



7. Copias de seguridad, cifrado y RAID

Autor	ⓧ Xerach Casanova
Clase	Sistemas Informáticos
Fecha	@Feb 27, 2021 5:42 PM

Copias de seguridad. Backup de datos

1.1. Copias de seguridad en Windows

Herramienta "Copias de seguridad de Windows"

1.2. Copias de seguridad en Linux

Empaquetar y comprimir archivos con tar

Extensiones utilizadas para la herramienta tar

Empaquetado y compresión con tar

2. Clonaciones e imágenes de discos duros y particiones

2.1. Conceptos. Herramientas

Clonaciones

Herramientas para crear imágenes y clonaciones.

2.2. Ejemplo. Crear una imagen con Clonezilla.aula

3. Cifrado de archivos y particiones

3.1. Cifrado de archivos en Windows con EFS "Encrypting File System". Sistema de encriptación de ficheros.

Procedimiento para cifrar un archivo o carpeta con EFS

Exportar certificado y clave

Importación de certificado

3.2. Cifrado de unidades lógicas en Windows con BitLocker

3.3. Cifrado de archivos y unidades lógicas con Veracrypt

Ejemplo completo. Instalar VeraCrypt y crear un contenedor seguro en una unidad extraíble.

Utilización del contenedor en Windows

Instalación en GNU-Linux

Utilización del contenedor en GNU-Linux.

4. Sistemas RAID

4.1. Sistemas RAID

Tipos de RAID

4.2. Funcionamiento de un disco de paridad.

4.3. RAID por hardware o por software. Ejemplo.

RAID por Software en Windows. Discos dinámicos

Ejemplo de creación de un RAID 0 por software en Windows

Copias de seguridad. Backup de datos

El objetivo de un backup o copia de seguridad es guardar las carpetas y archivos de los usuarios, No importa la instalación del sistema, sino que los datos estén guardados en más de un sitio para evitar su pérdida.

1.1. Copias de seguridad en Windows

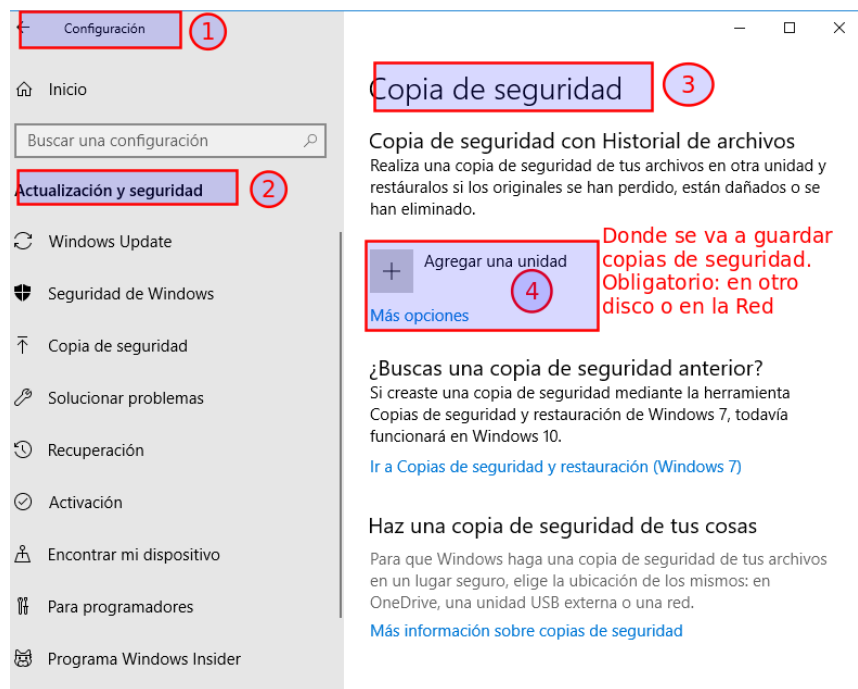
Existen distintos tipos:

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

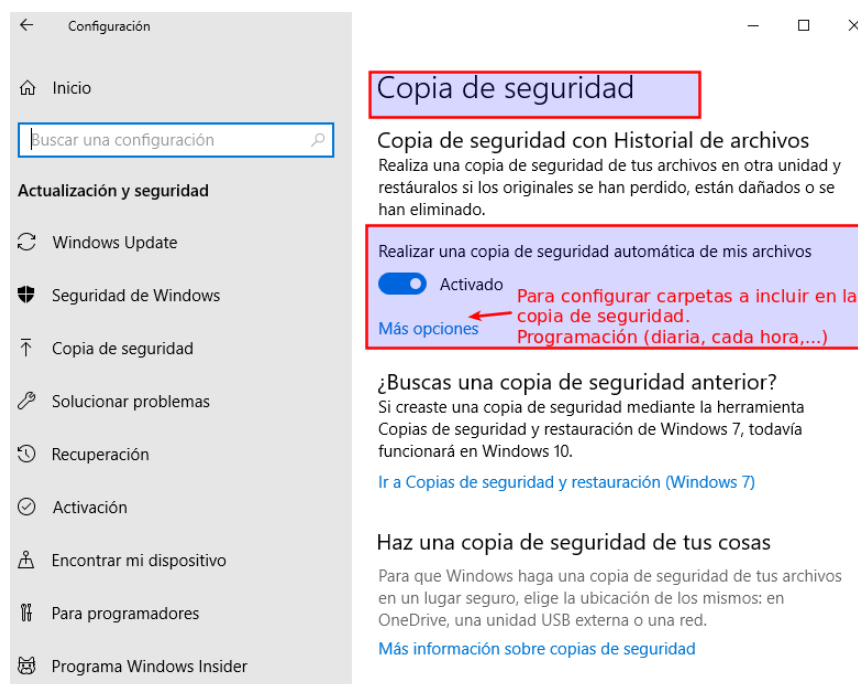
Herramienta "Copias de seguridad de Windows"

En Windows existe la herramienta "Copias de seguridad" (Configuración / Actualización y Seguridad / Copias de seguridad).

Agregar una unidad: Es obligatorio guardar la copia de seguridad en otro disco (interno, externo, pendrive o en la red).



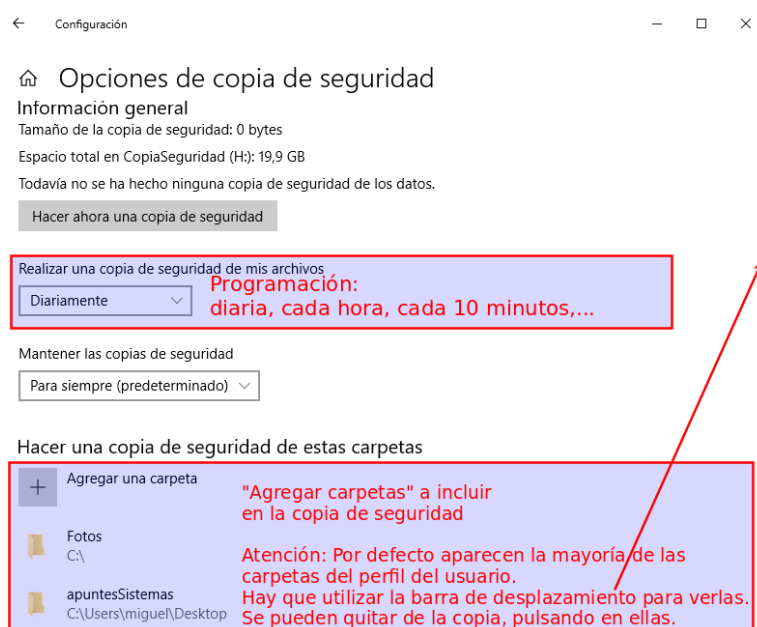
Una vez agregada la unidad, aparece activado "realizar una copia de seguridad", pulsando en "Más opciones se puede seleccionar carpeta y programación de tarea.



En la ventana que se abre, se configura:

- Periodicidad de la copia de seguridad.
- Durante cuanto tiempo se realizan las copias.

- Agregar una carpeta. Para seleccionar los archivos y carpetas a incluir en la copia de seguridad.



Restaurar una copia de seguridad: En la misma ventana de copias de seguridad, en la parte baja se encuentra la opción "Restaurar copia".

También hay herramientas externas como Ghost y Acronis para realizar copias de seguridad.

1.2. Copias de seguridad en Linux

En Linux hay bastantes herramientas de copias de seguridad: tar, rsync, scp y dump. Todas ellas se usan en modo comando. En el modo gráfico se puede utilizar tar.

Empaquetar y comprimir archivos con tar

La herramienta tar se utiliza para:

- Crear copias de seguridad.
- Empaquetar y comprimir archivos (como los zip o rar de Windows).
- Crear copias de seguridad idénticas a la original.

Cuando copiamos una carpeta, cambian muchas propiedades de los archivos. El usuario propietario es quien realizó la copia, independientemente del

propietario original, así que los permisos de los nuevos archivos serán los que se crean por defecto y no los originales. La copia tiene como fecha de creación la hora en la que se realizó, pero se puede preservar la fecha de modificación utilizando `cp -p` (p de preservar), para hacer una copia idéntica. En entorno gráfico no existe esta opción.

Extensiones utilizadas para la herramienta tar

En linux hablamos de: `.tar` (empaquetados), `.gz` (comprimidos), `.tar.gz` (empaquetados y comprimidos).

Empaquetado y compresión con tar

En este ejemplo crearemos una copia de seguridad con todos los directorios `$HOME` de los usuarios y la guardaremos y descomprimiremos en una carpeta llamada `/copy_home`

```
cd/home
tar -cvzf home.tar.gz *
mkdir /copia_home
mv /home/home.tar.gz /copia_home
cd /copia_home
tar -xvzf home.tar.gz
```

- Primero vamos al directorio `/home`
- Creamos el archivo `home.tar.gz` empaquetado y comprimido con todo lo que hay en el directorio.
- Creamos la carpeta `/copia_home`
- movemos el archivo a la carpeta `/copia_home`
- descomprimimos el archivo y desempaquetamos. El programa admite más sintaxis, en esta se refleja la sintaxis principal.

2. Clonaciones e imágenes de discos duros y particiones

2.1. Conceptos. Herramientas

Cuando instalamos un PC, nos interesa crear una imagen del sistema instalado, para que en el futuro, ante posibles errores o para obtener un sistema limpio,

podamos restaurar esa imagen.

Las opciones son:

- **Crear una imagen de una partición:** Empaquetar y comprimir toda la información de la partición en un único o unos pocos archivos. Estos los podremos guardar en otro disco duro o en otra partición del mismo.
- **Crear una imagen de un disco:** Se puede crear una imagen de un disco duro completo. En él se guardarán todas las particiones en el estado actual, la podremos guardar en otro disco pero no en una partición del mismo disco.
- **Restaurar una imagen en una partición:** Utilizamos el mismo software para restaurar la imagen. Será necesario que esa partición exista (nos pregunta el disco y la partición de destino). La partición se reescribe volcando la imagen, dejándola tal y como se creó.
- **Restaurar una imagen en un disco.** De la misma forma, restaurar un disco hará que se vuelque la imagen dejando el disco tal cual se creó la imagen.

Clonaciones

Hablamos de volcar la misma información de una partición o disco en otra partición o disco dejándola igual. Las opciones son:

- Clonar un disco a otro disco
- Clonar una partición a otra partición.

Herramientas para crear imágenes y clonaciones.

Se pueden utilizar tanto en Windows como en Linux:

Clonezilla

Software libre basado en GNU-Linux utilizable en Windows. Se utiliza un CD o pendrive de arranque. Existe una versión para realizar imágenes en la red (DRBL-Clonezilla).

Comando dd de GNU-Linux

el comando dd sirve para clonar discos duros, particiones, crear imágenes y copiar dvd.

Ejemplo:

Clonar toda la información de un disco origen (suponer sda) en otro disco destino (suponer sdb). Por supuesto el disco destino, tiene que ser igual o más grande que el origen (una vez clonado, se podrían redimensionar las particiones con Gparted)

```
sudo dd if=/dev/sda of=/dev/sdb bs=1M
```

Otras aplicaciones privativas o comerciales:

- Norton Ghost
- Acronis

La ventaja sobre Clonezilla es que si el origen de un disco es más grande que el destino, se redimensionan las particiones del destino de forma automática.

2.2. Ejemplo. Crear una imagen con Clonezilla.aula

Paso 1. Preparación inicial de la máquina de Windows.


Se va a crear una imagen de la partición del primer Windows instalado en la unidad 1. Para tener un disco bastante limpio, restaura la instantánea creada en la tarea SI01.

