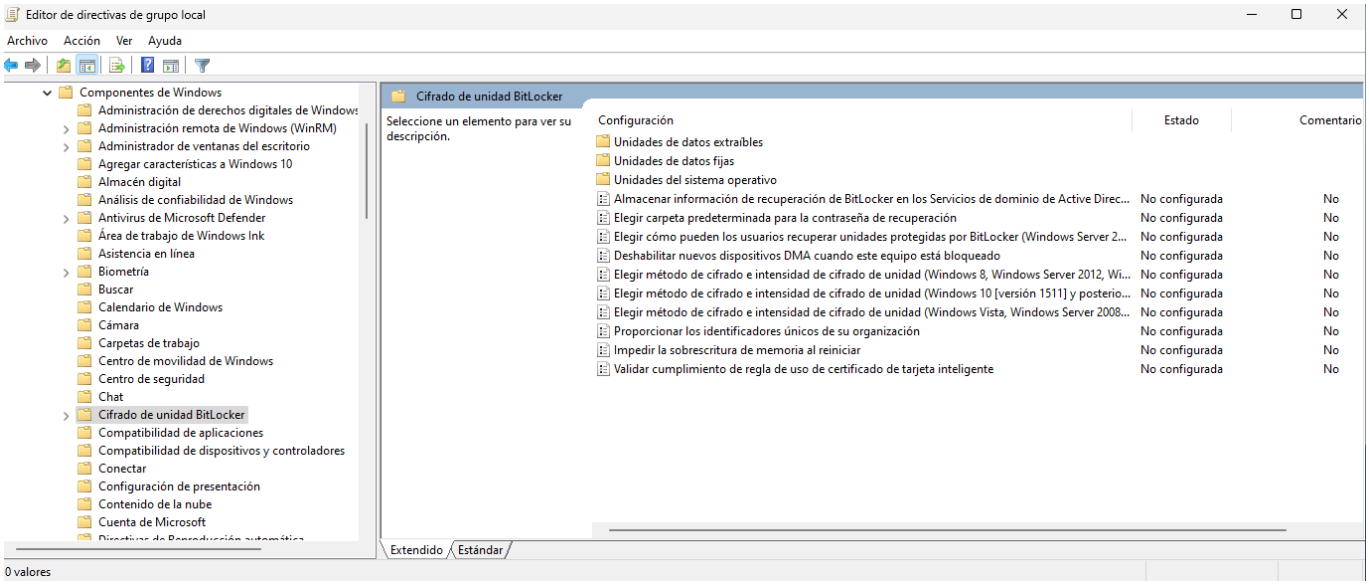
[FORT] Práctica 9: Fortificación de la información y auditoría de Windows 11

