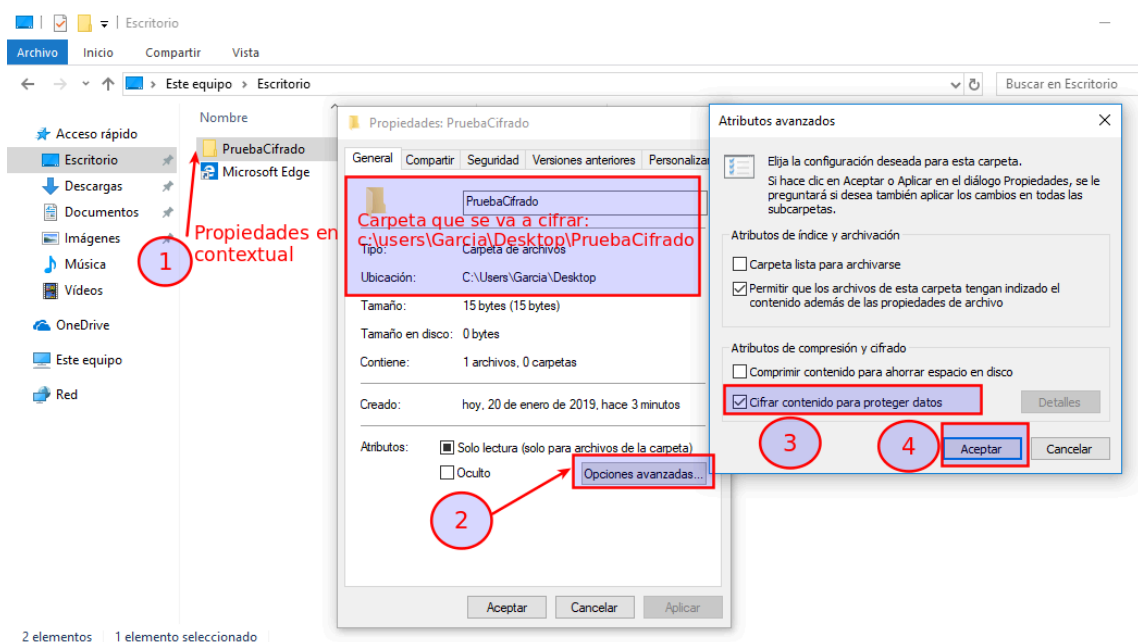
9. En una máquina virtual Windows 10, accede a “Copias de seguridad” e intenta programar una copia, como se indica en el apartado 1.1 de la UD7.

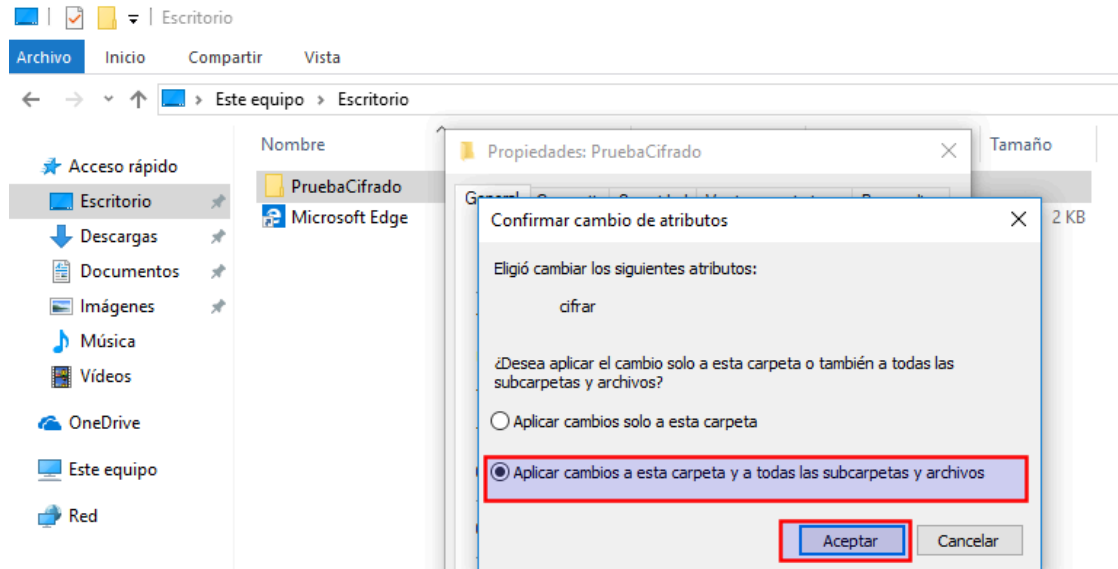
Necesitarás un disco duro extra (u otro dispositivo externo que reconozca la máquina virtual) en el que guardar la copia de las carpetas que selecciones. Si no lo tienes previamente, el siguiente tutorial muestra cómo añadirlo:

<https://www.youtube.com/watch?v=zPVvbmWE9q4>

Si no existe una unidad susceptible de albergar la copia, será necesario proveer una. Podemos crear un segundo disco (como se muestra en el tutorial) y posteriormente seguir los pasos indicados en el ap. 1.1. La herramienta permite añadir y eliminar las carpetas que deseemos incluir o excluir de la copia.

