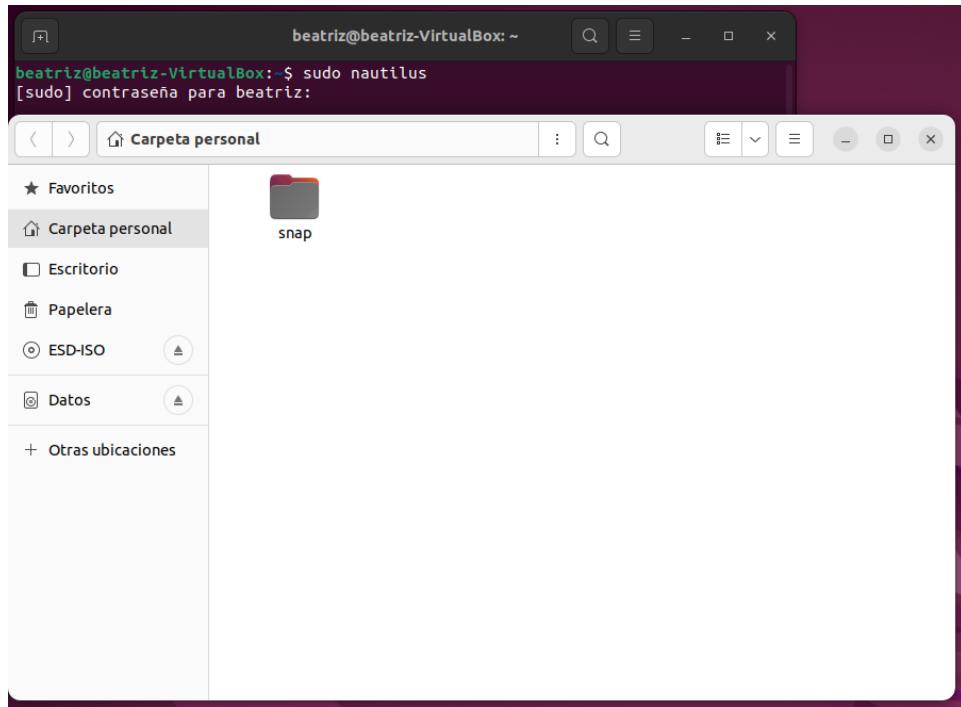


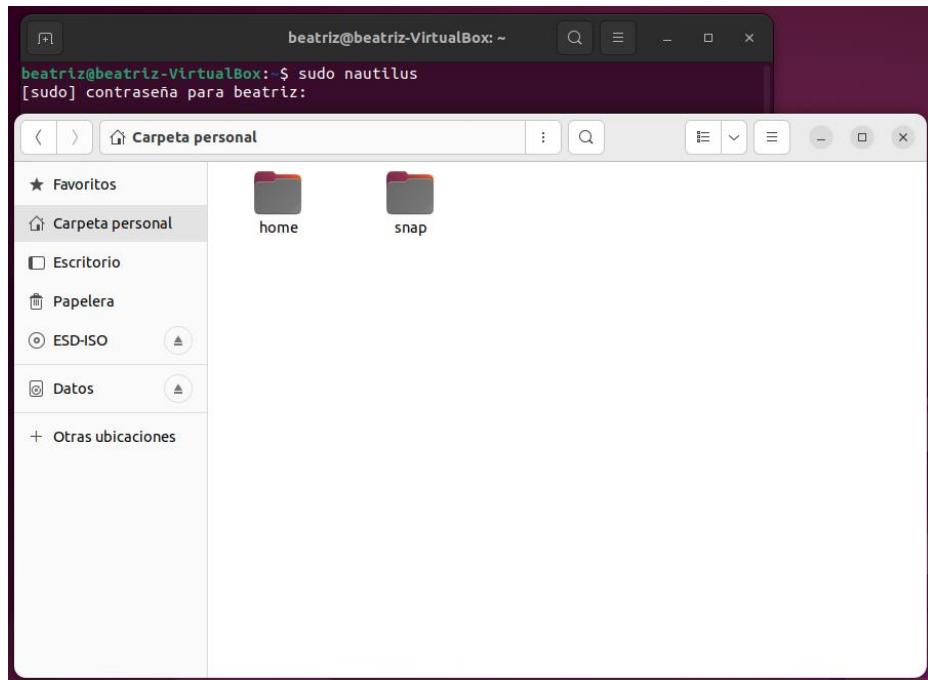
Tarea para SI07 – BEATRIZ GARCÍA HERRERO

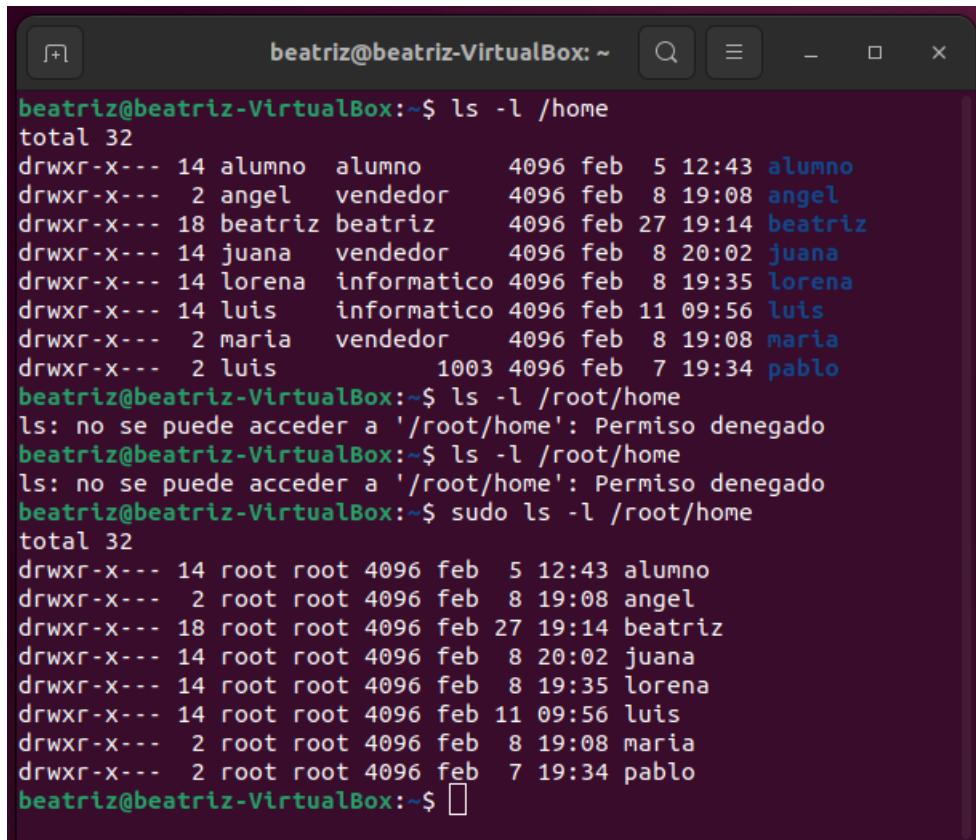
Ejercicio 1. Copia de seguridad en GNU-Linux. Descomprimir copia

1. Iniciar nautilus como root, para ello ejecutar sudo nautilus



2. Copiar gráficamente /home dentro de /root



3. En terminal, listar en formato largo /home y /root/home

A screenshot of a terminal window titled "beatriz@beatriz-VirtualBox: ~". The window contains the following text:

```
beatriz@beatriz-VirtualBox:~$ ls -l /home
total 32
drwxr-x--- 14 alumno alumno 4096 feb  5 12:43 alumno
drwxr-x---  2 angel  vendedor 4096 feb  8 19:08 angel
drwxr-x--- 18 beatriz beatriz 4096 feb 27 19:14 beatriz
drwxr-x--- 14 juana  vendedor 4096 feb  8 20:02 juana
drwxr-x--- 14 lorena informatico 4096 feb  8 19:35 lorena
drwxr-x--- 14 luis   informatico 4096 feb 11 09:56 luis
drwxr-x---  2 maria  vendedor 4096 feb  8 19:08 maria
drwxr-x---  2 luis   1003 4096 feb  7 19:34 pablo
beatriz@beatriz-VirtualBox:~$ ls -l /root/home
ls: no se puede acceder a '/root/home': Permiso denegado
beatriz@beatriz-VirtualBox:~$ ls -l /root/home
ls: no se puede acceder a '/root/home': Permiso denegado
beatriz@beatriz-VirtualBox:~$ sudo ls -l /root/home
total 32
drwxr-x--- 14 root  root 4096 feb  5 12:43 alumno
drwxr-x---  2 root  root 4096 feb  8 19:08 angel
drwxr-x--- 18 root  root 4096 feb 27 19:14 beatriz
drwxr-x--- 14 root  root 4096 feb  8 20:02 juana
drwxr-x--- 14 root  root 4096 feb  8 19:35 lorena
drwxr-x--- 14 root  root 4096 feb 11 09:56 luis
drwxr-x---  2 root  root 4096 feb  8 19:08 maria
drwxr-x---  2 root  root 4096 feb  7 19:34 pablo
beatriz@beatriz-VirtualBox:~$
```

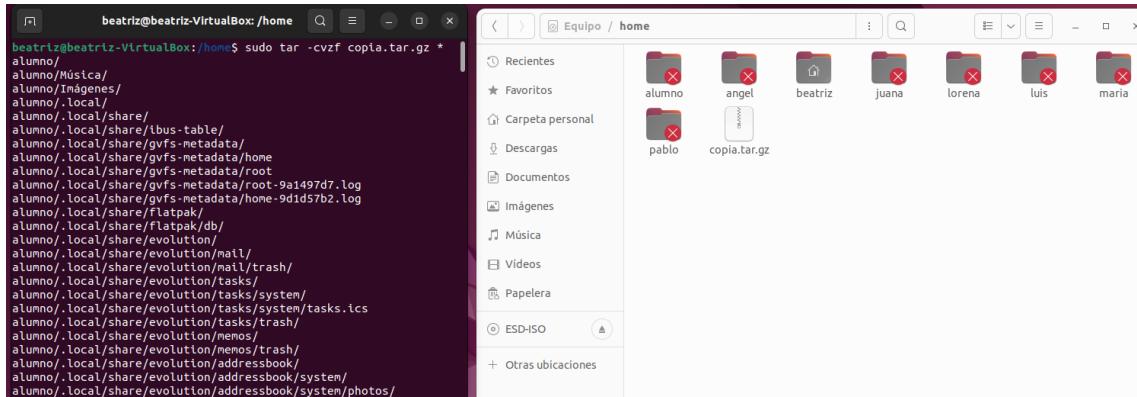
4. Observa las diferencias entre propietarios de los subdirectorios, permisos y fechas de modificación en ambas carpetas.

En /home, cada usuario es propietario de su carpeta.

Pero en /root/home, el propietario es root, y el grupo propietario también.

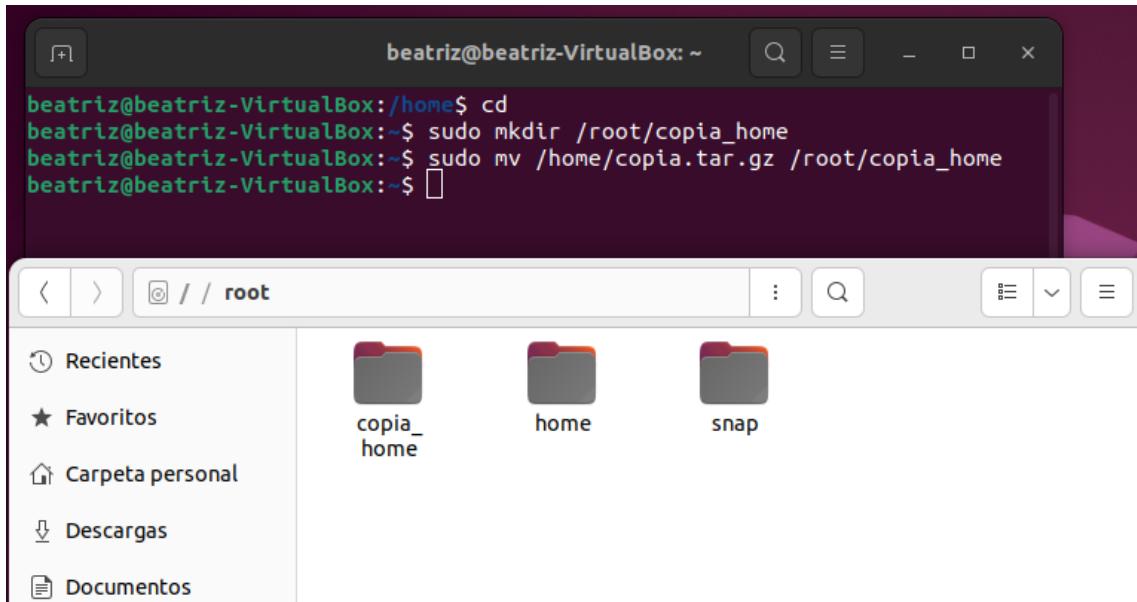
Los permisos y las fechas permanecen igual, pero ahora esos permisos le corresponderán al root en vez de al propietario anterior.

5. Crear en terminal un archivo de copia de seguridad de /home con el nombre copia.tar.gz



6. Mover copia.tar.gz a /root, y desempaquetar allí.

Creo una carpeta dentro de root, y copio el archivo comprimido.

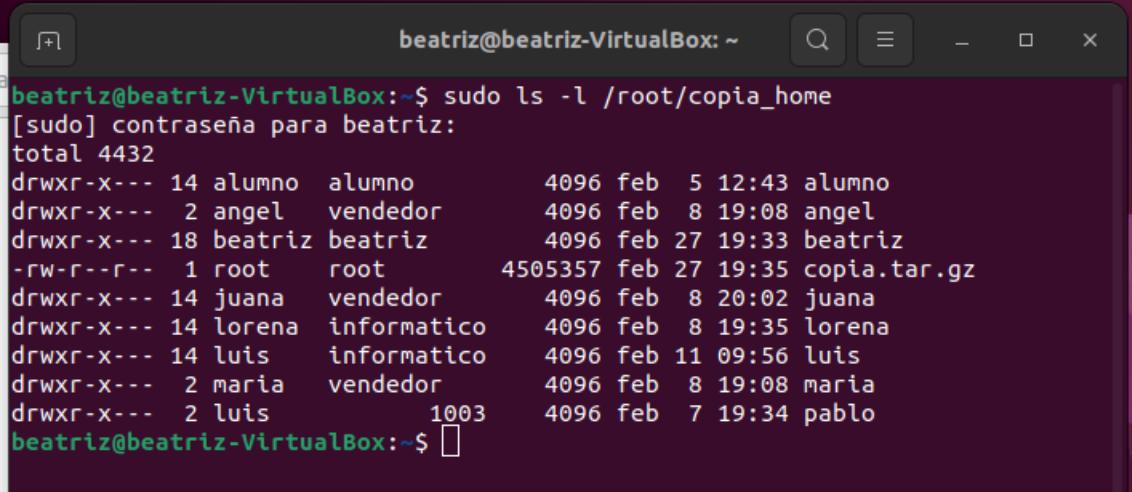


Me pongo dentro de la carpeta para descomprimir el archivo.

```
root@beatriz-VirtualBox:~# cd /root/copia_home
root@beatriz-VirtualBox:~/copia_home# tar -xvf copia.tar.gz
alumno/
alumno/Música/
alumno/Imágenes/
alumno/.local/
alumno/.local/share/
alumno/.local/share/ibus-table/
alumno/.local/share/gvfs-metadata/
alumno/.local/share/gvfs-metadata/home
alumno/.local/share/gvfs-metadata/root
alumno/.local/share/gvfs-metadata/root-9a1497d7.log
alumno/.local/share/gvfs-metadata/home-9d1d57b2.log
alumno/.local/share/flatpak/
alumno/.local/share/flatpak/db/
alumno/.local/share/evolution/
alumno/.local/share/evolution/mail/
alumno/.local/share/evolution/mail/trash/
alumno/.local/share/evolution/tasks/
alumno/.local/share/evolution/tasks/system/
alumno/.local/share/evolution/tasks/system/tasks.ics
alumno/.local/share/evolution/tasks/trash/
alumno/.local/share/evolution/venos/
alumno/.local/share/evolution/venos/trash/
alumno/.local/share/evolution/addressbook/
alumno/.local/share/evolution/addressbook/system/
alumno/.local/share/evolution/addressbook/system/photos/
```

7. Realizar otra vez apartado 3, y observar las diferencias.

Se mantienen las mismas características que tenían los directorios en su origen, en /home.



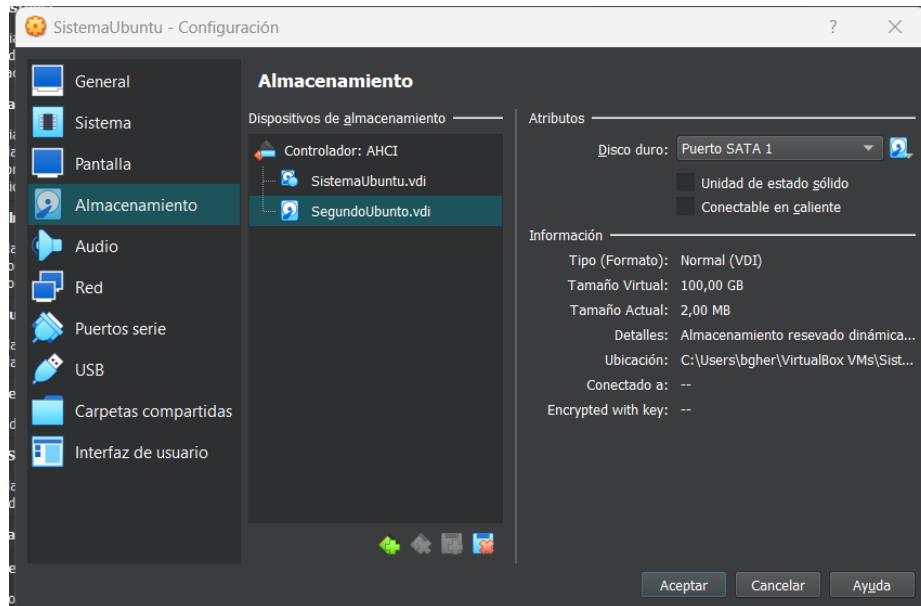
```
beatriz@beatriz-VirtualBox:~$ sudo ls -l /root/copia_home
[sudo] contraseña para beatriz:
total 4432
drwxr-x--- 14 alumno alumno 4096 feb  5 12:43 alumno
drwxr-x---  2 angel  vendedor 4096 feb  8 19:08 angel
drwxr-x--- 18 beatriz beatriz 4096 feb 27 19:33 beatriz
-rw-r--r--  1 root   root    4505357 feb 27 19:35 copia.tar.gz
drwxr-x--- 14 juana  vendedor 4096 feb  8 20:02 juana
drwxr-x--- 14 lorena informatico 4096 feb  8 19:35 lorena
drwxr-x--- 14 luis   informatico 4096 feb 11 09:56 luis
drwxr-x---  2 maria  vendedor 4096 feb  8 19:08 maria
drwxr-x---  2 luis   1003    4096 feb  7 19:34 pablo
beatriz@beatriz-VirtualBox:~$
```

Ejercicio 2. Clonación de un disco duro con dd

Antes de realizar este ejercicio, si no tienes ninguna instantánea, créala por si cometes errores.

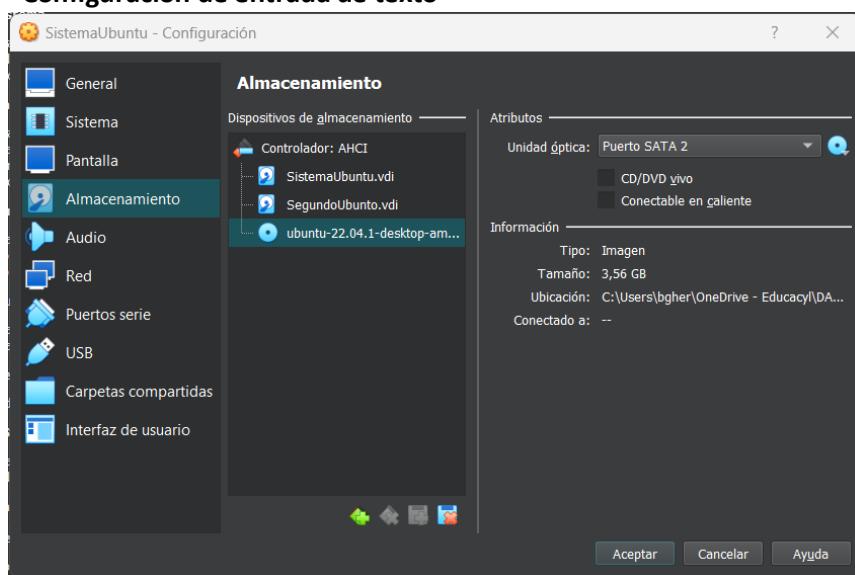
Objetivo: Clonar un disco duro con el comando dd

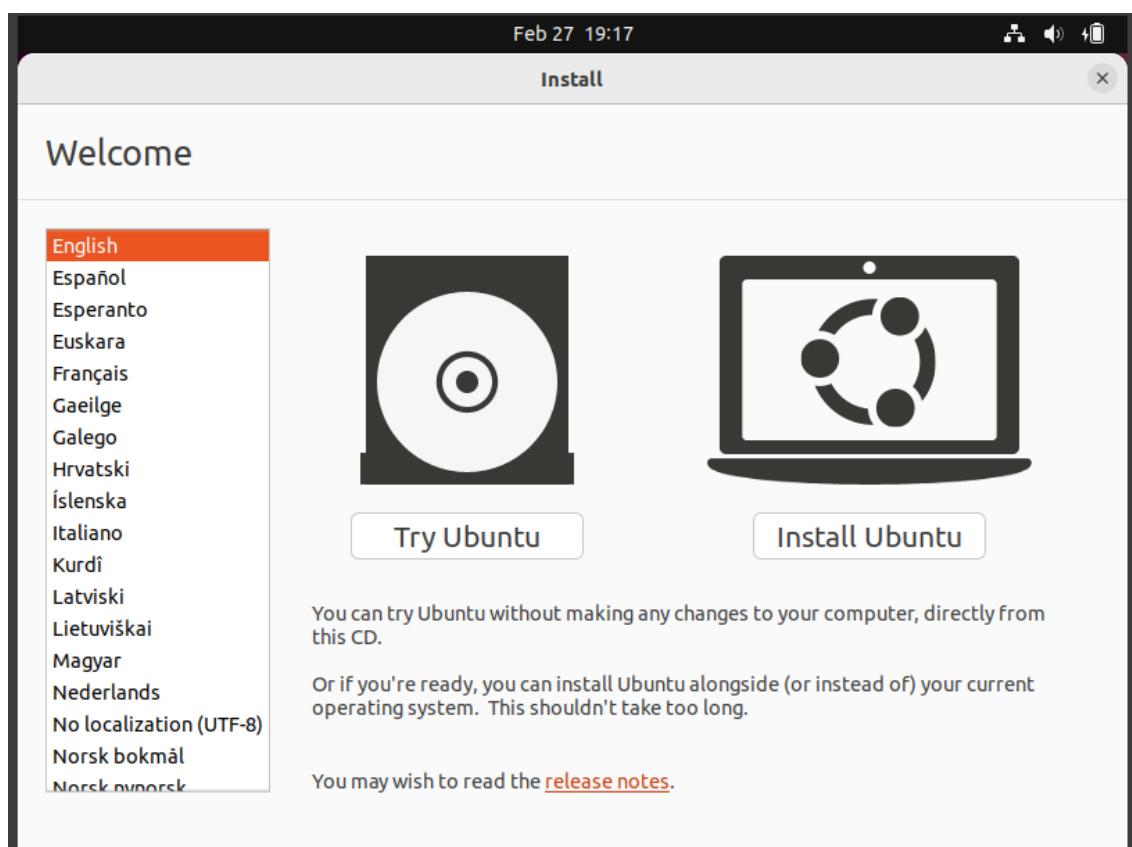
1. Copiar el disco donde tenemos instalado Ubuntu en otro disco. Para ello, seguir los pasos siguientes:
2. Añadir a la máquina UbuntuSistemas un disco duro nuevo de 100 GB. Llamar a este disco “Segundo Ubuntu” nuevo disco)



3. Arrancar la máquina con la iso de Ubuntu, en Probar Ubuntu, sin instalar.

El teclado está en inglés. Para ver cómo escribir las teclas, ir a la esquina superior derecha, donde aparece “En”. Si pulsas, en “Gráfico de distribución del teclado” ves la distribución del teclado actual. También, puedes añadir el teclado en español, en “Configuración de entrada de texto”





4. Una vez arrancada, ejecutar dd para copiar el primer disco en el segundo (comando en el capítulo 7.3)

Observación:

Antes de ejecutar dd, comprueba que el disco origen es sda y el destino sdb. Para ello ejecuta fdisk -l Observa que sda debe tener las particiones y sdb está virgen. De esa forma te aseguras cual es origen y cual es destino.

Ejecuto: sudo fdisk -l. Y compruebo que el disco sda está escrito y el disco sdb está virgen.

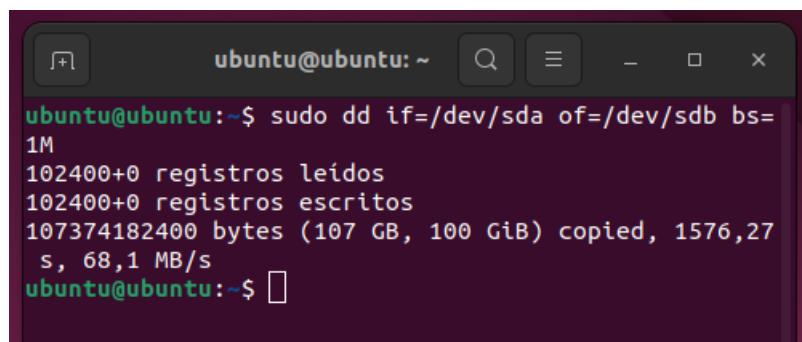
```
Disco /dev/sda: 100 GiB, 107374182400 bytes, 209715200 sectores
Disk model: VBOX HARDDISK
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: gpt
Identificador del disco: 277471E5-67C1-4C32-A365-1C4FE0C25169

Dispositivo Comienzo Final Sectores Tamaño Tipo
/dev/sda1      2048  97656831 97654784  46,6G Siste
/dev/sda2     97656832 113281023 15624192   7,5G Linux
/dev/sda3    113281024 134252543 20971520    10G Siste

Disco /dev/sdb: 100 GiB, 107374182400 bytes, 209715200 sectores
Disk model: VBOX HARDDISK
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
```

Ejecuto lo siguiente para crear la copia del primer disco al segundo:

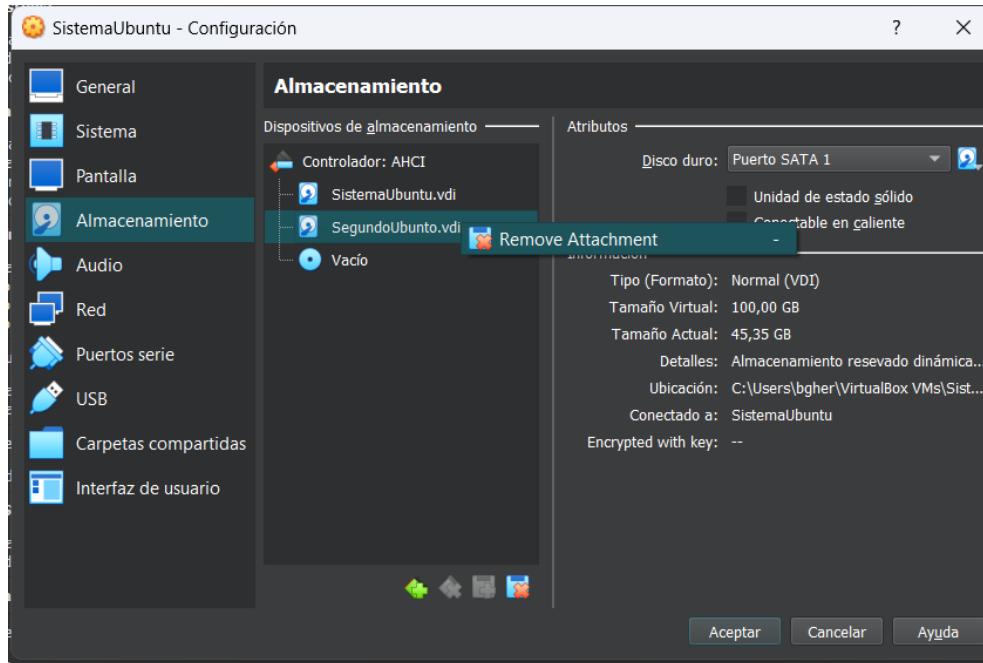
```
sudo dd if=/dev/sda of=/dev/sdb bs=1M
```



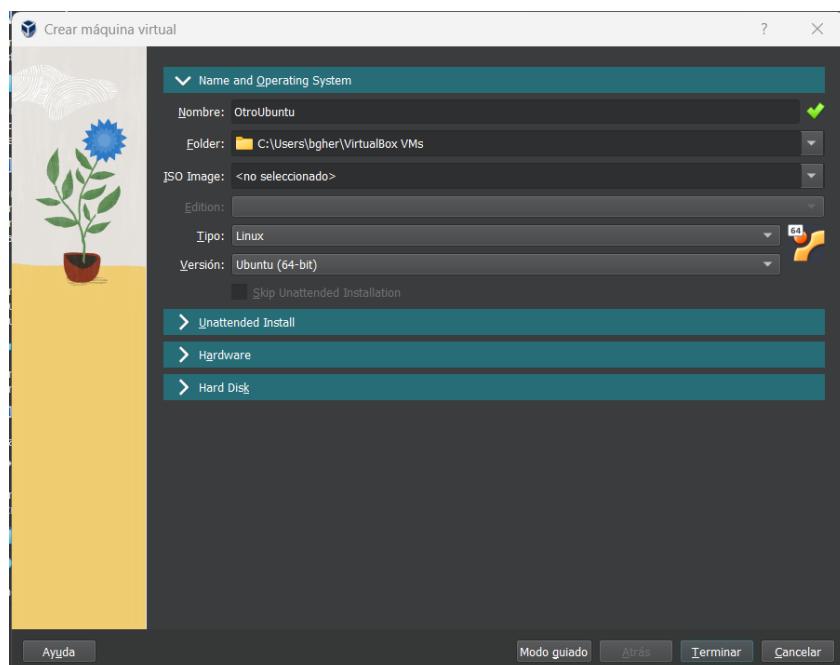
A terminal window titled "ubuntu@ubuntu: ~". The command "sudo dd if=/dev/sda of=/dev/sdb bs=1M" is run, followed by its output: "102400+0 registros leídos", "102400+0 registros escritos", "107374182400 bytes (107 GB, 100 GiB) copied, 1576,27 s, 68,1 MB/s". The window has standard Linux window controls at the top.