Sino creaste esa instantánea, utiliza el administrador de discos para eliminar las particiones creadas para segundo Windows y posteriores. Se parte de una situación parecida a la siguiente: Disco de 100 GB con 2 particiones y espacio libre:


- Partición de 550MB con el espacio reservado para Windows.
- Partición de 50000MB con primer Windows instalado en tarea SI01.
- Espacio libre en resto del disco.

Con el administrador de discos de Windows crear una partición de 40000MB en espacio libre con sistema de archivos NTFS. La situación del disco será aproximadamente:

🏠 Opciones de copia de seguridad

 Música
C:\Users\miguel

Excluir estas carpetas

 Agregar una carpeta

Realizar una copia de seguridad en una unidad distinta

Debe dejar de usar la unidad de copia de seguridad actual antes de agregar una nueva. Esto no eliminará ningún archivo de la unidad de copia de seguridad actual.

Dejar de usar la unidad

Opciones de configuración relacionadas

[Ver la configuración avanzada](#)

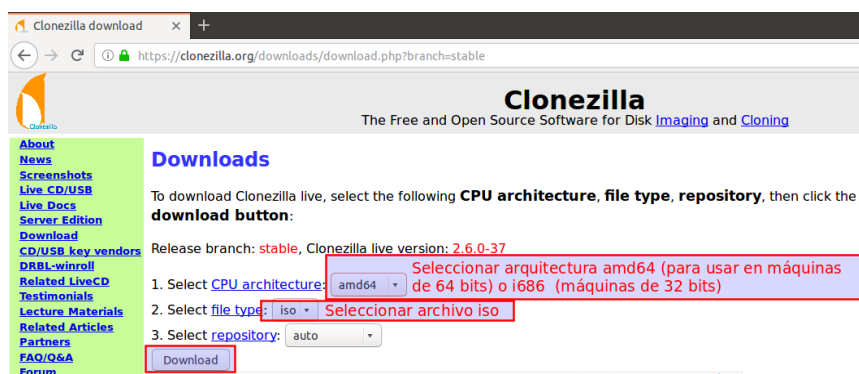
Restaurar copia de seguridad

[Restaurar archivos desde una copia de seguridad actual](#)

¿Tienes alguna pregunta?

[Obtener ayuda](#)

Paso 2. Descarga de Clonezilla. Descargar la versión estable (stable 2.6.0.37 en el momento de la realización de este material). El archivo a descargar, es el archivo iso correspondiente al CD de Clonezilla. Para su descarga, seleccionar archivo iso de 32 o 64 bits, según Windows instalado. En principio, la de 64 bits será más eficiente en PC de 64 bits, pero sin embargo la de 32 bits funcionará en todos los PC.



Como se dijo en epígrafe anterior, estos programas se ejecutan desde autoarranque, por lo que siempre tendremos un archivo iso para grabar en CD o ponerlo en un pendrive de autoarranque con Yumi como hicimos en la tarea de la unidad 2.

En nuestro caso, vamos a realizar la práctica en VirtualBox, por lo que solo hay que descargar el archivo iso y montarlo como CD en la máquina virtual.

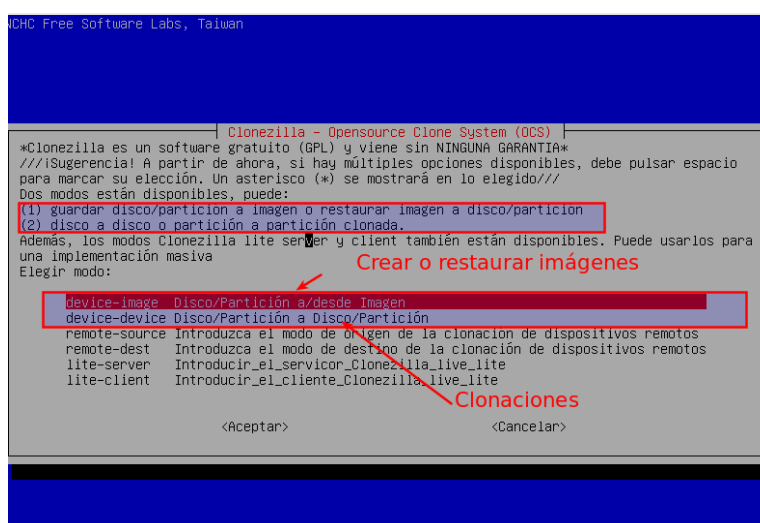
Paso 3. Inicio de Clonezilla.

Apagar la máquina Windows y poner como CD la iso descargada de Clonezilla. Iniciar la máquina con Clonezilla. Van apareciendo pantallas sucesivas, ir respondiendo:

- Clonezilla live
- Idioma español
- Mantener la distribución del teclado
- Iniciar Clonezilla

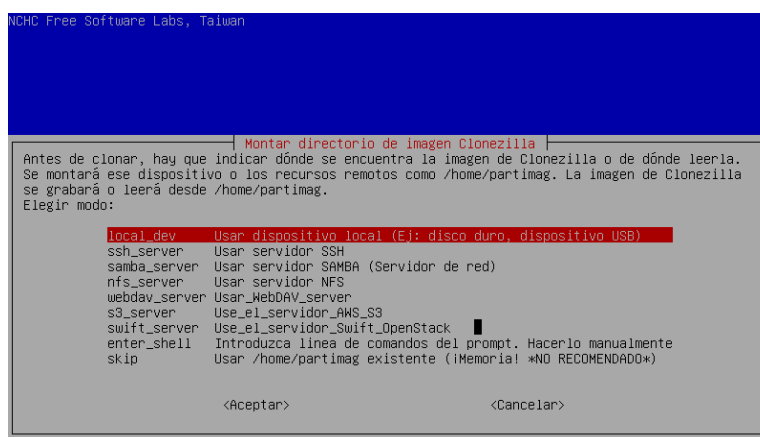
Paso 4. ¿Imagen o clonación?

En la siguiente ventana, aparece la primera opción importante. En nuestro caso seleccionar la primera opción "Disco particion a/desde Imagen", pues queremos crear una imagen. Fijarse que la segunda opción sería para realizar clonaciones.

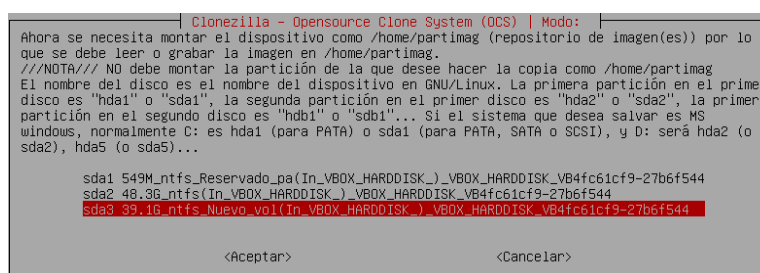


Paso 5. Seleccionar particion donde vamos a guardar o leer la imagen

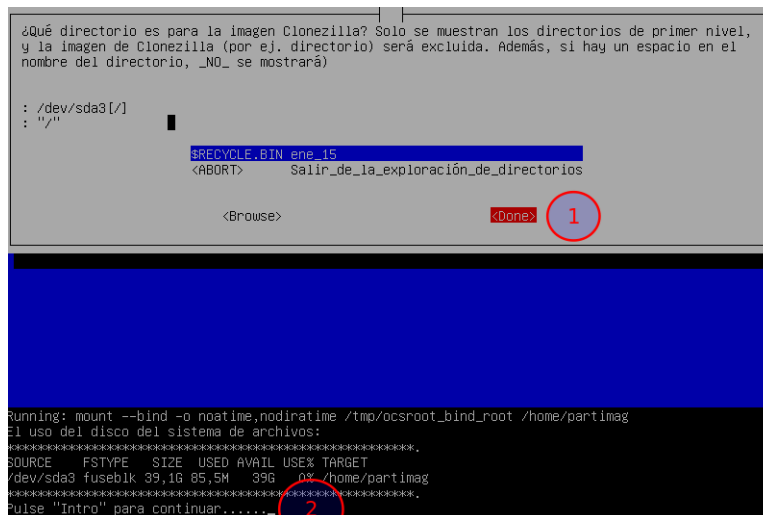
La ventana siguiente es muy importante interpretarla bien. Solo hay que pulsar Intro, pero tenemos que entender que vamos a seleccionar el disco y partición donde tenemos o vamos a guardar la imagen, en nuestro caso habrá que seleccionar la partición 3 donde guardaremos la imagen. De momento, pulsar Intro con la opción por defecto.



En la siguiente ventana, como solo hay un disco duro, nos pregunta directamente la partición. Seleccionamos sda3 que es donde vamos a guardar la imagen.

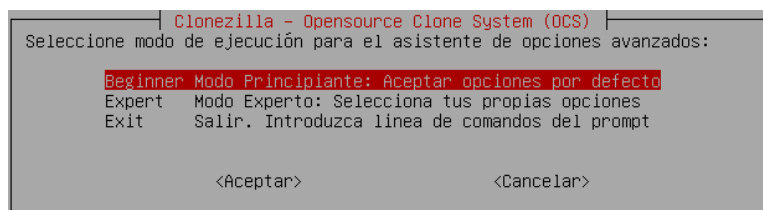


Al decirle que la imagen se va a guardar o se encuentra en sda3, explora la unidad y ve que no hay ninguna imagen, por lo que ya sabe que vamos a crear una imagen. De forma, que la siguiente pregunta es para decir en qué directorio guardamos, dejamos opciones por defecto. Pulsamos "Done" e "Intro"



Paso 6. Seleccionar modo principiante

En la siguiente ventana simplemente seleccionamos modo principiante.



Paso 7. Seleccionar particiones a incluir en la imagen

Después se pregunta si queremos crear una imagen del disco o de particiones. En nuestro caso la creamos de particiones.

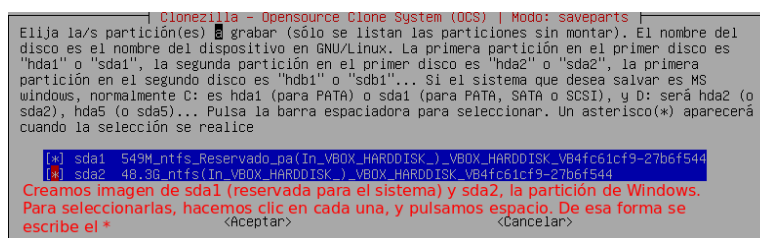
Recuerda que si quisiéramos crear una imagen del disco entero, deberíamos tener otro disco o pendrive, para guardar la imagen en otro sitio distinto.

Marcamos “ **Guardar particiones locales como imagen**”. En la imagen se ha marcado un cuadro que se entenderá en posteriores ventanas.

El siguiente mensaje solo es informativo, se crea una carpeta con la fecha para guardar la imagen. Pulsamos Aceptar.

En la siguiente ventana, debemos seleccionar las particiones a incluir en la imagen. Seleccionamos sda1 y sda2, de esta forma estamos guardando la imagen tanto de la partición reservada para el sistema como de la partición de

Windows. Para seleccionarlás, hay que hacer clic en cada una, y pulsar espacio. De esta forma aparece un * de que la partición está seleccionada.

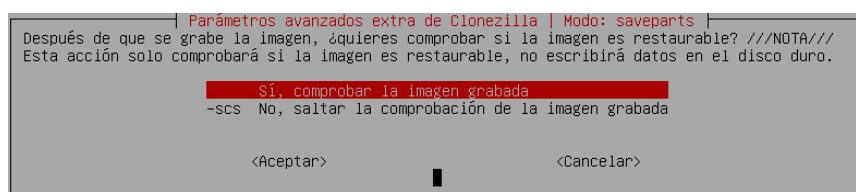


Paso 8. Últimas opciones

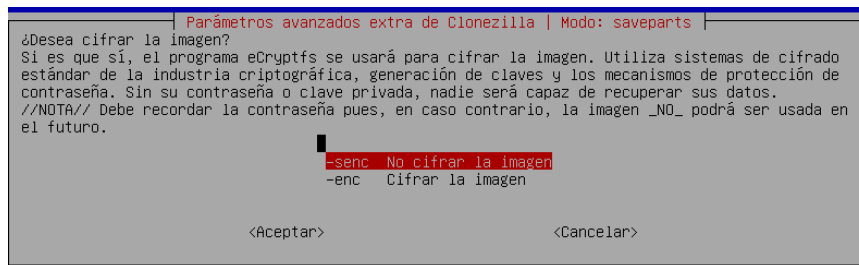
Las 2 ventanas siguientes preguntan si se quiere comprobar errores. En la primera pregunta si comprueba los errores de las particiones origen, le decimos omitir, pues ya dice la propia ventana que solo comprueba errores de sistemas de archivos de Linux.