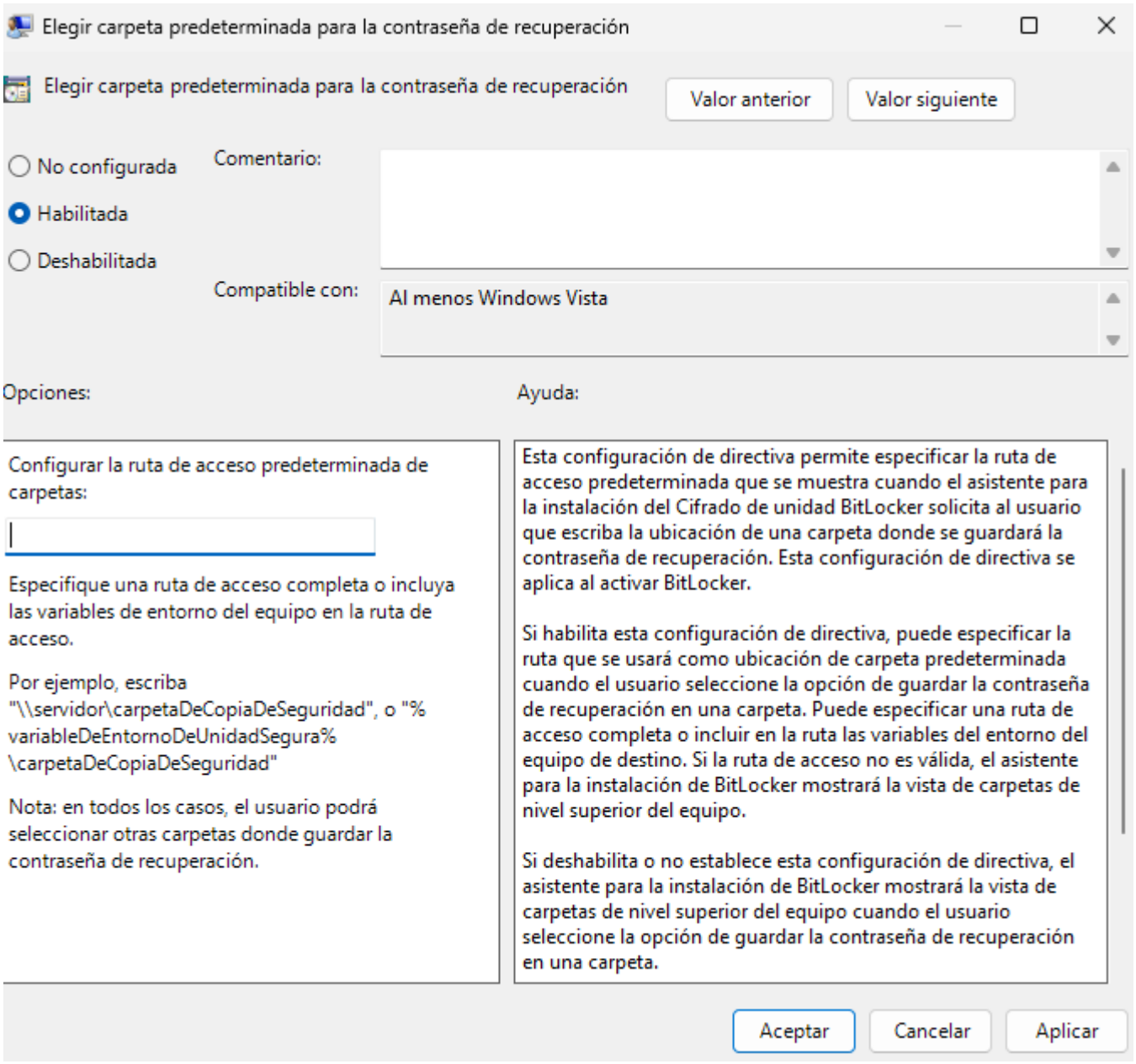
1. Cifrado de información con BitLocker

a) Revisa las políticas de seguridad de Bitlocker que se encuentran en la configuración del equipo:

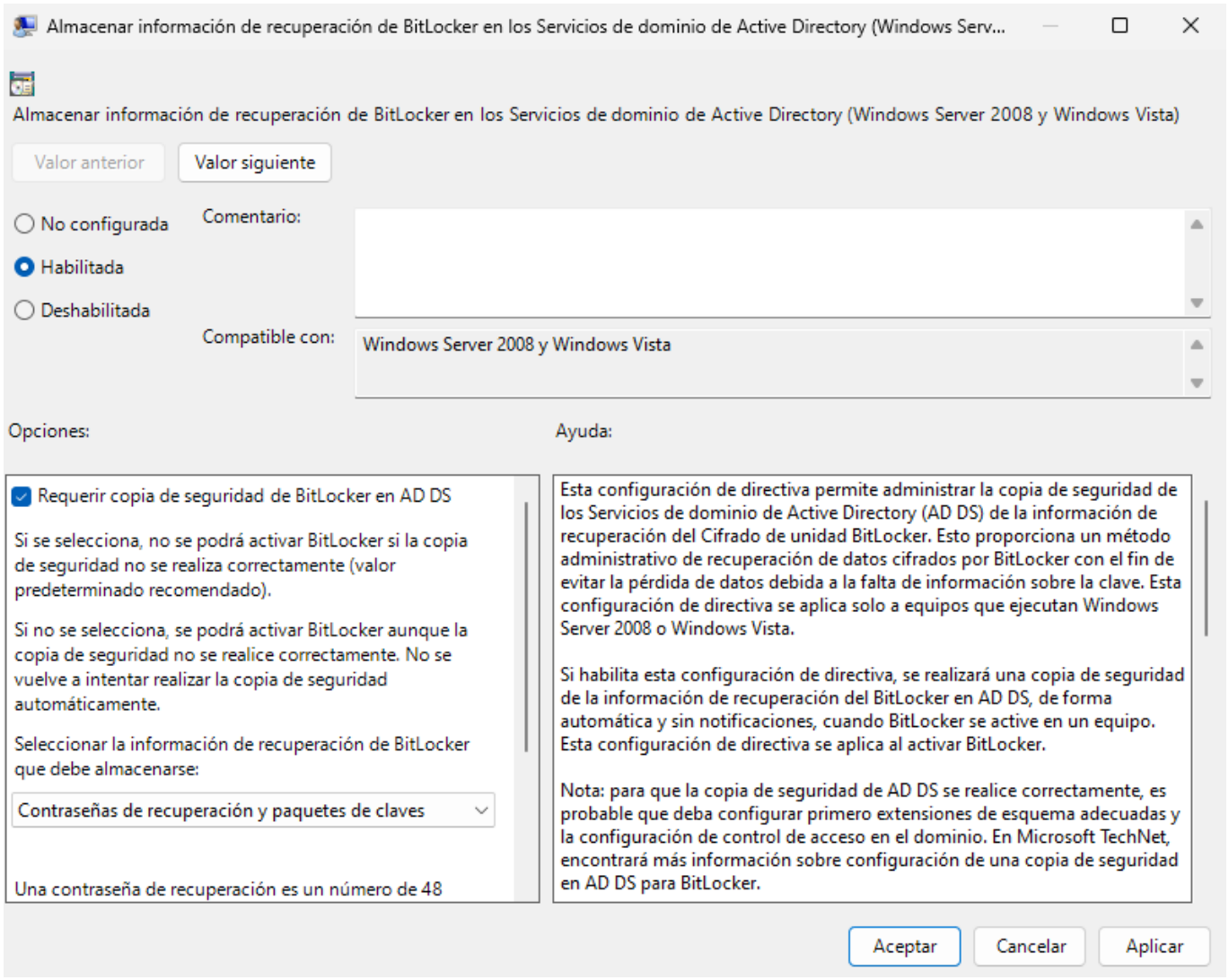


i. ¿Es necesario realizar algún ajuste para activarlo? ¿Es necesario realizar algún cambio para mejorar dicho cifrado?

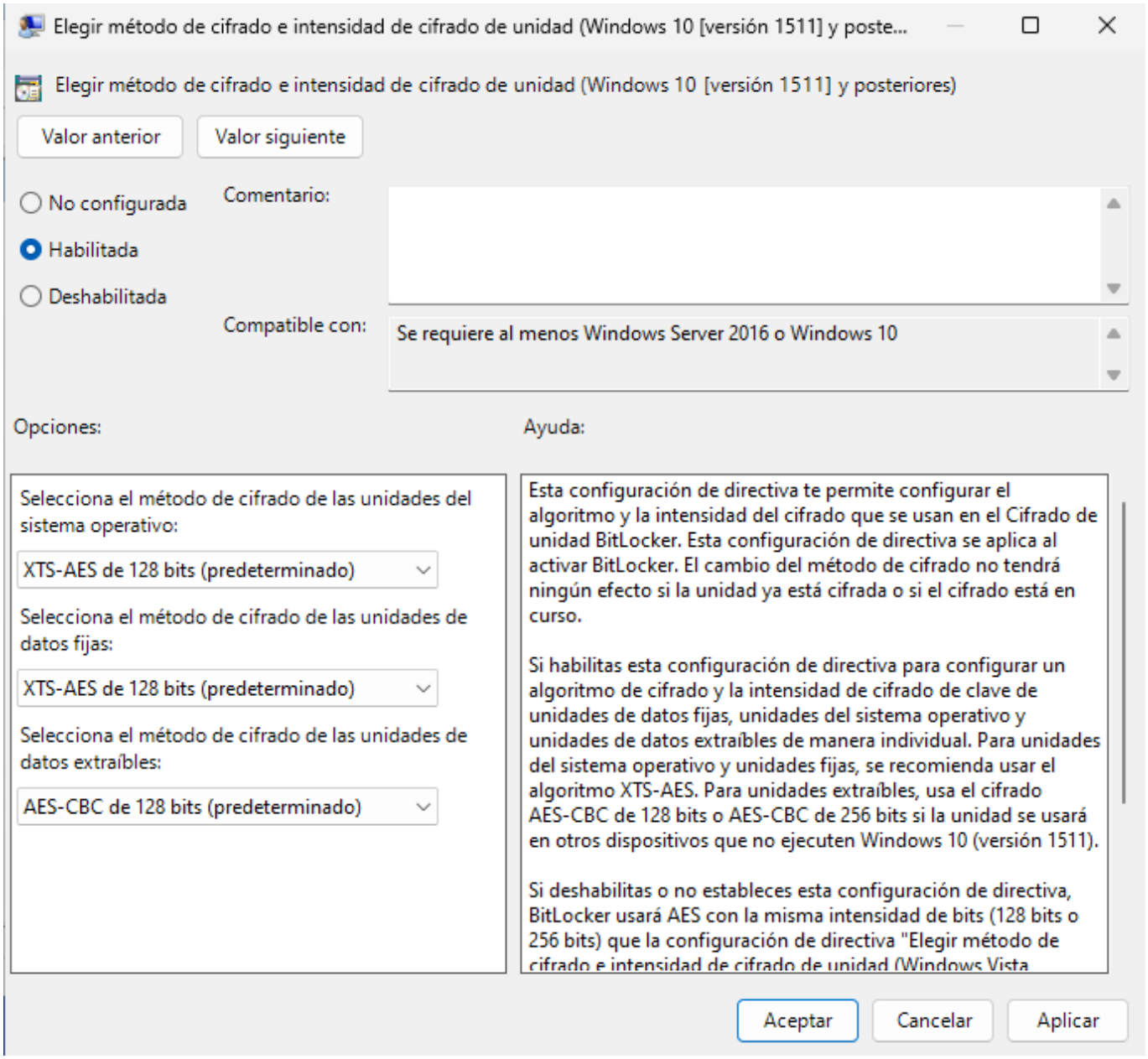
Para activar bitlocker mediante directivas de grupo local es necesario configurar donde está localizada la carpeta para la contraseña de recuperación