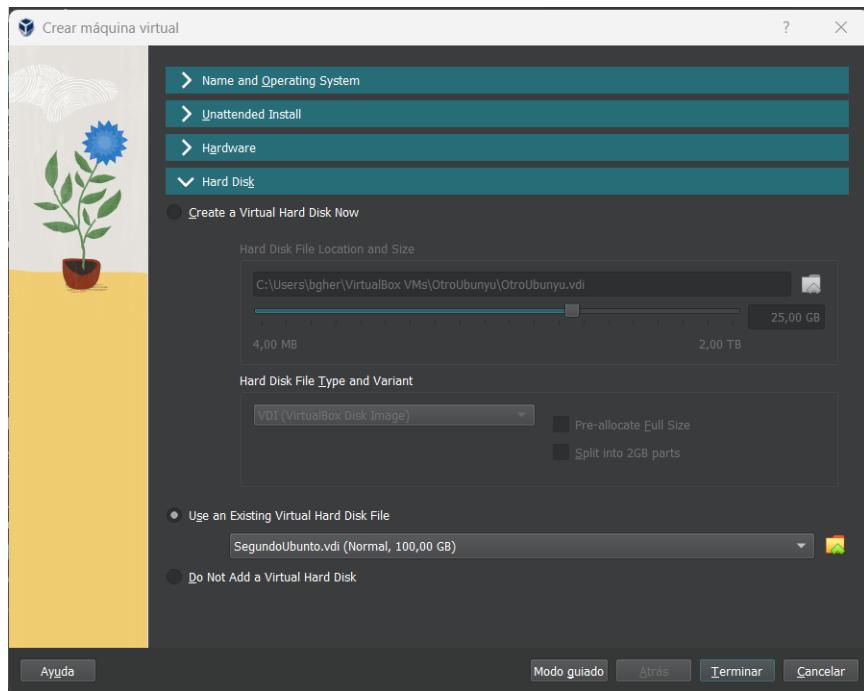
```
ubuntu@ubuntu:~$ sudo dd if=/dev/sda of=/dev/sdb bs=1M
102400+0 registros leídos
102400+0 registros escritos
107374182400 bytes (107 GB, 100 GiB) copied, 1576,27 s, 68,1 MB/s
ubuntu@ubuntu:~$
```

5. Una vez terminada la clonación (tardará un rato, tiene que aparecer el Shell de nuevo), apagamos la máquina y vamos a comprobar, que hemos clonado bien al segundo disco duro. Para ello:
- En configuración de VirtualBox en la máquina, ir a Almacenamiento, y en disco “Segundo Ubuntu”, elegir “eliminar conexión”



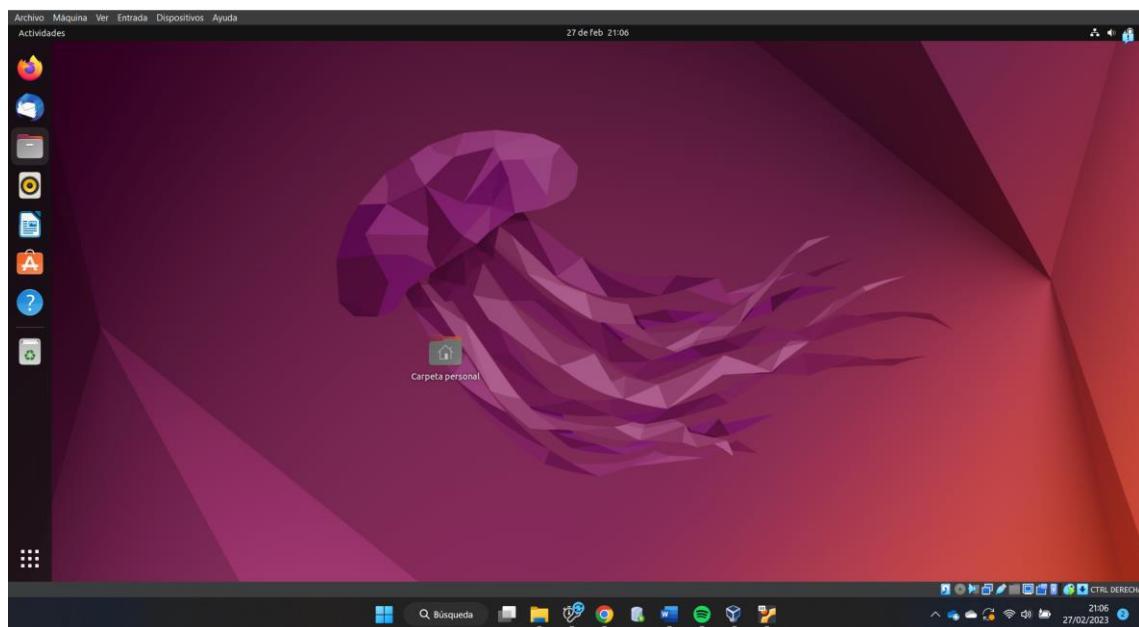
6. Crear una máquina nueva, llamarla “Otro Ubuntu”. Cuando pregunte por disco duro, decirle “Usar disco existente” y seleccionar “Segundo Ubuntu.vdi”. (Recuerda que para buscar “Segundo Ubuntu.vdi”, tienes que hacerlo en tu carpeta de usuario, en la carpeta “VirtualBox VMs” y “UbuntuSistemas”)





7. Iniciar la máquina. Debe iniciar perfectamente!!!

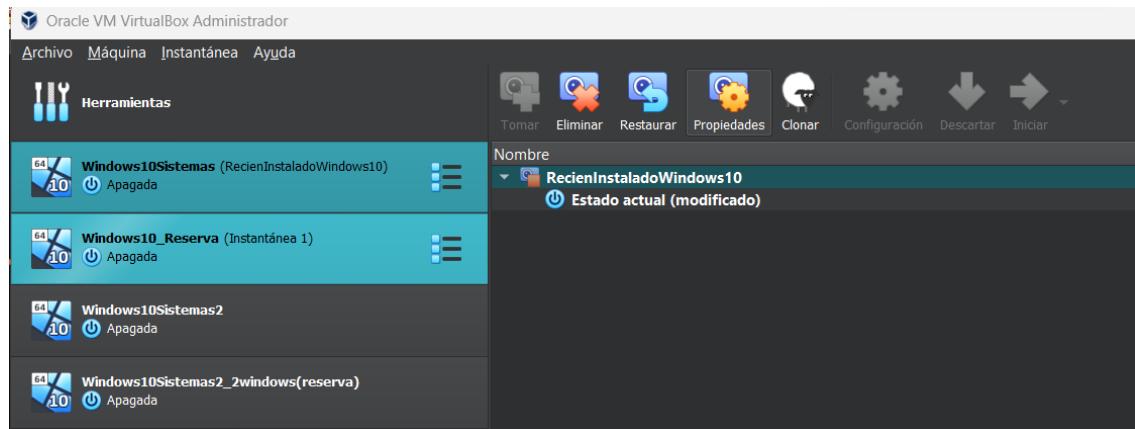
Se abre sin problema.



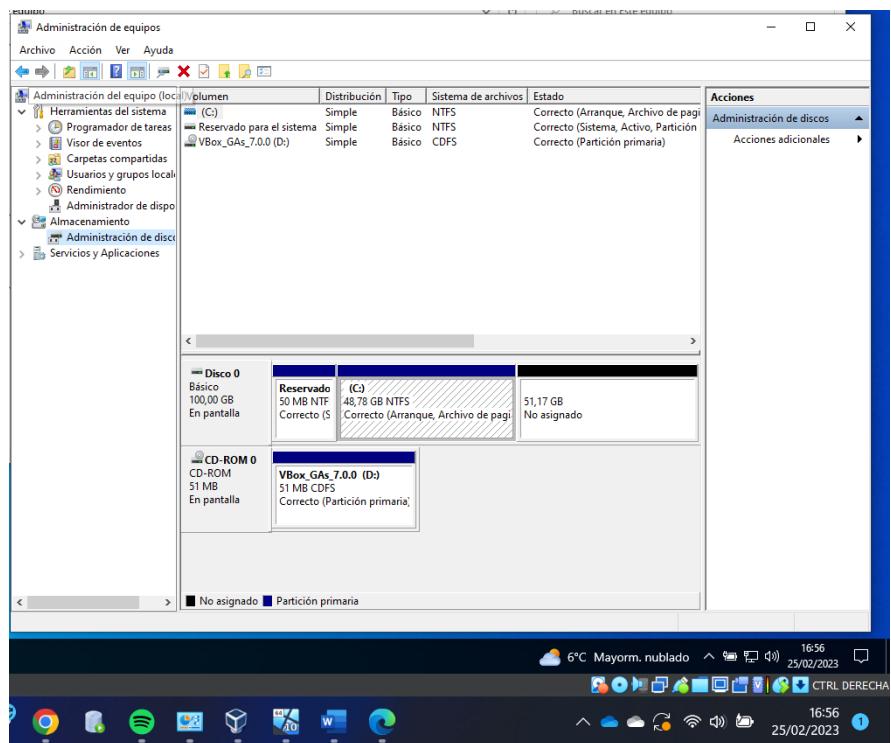
Ejercicio 3. Creación de una imagen con Clonezilla**Crear una imagen de la instalación de “Windows10Sistemas”.****Corresponde con el ejemplo del capítulo 7.3****Seguir los pasos del ejemplo. Como resumen:**

1. **Crear una partición de 40 GB donde guardar la imagen.**
2. **Descargar Clonezilla**
3. **Iniciar máquina con la iso y crear una imagen de las 2 particiones de Windows, guardándolas en la nueva partición.**

Restablezco mi máquina virtual Windows10Sistemas con la instantánea que saqué con Windows10 recién instalado.

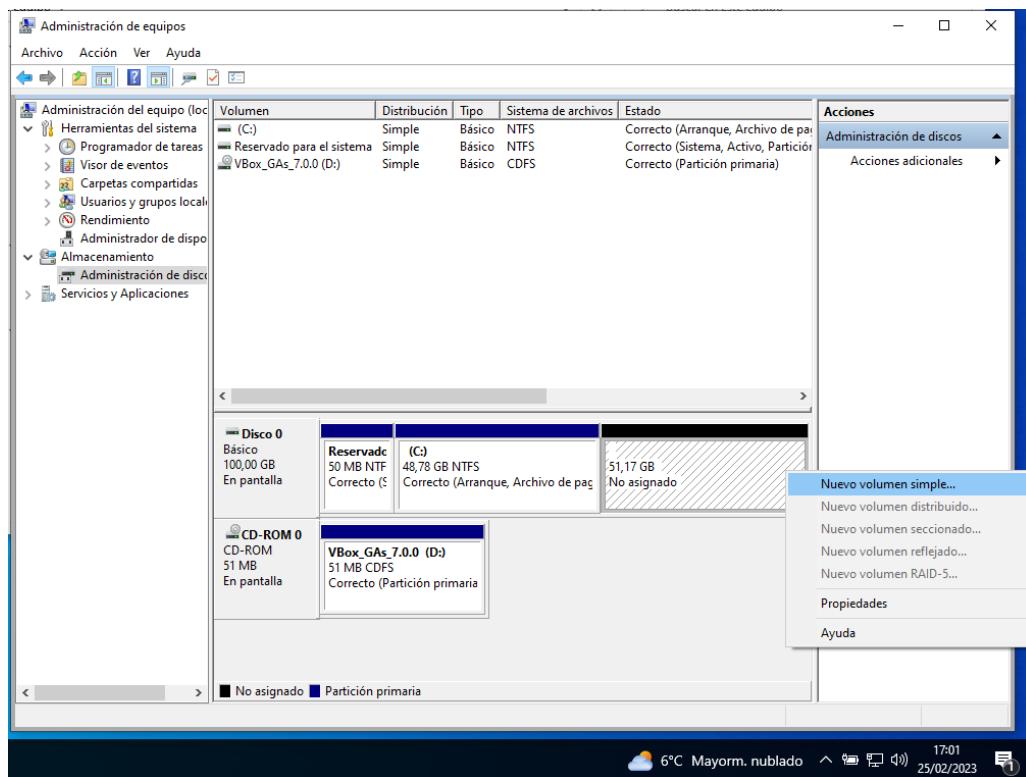


Las particiones que tiene mi máquina en este momento son:

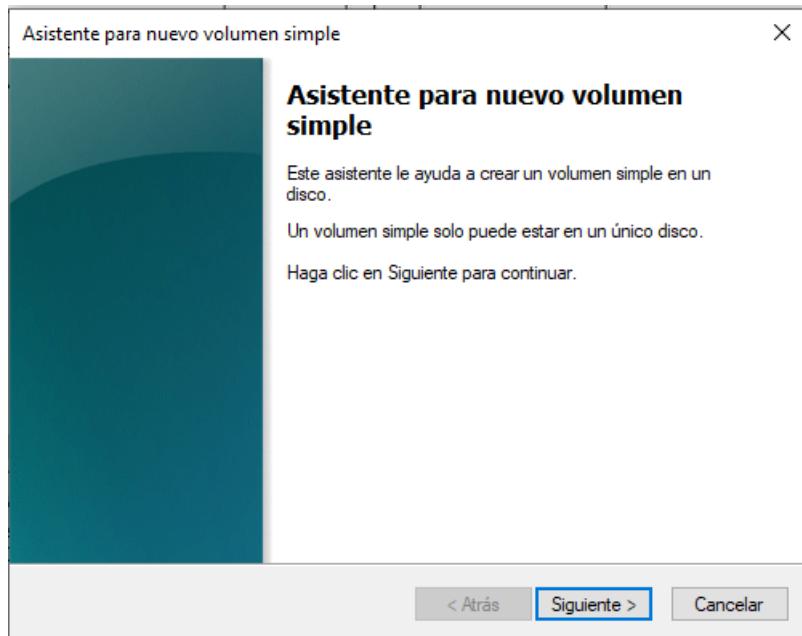


Creo una partición de 40000MB en el espacio libre con sistema de archivos NTFS.

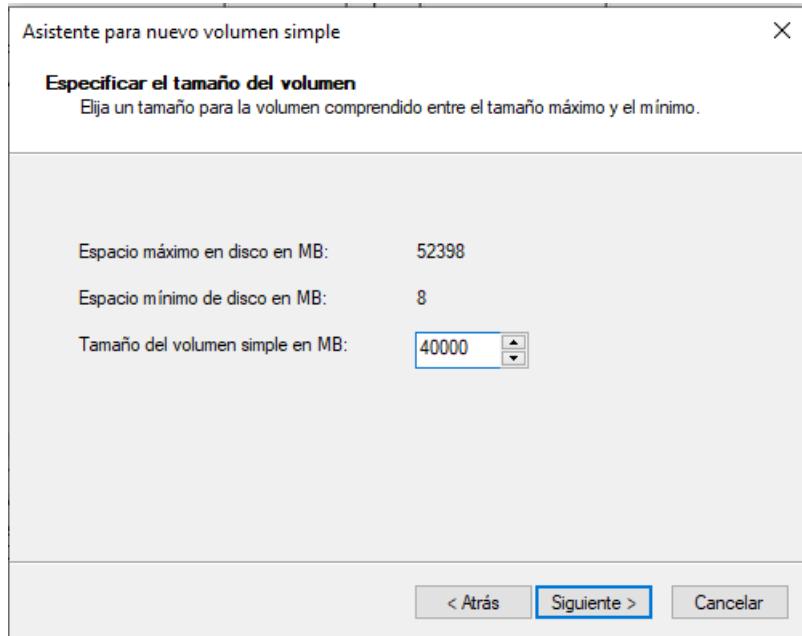
Selecciono el espacio libre, no asignado y con el botón derecho click en “Nuevo volumen simple..”

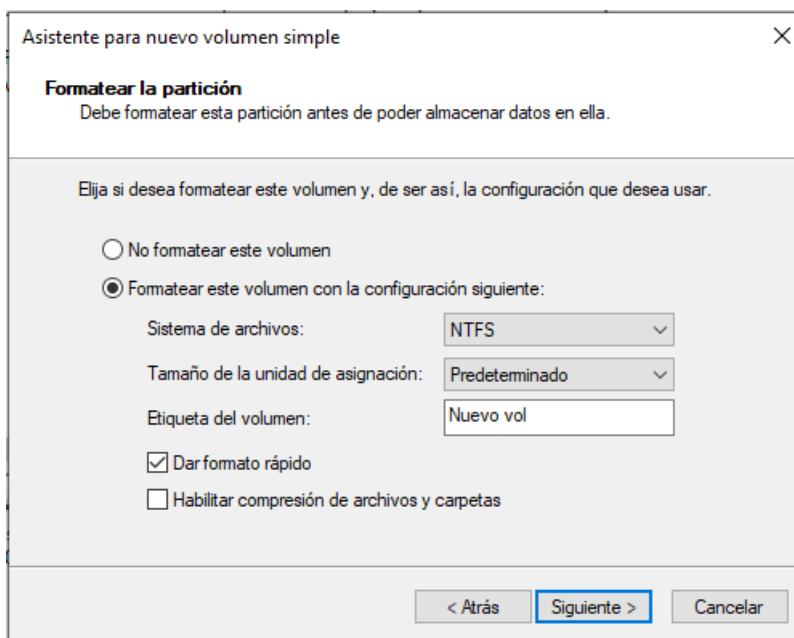
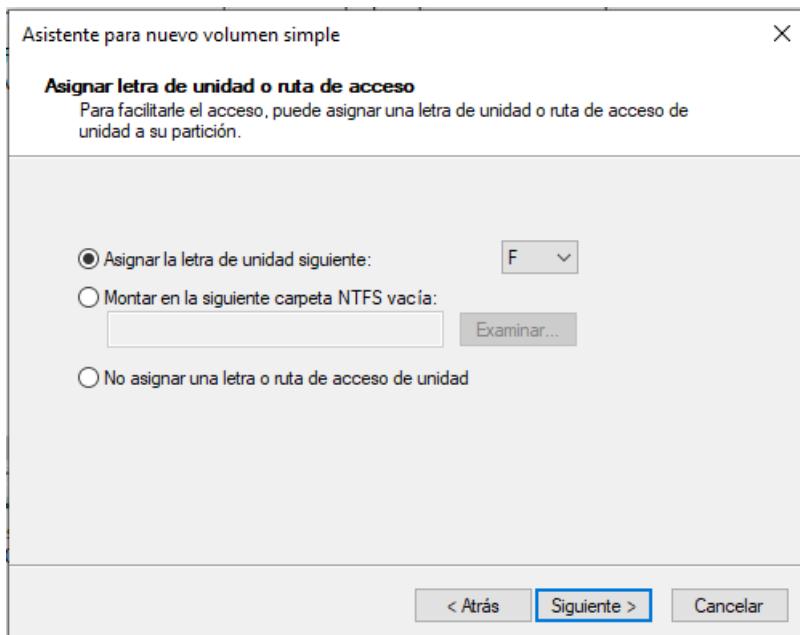


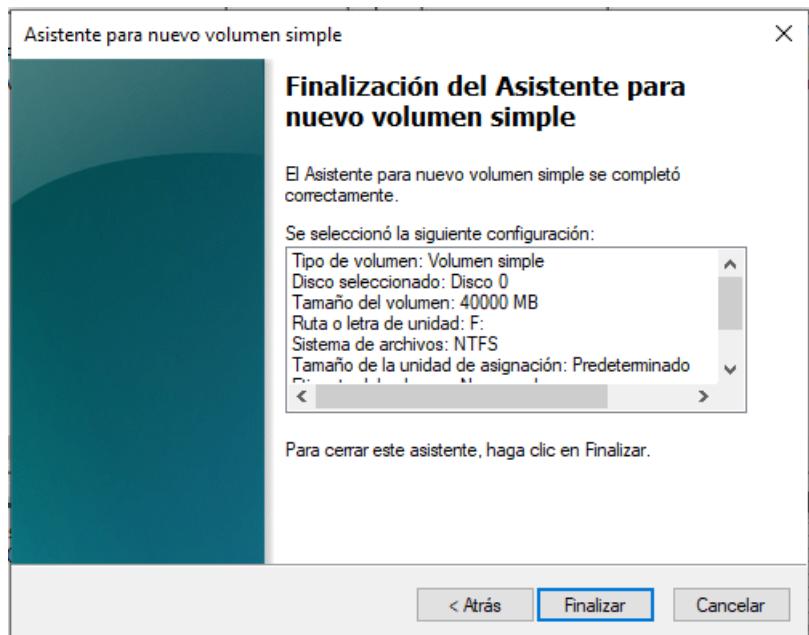
Aparece la siguiente ventana, voy siguiendo los pasos.



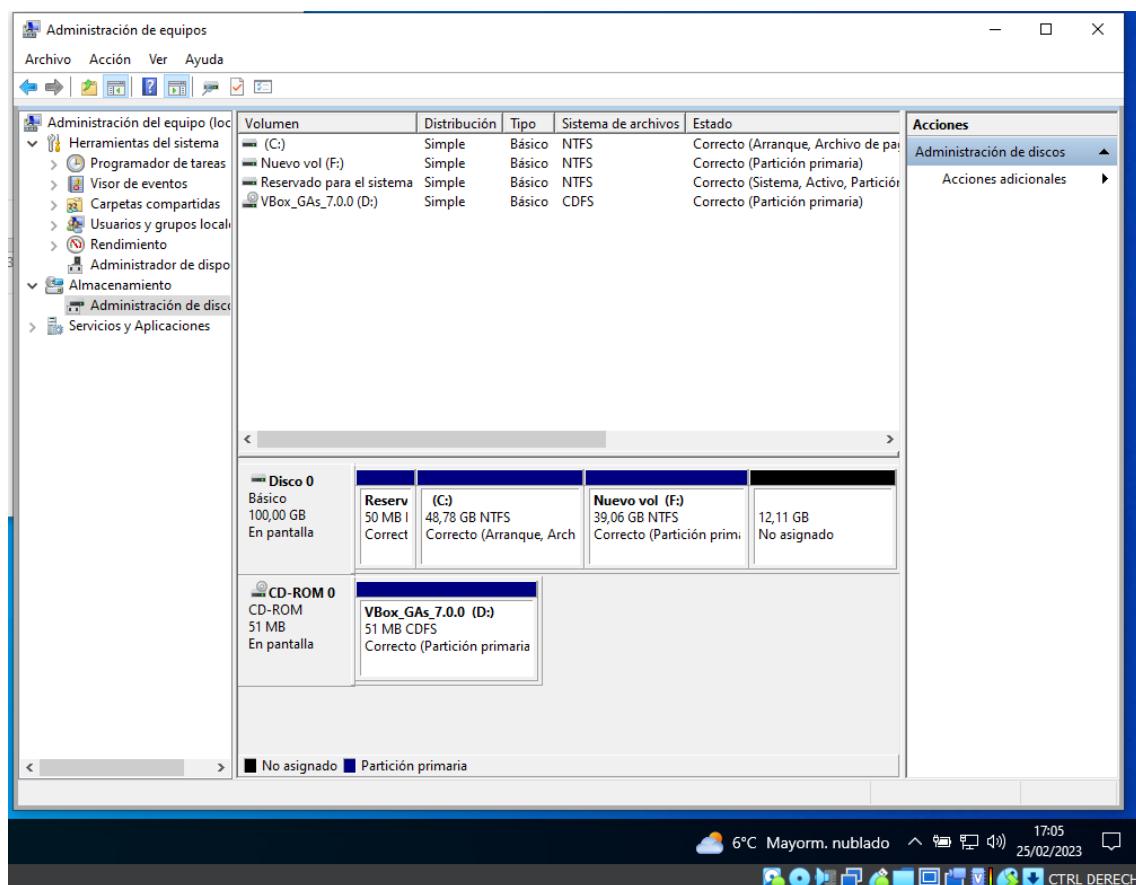
Escribo el tamaño.







Ya tengo la partición creada.



A continuación descargo Clonezilla como archivo iso de 64 bits.