En la segunda ventana, pregunta si se quiere comprobar errores de la imagen una vez creada. Le podemos decir que Sí y Aceptar. Esto alargará el tiempo de la creación de imagen, pero se sabrá que la imagen es correcta. Lo más importante, para tener éxito en la creación y restauración de imágenes, es que las particiones no tengan errores cuando se realiza la imagen, y que la última vez se haya apagado bien la máquina. Por ejemplo, es habitual ver la siguiente situación:

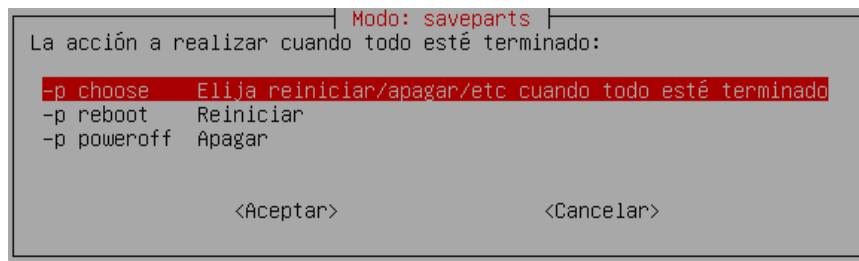
Se quiere clonar o crear una imagen. Se utiliza un CD o pendrive para arrancar el programa: Clonezilla, Acronis, Ghost,.. y al iniciar, se omite cambiar la BIOS para que inicie el CD (o pendrive). Windows empieza a arrancar, y se apaga a lo bruto, para iniciar el Cd. Ese estado del disco es inestable, si se crea la imagen así, lo normal es que falle.



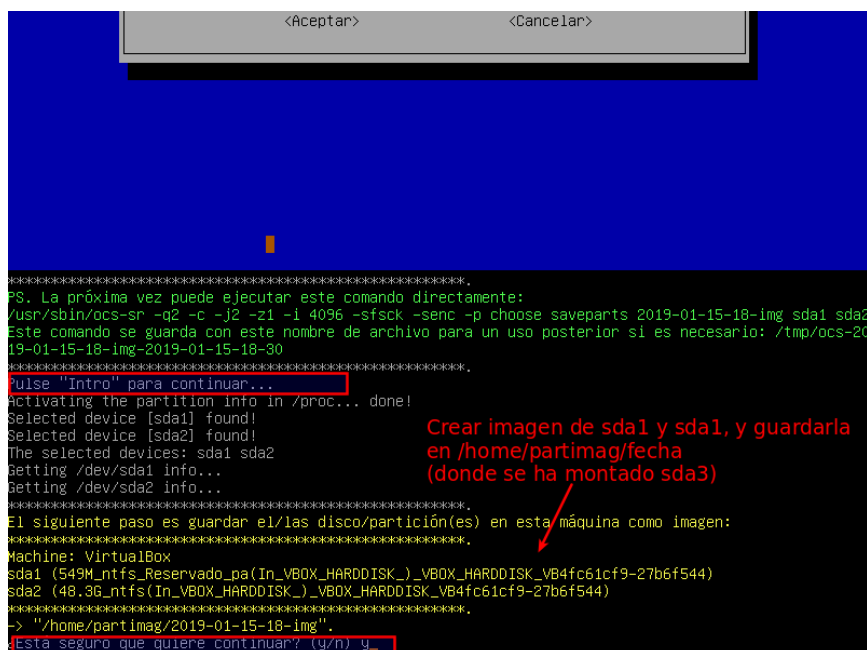
En la siguiente ventana, le decimos "No cifrar la imagen". Si la ciframos, nos pedirá una contraseña que tendríamos que usar al restaurar.



En la siguiente se pregunta que se quiere cuando se acabe de crear la imagen. Se ha seleccionado que presente un menú "Elija reiniciar/apagar...". Si prefieres, puedes pulsar Apagar.



La siguiente ventana es informativa de las acciones que se van a realizar. Se pulsa Intro e y para continuar.



Paso 9. Realizando las imágenes

Por fin se están realizando las imágenes de ambas particiones. Se pone captura del proceso en 2 instantes distintos.

```
Partclone
Partclone v0.3.12 http://partclone.org
Starting to clone device (/dev/sda1) to image (-)
Reading Super Block
Calculating bitmap... Please wait... done!
File system: NTFS
Device size: 575.7 MB = 140543 Blocks
Space in use: 415.7 MB = 101495 Blocks
Free Space: 159.9 MB = 39048 Blocks
Block size: 4096 Byte
```

Realizando imagen de sda1

Tiempo y velocidades en la creación de la imagen
Elapsed: 00:00:10 Remaining: 00:00:20 Rate: 812.19MB/min
Current Block: 72096 Total Block: 140543

Data Block Process:	<div><div></div></div>	32.56%
Total Block Process:	<div><div></div></div>	51.30%

```
Partclone
Partclone v0.3.12 http://partclone.org
Starting to clone device (/dev/sda2) to image (-)
Reading Super Block
Calculating bitmap... Please wait... done!
File system: NTFS
Device size: 51.9 GB = 12659199 Blocks
Space in use: 17.8 GB = 4348406 Blocks
Free Space: 34.0 GB = 8310793 Blocks
Block size: 4096 Byte
```

Realizando imagen de sda2

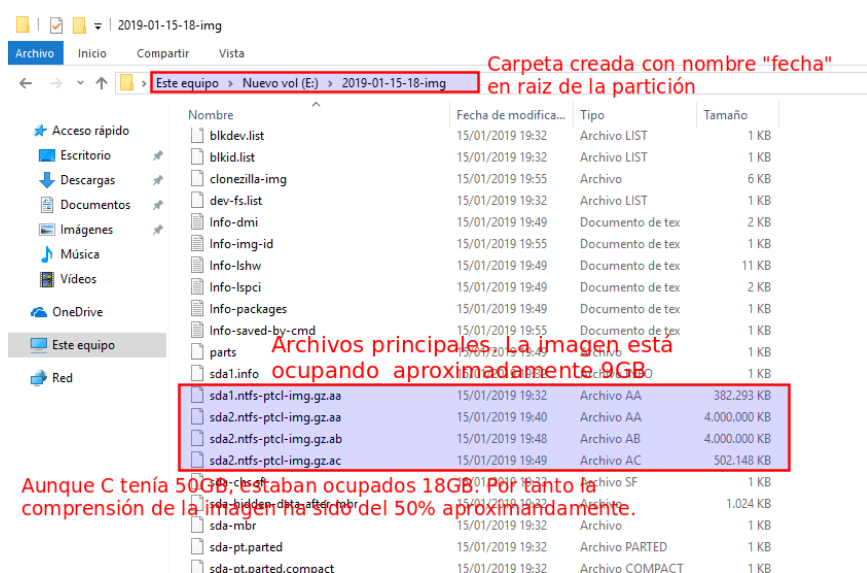
Elapsed: 00:15:09 Remaining: 00:01:10 Rate: 1.09GB/min
Current Block: 4260880 Total Block: 12659199

Data Block Process:	<div><div></div></div>	92.82%
Total Block Process:	<div><div></div></div>	33.66%

Una vez acabada, volverá al menú, donde se selecciona apagar el equipo.

Paso 10. Imágenes finalizadas. Comprobación de la carpeta creada con la imagen.

Iniciamos de nuevo la máquina Windows Sistemas en Windows (comprobando previamente que no esté montada la iso de Clonezilla). Una vez iniciada, se comprueba que se ha creado la imagen. Se pone captura. La partición de C tenía 50 GB, de los que estaban ocupados unos 18GB. Sin embargo la imagen ha ocupado 9 GB, es decir que la compresión es de un 50% aproximadamente.



Si fallara Windows en un futuro, podríamos restaurar las particiones "Reservado para el Sistema" sda1 y la partición "C:" sda2 de una forma muy similar con algún pequeño cambio en los menús.

3. Cifrado de archivos y particiones

3.1. Cifrado de archivos en Windows con EFS "Encrypting File System". Sistema de encriptación de ficheros.

Las herramientas EFS que ofrece Windows puede cifrar carpetas pero no particiones.

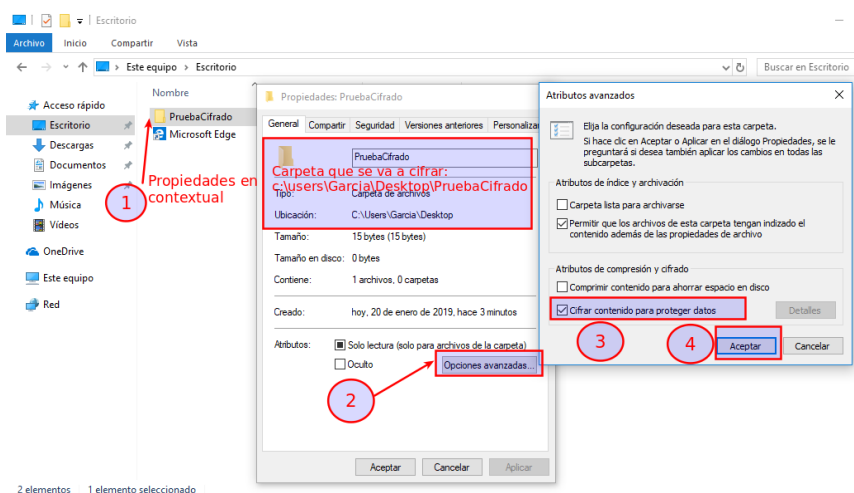
Características destacadas de EFS:

- Se realiza activando una casilla en las propiedades del archivo o carpeta.
- Ningún otro usuario que acceda a ese archivo o carpeta podrá abrirlo.

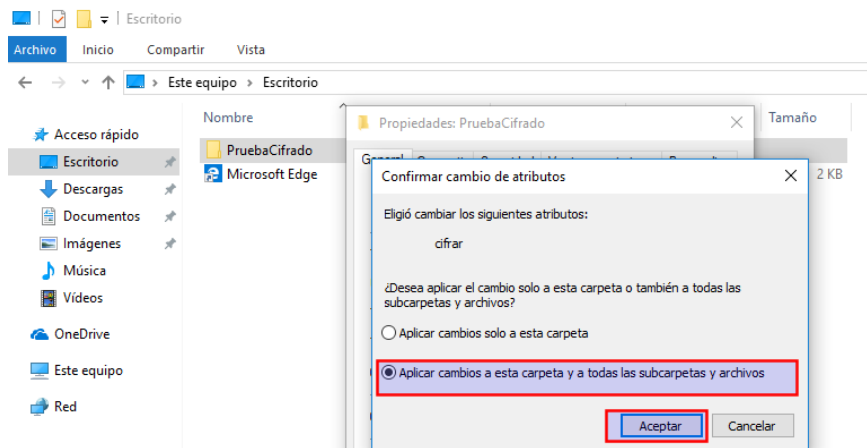
- El sistema EFS basa su seguridad en usuario, no en contraseña. El usuario cifra el archivo y lo puede abrir, pero no podrán hacerlo otros usuarios.
- Se puede desactivar el cifrado desactivando la casilla en las propiedades.
- Solo se puede en sistemas NTFS.
- Al cifrar archivos y carpetas comprimidos, estos se descomprimen.
- Los archivos marcados con el atributo del sistema no se pueden cifrar
- EFS se instala en Windows 10 Profesional y superiores.

Procedimiento para cifrar un archivo o carpeta con EFS

En el explorador de Windows, se selecciona Propiedades en el menú contextual del archivo o carpeta. Se abre la solapa General / Avanzadas y se activa la casilla Cifrar contenido para proteger datos y Aceptar.

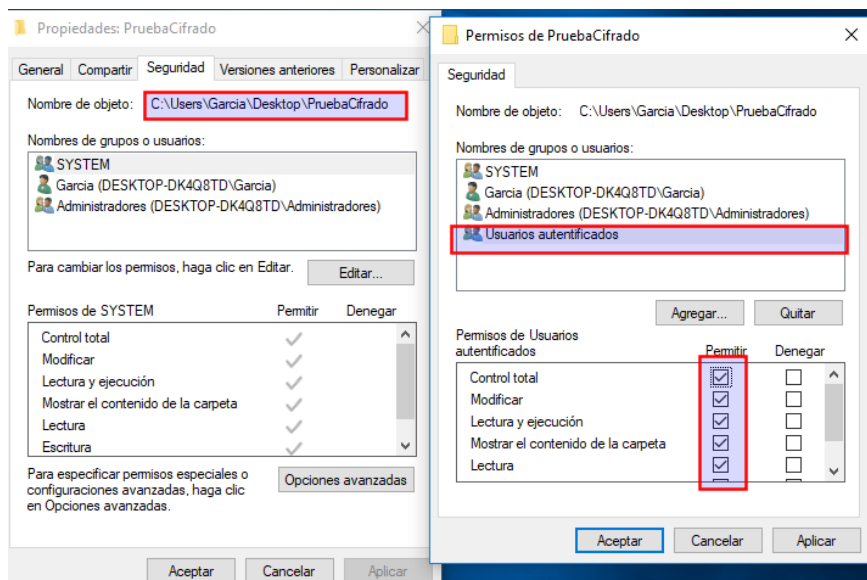


Si estamos cifrando una carpeta, nos preguntará si queremos cifrar todo el contenido o solo la carpeta.