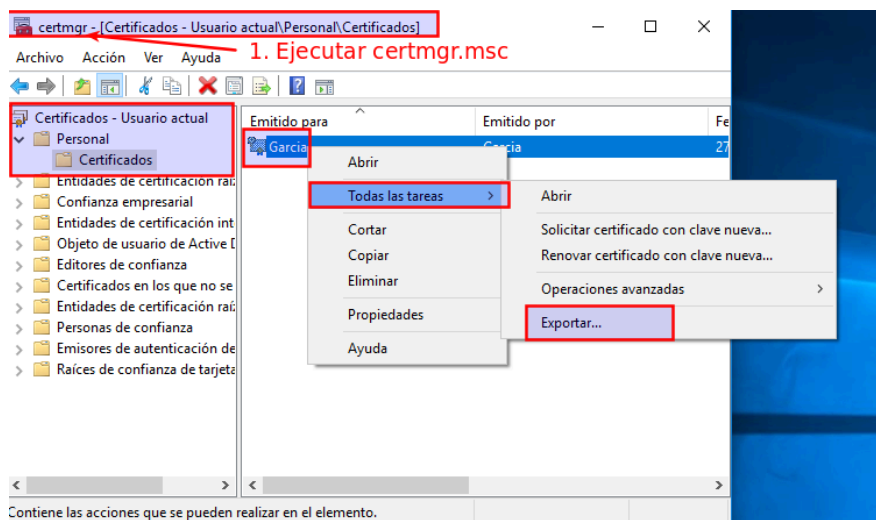
10. ¿De qué dos elementos podemos hacer imágenes? ¿Dónde se podría guardar cada tipo de imagen?
- Particiones y discos.
- Particiones: se pueden guardar en discos del sistema o dispositivos externos.
- Discos: se pueden guardar en dispositivos externos.
11. Si queremos hacer copias incrementales en Linux, ¿Qué herramientas podríamos usar?
- Rsync y Dump.
12. ¿Qué indican las siguientes extensiones de archivo generadas por tar: .tar .gz .tar.gz?
- Archivos .tar significa que están empaquetados.
 - Archivos .gz significa que están comprimidos.
 - Archivos .tar.gz significa que están empaquetados y comprimidos.
13. ¿Cuál es la diferencia entre clonar una partición y crear una imagen de una partición según el texto?
- Clonar: supone volcar exactamente la misma información de una partición a otra, incluyendo estructuras de archivos.
- Crear una imagen de una partición: implica el empaquetado (y, generalmente, compresión) de toda la información de la partición en un único archivo.
14. En Windows ¿Qué es EFS, para qué sirve? ¿Cómo se activa/desactiva y qué características tiene?
- Encrypting File System. Sirve para cifrar archivos y carpetas en el sistema de archivos NTFS, con acceso basado en usuario. Permite la activación y desactivación, mediante una casilla de selección accesible en las propiedades del archivo (Pestaña General/Avanzadas, casilla "Cifrar contenido para proteger datos"). En el caso de carpetas, también permite el cifrado recursivo de subcarpetas.
15. ¿Qué se recomienda hacer una vez se ha cifrado un archivo o carpeta con EFS en Windows?
- Hacer una copia de seguridad del certificado y la clave de cifrado en una unidad extraíble para poder recuperar los datos en caso de pérdida o daño de la clave original.





16. ¿Cuál es el procedimiento para exportar el certificado y la clave de cifrado en Windows utilizando EFS?

Se ejecuta el programa de certificados de Windows 10 (certmgr.msc). Se selecciona el certificado personal creado al cifrar la carpeta, y luego se exporta la clave privada con una contraseña.



17. Describe las ventajas y desventajas de RAID por hardware frente a RAID por software:

Ventajas HW:

- **Mejor rendimiento:** la tarjeta controladora se encarga de las transferencias (no ocupa al SO ni la CPU)
- **Fácil de configurar**
- **Si se estropea un disco, se cambia y la controladora replica (reconstruye) la información.**

Desventajas HW:

- **Coste económico de la tarjeta**
- **La tarjeta controladora se puede estropear.**
- **El RAID hay que crearlo con los discos enteros, mientras que en un RAID por software también se puede crear con porciones de discos duros.**

18. ¿Qué significa que un volumen sea dinámico y qué configuraciones de discos permite establecer, Windows, cuando creamos un volumen dinámico?

Un volumen dinámico permite utilizar porciones de distintos discos (volumen distribuido) o no contiguas del mismo disco (volumen simple).

Al crear volúmenes dinámicos en Windows, podremos seleccionar que se cree un RAID por software con ellos:

- **Volumen reflejado:** equivale a crear un RAID 1.
- **Volumen seccionado:** equivale a crear RAID 0
- **Volumen RAID 5:** como indica su nombre sirve para crear un RAID 5.

19. En una máquina virtual Windows 10, crea las siguientes configuraciones:

- **Un RAID0 de 2 discos.**
- **Un RAID1 de 2 discos.**
- **Un RAID5 de 3 discos (será necesario añadir tres unidades de almacenamiento en disco, aparte de la del sistema).**

Tutoriales de ejemplo con creación de RAID:

RAID0: <https://www.youtube.com/watch?v=8Spalnvz2zo>

RAID1: <https://www.youtube.com/watch?v=cpBCqax2pN4>

RAID5: <https://www.youtube.com/watch?v=K7y0p9uevXA>

En el canal podéis encontrar tutoriales de otras configuraciones de RAID (que se escapan al alcance de este módulo, pero pueden ser de vuestro interés)

20. En una máquina virtual Windows 10 de la actividad, cifra un volumen con Bitlocker, activando el acceso mediante contraseña (como se indica en el apartado 3.2 de la UD7).

Tutorial de cifrado de disco con Bitlocker: <https://www.youtube.com/watch?v=BfEJXX3oTf4>