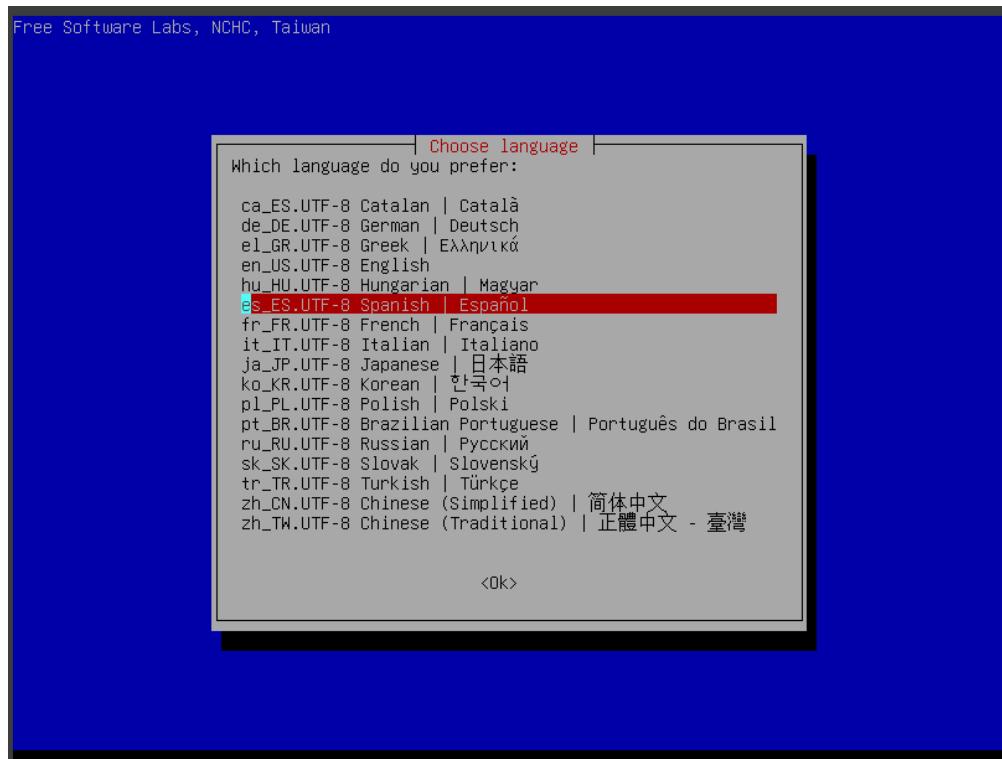
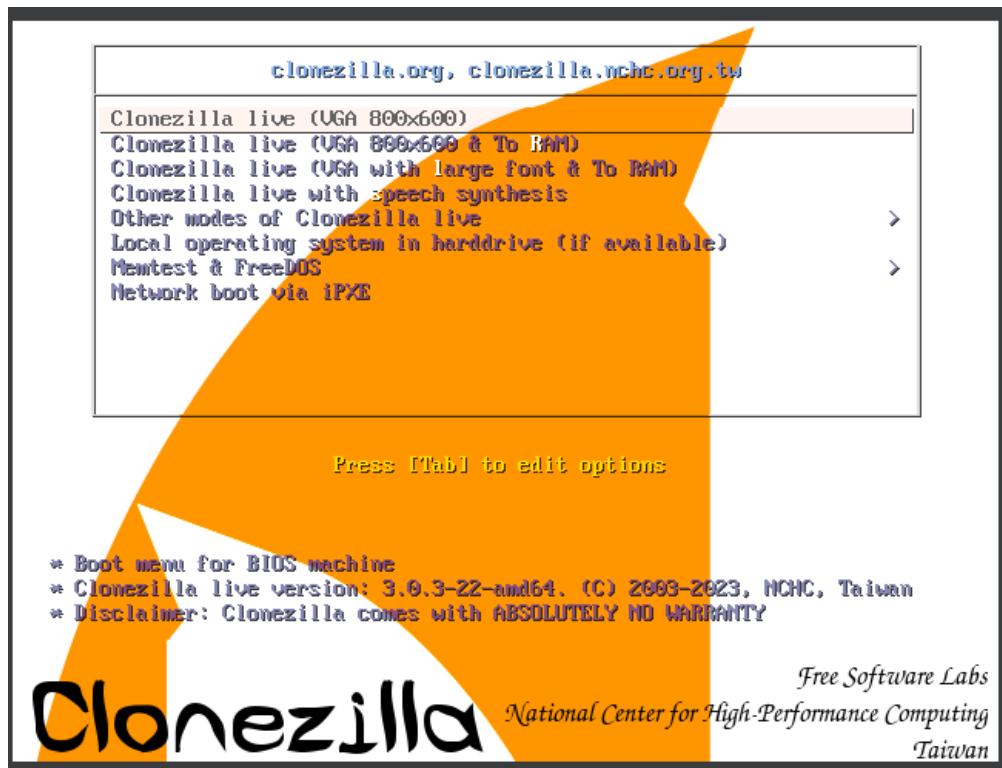
The screenshot shows the Clonezilla website at clonezilla.org/downloads/download.php?branch=stable. The main content area is titled "Downloads" and contains instructions: "To download Clonezilla live, select the following CPU architecture, file type, repository, then click the download button." Below this, it specifies "Release branch: stable, Clonezilla live version: 3.0.3-22". A form allows selecting "CPU architecture" (amd64), "file type" (iso), and "repository" (auto). A "Download" button is present. To the right, there's a promotional box for an eBook about network modernization. At the bottom, a "Notes" section includes a note about Ubuntu 19.10 dropping support for i386 architecture.

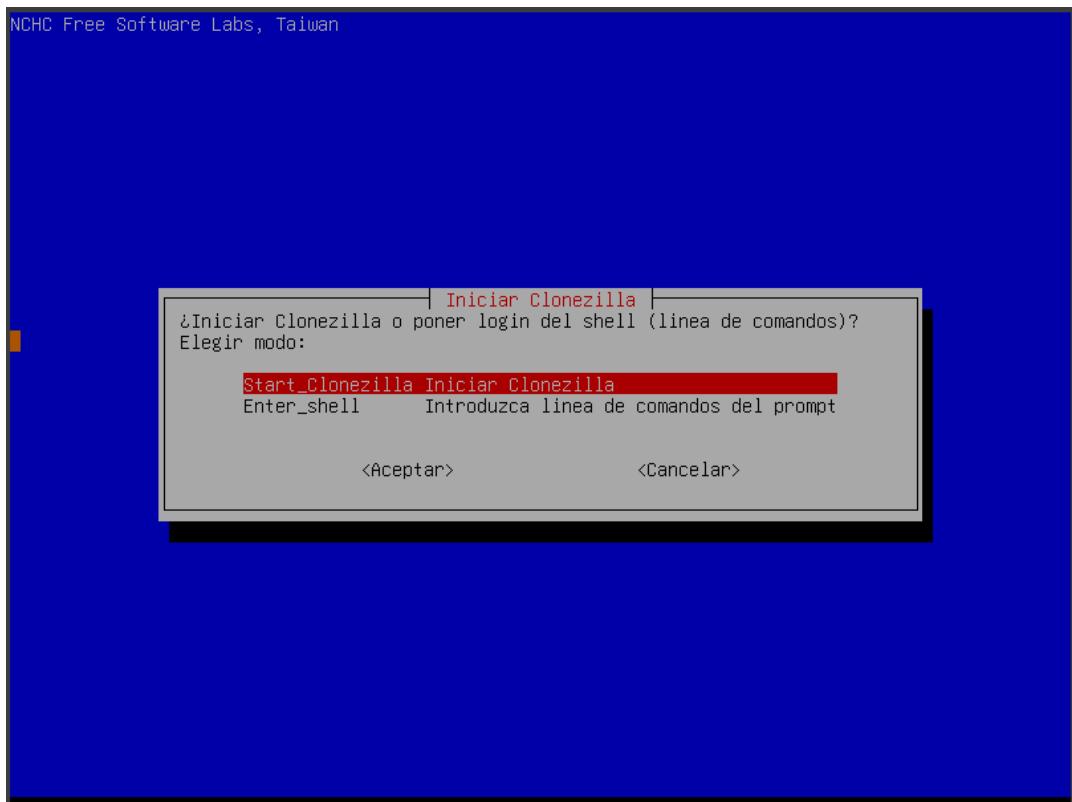
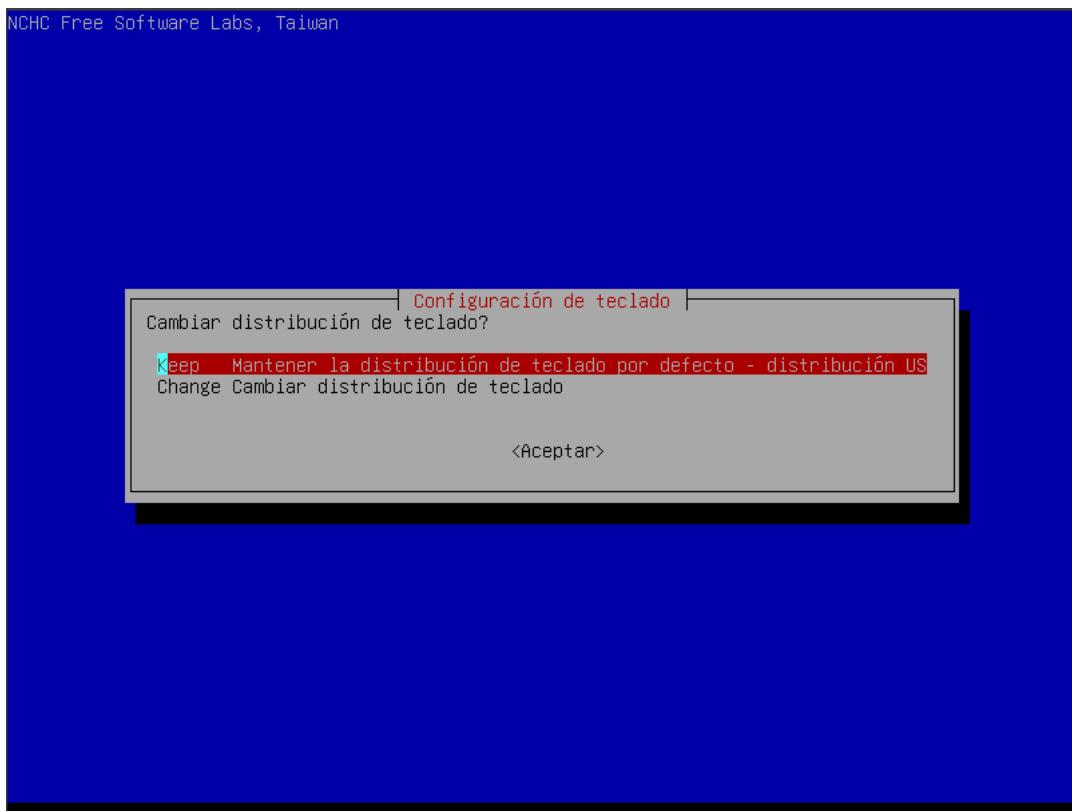
Apago la máquina Windows y pongo como CD la iso descargada de Clonezilla.

The screenshot shows the Oracle VM VirtualBox Manager interface. A virtual machine named "Windows10Sistemas" is selected. In the "Almacenamiento" (Storage) tab, under "Controlador: SATA", the "Puerto SATA 1" dropdown menu is open, showing a list of available ISO files. The item "clonezilla-live-3.0.3-22-amd64.iso" is highlighted with a checkmark, indicating it is selected as the bootable ISO for the virtual machine.

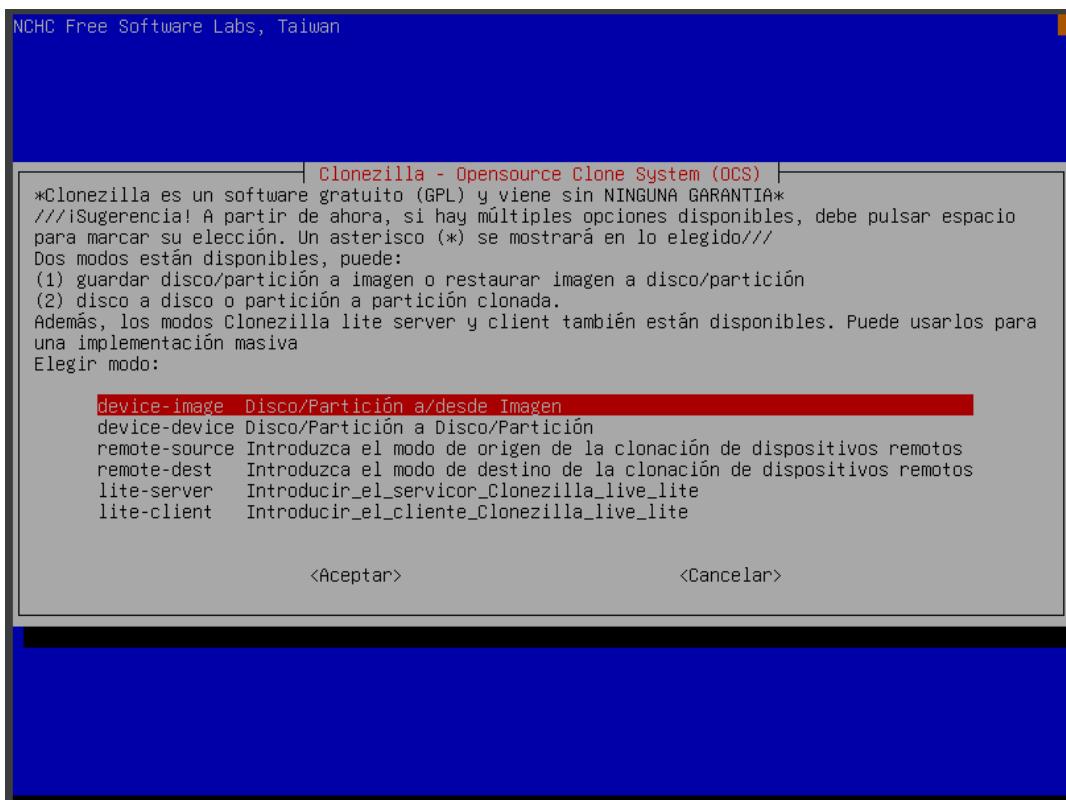
Vuelvo a iniciar la máquina. Y me van a pareciendo las siguientes ventanas.

Voy seleccionando lo que aparece en las capturas.

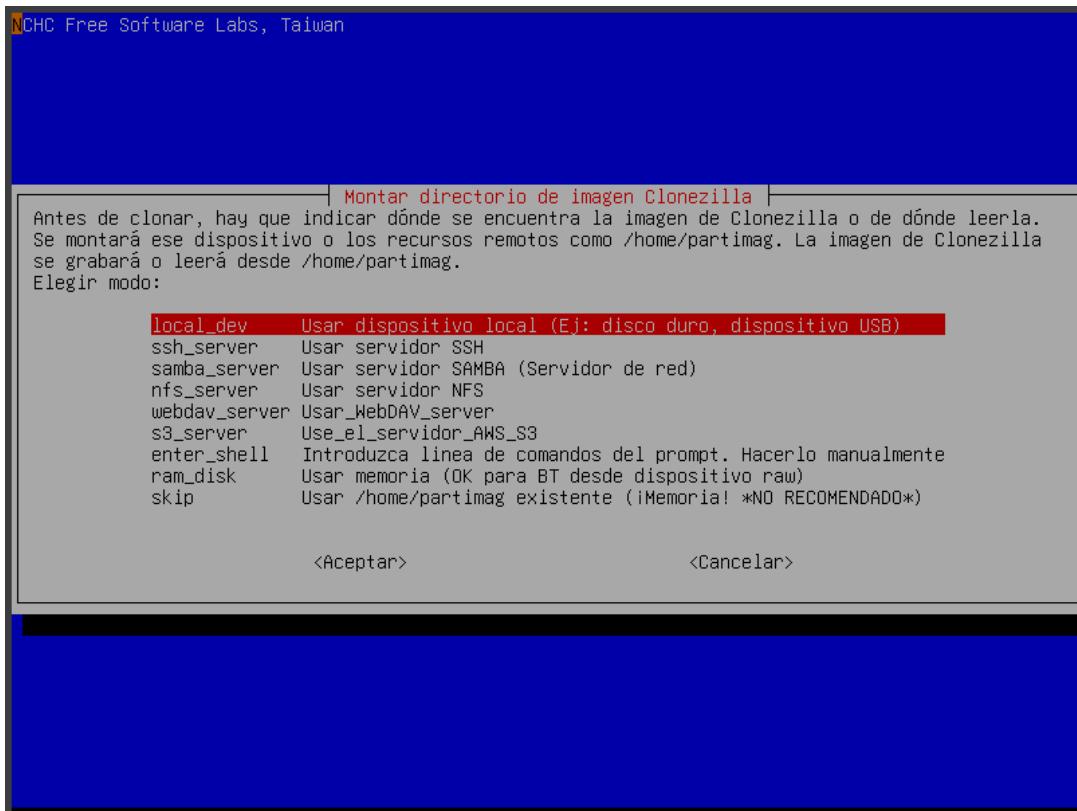




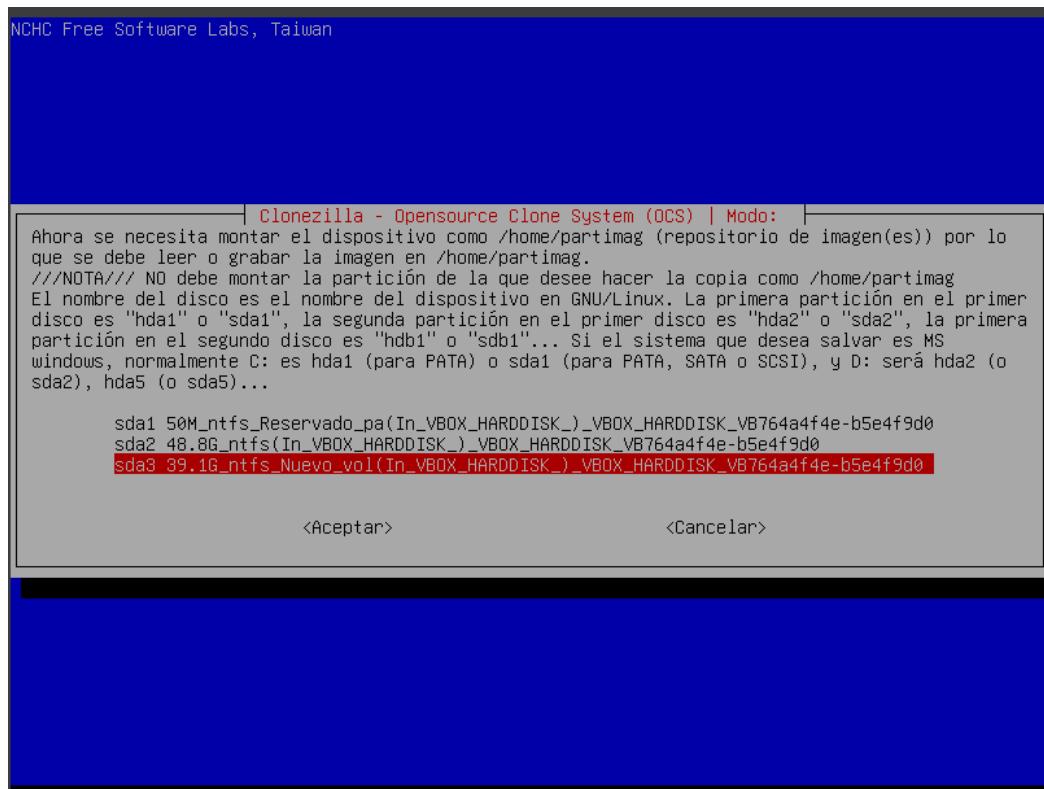
A continuación selecciono la primera opción *device-image*, ya que lo que queremos es crear una imagen. La segunda opción *device-device* sería para realizar clonaciones.



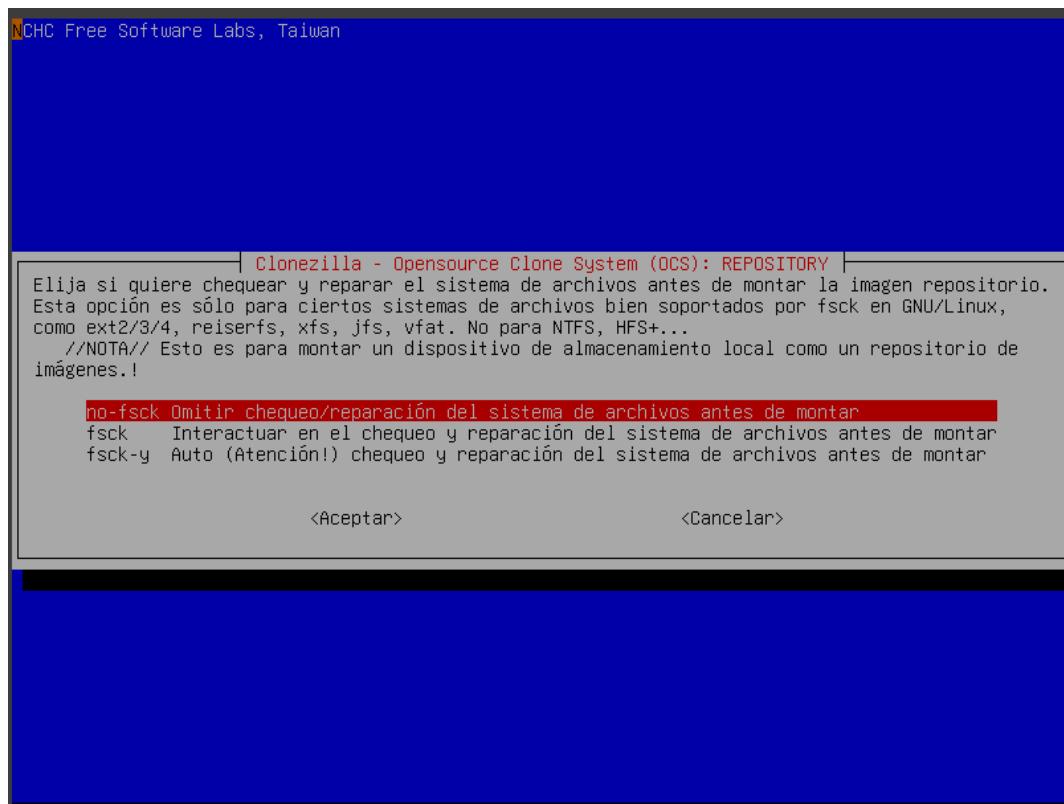
Vuelvo a seleccionar la primera opción.



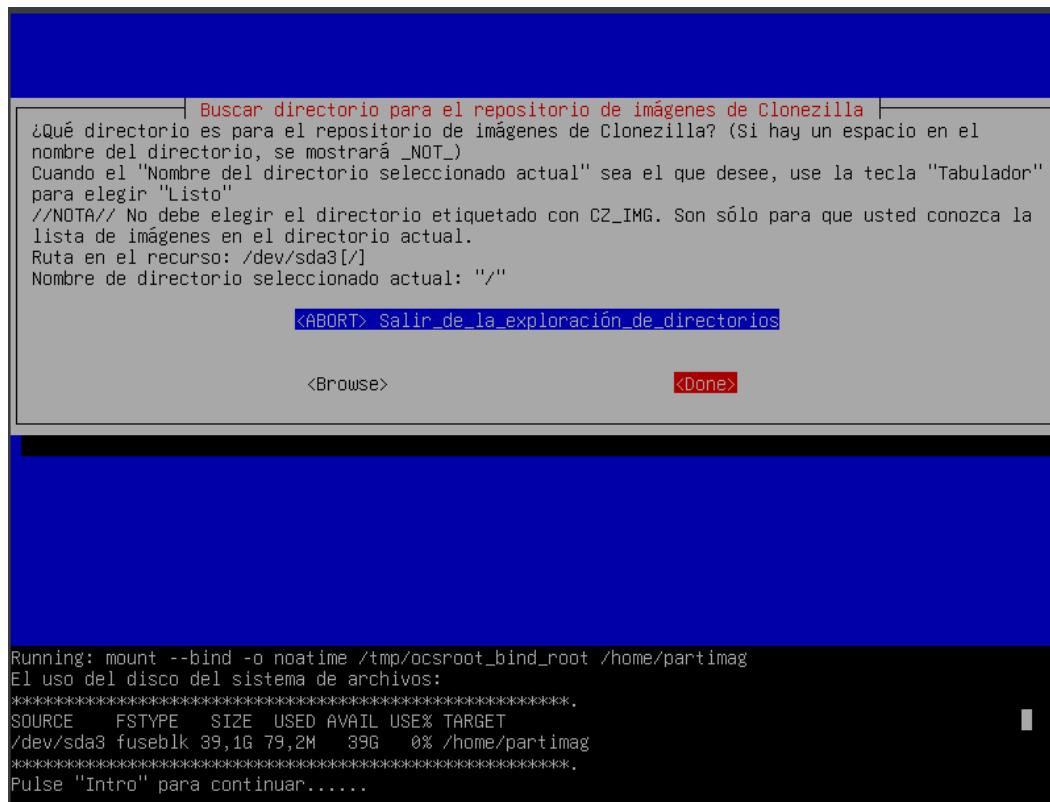
A continuación selecciono la partición sda3 para guardar la imagen, la partición que acabo de crear.



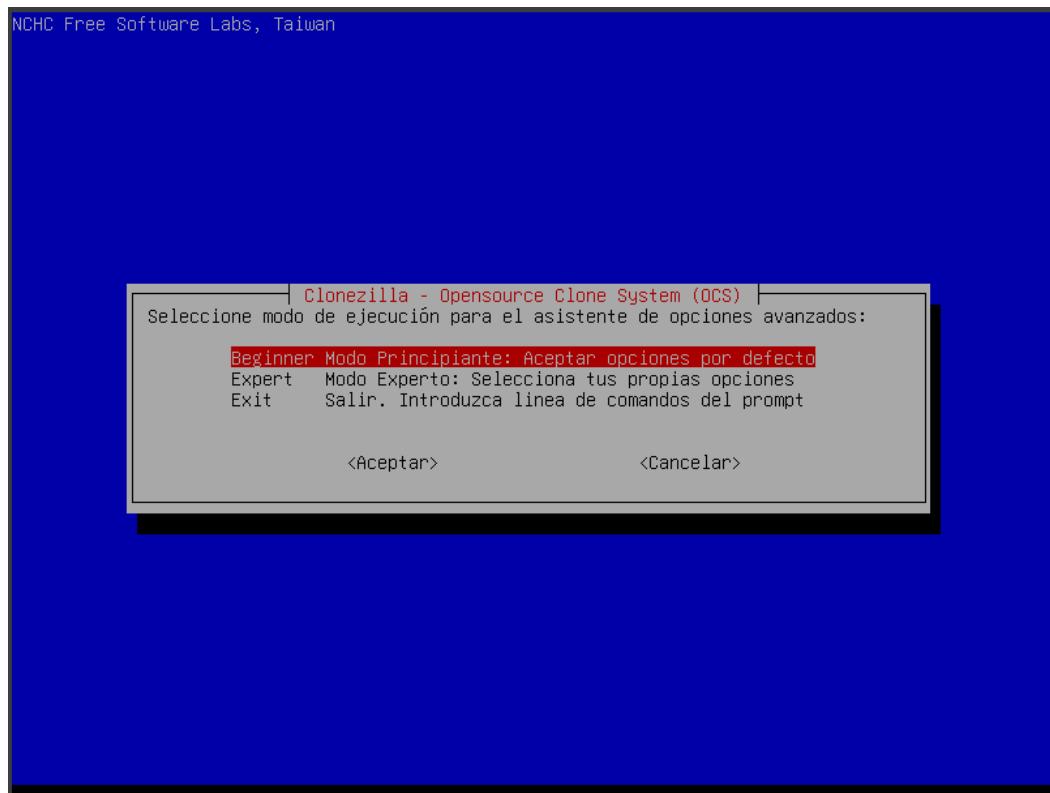
Como mi partición está en NTFS, no hace falta chequear y reparar el sistema de archivos.



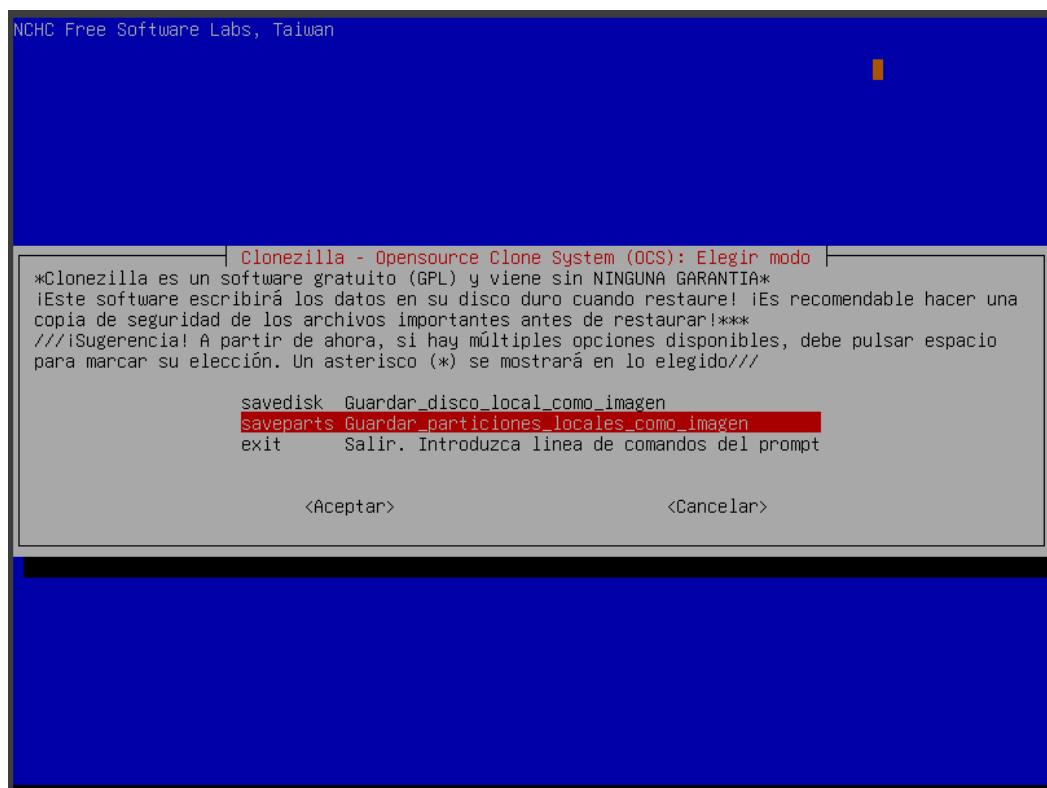
La siguiente ventana es para seleccionar el directorio para guardar la imagen. Dejo las opciones por defecto. Pulso “Done” e “Intro”.