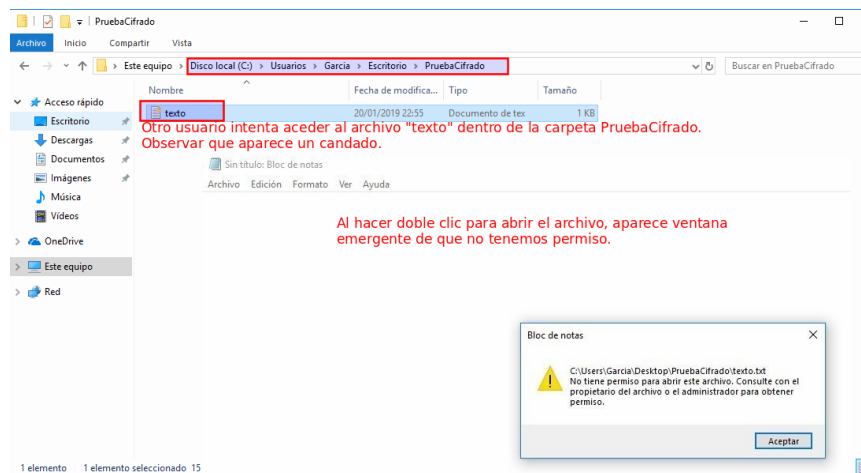


La carpeta ya está cifrada. Se puede observar un candado pequeño en el nombre de la carpeta. El usuario no tendrá que introducir en ningún momento clave para acceder a ella, pero otro usuario no podrá acceder. **Comprobación de que otro usuario no tiene acceso a los archivos contenidos en la carpeta**

Antes de comprobarlo, vamos a asegurarnos de que ese otro usuario va a poder acceder por permisos NTFS. Para ello, se ha incluido a "Usuarios autenticados" con permiso total en la carpeta, tal como se ve en la imagen.



Al iniciar sesión con otro usuario, debería acceder a los archivos que hay dentro de la carpeta, pero al intentar abrir el archivo texto.txt dentro de la carpeta no se tiene permiso.



Exportar certificado y clave

Una vez cifrada el archivo o carpeta, aparece en el área de notificaciones qué se debe hacer una copia de seguridad del certificado y la clave de cifrado en una unidad extraíble. Si la clave de cifrado se pierde o queda dañada y no tenemos copia de seguridad, no podremos recuperar los datos.

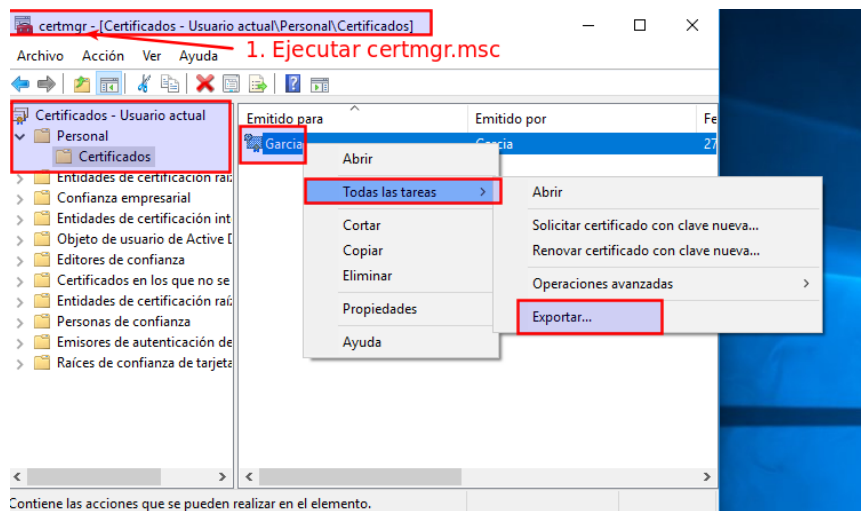
En el proceso de exportar certificado, se solicita una clave al usuario que tendrá que guardar en sitio seguro.

Si hubiera problema en el futuro con la clave original, habría que importar este certificado.

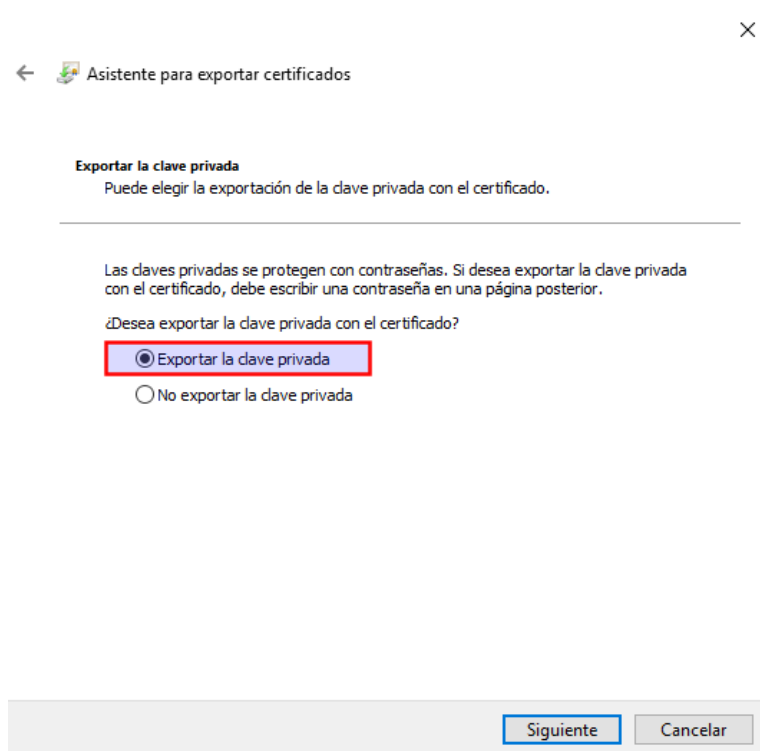
Procedimiento para exportar certificado y clave. Pasos.

En vez de utilizar el proceso del asistente de notificaciones, se ha optado por mostrar el procedimiento general completo, que no depende de la notificación.


- Ejecutar el programa de certificados de Windows 10: certmgr.msc
- Ir a Certificados/Personal/Certificado. Aparecerá el certificado creado al cifrar una carpeta, con el nombre de usuario.
- Pulsar en menú contextual Todas las tareas / Exportar





- En la ventana siguiente, seleccionar “Exportar la clave privada” y pulsar Siguiente.



- El archivo a exportar con el certificado, puede tener distintas extensiones. Dejamos opción por defecto, extensión pfx
-



  Asistente para exportar certificados

Formato de archivo de exportación
Los certificados pueden ser exportados en diversos formatos de archivo.

Seleccione el formato que desea usar:

☐ DER binario codificado X.509 (.CER)

☐ X.509 codificado base 64 (.CER)

☐ Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)

☐ Incluir todos los certificados en la ruta de certificación (si es posible)

☒ Intercambio de información personal: PKCS #12 (.PFX)

☒ Incluir todos los certificados en la ruta de certificación (si es posible)

☐ Eliminar la clave privada si la exportación es correcta

☐ Exportar todas las propiedades extendidas


☒ Habilitar privacidad de certificado



☐ Almacén de certificados en serie de Microsoft (.SST)

Siguiente

Cancelar

Hacer clic en Contraseña y escribirla 2 veces. Pulsar siguiente.



  Asistente para exportar certificados

Seguridad
Para preservar la seguridad, debe proteger la clave privada en una entidad de seguridad o con una contraseña.

☐ Grupo o nombres de usuario (recomendado)

Agregar

Quitar

☒ Contraseña:

••••••••

Confirmar contraseña:

••••••••

Cifrado: TripleDES-SHA1

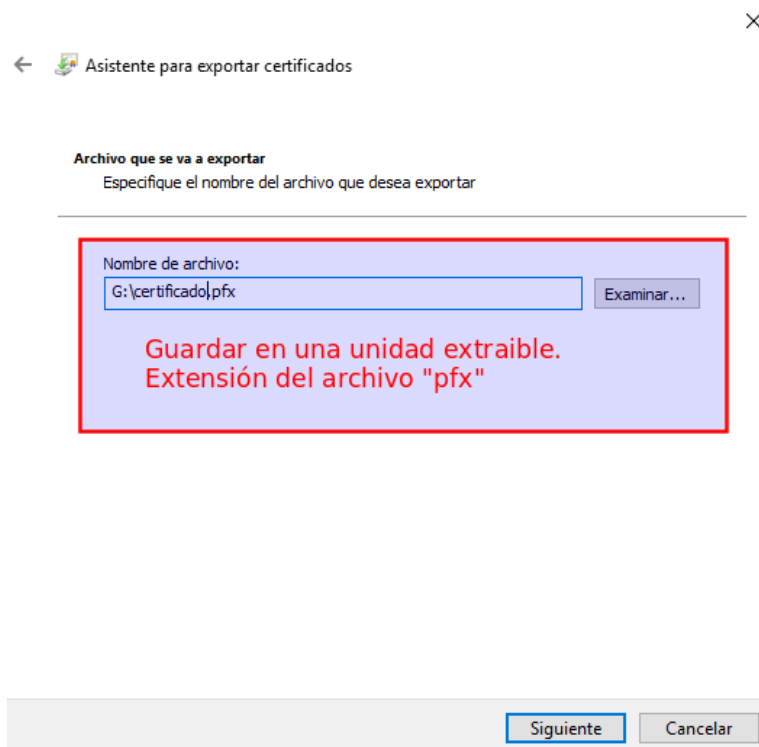
Siguiente

Cancelar

Pulsar en examinar para guardar el certificado en una unidad extraíble.

7. Copias de seguridad, cifrado y RAID

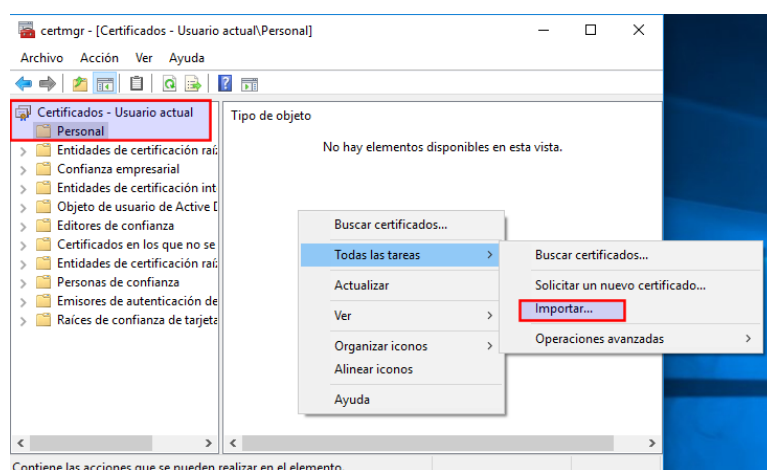
20



Importación de certificado

En caso de que el certificado original fallara, se importaría el certificado y clave de forma similar. Para ello:

- Ejecutar certmgr.msc
- Ir a Certificados / Personal y menú contextual “Todas las tareas / Importar”



- A partir de esta ventana solo queda buscar el certificado en la unidad extraíble.

3.2. Cifrado de unidades lógicas en Windows con BitLocker

Bitlocker permite cifrar las unidades lógicas, incluso en la que está instalado el Sistema Operativo.