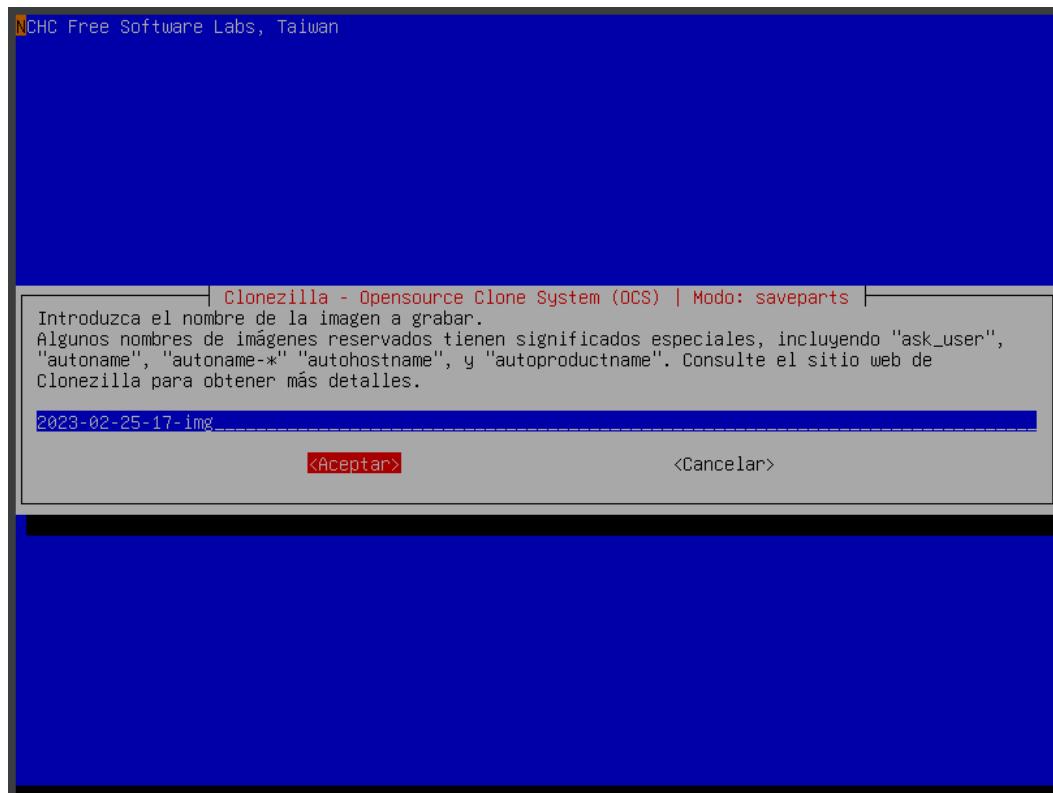
Selecciono el Modo Principiante.



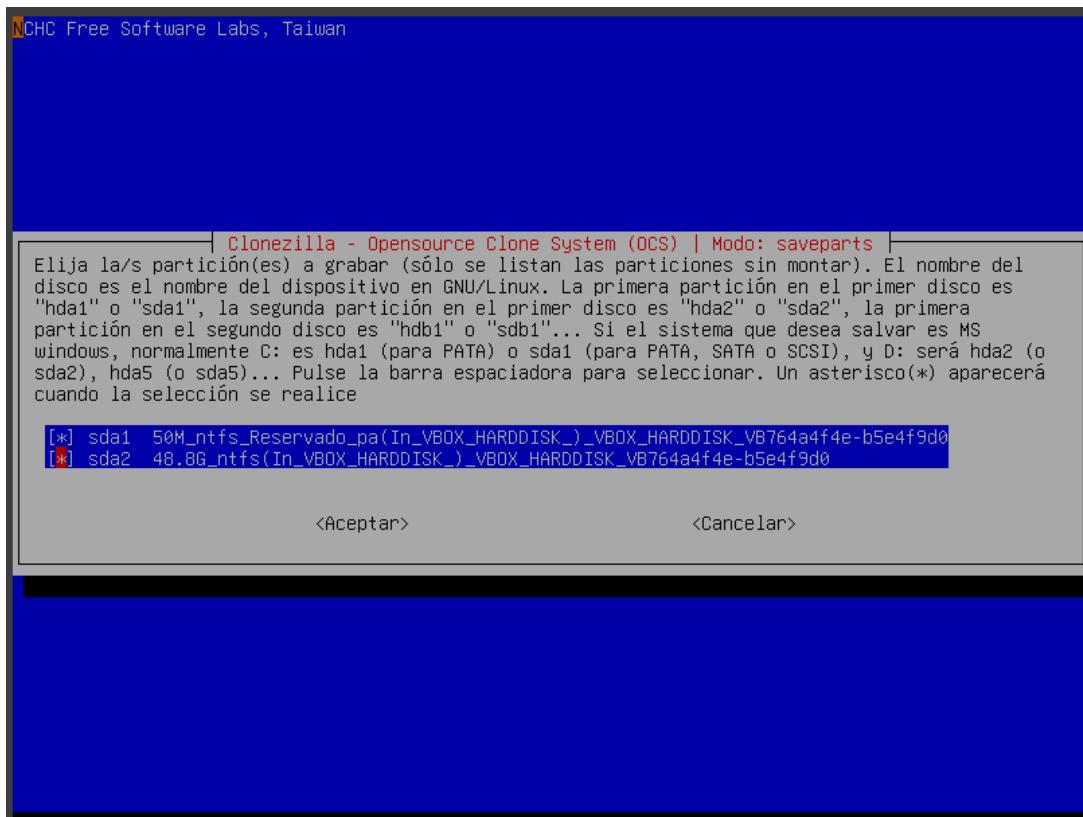
Marco “Guardar particiones locales como imagen”



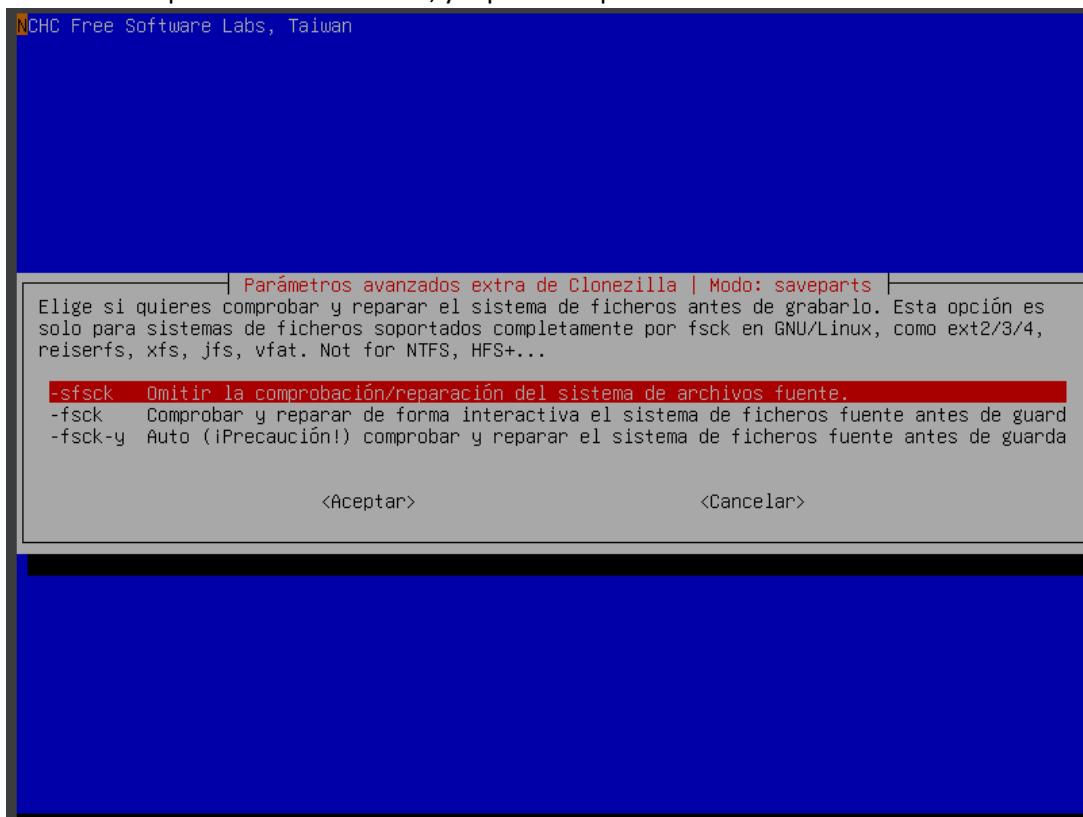
Pulso “Aceptar” y se crea una carpeta con la fecha para guardar la imagen.



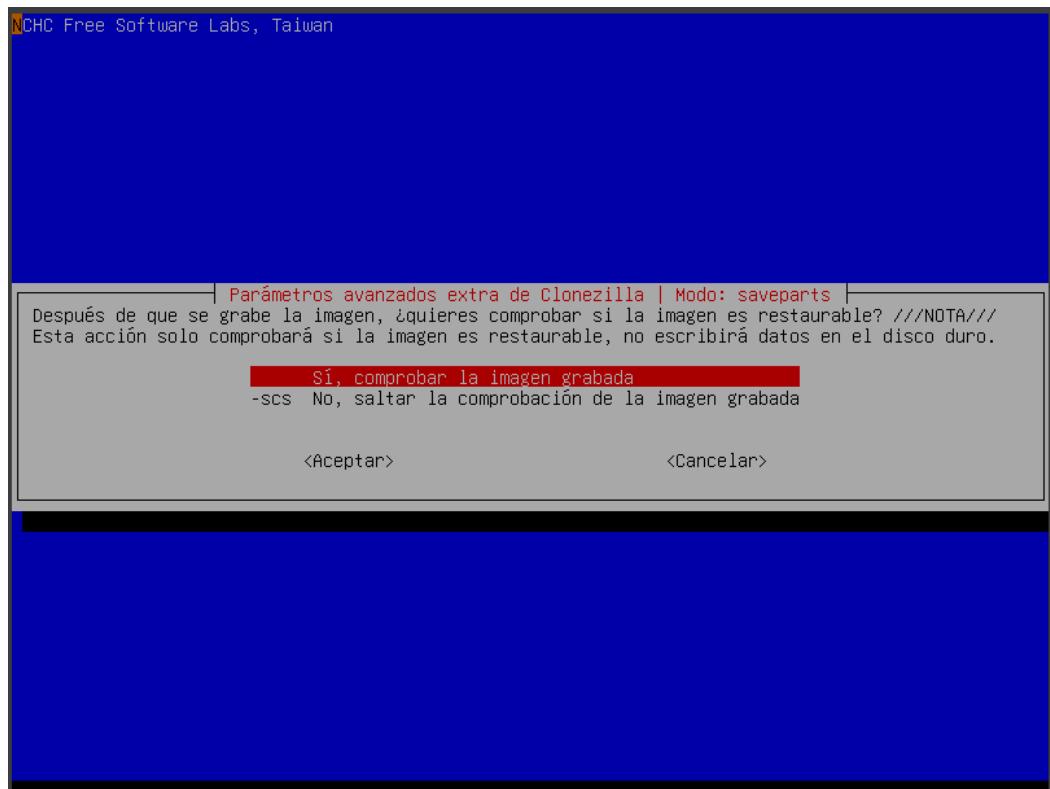
A continuación se eligen las particiones a incluir en la imagen. Para seleccionar las dos, hay que pulsar espacio sobre una de ellas, luego ir a la siguiente y pulsar espacio de nuevo. Aparece un * al lado de las particiones seleccionadas.



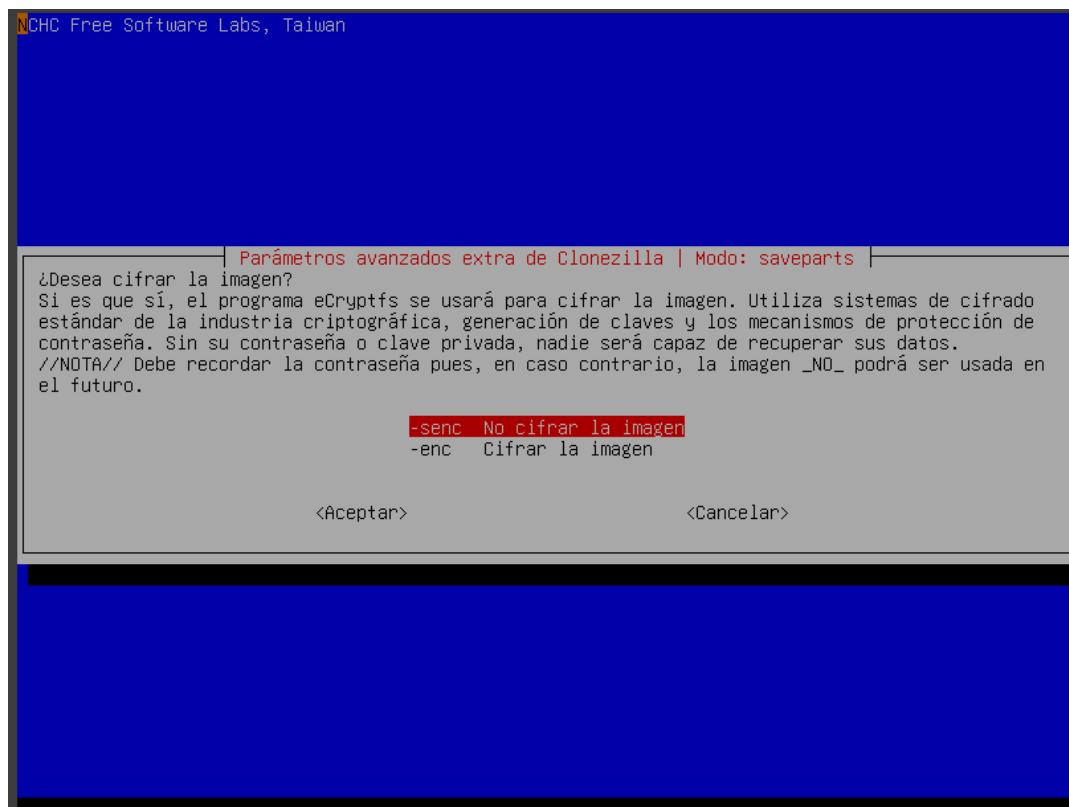
Omito la comprobación del sistema, ya que no es para NTFS.

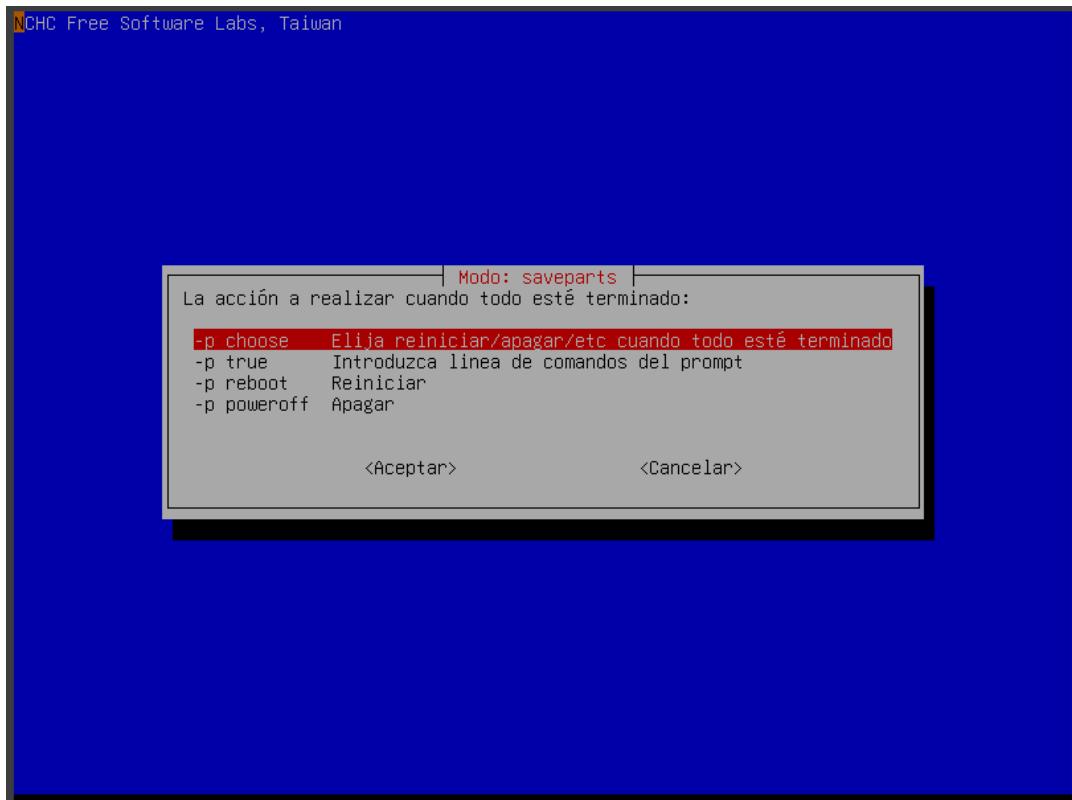


Selecciono “Sí, comprobar la imagen grabada”, tarda un poco más en crearse, pero me aseguro que la imagen es correcta.

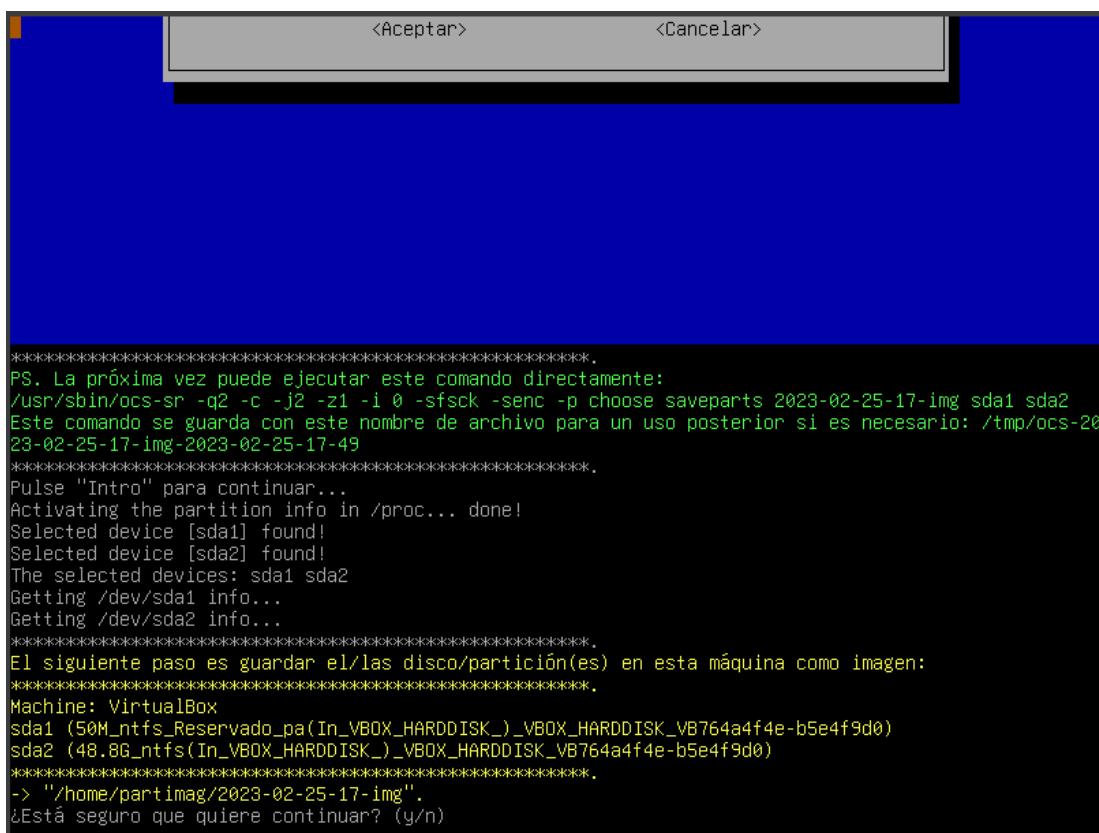


No pongo contraseña en la imagen.

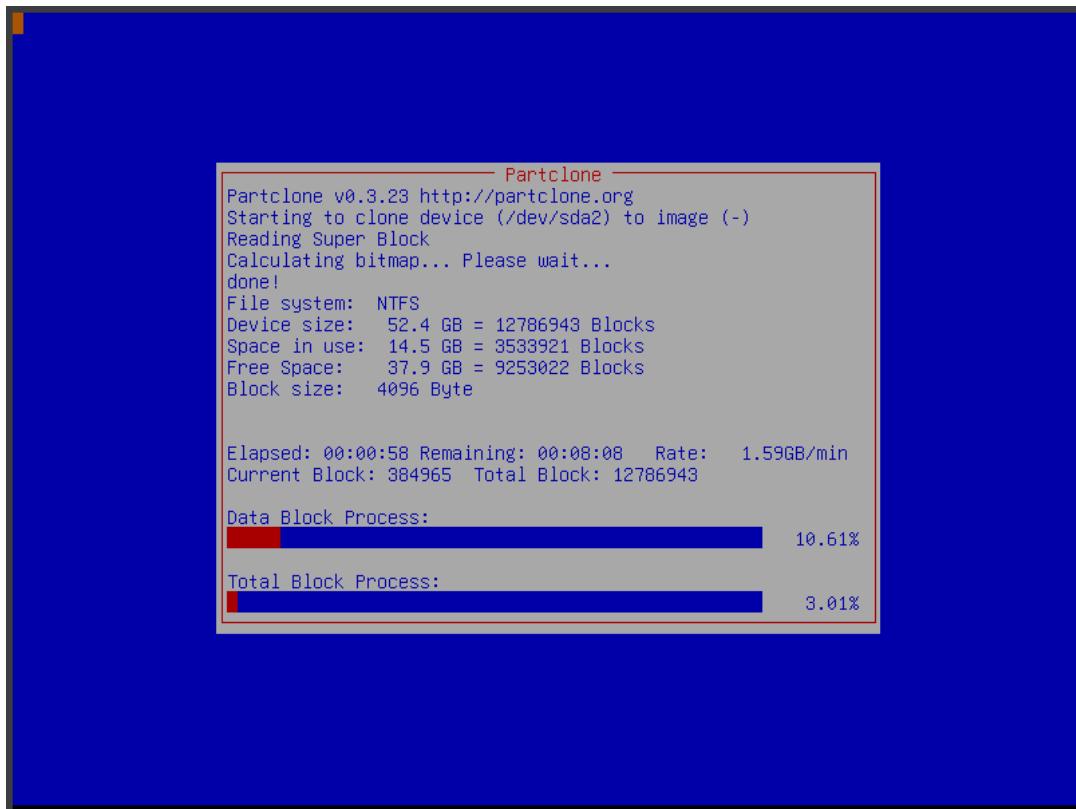




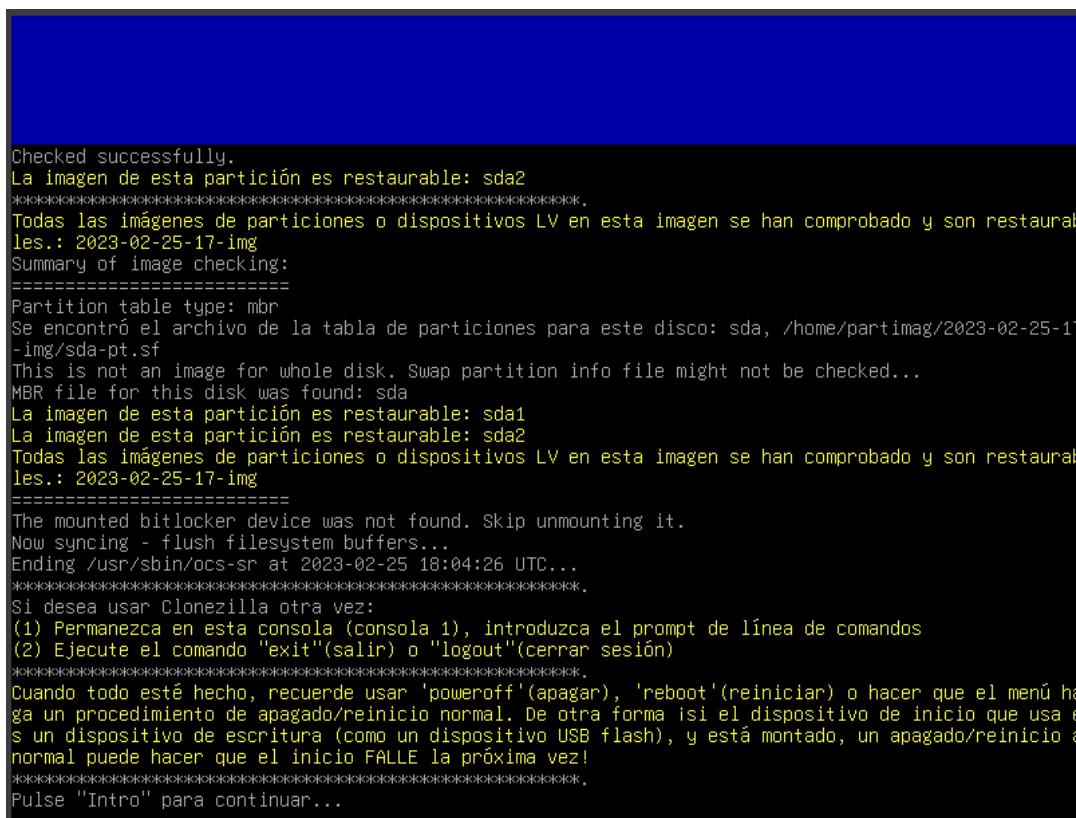
Aparece lo siguiente a título informativo.

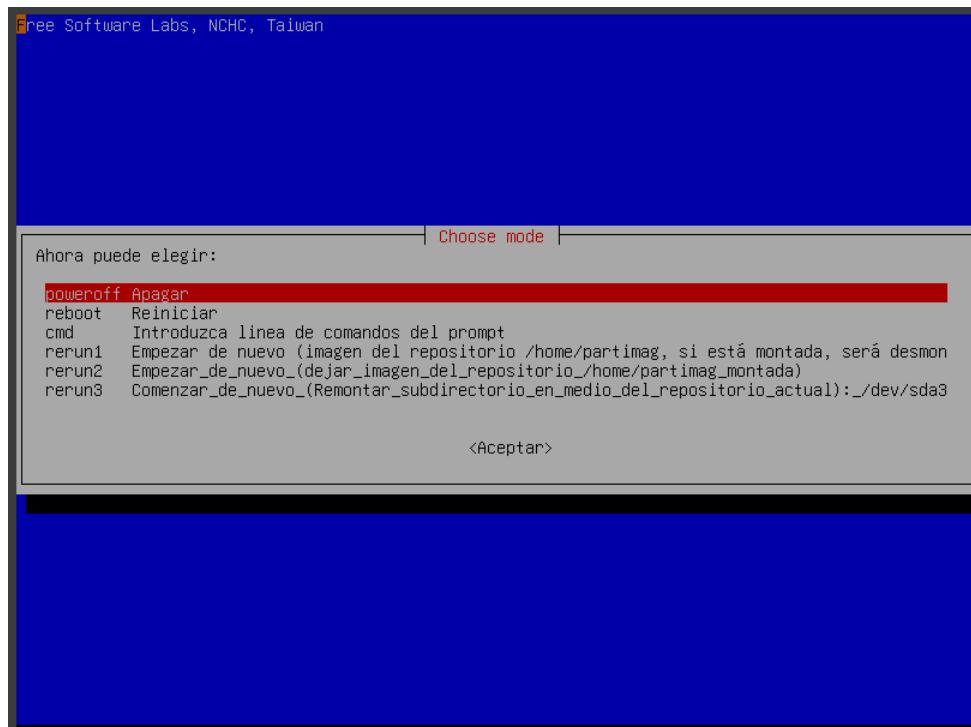


Y empiezas a crearse las imágenes de las dos particiones.



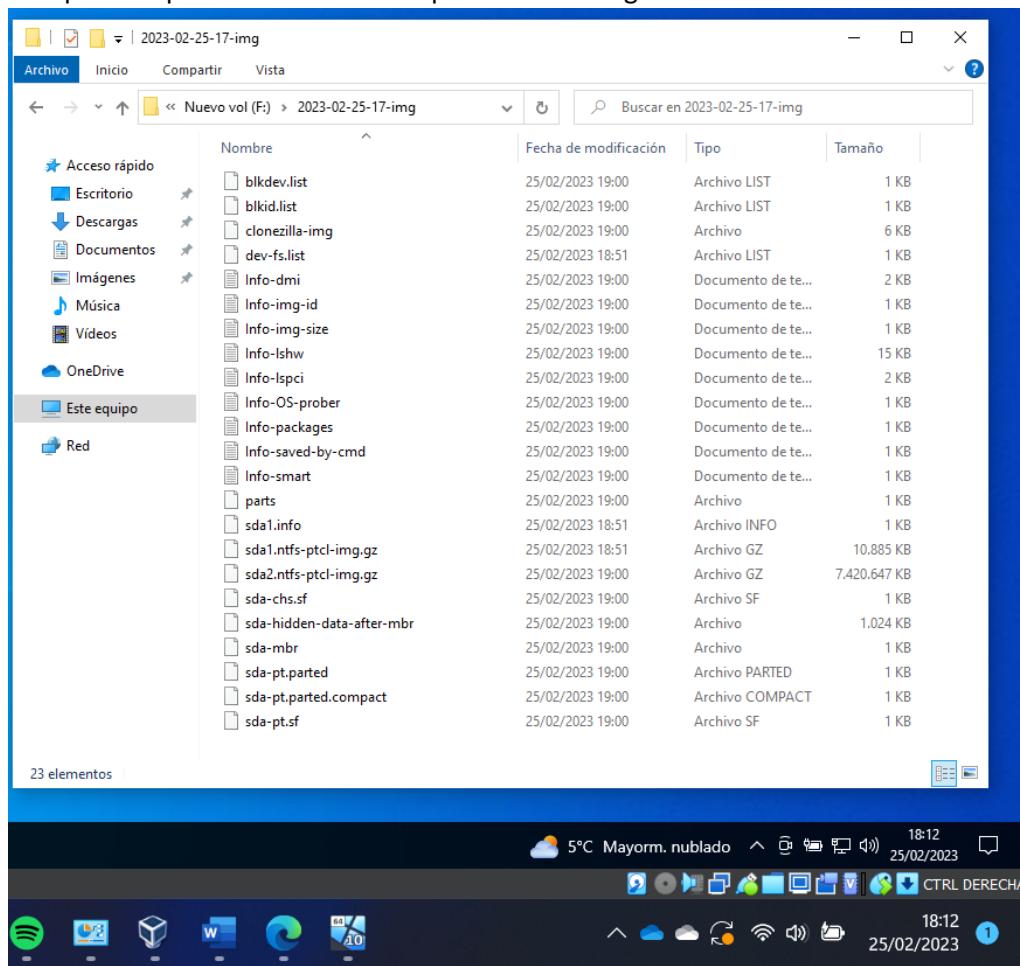
Cuando termina, apago la máquina.





Vuelvo a encender la máquina Windows, sin la imagen iso de Clonezilla.

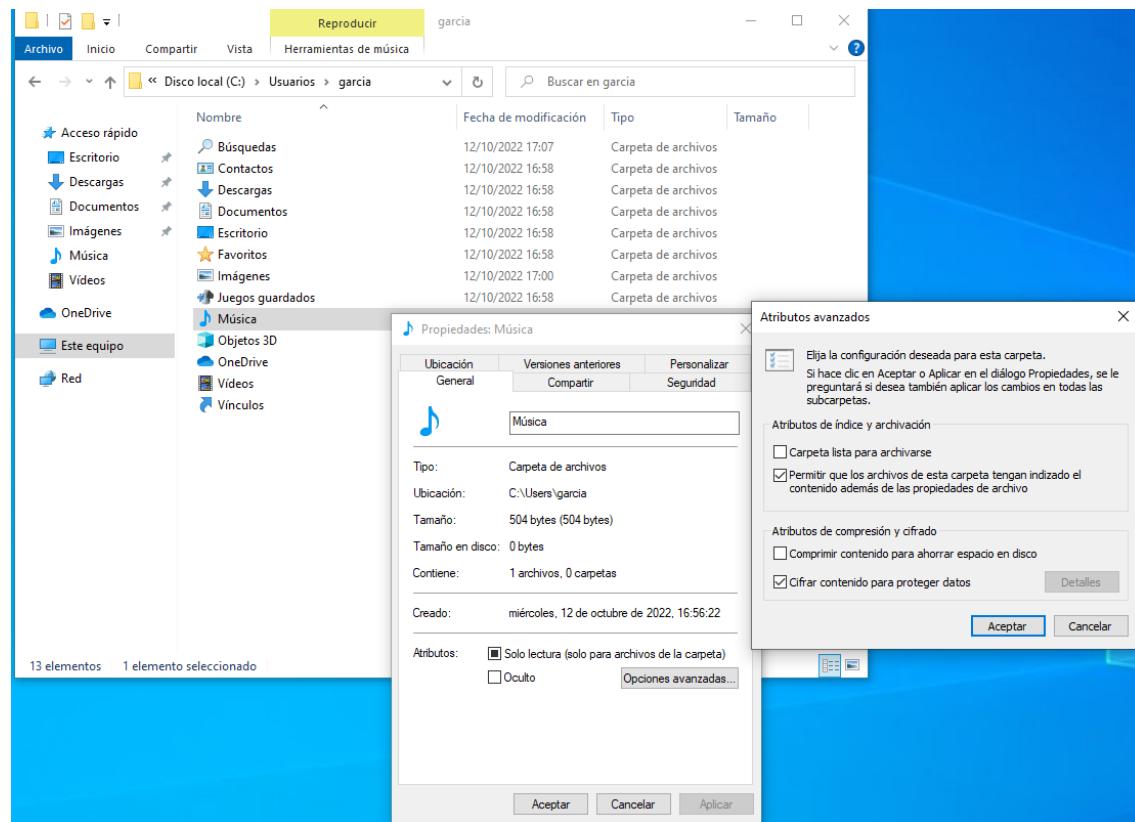
Compruebo que se ha creado la carpeta con las imágenes.



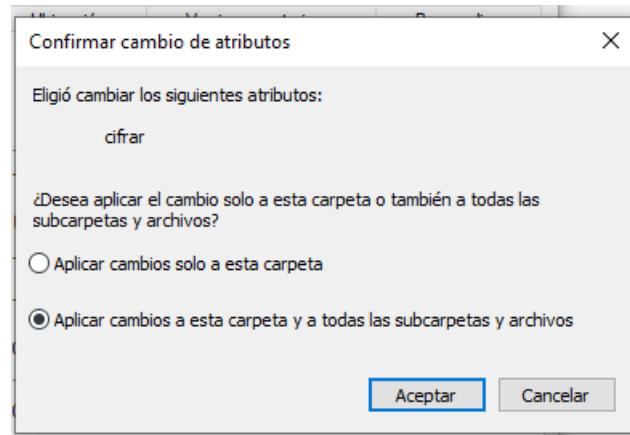
Ejercicio 4. Servicio EFS de Windows

Cifra una carpeta cualquiera de tu máquina Windows y exporta el certificado, tal como se realiza en capítulo 7.3

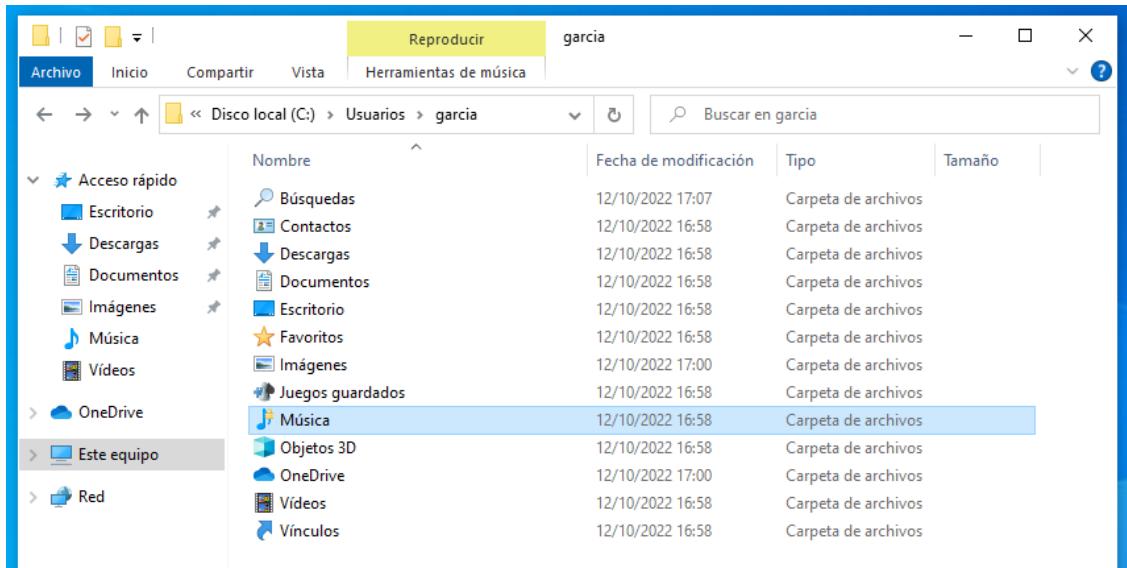
Sobre la carpeta que quiero cifrar, con el botón derecho hago click y selecciono **Propiedades**, en la solapa **General/Opciones avanzadas** yactivo la casilla **Cifrar contenido para proteger datos** y **Aceptar**.



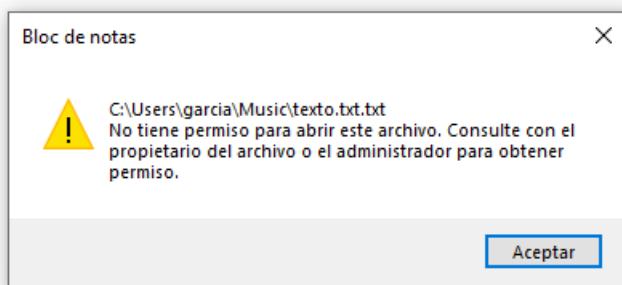
Me pregunta si queremos cifrar todo el contenido o solo esa carpeta. Elijo todo el contenido.



Ahora me aparece un pequeño candado sobre la carpeta que he cifrado.

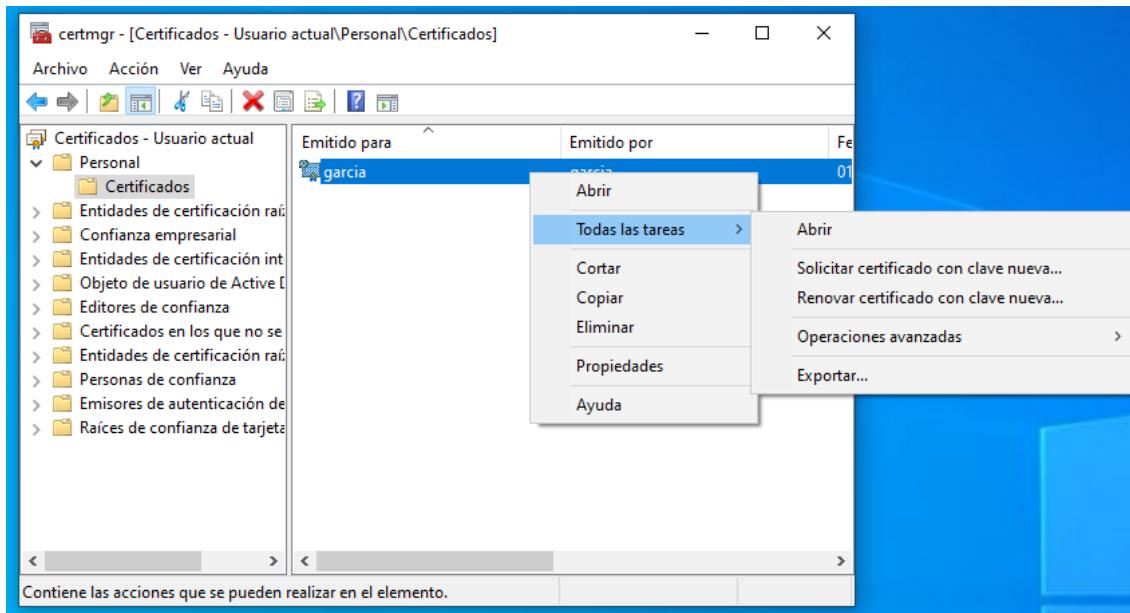


Intento acceder desde otro usuario que tiene acceso total a esa carpeta, y compruebo que no me deja acceder.

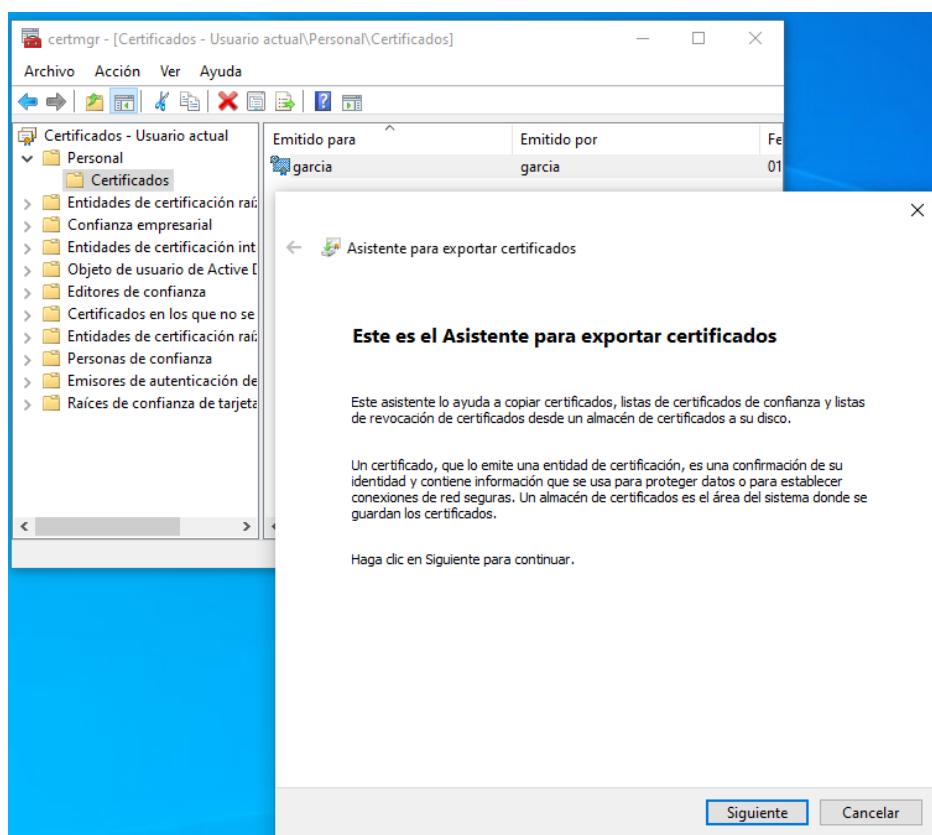


Para exportar el certificado:

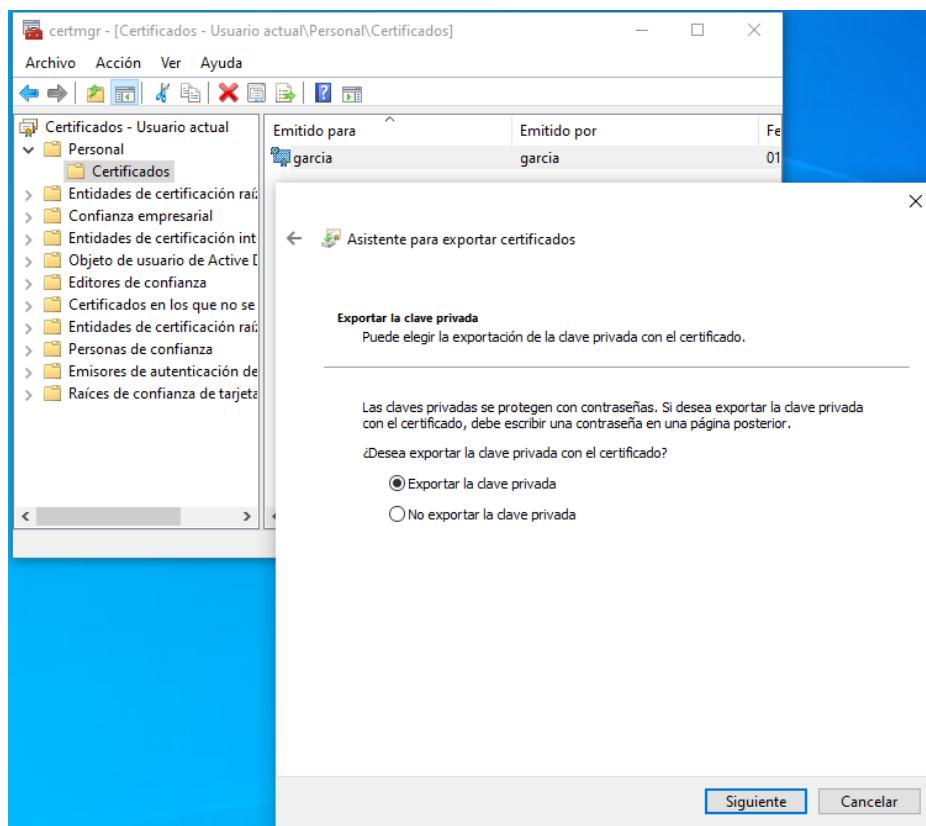
- Ejecuto el comando: certmgr.msc. Se abre una ventana.
- Voy a Certificados/Personal/Certificado.
- Pulso con el botón derecho y voy a Todas las tareas/Exportar



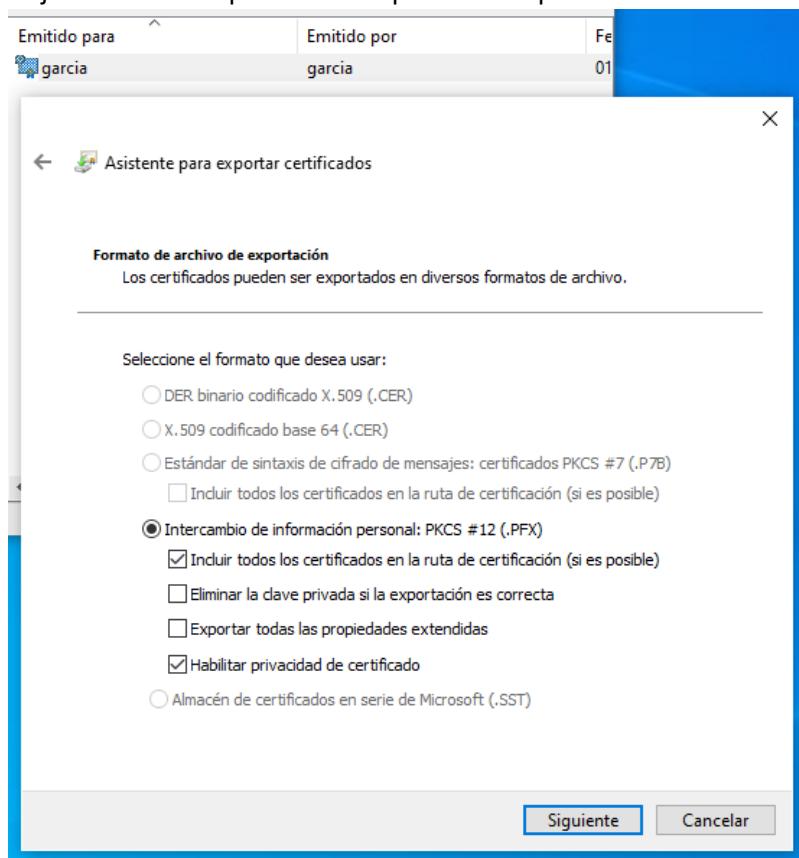
Aparece un Asistente para exportar certificados.



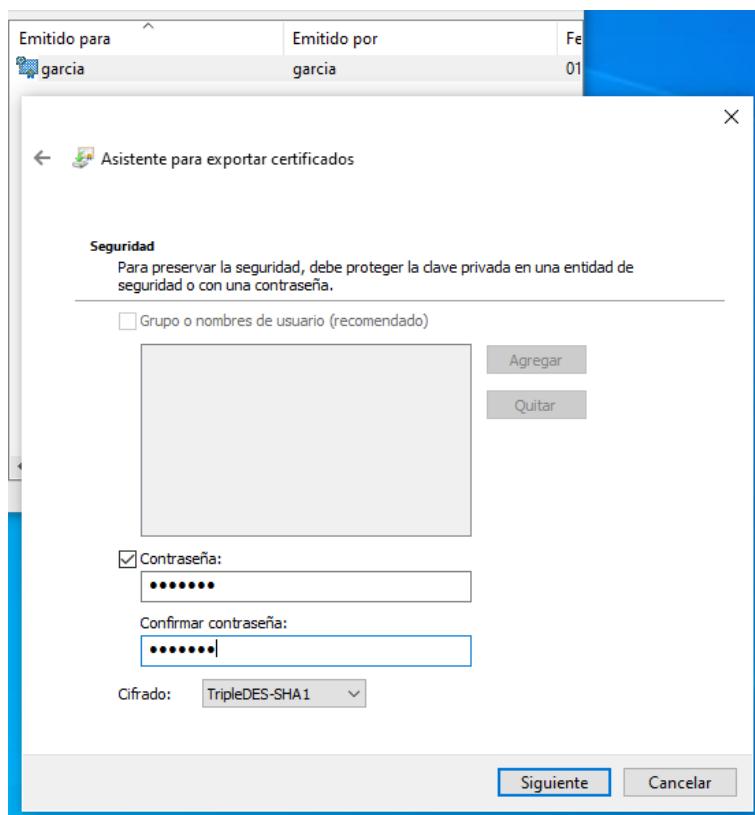
Selecciono Exportar la clave privada.



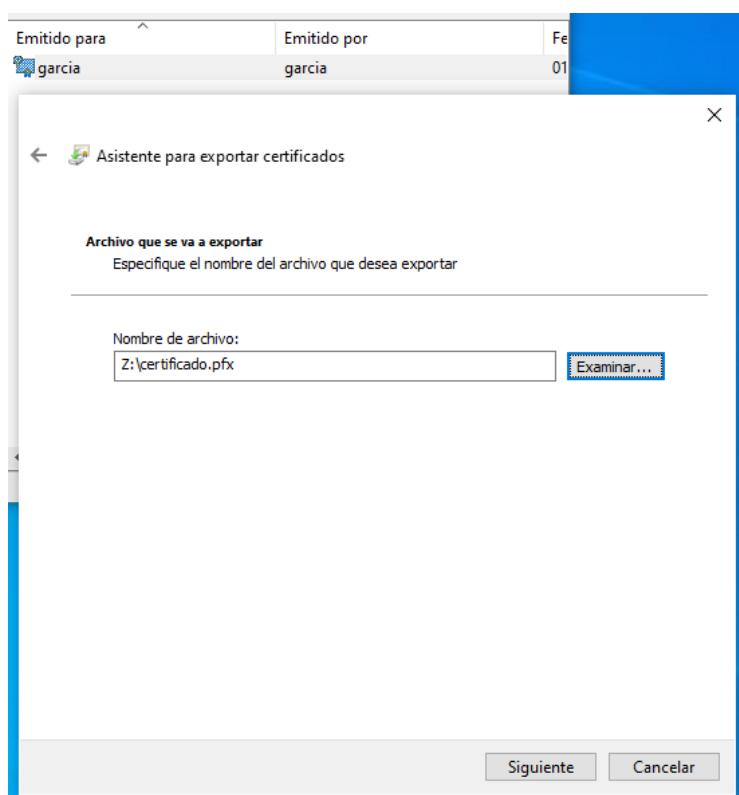
Dejo la extensión que nos viene por defecto pfx.



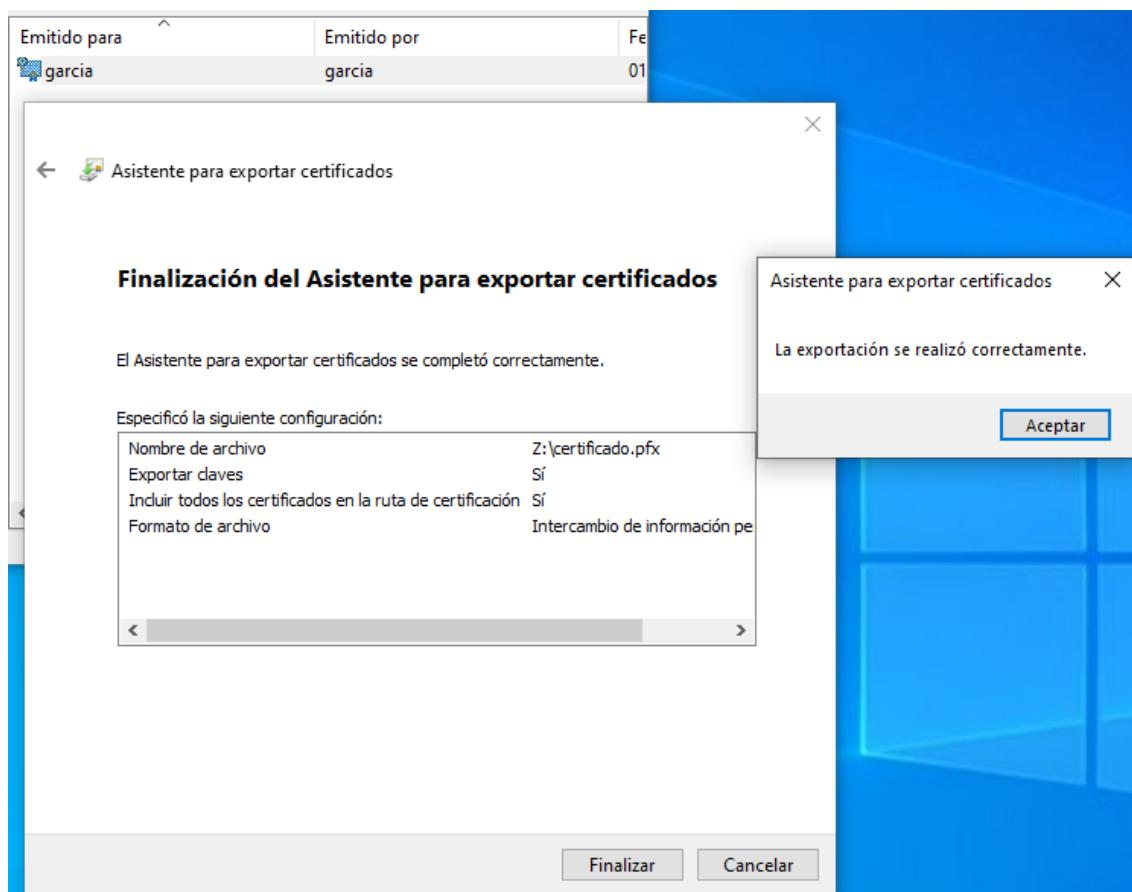
Elijo la contraseña, y la escribo dos veces.



Selecciono donde voy a guardar el certificado y su nombre.



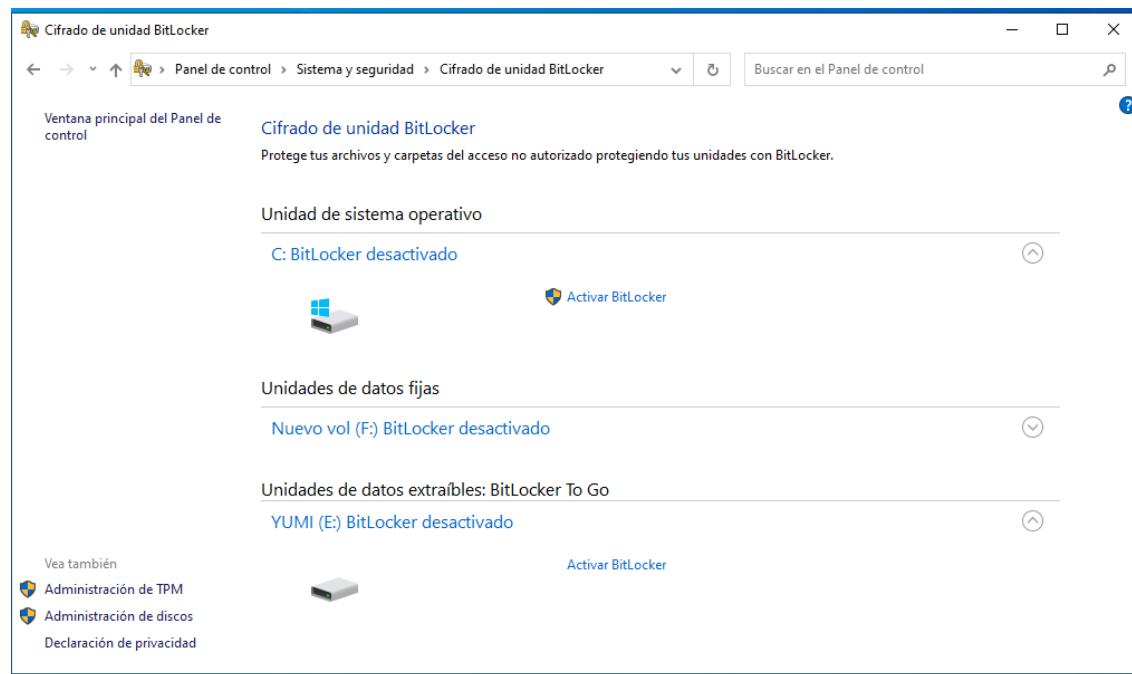
Y ya estaría exportado el certificado.