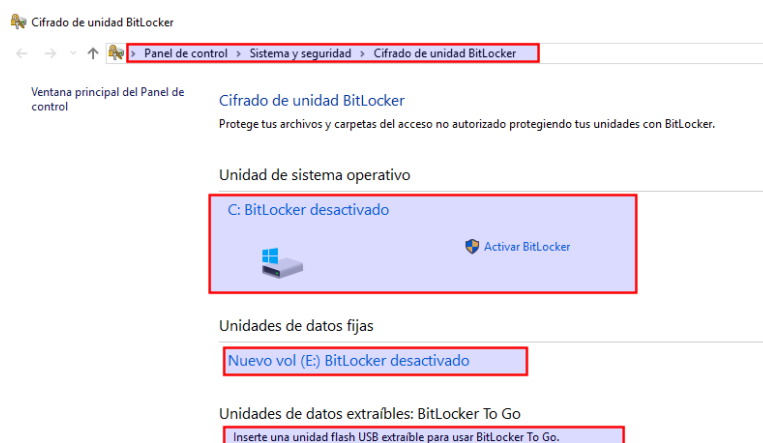
Para ello es necesario tener una partición reservada para el sistema. Por este motivo, cuando se instala Windows se crea una partición de 550MB, ya que los archivos del sistema necesario para el inicio no pueden estar cifrados.

Bitlocker To Go permite cifrar dispositivos de almacenamiento portátiles como unidades USB y disco duros externos.

Para utilizar BitLocker es necesario que el hardware del PC incorpore el módulo TPM de seguridad (Trusted Platform Module), en su defecto utilizaremos un medio de almacenamiento externo para almacenar la clave. El objetivo de TPM es dar seguridad basada en hardware, más difícil de romper que la basada en software.

Para abrir BitLocker ir a:

Panel de control / Sistema y seguridad / Cifrado de unidad BitLocker. Aparece la ventana de la imagen, en la que nos da la opción de activarlo en C y resto de particiones del disco, así como activar BitLocker To Go en las unidades extraíbles.



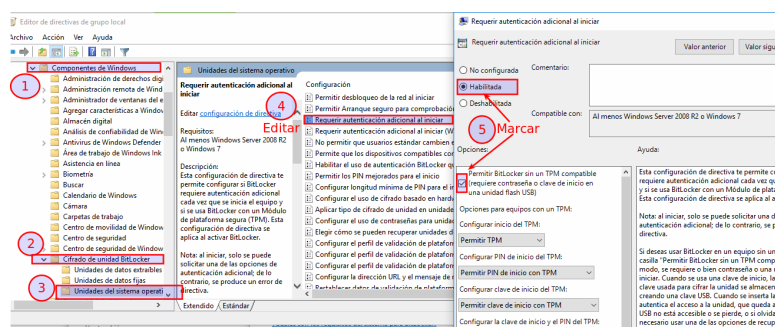
Se va a desarrollar el ejemplo de cifrar C. Este ejemplo se va a desarrollar en una máquina anfitrión Windows. Para la tarea se va a solicitar cifrar BitLocker To Go en un pendrive, para evitar manipulaciones en las máquinas anfitriones de los alumnos.

En la imagen se ha seleccionado “

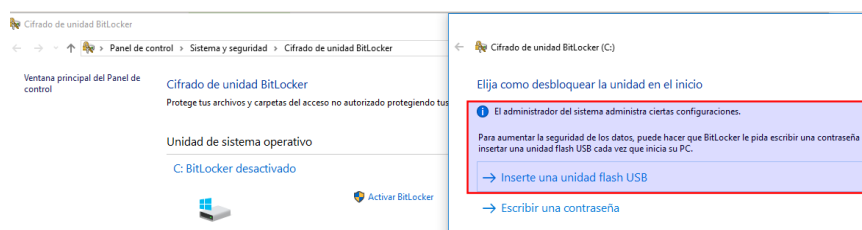
Activar BitLocker en C”. Al pulsar, se abre la ventana de que el PC no tiene el módulo TPM, por lo que hay que editar la directiva local “Requerir autenticación adicional al iniciar”

Tal como se vio en la unidad 4, abrimos el editor de directivas, ejecutando gpedit.msc.

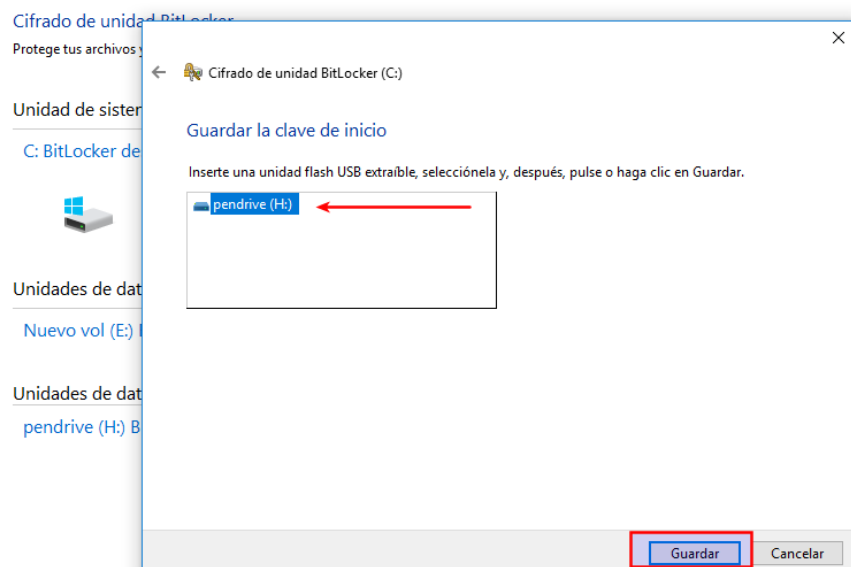
Para llegar y editar la directiva, seguimos los pasos de la imagen:



Una vez realizado el cambio de directiva, volvemos al paso anterior para cifrar C. Ahora al seleccionar “Activar BitLocker en C” se abre la ventana siguiente. Seleccionar “Inserte una unidad flash USB”



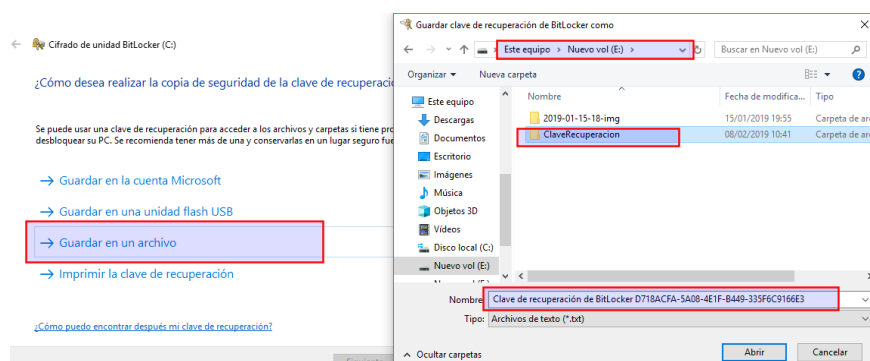
En la siguiente ventana, solo hay que seleccionar nuestra unidad flash y pulsar Guardar.



En la siguiente ventana, se pregunta dónde queremos guardar la clave de recuperación. Es necesario explicar, que esta clave se necesitará en caso de desastre. Supongamos que en un futuro, fallara el pendrive, pues tendríamos esta clave guardada en un archivo de texto plano en otro sitio; como clave de rescate.

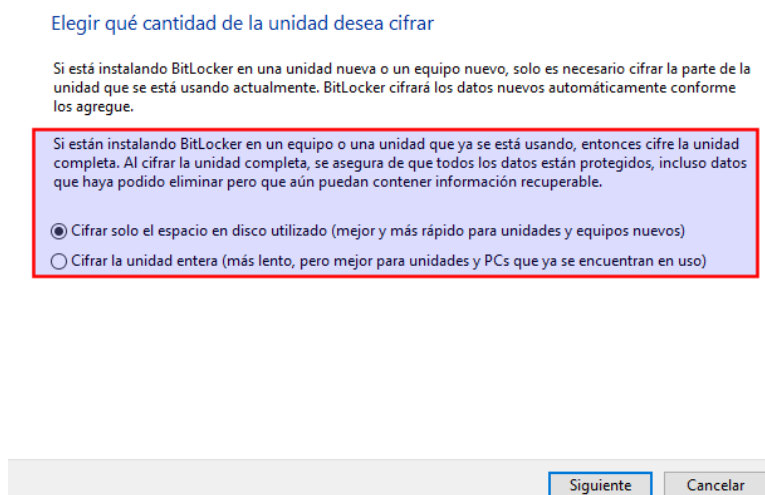
Por este motivo, en este caso se ha decidido “Guardar en un archivo”.

Al pulsar “**Guardar en un archivo**” hay que seleccionar donde guardar ese archivo. De momento, lo he guardado en el equipo local (tiene que ser en otra unidad distinta de la que se está cifrando, aunque lo coherente será guardarlo en otro extraíble distinto).

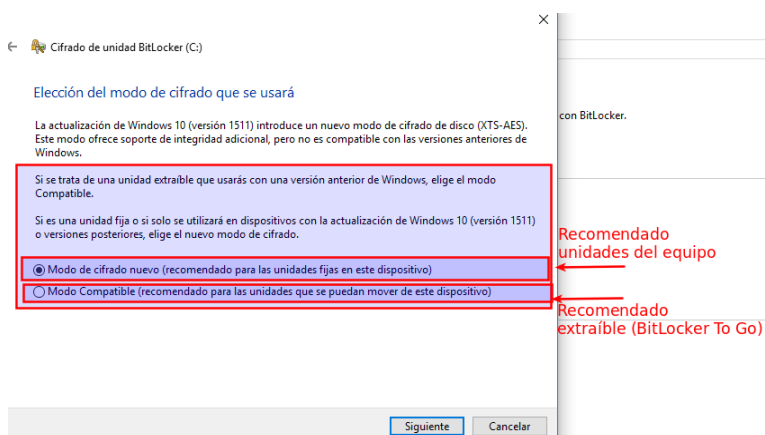


En la siguiente ventana, se pregunta si queremos cifrar solo el contenido utilizado o toda la unidad. En este caso se ha decidido “**sólo espacio utilizado**” para tardar menos tiempo por ser un ejemplo didáctico, pero lo normal será “**Cifrar la unidad entera**”.

Explicar aquí, que cuando se borran los archivos, realmente no se borran, sino que se borra la entrada en el directorio. Para entenderlo, si se copia un archivo de 10 GB, se tarda un rato; sin embargo si se borra, se tardan segundos. ¿Por qué?, porque realmente no se borra el archivo, sino que se borra la entrada al directorio; por eso en muchos casos se puede recuperar la información borrada en un PC. Un software para este fin es Recuva.



En la siguiente ventana hay 2 opciones. La primera pensada si ciframos particiones del PC, la segunda si ciframos unidades extraíbles. Por tanto en este caso seleccionamos “Modo de cifrado nuevo...”



Finalmente, aparece la ventana de que el sistema va a realizar las comprobaciones y el cifrado de la unidad. Una vez pulsado Continuar, habrá que reiniciar el equipo.

¿Está listo para cifrar esta unidad?

El cifrado podría tardar varios minutos, según el tamaño de la unidad.

Puede continuar trabajando mientras se cifra la unidad, aunque es posible que se ralentice el funcionamiento del equipo.

☒ Ejecutar la comprobación del sistema de BitLocker

La comprobación del sistema confirmará que BitLocker pueda leer correctamente las claves de recuperación y de cifrado antes de que se cifre la unidad.

BitLocker reiniciará el equipo antes de iniciar el cifrado.

Nota: esta comprobación puede tardar un tiempo, pero se recomienda asegurarse de que el método de desbloqueo seleccionado funciona sin que sea necesario usar la clave de recuperación.

Continuar

Cancelar

Al reiniciar el equipo, si no ha habido ningún problema, el equipo se encuentra cifrado.

Una vez activado Bitlocker, cada vez que se inicie el equipo habrá que utilizar el dispositivo extraíble donde hemos almacenado la clave.

3.3. Cifrado de archivos y unidades lógicas con Veracrypt

Linux también tiene herramientas propias de cifrado de particiones y unidades lógicas, pero en este caso se lo dedicaremos a VeraCrypt.

VeraCrypt nace del proyecto abandonado de TrueCrypt, utilizando su código abierto. Tiene las siguientes ventajas:

- Se puede utilizar en Windows, GNU-Linux y MacOS.
- Sirve para cifrar particiones como archivos (para ellos e crea un contenedor).

Para cifrar una unidad extraíble que queramos utilizar en distintas máquinas debemos utilizar VeraCrypt, porque da más versatilidad.

Ejemplo completo. Instalar VeraCrypt y crear un contenedor seguro en una unidad extraíble.

El ejemplo que se detalla en este apartado, es crear un contenedor seguro en un pendrive. Este contenedor estará cifrado, e introduciremos dentro los archivos a esconder. El contenedor, realmente será un fichero que ocupará el espacio que le reservemos.