Ejercicio 5. BitLocker To Go

Cifra un pendrive con BitLocker To Go tal como se realiza en libro capítulo 7.3.

Para abrir BitLocker voy a : Panel de control / Sistema y seguridad / Cifrado de unidad Bitlocker.



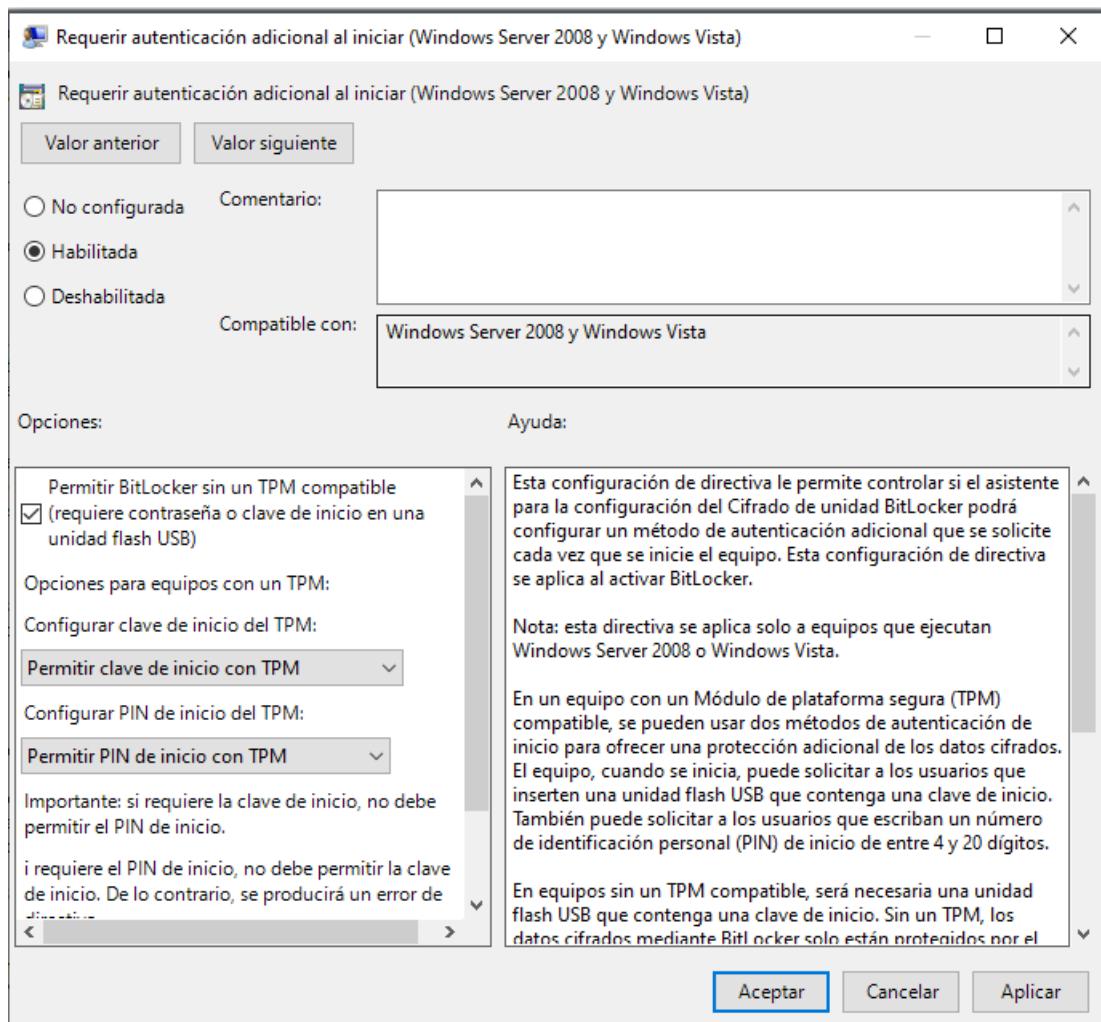
Como el PC no tiene el módulo TPM, tengo que editar la directiva local “Requerir autentificación adicional al iniciar”

Ejecuto gpedit.msc. Dentro de Directiva Equipo local / Configuración del equipo / Plantillas administrativas / Componentes de Windows / Cifrado de unidad BitLocker / Unidades del sistema operativo.

Configuración	Estado	Comentario
Permitir desbloqueo de la red al iniciar	No configurada	No
Permitir Arranque seguro para comprobación de integridad	No configurada	No
Requerir autenticación adicional al iniciar	No configurada	No
Requerir autenticación adicional al iniciar (Windows Server 2008 y Windows Vista)	No configurada	No
No permitir que usuarios estándar cambien el PIN o la contr...	No configurada	No
Permite que los dispositivos compatibles con InstantGo o H...	No configurada	No
Habilitar el uso de autenticación BitLocker que requiera entr...	No configurada	No
Permitir los PIN mejorados para el inicio	No configurada	No
Configurar longitud mínima de PIN para el inicio	No configurada	No
Configurar el uso de cifrado basado en hardware para unida...	No configurada	No
Aplicar tipo de cifrado de unidad en unidades de sistema op...	No configurada	No
Configurar el uso de contraseñas para unidades de sistema ...	No configurada	No
Elegir cómo se pueden recuperar unidades del sistema oper...	No configurada	No
Configurar el perfil de validación de plataforma del TPM par...	No configurada	No
Configurar el perfil de validación de plataforma de TPM (Wi...	No configurada	No
Configurar el perfil de validación de plataforma del TPM par...	No configurada	No
Configurar la dirección URL y el mensaje de recuperación pr...	No configurada	No
Restablecer datos de validación de plataforma después de la...	No configurada	No
Usar perfil de comprobación de datos de configuración de a...	No configurada	No

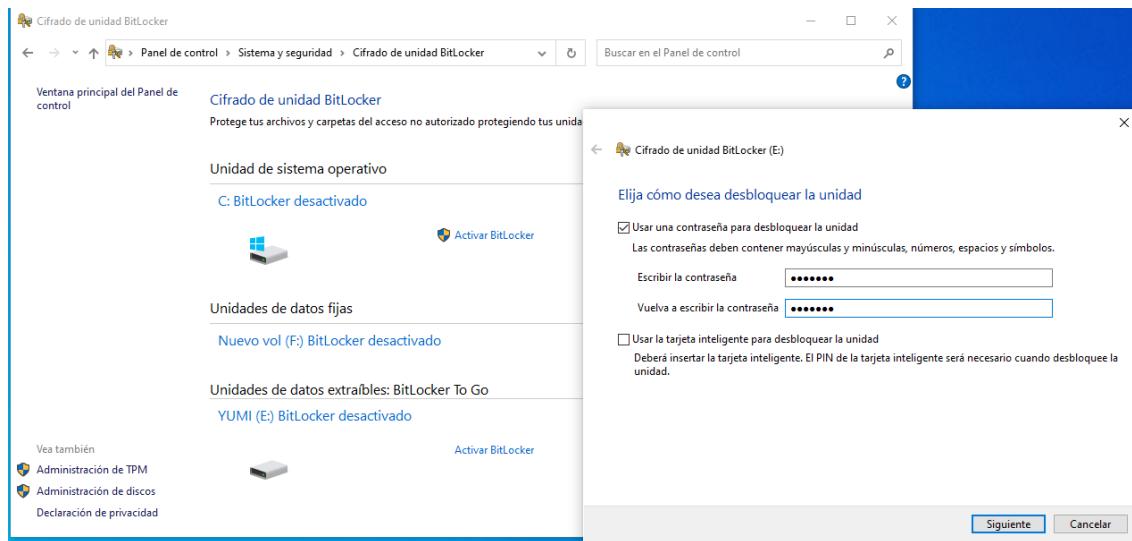
Abro la directiva “Requerir autenticación adicional al iniciar”

Selecciono “Habilitada”. Automáticamente se me selecciona también “Permitir BitLocker sin un TPM compatible”.

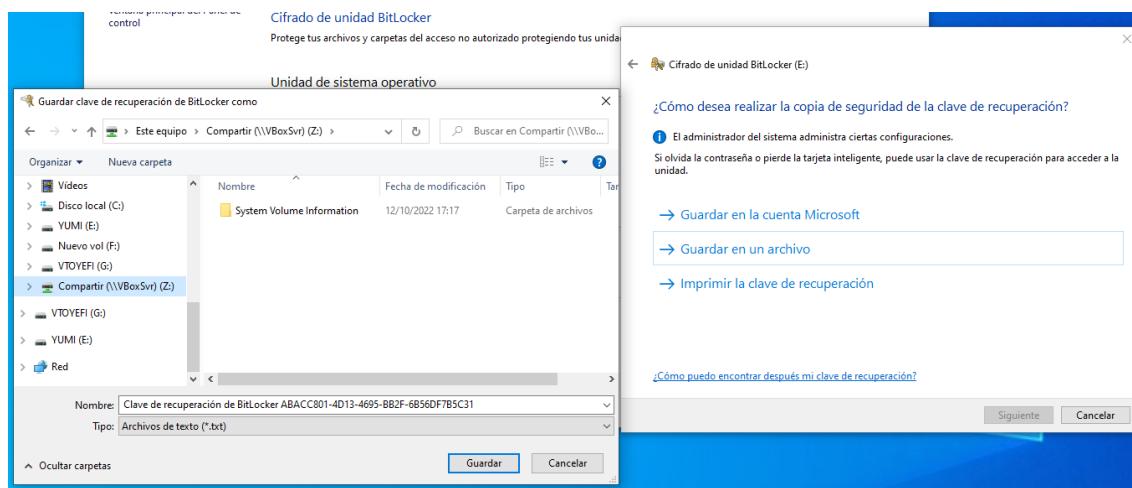


Ahora ya puedo darle a “Activar BitLocker” en el pendrive que voy a cifrar.

Escribo la contraseña elegida dos veces.

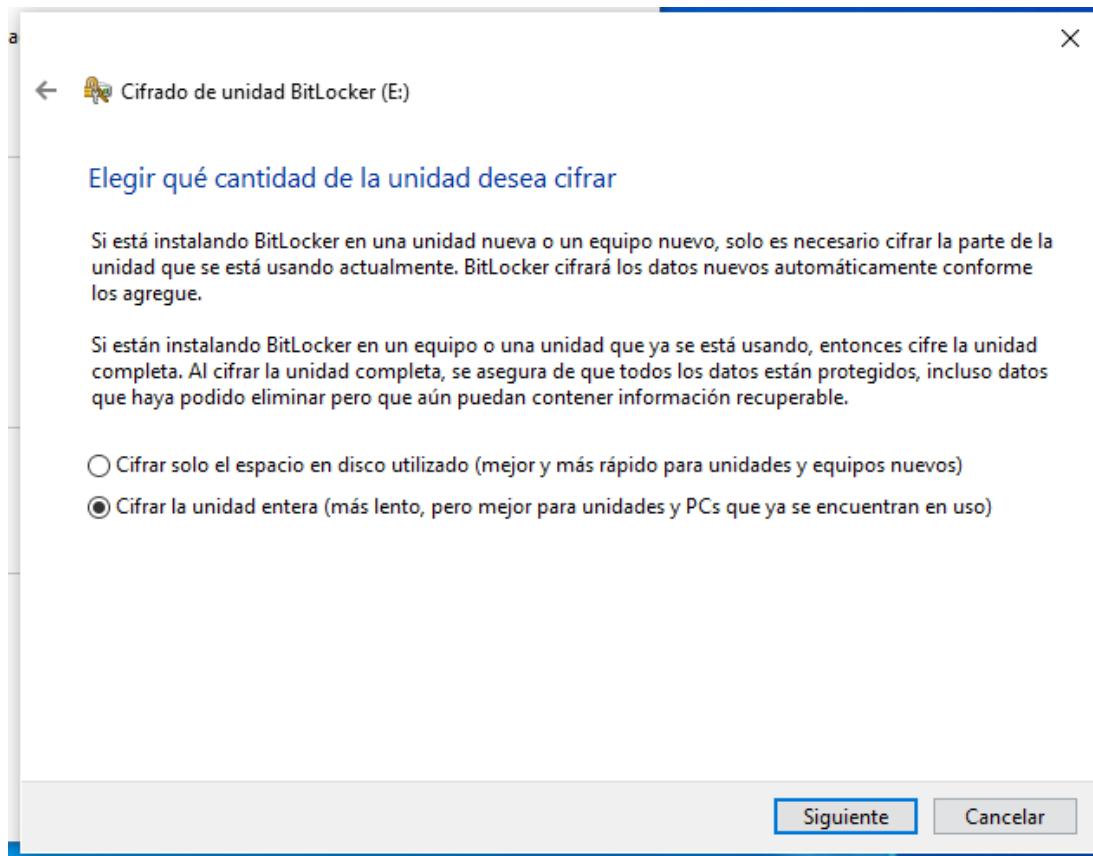


Elijo guardar la copia de seguridad de la clave de recuperación en un archivo, y selecciono lo guardo.

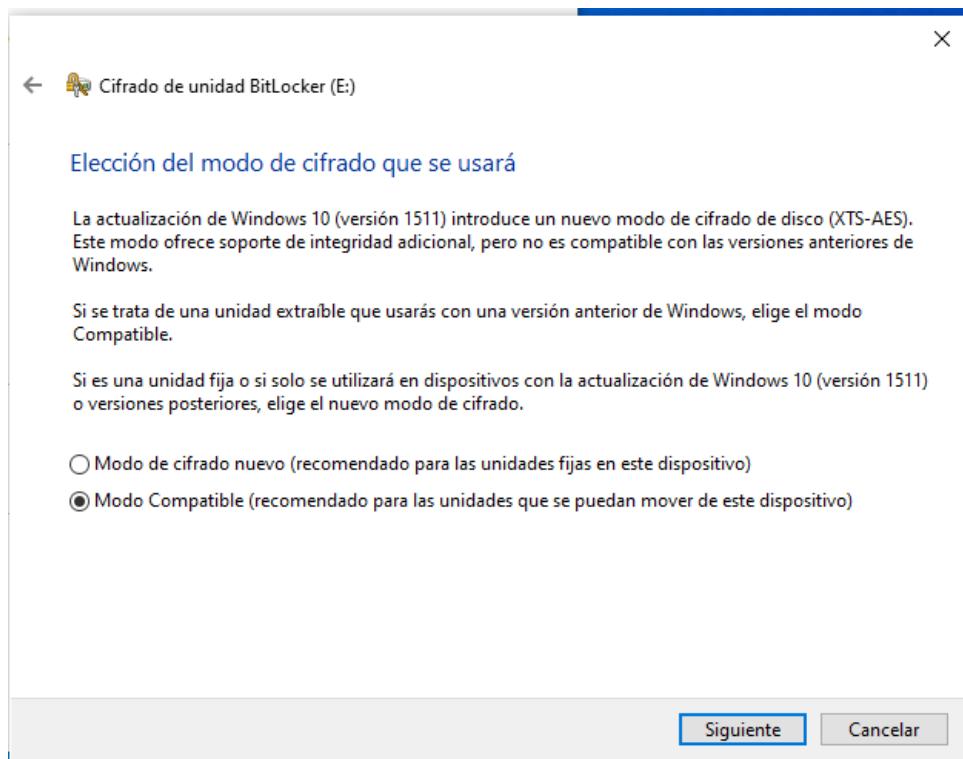


A continuación, pregunta si queremos cifrar solo el espacio utilizado, o la unidad entera.

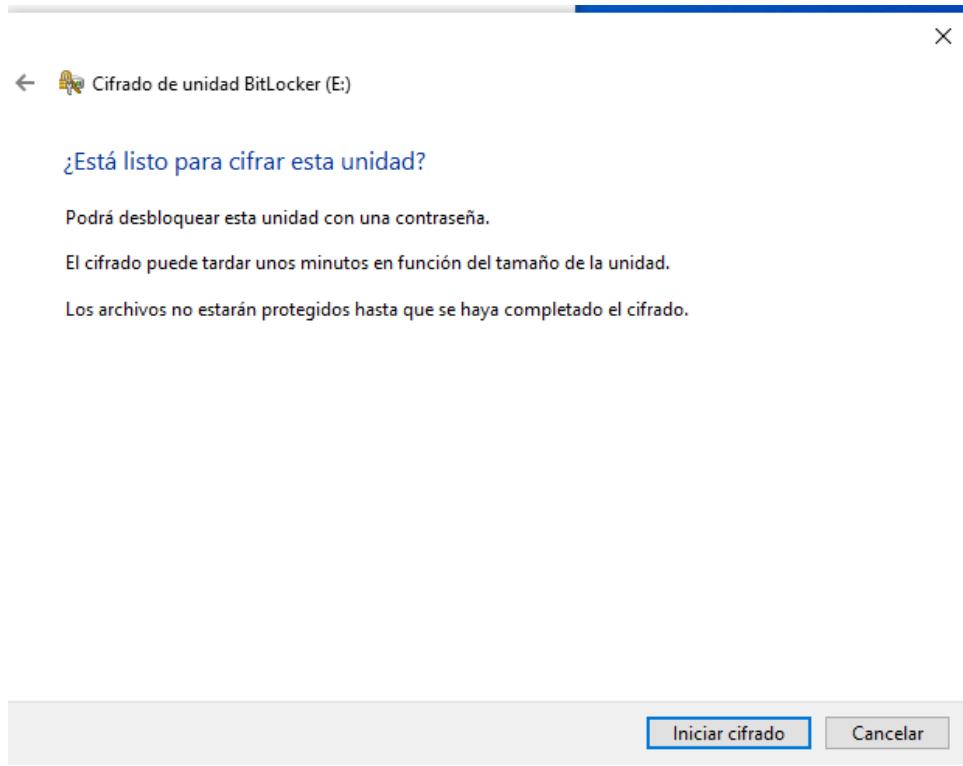
Selecciono la unidad entera, ya que quiero cifrar el pendrive entero.



En el siguiente paso te da a elegir el modo de cifrado, dependiendo de si es para una unidad fija o móvil. Como en mi caso es un pendrive, le doy a la segunda opción.



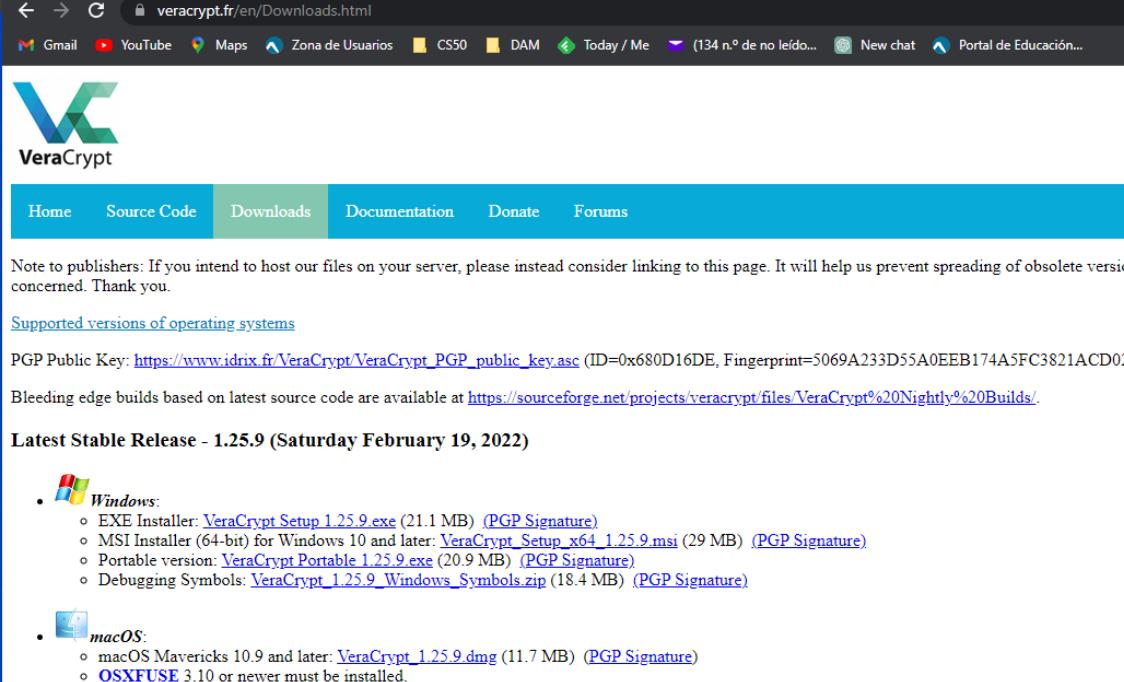
Y por último Iniciar cifrado.



Ejercicio 6. VeraCrypt

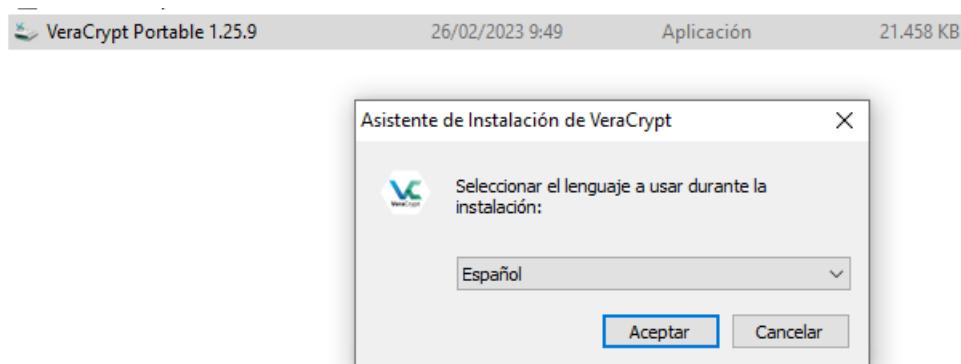
Crea un archivo contenedor de 200MB en un pendrive tal como se realiza en el libro capítulo 7.3

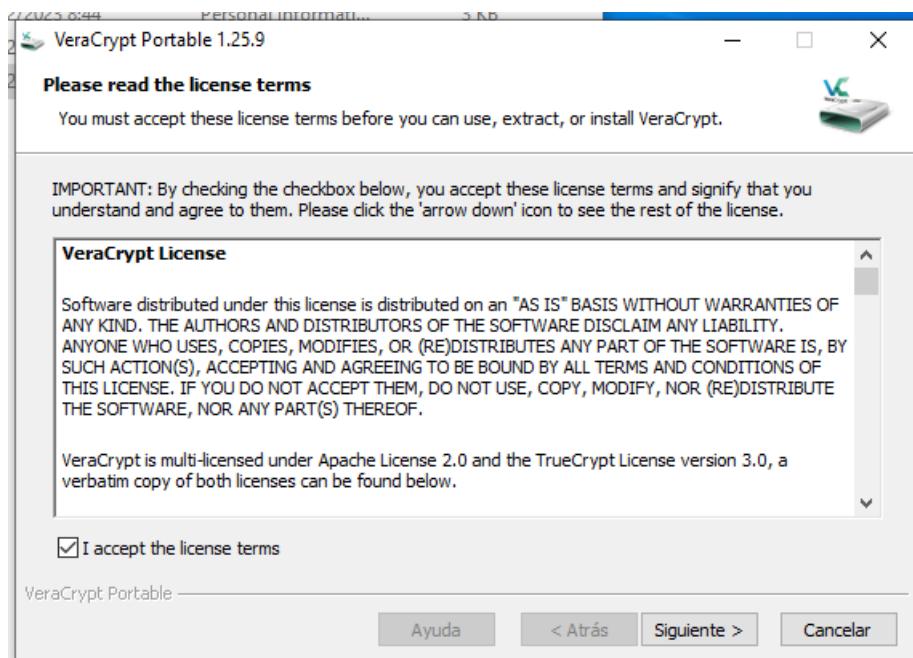
Me descargo la versión portable de VeraCrypt.



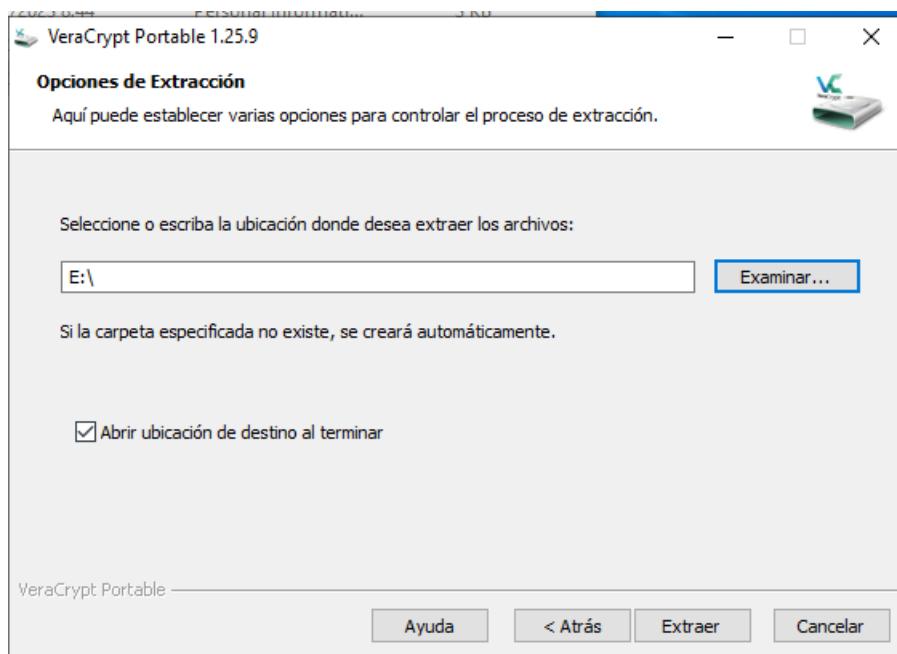
The screenshot shows a web browser window with the URL veracrypt.fr/en/Downloads.html. The page header includes the VeraCrypt logo and navigation links for Home, Source Code, Downloads, Documentation, Donate, and Forums. A note to publishers about linking to the page is present. Below it, sections for Supported versions of operating systems, PGP Public Key, and Bleeding edge builds are shown. The Latest Stable Release section highlights version 1.25.9 from February 19, 2022. It provides download links for Windows (EXE, MSI, Portable, Symbols) and macOS (DMG, OSXFUSE). The Windows section also notes that OSXFUSE 3.10 or newer must be installed for macOS users.

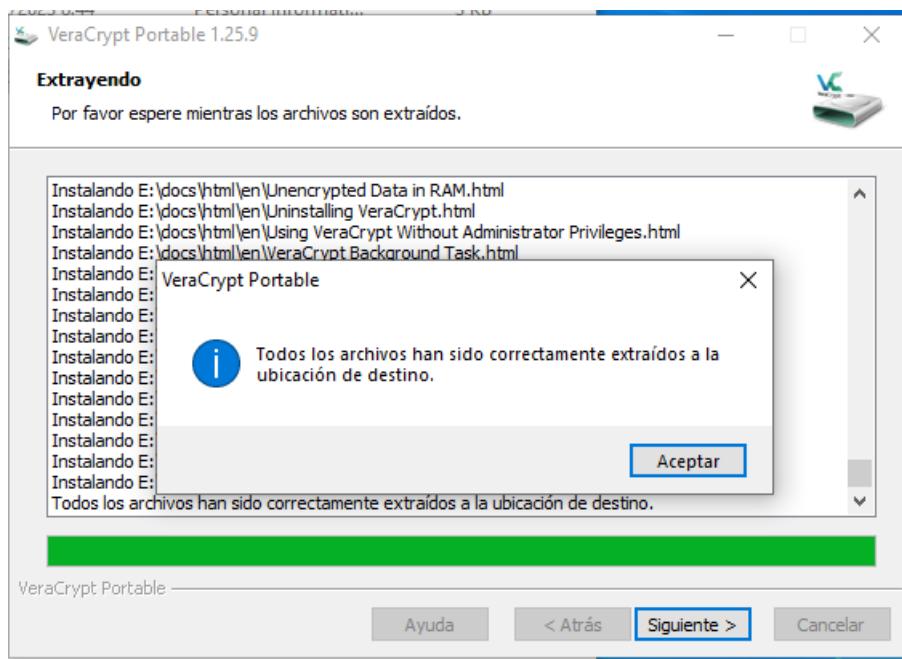
Ejecuto el archivo descargado.