Montaremos el contenedor en un **volumen lógico** (una letra de partición)

Paso 1. Descarga VeraCrypt portable para Windows

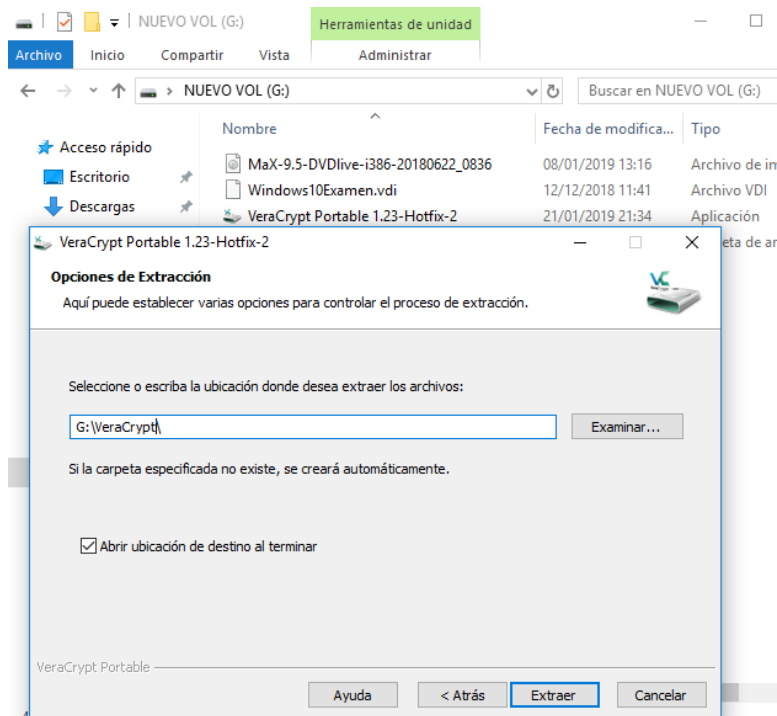
Descargar el programa desde su [página oficial](#):

Podemos descargar versión estándar o versión portable. Si descargamos la versión estándar, tendríamos que instalarla en todos los equipos con Windows que vayamos a utilizar VeraCrypt.

En nuestro caso, vamos a descargar la versión portable, de forma que la instalaremos en el pendrive, y ya no tendremos que instalarla en el resto de equipos con Windows que queramos utilizar el contenedor.

Paso 2. Instalar VeraCrypt.

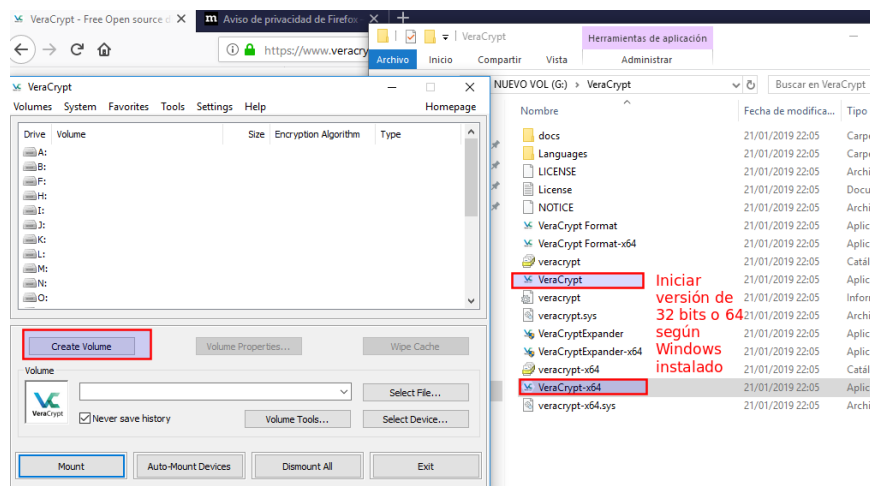
La instalación no tiene dificultad, lo único a reseñar es que al descomprimir la aplicación, el destino será en una carpeta del pendrive. En la imagen, se ha dejado la carpeta por defecto.



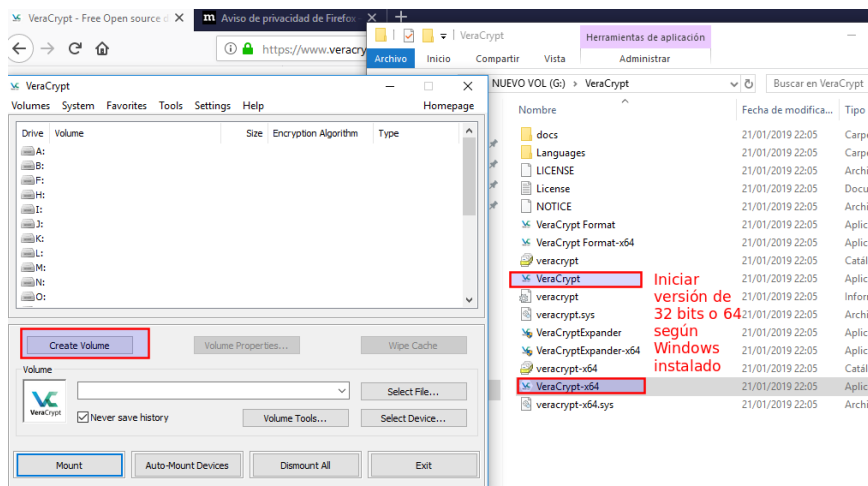
Al finalizar la instalación, el programa pregunta si se quiere realizar una donación para facilitar el mantenimiento del software al creador.

Paso 3. Abrir el programa

Se abre el programa con el ejecutable que se encuentra en la carpeta donde se ha instalado VeraCrypt. Se ejecuta el ejecutable adecuado (32 o 64 bits) según Windows instalado.



Una vez abierto, se pulsa en “Create Volume” para crear el contenedor donde se guardaran los ficheros a encriptar.



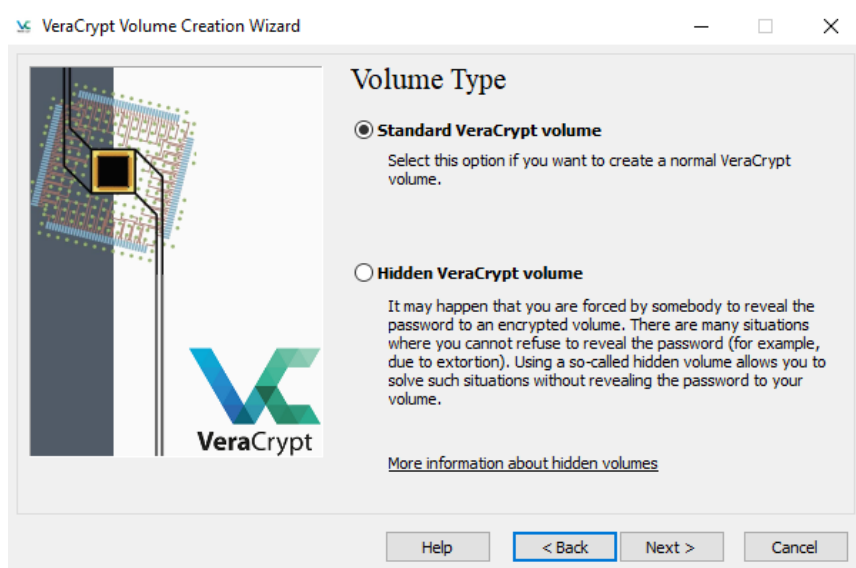
Paso 4. Crear volumen

Al pulsar Crear volumen, nos aparece una ventana, en la que se pregunta la opción que se desea:

- Crear un fichero contenedor
- Encriptar una partición o unidad que no tenga el Sistema Operativo
- Encriptar la partición o unidad completa con el Sistema Operativo

Se selecciona **“Crear un fichero contenedor”**.

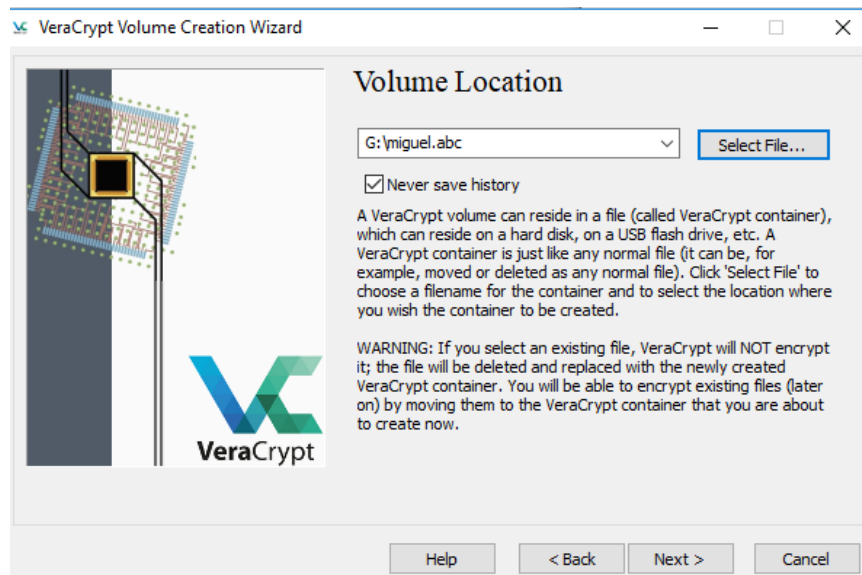
En la siguiente ventana se pregunta si se quiere crear un “Volumen estándar” o un “Volumen oculto”. El volumen oculto, permite establecer 2 niveles distintos de visibilidad dentro del contenedor. En nuestro caso, seleccionar "Volumen estándar".



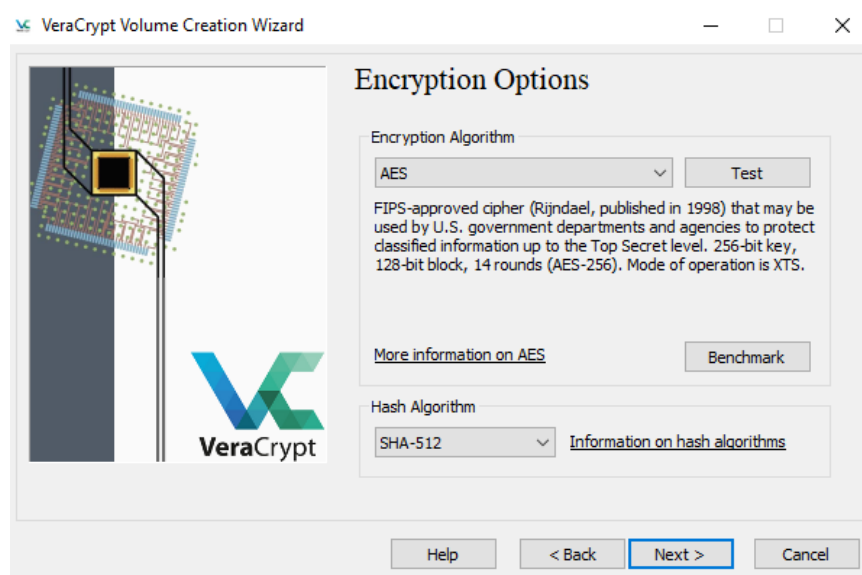
En la siguiente ventana se selecciona el fichero que va a ser el contenedor. Se suele crear un fichero con un nombre que despiste, en este caso se ha decidido poner una extensión extraña al fichero

miguel.abc de esta forma se despista en caso de perderse la unidad.

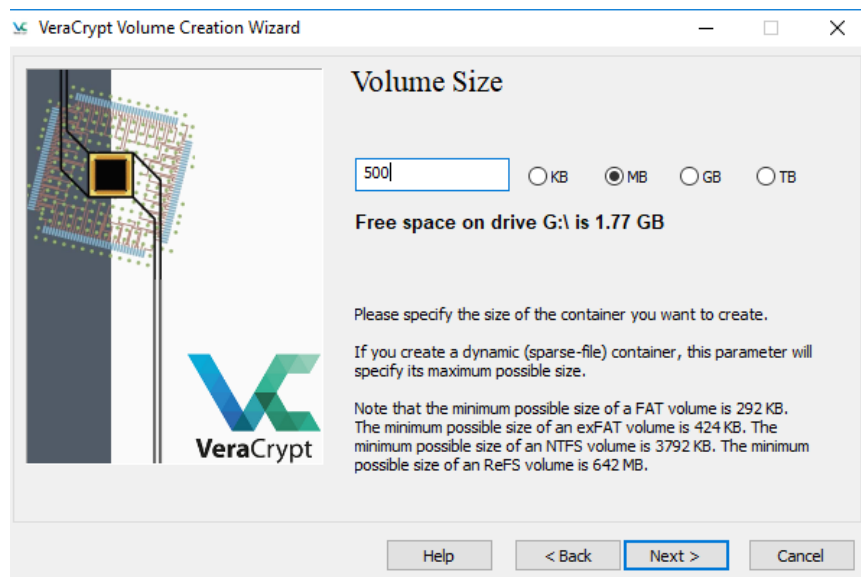
VeraCrypt va a convertir este fichero en el contenedor.



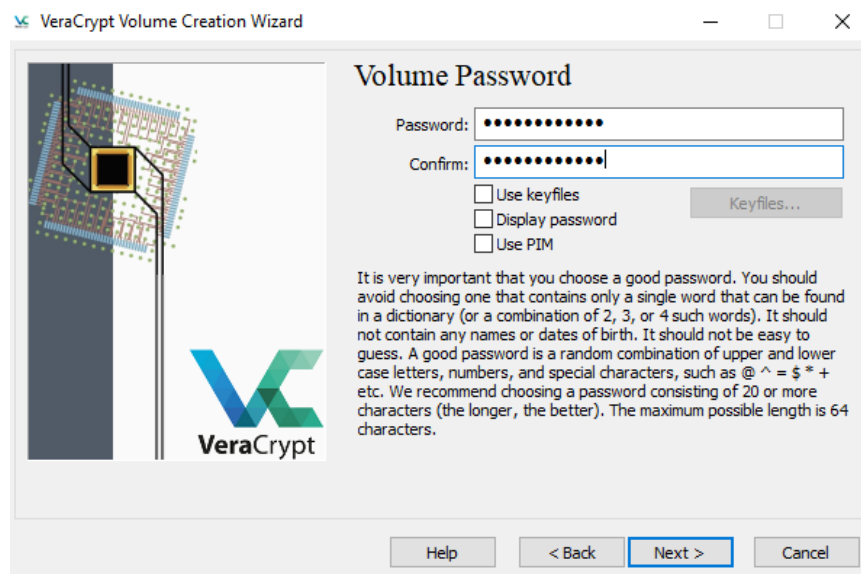
En la siguiente ventana, se pregunta qué algoritmos se van a utilizar para guardar la clave. Se dejan las opciones por defecto y se pulsa Next.



En la siguiente ventana, se pregunta tamaño del fichero contenedor.



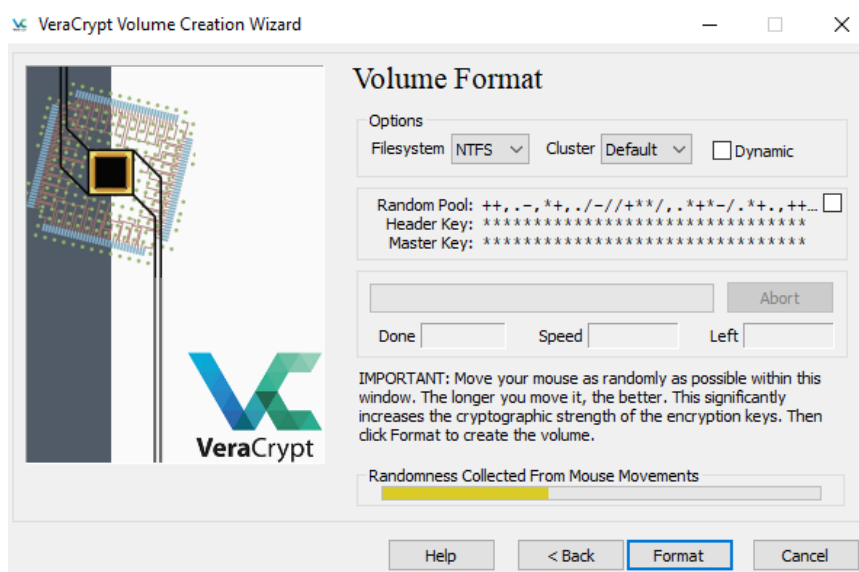
Después escribimos el password que queremos utilizar 2 veces. VeraCrypt da mucha importancia a este tema, pues uno de los problemas habituales de la seguridad informática comienza por el mismo usuario, pues se tiene la mala costumbre de utilizar contraseñas fáciles de recordar.



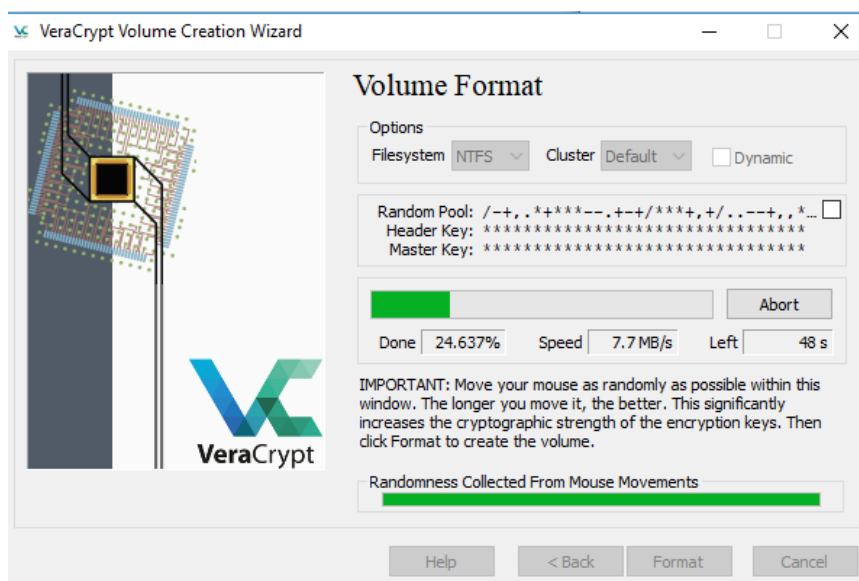
Ahora se pregunta con que sistema de ficheros se crea el contenedor: fat, ntfs. Si se selecciona NTFS, se debe tener en cuenta que los sistemas operativos posteriores que utilicemos con ese contenedor deben permitir leer y escribir particiones NTFS.

- Seleccionar NTFS (en nuestro caso, Ubuntu lee y escribe particiones NTFS)
- Después, mover el ratón por la pantalla contantemente. Hasta que aparezca en color verde la barra "Randomness..."

- Esto sirve para dar más fuerza a la password.
- Pulsar “Format”



Se pone una imagen donde se está formateando la partición.

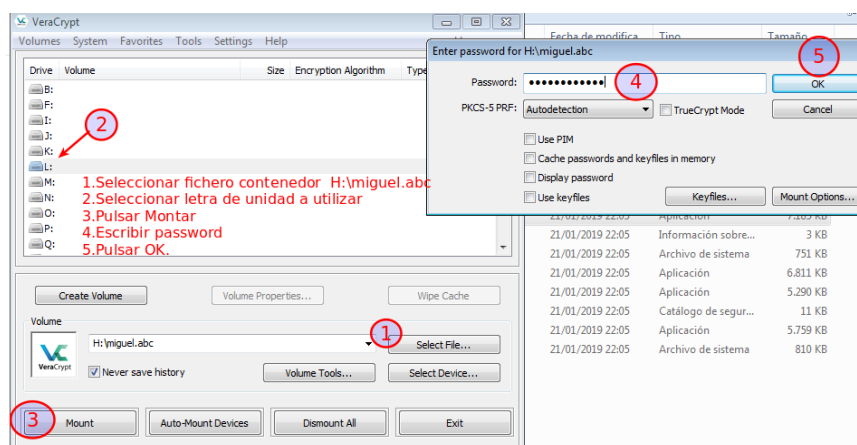


Cuando acaba, aparece un mensaje de finalización de crear volumen.

Utilización del contenedor en Windows

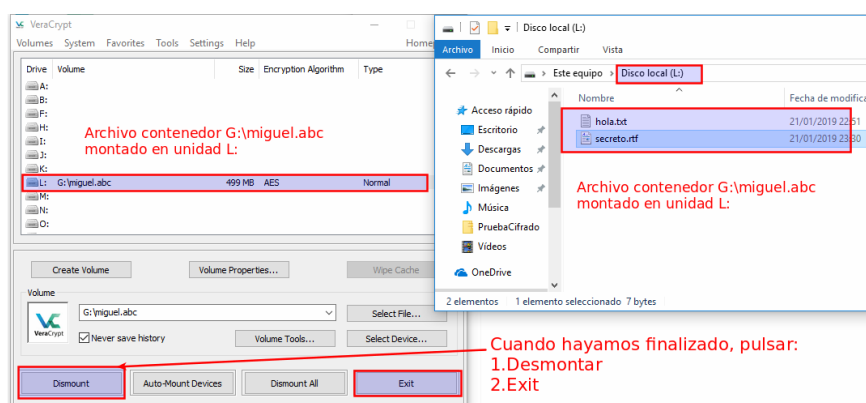
Una vez creado el volumen, ya se está en disposición de utilizarlo en cualquier máquina Windows. Además llevamos el programa instalado en la unidad extraíble, por lo que solo se abrirá el programa en cualquier PC y se siguen los pasos siguientes:

- Se selecciona el fichero contenedor **H:\miguel.abc**
- Se selecciona **una letra de unidad libre**, donde se va a montar el contenedor. En la imagen se ha seleccionado L.
- Se pulsa **“Mount”**.
- Se abre ventana donde **rellenamos el password** y pulsamos OK.



A partir de ese momento, la unidad lógica L es como una partición más de nuestro sistema, donde podemos crear o copiar ficheros y carpetas de las formas habituales. Cuando acabemos de utilizar la unidad, es importante seguir los 2 pasos siguientes:

1. Pulsar **Desmontar**
2. Pulsar **Exit**



Instalación en GNU-Linux

Para utilizar nuestro contenedor en una máquina Linux, tenemos que instalar el programa. Para ello, añadimos el repositorio y lo instalamos, tal como se

explicó en la unidad 5.

Se ejecutan los 3 comandos siguientes:
`#add-apt-repository
ppa:unit193/encryption.....`

Pulse [ENTRAR] para continuar o Ctrl+C para cancelar la adición.

Añadimos el repositorio. A mitad de ejecución tenemos que pulsar Intro.

`#apt update`

Actualizamos los paquetes a instalar

`#apt install veracrypt`

Instalamos el programa

Utilización del contenedor en GNU-Linux.

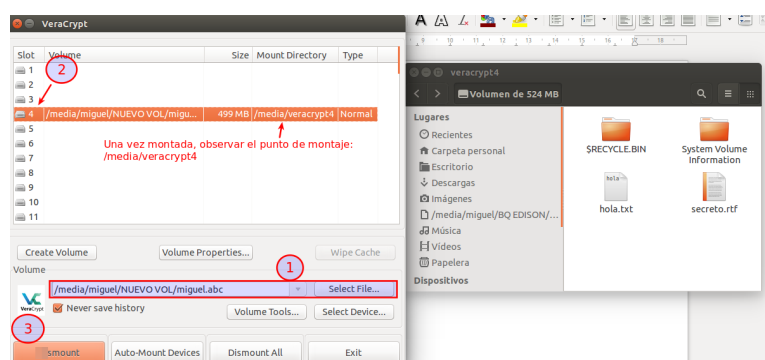
Una vez instalado el programa, se puede utilizar tanto de forma gráfica como en terminal. El funcionamiento del programa gráfico es idéntico a Windows, tanto en crear volumen como en montar el contenedor. En el caso de GNU-Linux los contenedores se montarán en `/media`.

Para abrir el programa, escribir en terminal **veracrypt**. A continuación, como ya tenemos creado el volumen, solo tenemos que montar el contenedor:

- Seleccionar fichero contenedor
- Seleccionar número de montaje
- Pulsar "Mount"

Una vez montado, se abre gráficamente el explorador **nautilus** con el contenido de la unidad lógica.

En la imagen se muestra el programa, con el **contenedor montado en `/media/veracrypt4`**



4. Sistemas RAID

Un sistema RAID consiste en que varios discos duros funcionen como un solo disco, en el cual se almacenará información redundante. De esta forma, si un disco falla, el sistema sigue funcionando sin pérdida de información automática.

También se incrementa la velocidad de transferencia, en lectura y escritura.

Existen varios tipos de RAID, donde cada tipo exige un mínimo de discos duros e información redundante. A mayor cantidad de info repetida, más fiabilidad.

Para obtener las mejores prestaciones en los RAID, los discos duros deben ser de igual tamaño y misma geometría.

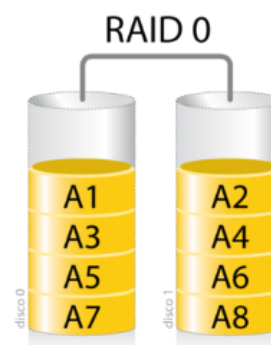
4.1. Sistemas RAID

Tipos de RAID

RAID 0. Data stripping (volumen seleccionado).