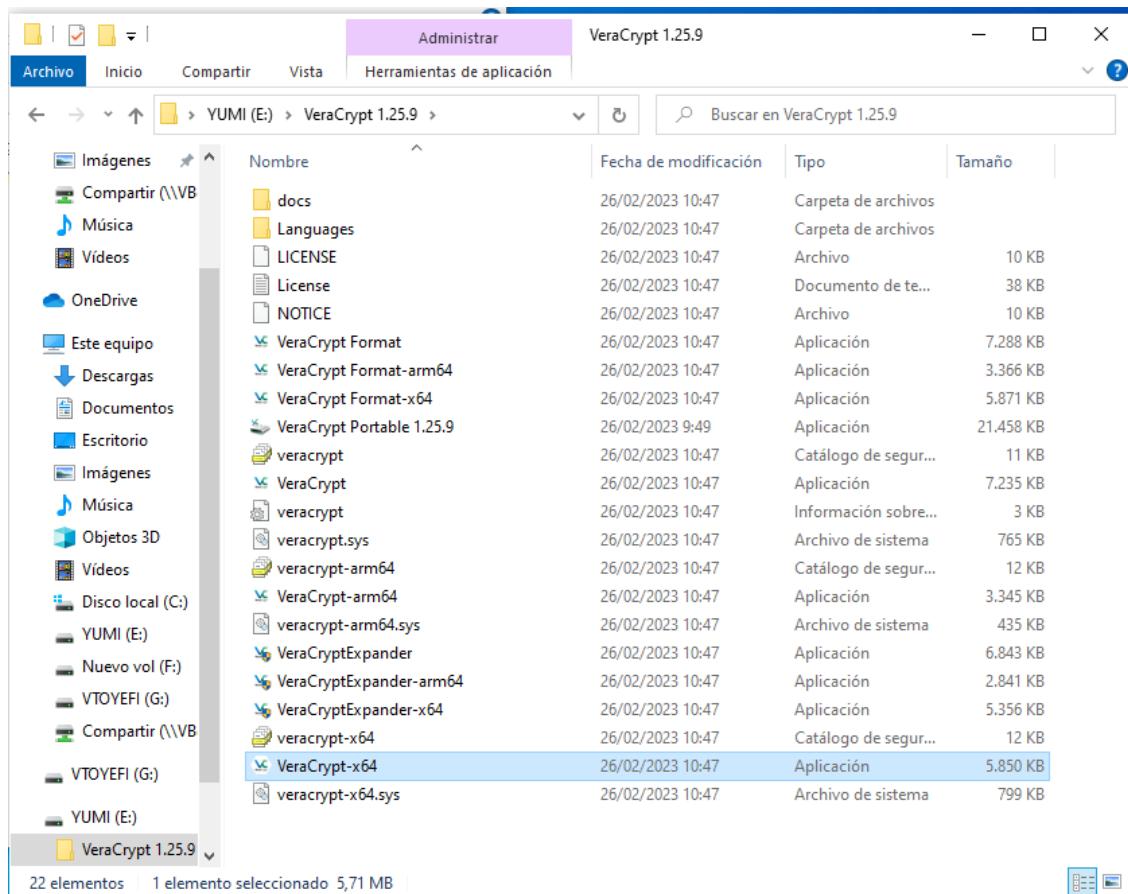


Elijo el pendrive para extraer los archivos de la instalación.

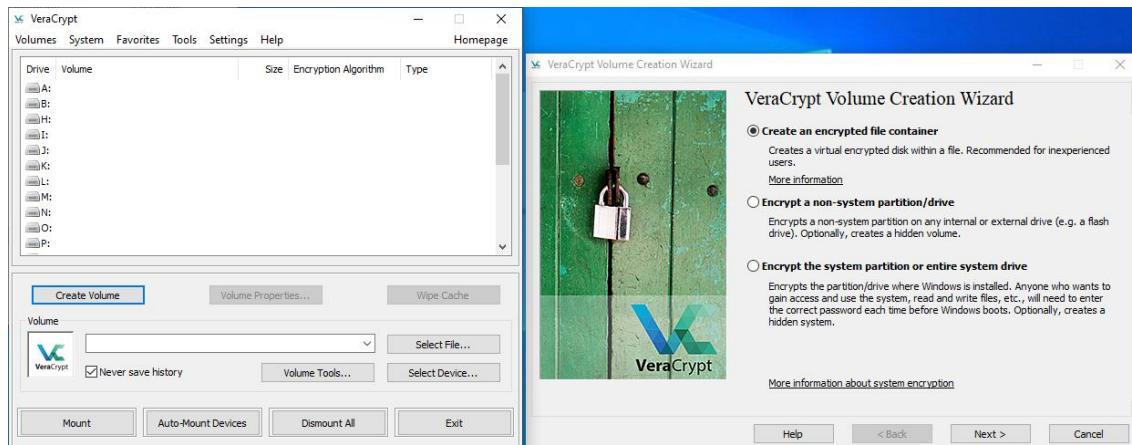




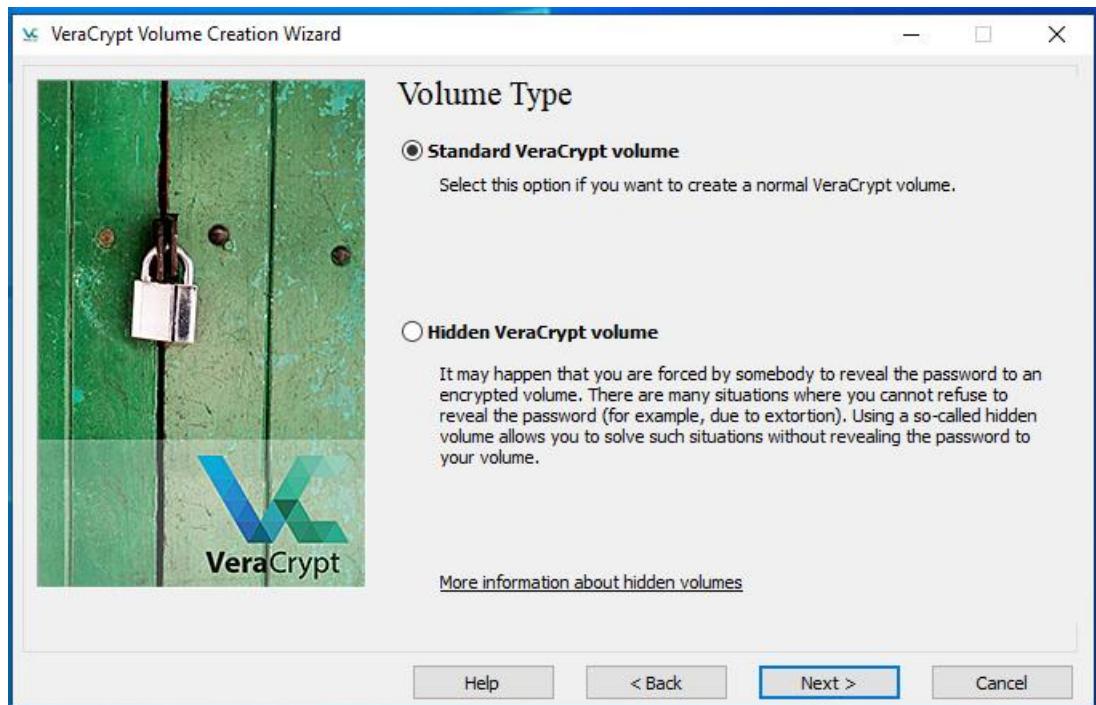
Una vez extraídos los archivos, ejecuto VeraCrypt-x64.



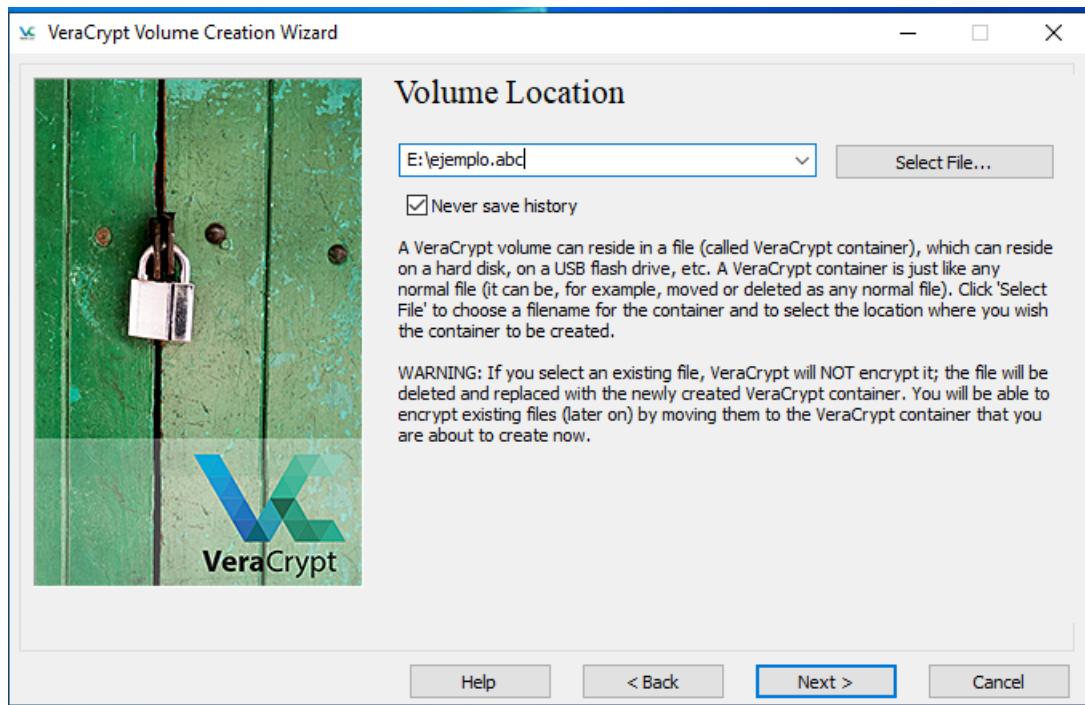
Se abre VeraCrypt. Le damos a Create Volume y nos aparece otra ventana con diferentes opciones. Seleccionamos la primera opción porque lo que queremos es crear un fichero contenedor.



A continuación, nos quedamos con la opción de “Volumen estándar”



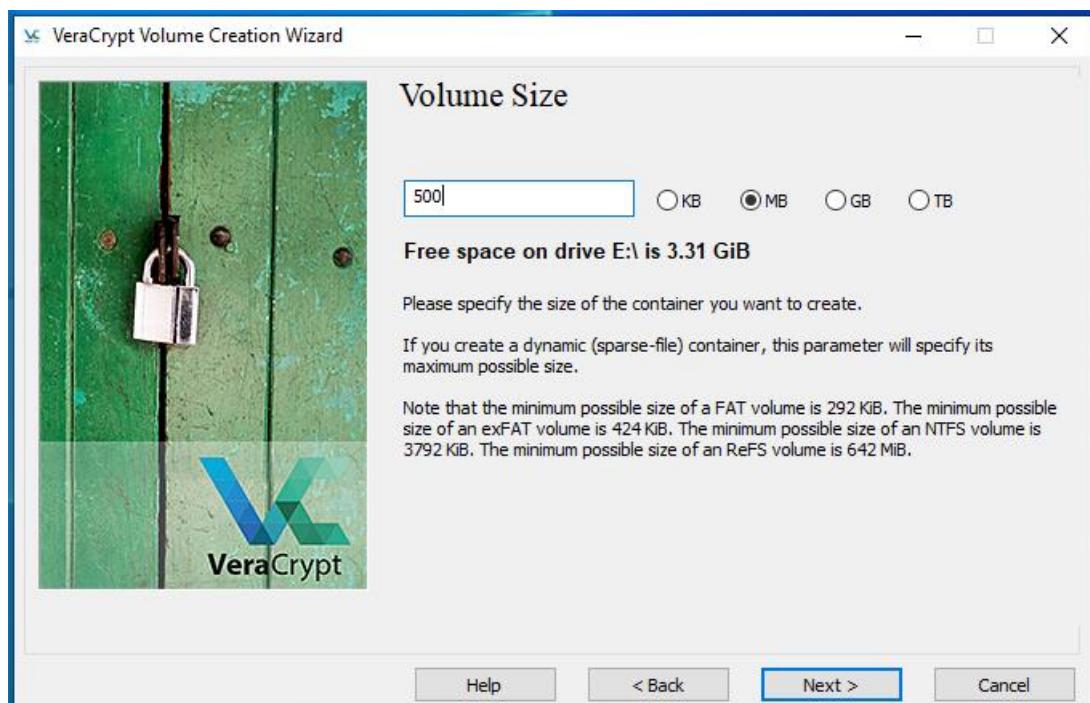
Creo un fichero que va a ser el contendor. "ejemplo.abc" he elegido.



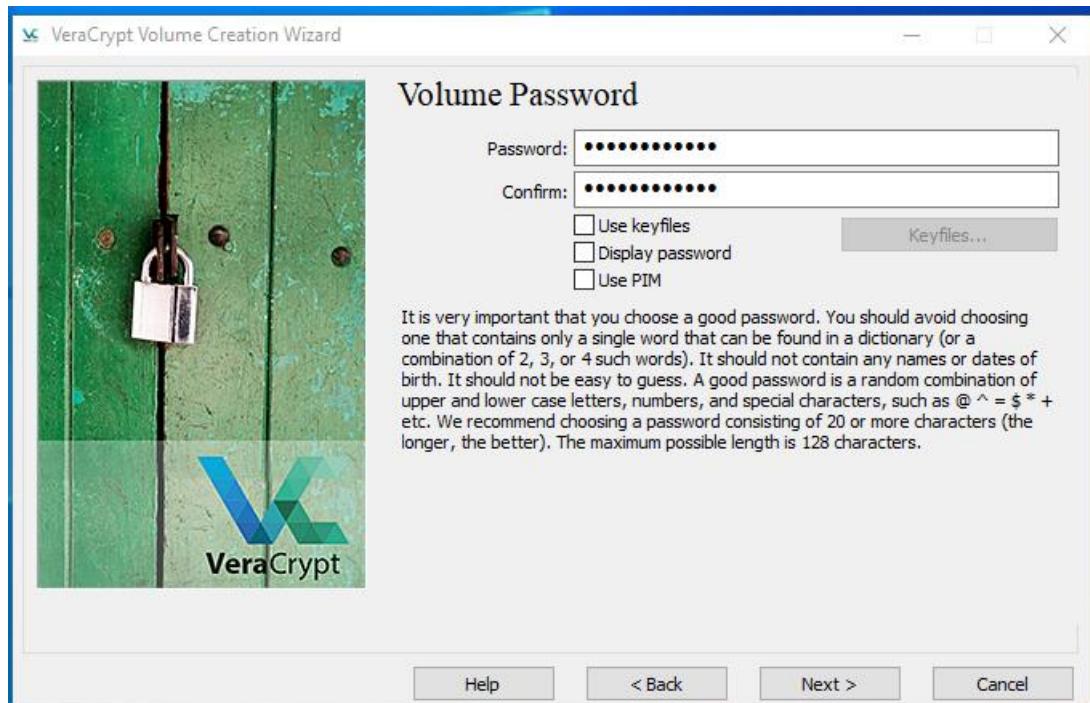
En la siguiente ventana, dejo las opciones que vienen por defecto.



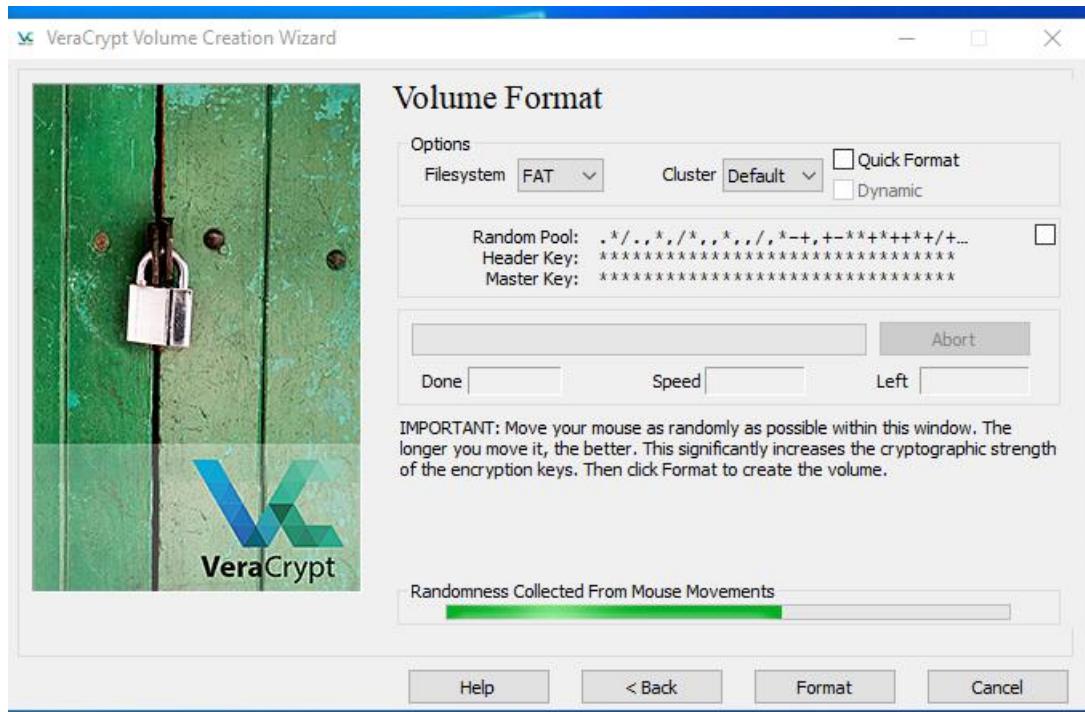
Escribo el tamaño que va a tener el fichero contenedor.



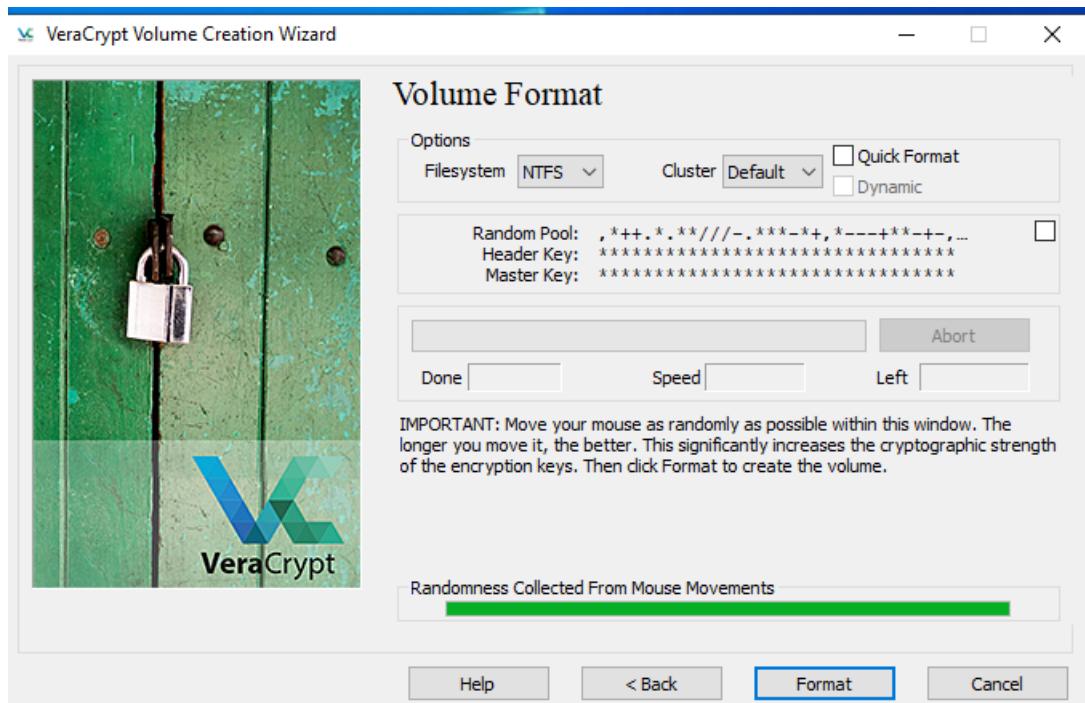
Hay que elegir una contraseña que cumpla con las condiciones que te indica. Te aconseja utilizar una contraseña de 20 o más caracteres



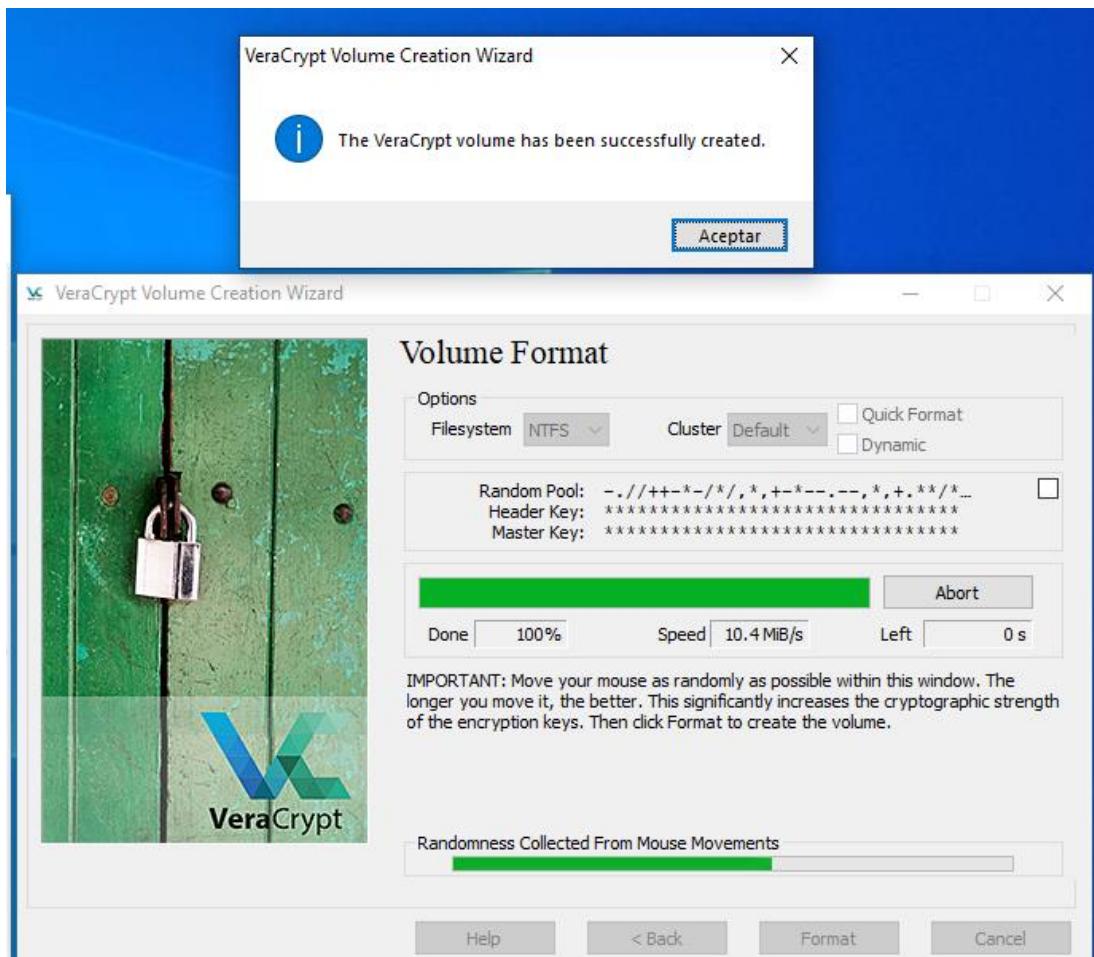
En la siguiente ventana hay que mover el ratón por la pantalla hasta que se ponga en verde la barra Randomness.



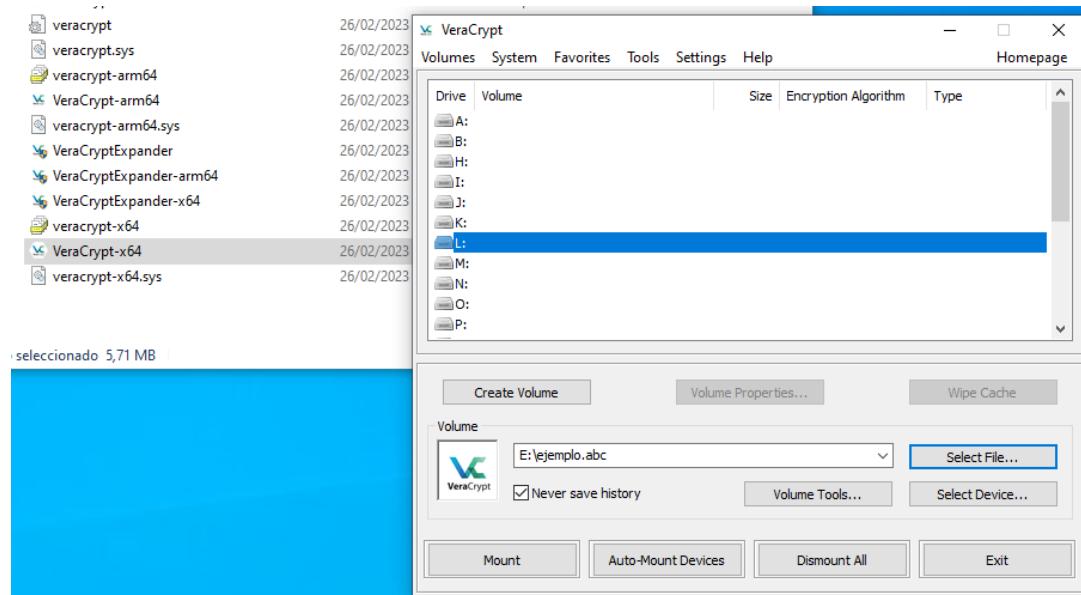
Elijo el formato NTFS (Ubuntu lee y escribe particiones NTFS). Y pulso "Format"



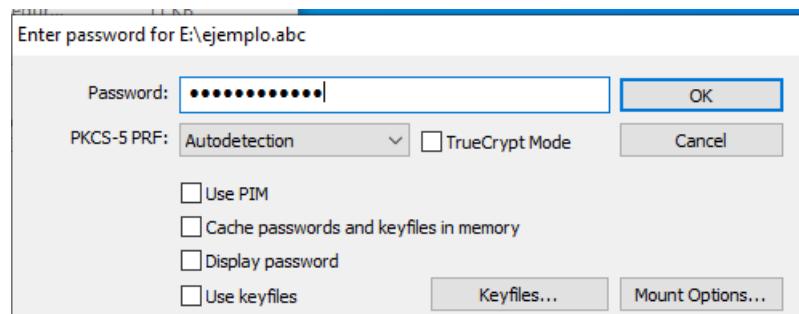
Esperamos hasta que se complete el proceso.



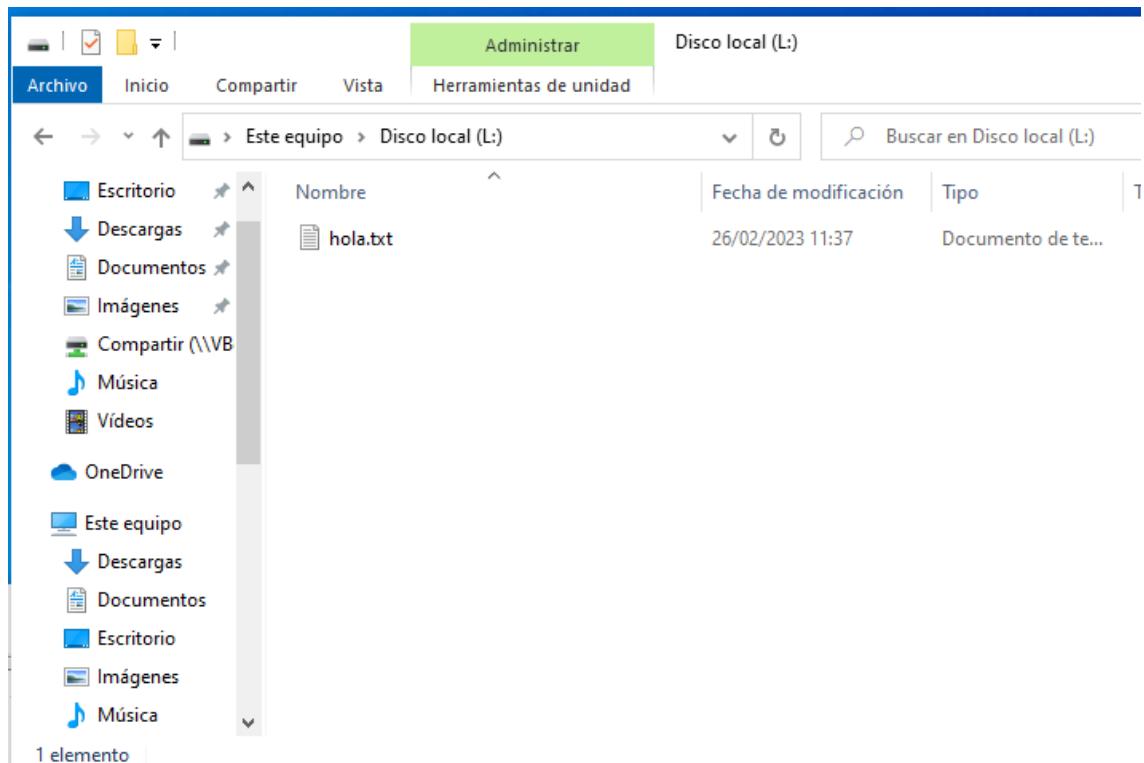
Para acceder al fichero contenedor. Volvemos a ejecutar “VeraCrypt-x64” pero esta vez en vez de “Create Volume”, selecciono una unidad, en este caso “L:” y selecciono el fichero creado “ejemplo.abc”. A continuación pulso en “Mount”.