Se necesitan un mínimo de 2 discos duros, la info se divide en bloques de igual tamaño y se reparten los bloques entre los 2 discos de forma uniforme.

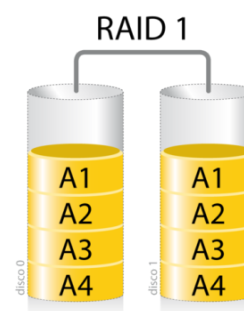
Se consigue mayor velocidad de transferencia, pues se lee o se escribe al doble de velocidad que con un disco duro, pero no se puede recuperar la información en caso de fallo. Utilizando dos discos de 1 TB se obtendrá un disco de 2 TB.



RAID 1. Mirror (Volumen espejo)

Se necesitan 2 discos duros, la info se divide en bloques de igual tamaño pero se escriben todos los bloques en dos discos.

Mayor tolerancia a fallos, pues la info está repetida en ambos discos. Se gana en velocidad de lectura (se lee en ambos discos a la vez), pero no de escritura, ya que la info se escribe en los dos discos.

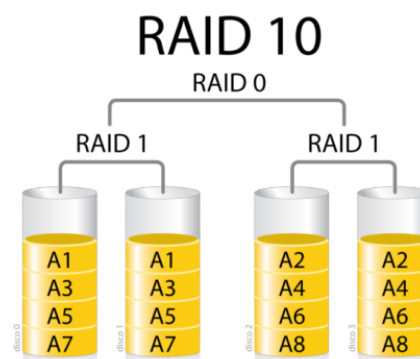


Con dos discos duros de 1TB se obtendrá un disco de 1TB.

RAID 10

También llamado RAID 1 + 0, se necesitan 4 discos duros, se implanta tanto un RAID 1 como un RAID 0 obteniendo las ventajas de ambos.

Si se utilizan 4 discos duros de 1TB se obtiene un único disco de 3TB, consiguiendo gran tolerancia a fallos y máxima velocidad de transferencia. Se pueden crear RAID 10 de 6 discos con 3 RAID 1 de 2 discos y un RAID 0 con ellos.

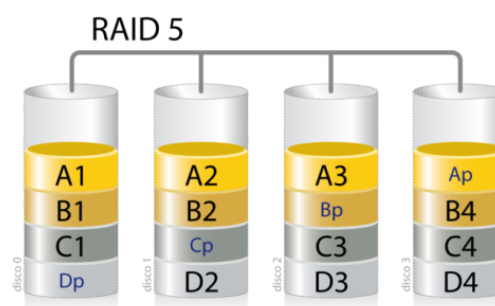


RAID 5

Se necesita un mínimo de 3 discos duros. La info se divide en bloques que se reparten entre todos los discos duros, pero en un disco se guarda información de paridad (redundante), la cual sirve para reconstruir la información en caso de fallo.

En la imagen, se tiene un RAID 5 de 4 discos, en la primera transferencia se ponen 3 bloques (A1, A2 y A3) de igual tamaño en los 3 primeros discos, mientras que el cuarto disco guarda información de paridad.

La segunda transferencia se ponen (BD1, BD2 y BD4) en los discos 1, 2 y 4, el tercer disco guarda información de paridad y así con el resto de bloques. La información redundante se reparte entre los discos, obteniendo entre los 4 discos un disco de paridad.



Para crear un RAID 5 se pierde solo el tamaño de uno de los discos utilizados, de esta forma obtenemos la mejor relación rendimiento-coste.

4.2. Funcionamiento de un disco de paridad.

Para entender el concepto de paridad se trabajan 2 tipos de paridades:

- Paridad PAR significa que el número 1 es par (puede haber 0 unos, 2 unos, 4 unos...)
- Paridad IMPAR significa que el número 1 es impar (puede haber 1 uno, 3 unos, 5 unos...).

Ejemplo con paridad PAR.

Se suponen 3 discos duros de datos y el cuarto para paridad.

En la tabla tenemos datos arbitrarios en los primeros discos, en el cuarto se escriben 1 o 0, de forma que en cada columna tengamos un nº par de unos.

Disco 1	1 0 0 0 1 0 1
Disco 2	0 1 0 0 1 1 0 1
Disco 3	1 0 1 1 1 0 0 1
Disco 4	0 1 1 1 0 0 0 1
Nº de unos	2 2 2 2 2 0 4

Reconstrucción de un disco

Si se estropea cualquier disco en un RAID por hardware, al poner un disco nuevo la misma controladora reconstruye la información. La reconstrucción se haría de la misma forma.

La información de paridad en realidad se distribuye en distintos discos. Se realiza así para optimizar lecturas y escrituras.

4.3. RAID por hardware o por software. Ejemplo.

Cuando creamos un RAID lo podemos hacer por hardware o por software. Por hardware significa que el PC admite RAID o que utilizamos una tarjeta RAID donde se conectan los distintos discos duros.

- Ventajas de RAID por hardware:
 - Mejor rendimiento, la tarjeta controladora se encarga de las transferencias, liberando al S.O. y procesador.
 - Fácil de configurar.
 - Si se estropea un disco, se cambia y la controladora replica la información.
- Desventajas de un RAID por hardware:
 - El coste de la tarjeta

- Si se estropea la tarjeta.
- El RAID hay que crearlo con discos enteros.

RAID por Software en Windows. Discos dinámicos

Hasta ahora hemos trabajado con particiones en discos básicos (particiones y unidades lógicas). En los discos dinámicos hablamos de volúmenes dinámicos. Con volúmenes dinámicos podremos utilizar trozos de distintos discos o del mismo disco que no estén contiguos.

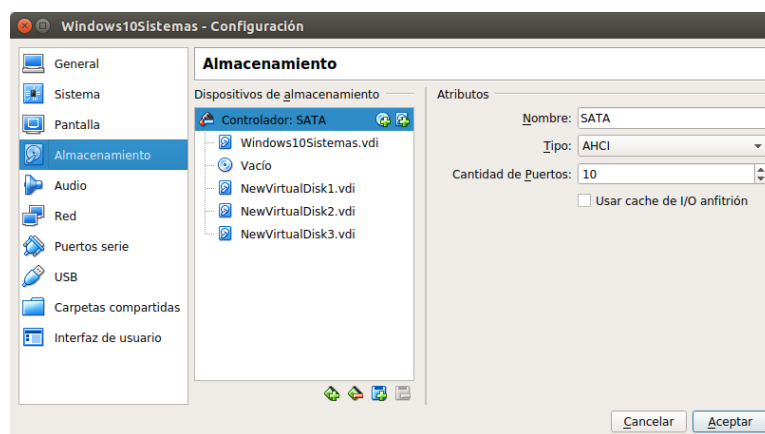
Creando volúmenes dinámicos en Windows podemos seleccionar que se cree un RAID por software con ellos.

Los volúmenes don de 5 tipos:

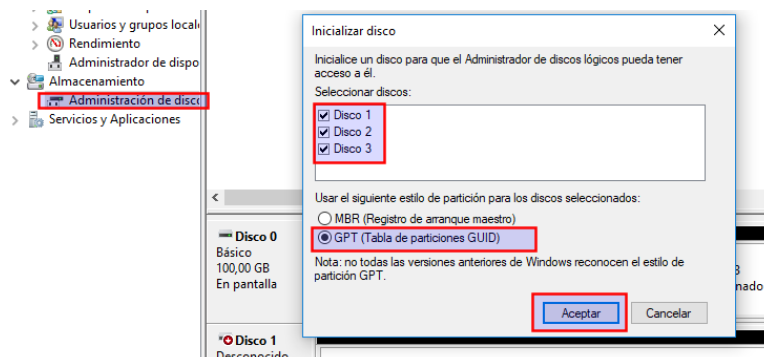
- **Simple:** sirve para unir en un único trozo volúmenes de zonas no contiguas del mismo disco.
- **Volumen distribuido:** sirve para unir en un único disco volumen zonas de distintos discos.
- **Volumen reflejado:** equivale a crear un RAID 1
- **Volumen seccionado:** equivale a crear RAID 0.
- **Volumen RAID 5.**

Ejemplo de creación de un RAID 0 por software en Windows

Este ejemplo formará parte de la tarea SI07. En máquinas virtuales solo se pueden crear RAID por software. Se comienza insertando 3 discos duros nuevos en la máquina “Windows10Sistemas”. Se ha insertado de 50 GB con tamaño dinámico.

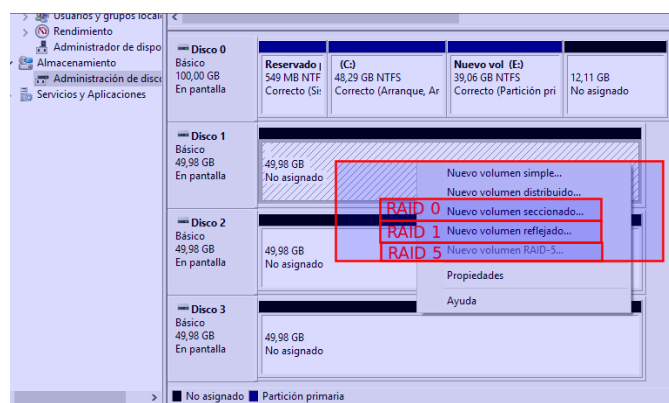


Iniciamos Windows y el Administrador de discos. Al iniciarlos, para crear discos dinámicos, los discos tienen que ser GPT.



Una vez iniciados los discos, pulsamos el menú contextual en el primer disco. Aparecen las opciones que admite GPT, tal como aparecen en la imagen y comentadas antes. En nuestro caso seleccionamos “Nuevo volumen seccionado” para crear un RAID 0.

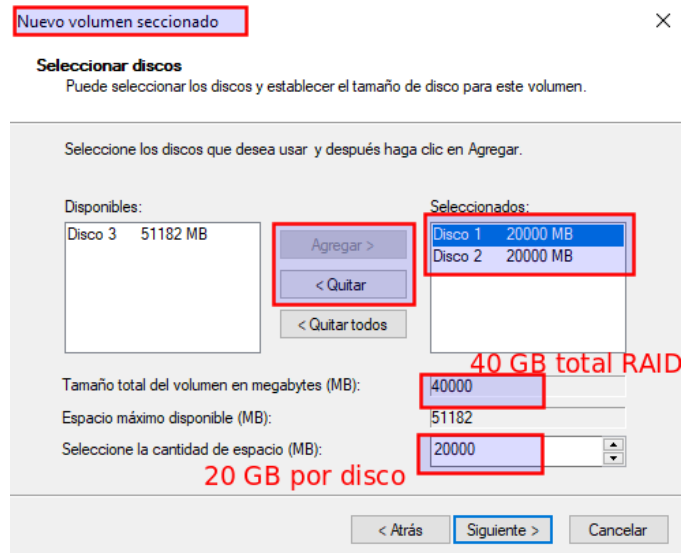
Se puede observar, que aunque tengamos 3 discos, el mínimo para crear un RAID 5, no aparece habilitada dicha opción. Eso es por una limitación de Windows 10 Profesional.



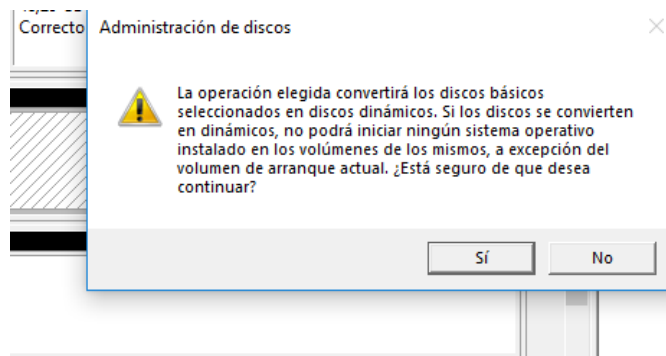
Ahora hay que decir que los discos van a formar parte del RAID 0. Se van a utilizar los **discos 1 y disco 2**, para ello hay que **seleccionarlos** y pulsar **Agregar**.

También se configura el tamaño, se ha decidido utilizar **20.000 MB** de cada disco por lo que el **volumen RAID 0** final va a ser de **40.000 MB**.

Pulsar Siguiente.



Aparece la ventana, que para crear volúmenes dinámicos, primero tiene que convertir los discos básicos en dinámicos.



Una vez convertidos los discos a dinámicos, y creado el RAID 0, aparece la ventana del administrador de discos con la misma letra en la partición de los 2 discos. Si se abre Equipo, se comprueba que el volumen resultante es de 40000 MB.