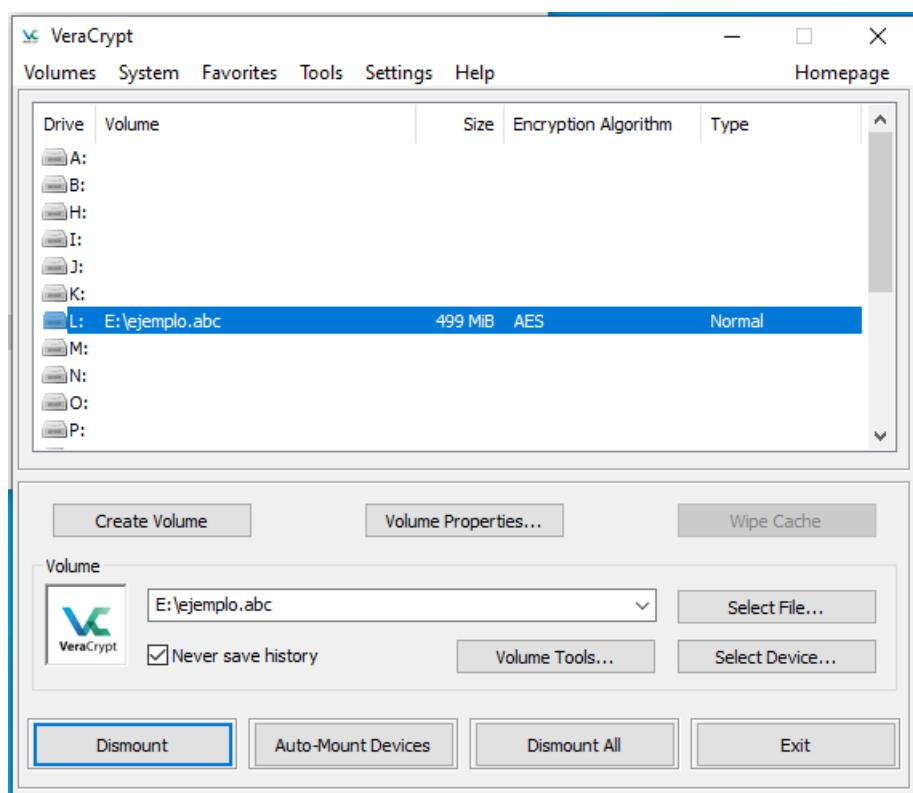
Me pide la contraseña, luego pulso OK.



Y nos aparece una unidad L donde puedo crear o copiar ficheros.



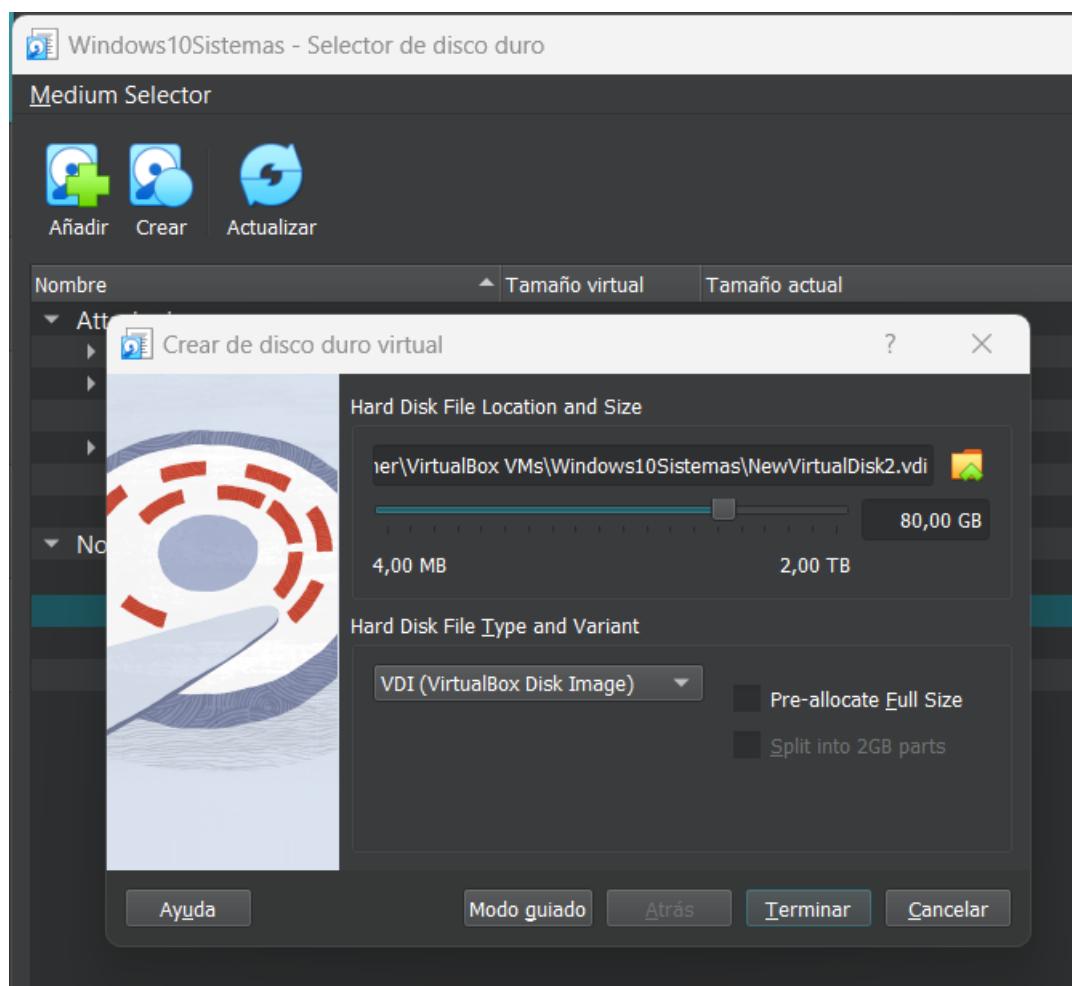
Una vez haya terminado. Pulso “Dismount”.

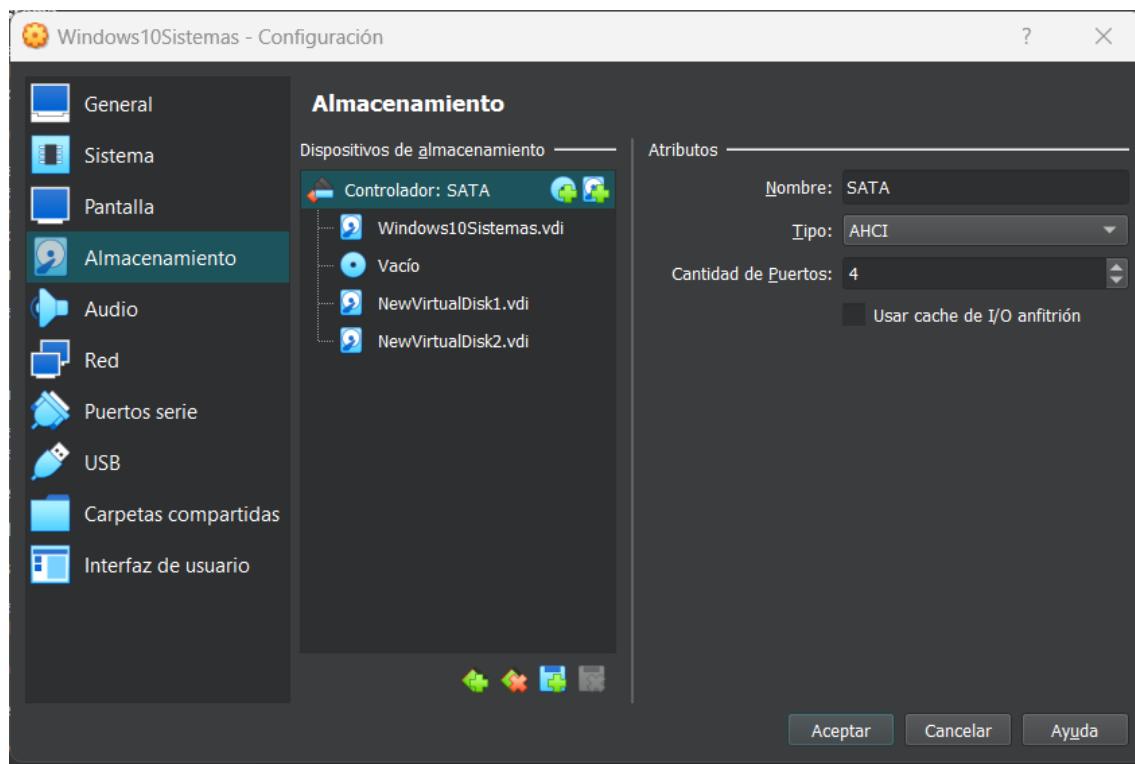


Ejercicio 7. RAID por software en Windows

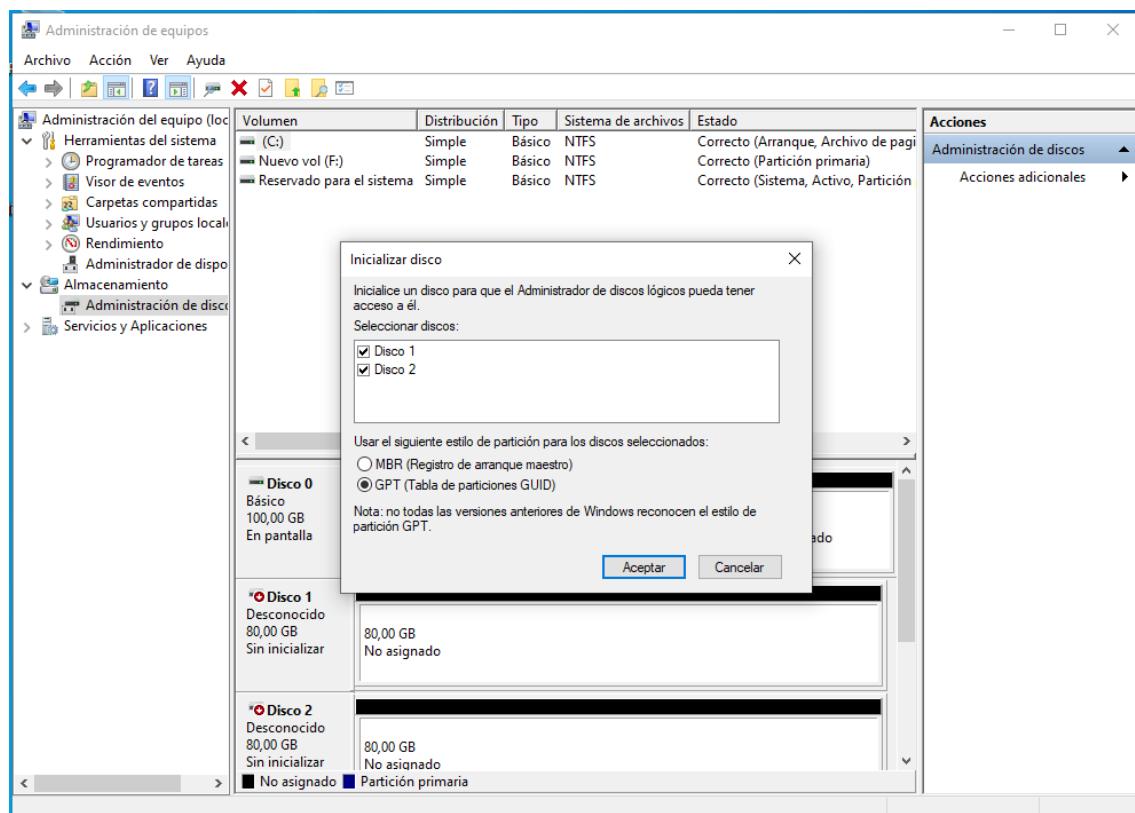
Incorpora 2 discos de 80 GB a la máquina Windows 10 Sistemas y crea un RAID 0 de 60 GB tal como se realiza en el capítulo 7.4

Creo 2 discos nuevos de 80 GB.

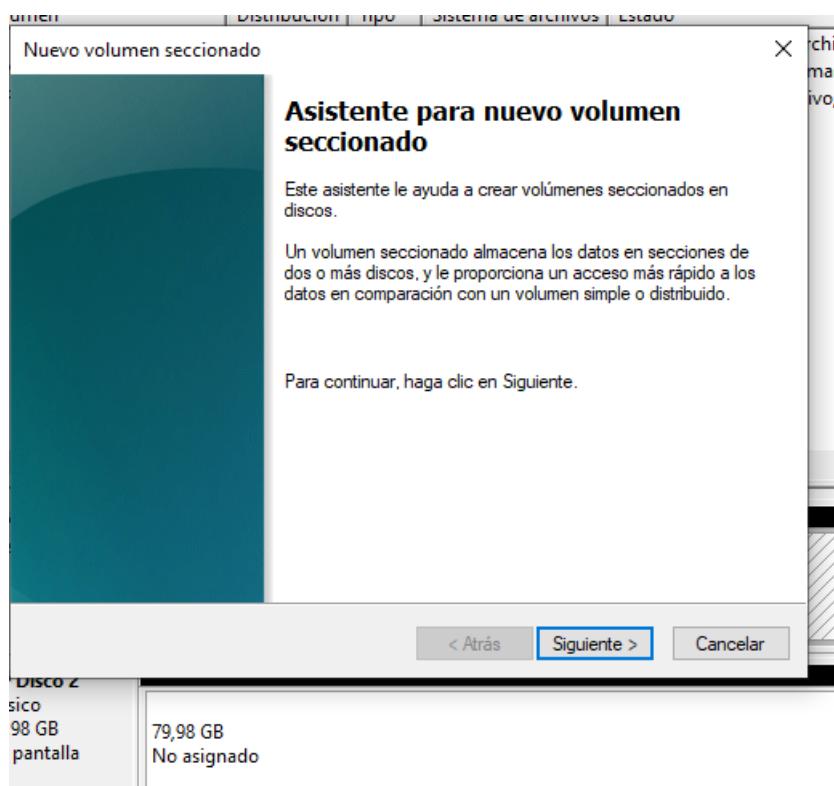
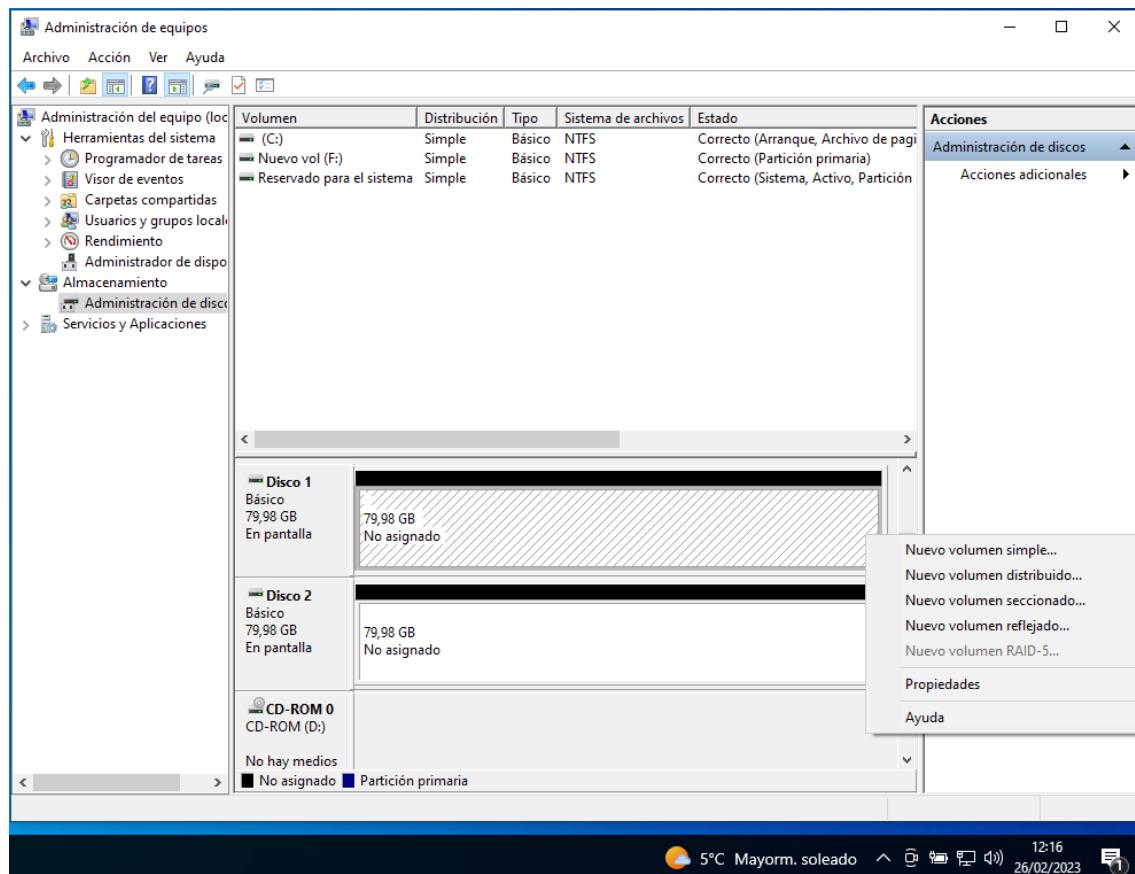




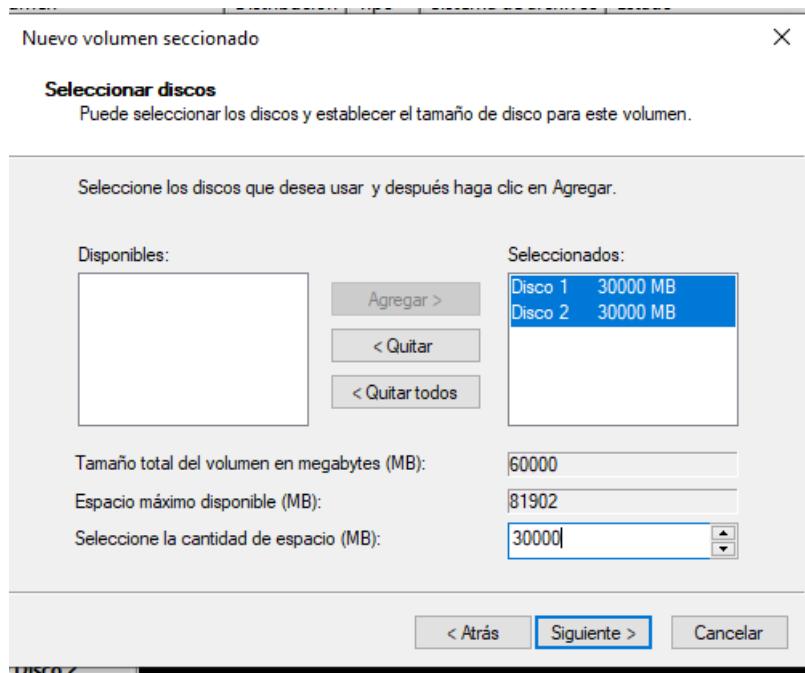
Inicio Windows y el Administrado de equipos. Para crear discos dinámicos, tenemos que seleccionar GPT.



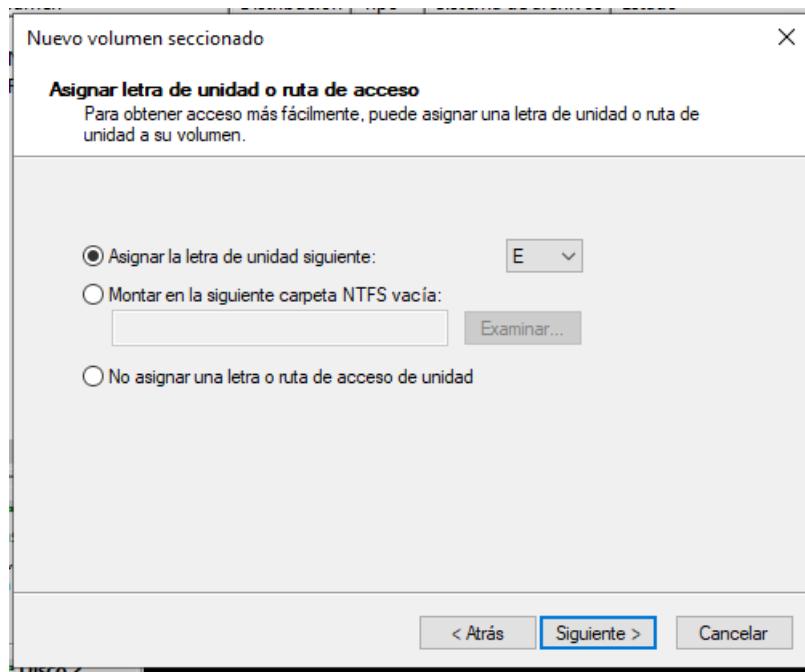
Pulsamos con el botón derecho sobre el Disco 1 y seleccionamos “Nuevo volumen seleccionado...” para crear un Raid 0.



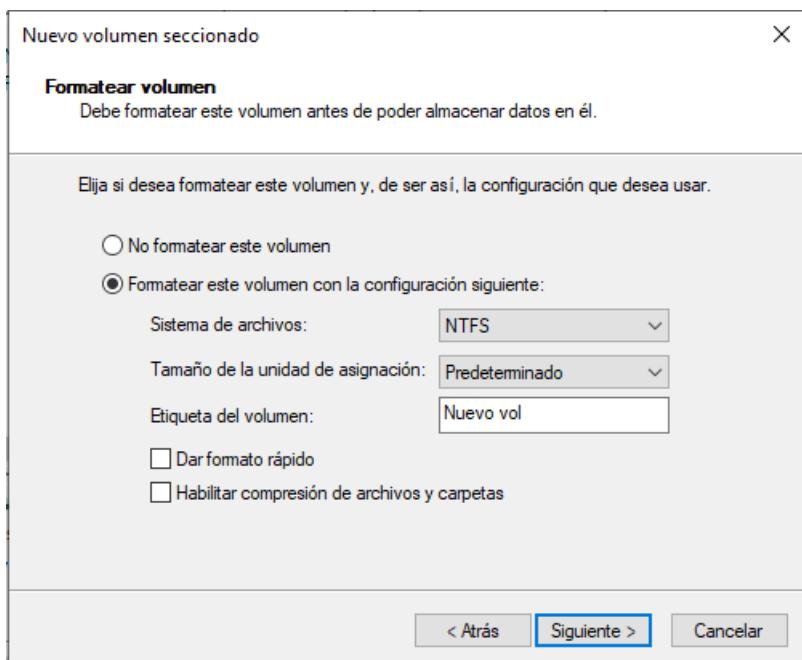
Hay que seleccionar los discos que vamos a utilizar. También hay que elegir el tamaño, queremos crear una RAID 0 de 60GB, por lo que utilizaremos 30GB de cada disco.



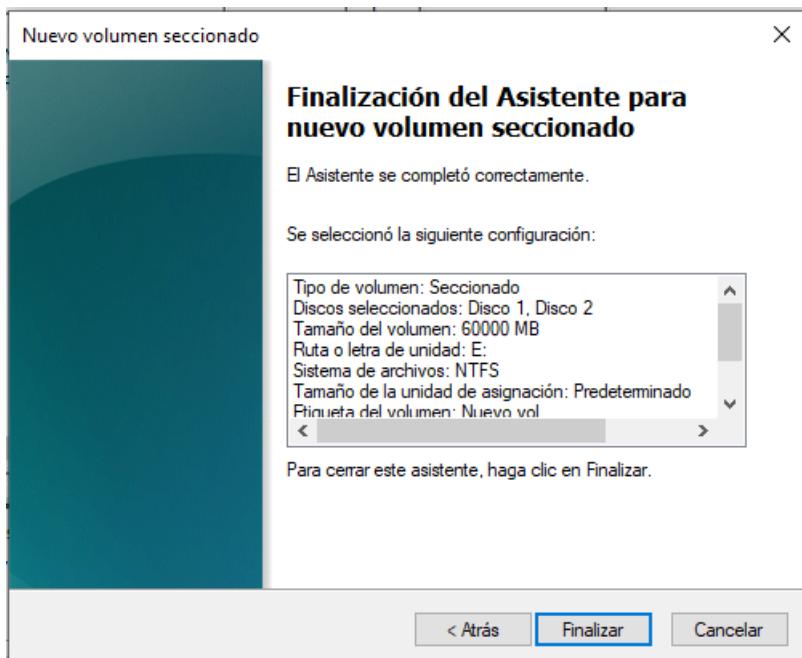
Asigno la letra de la unidad donde quiero crearlo.



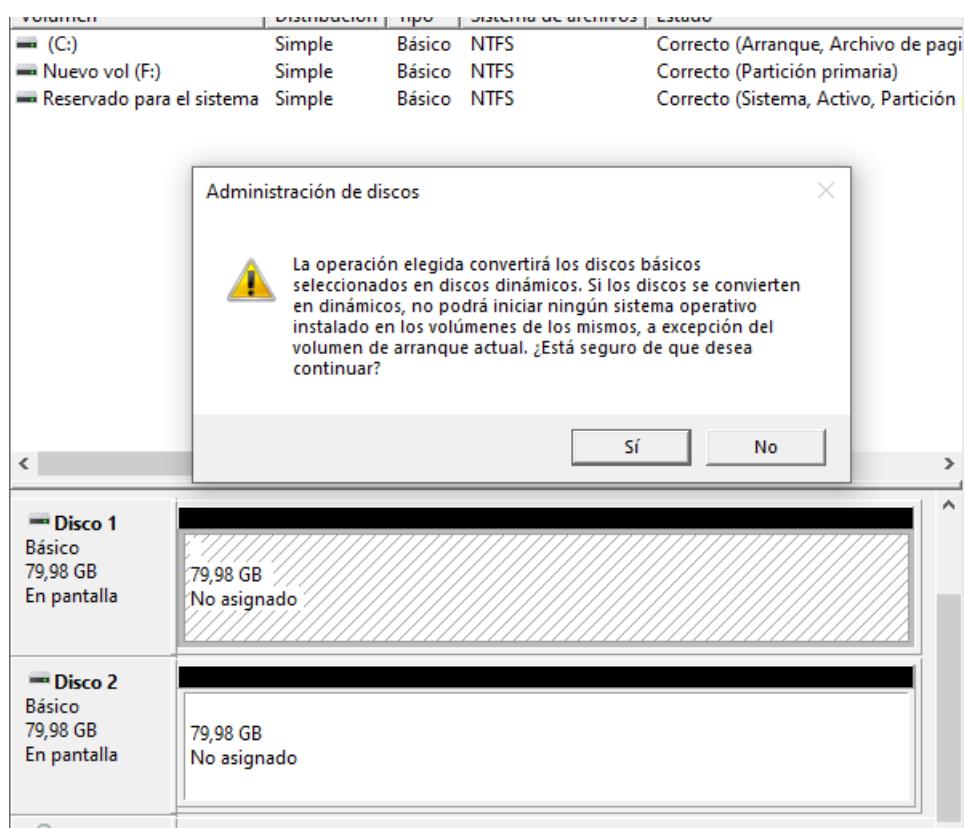
Le doy a siguiente.



Finalizamos.



Aparece una ventana de advertencia, ya que tiene que convertir los discos básicos en dinámicos.



Una vez convertidos los discos a dinámicos y creado el RAID 0, podemos comprobar que se ha creado el volumen E de 60GB.