Si el equipo está en un dominio también se recomienda activar la opción “Almacenar información de Bitlocker en los Servicios de dominio de Active Directory” para almacenar la clave de recuperación en el servidor del dominio.



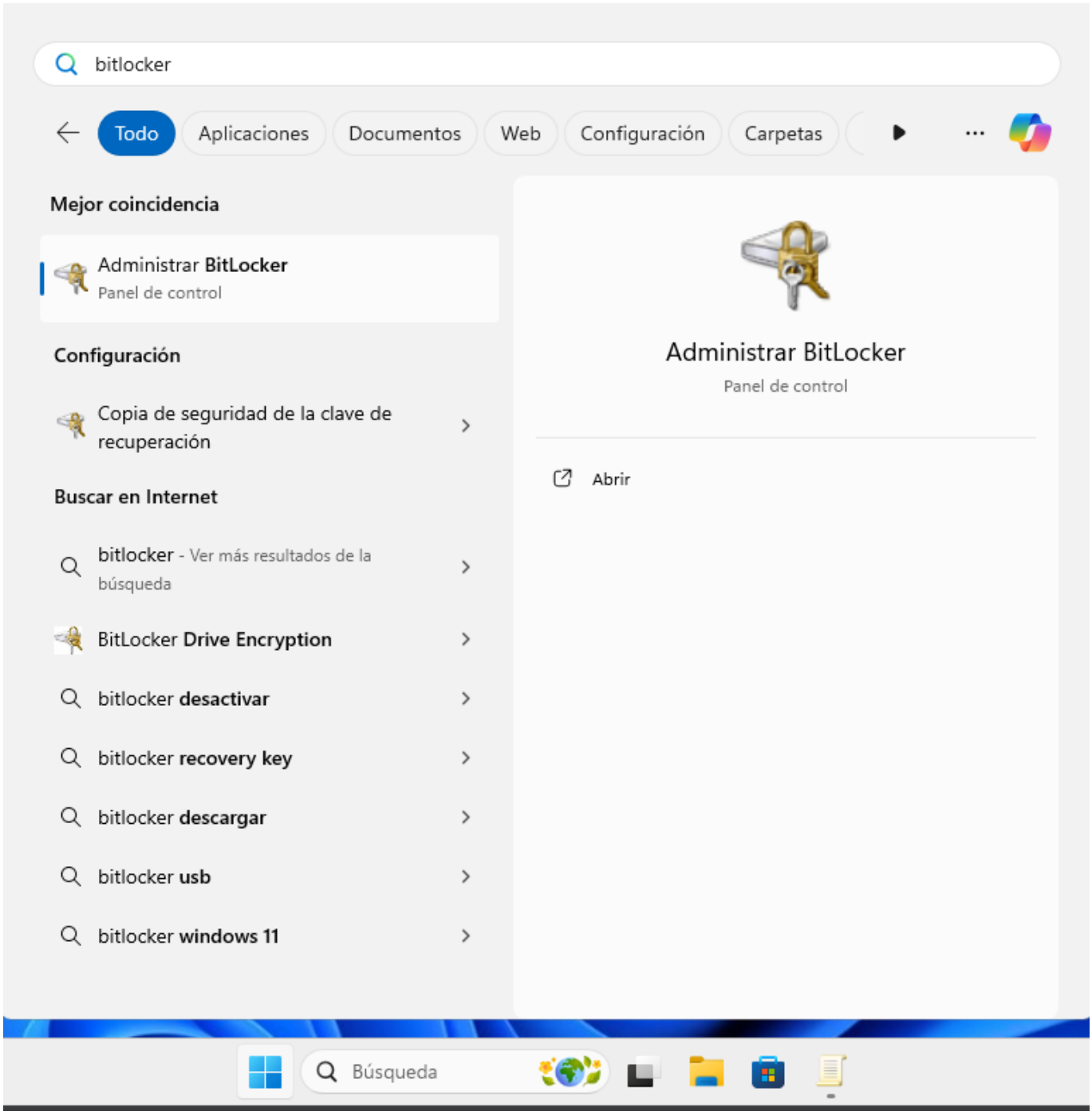
Para mejorar el cifrado podemos modificar la política de “Elegir método de cifrado e intensidad de cifrado de unidad” para sistemas de Windows 10 en adelante:



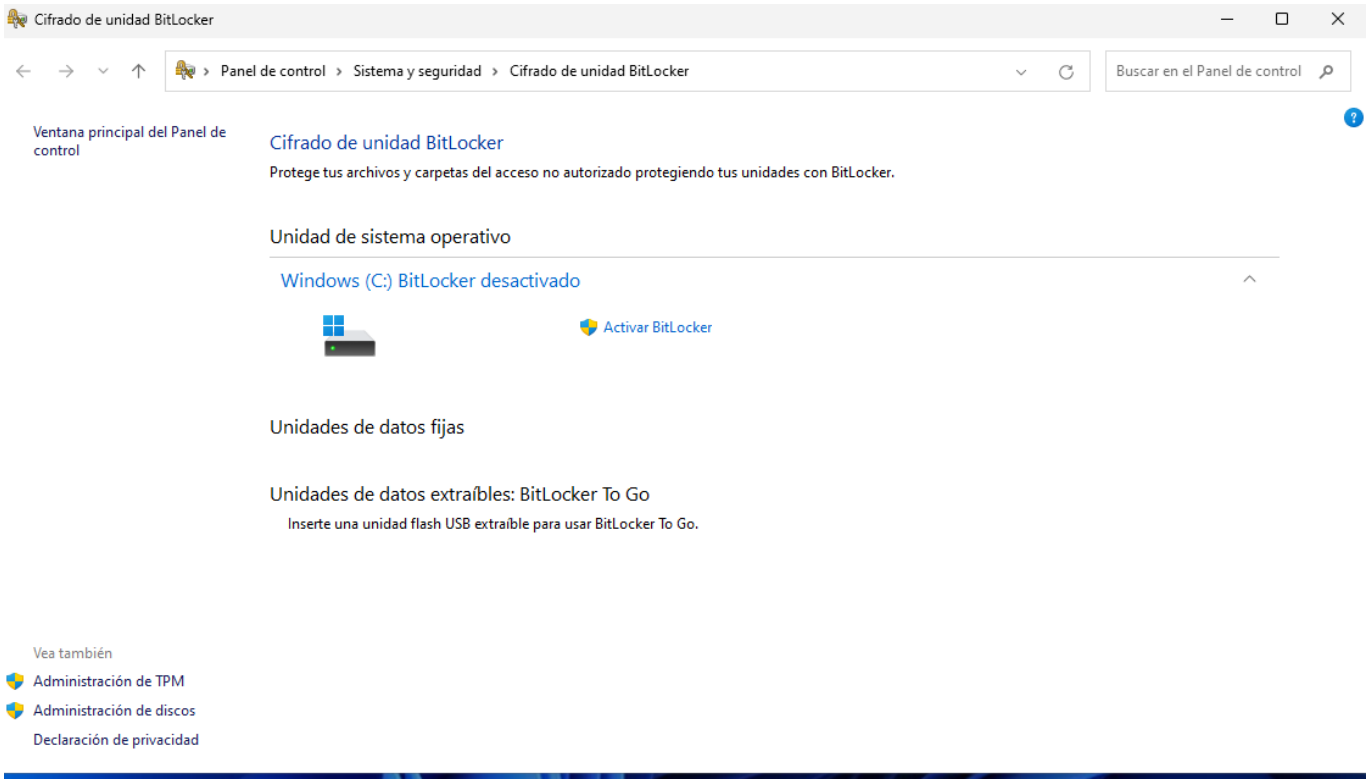
b) Realiza la activación de firado Bitlocker sobre C:\

i. Indica los pasos a seguir para realizar dicho cifrado

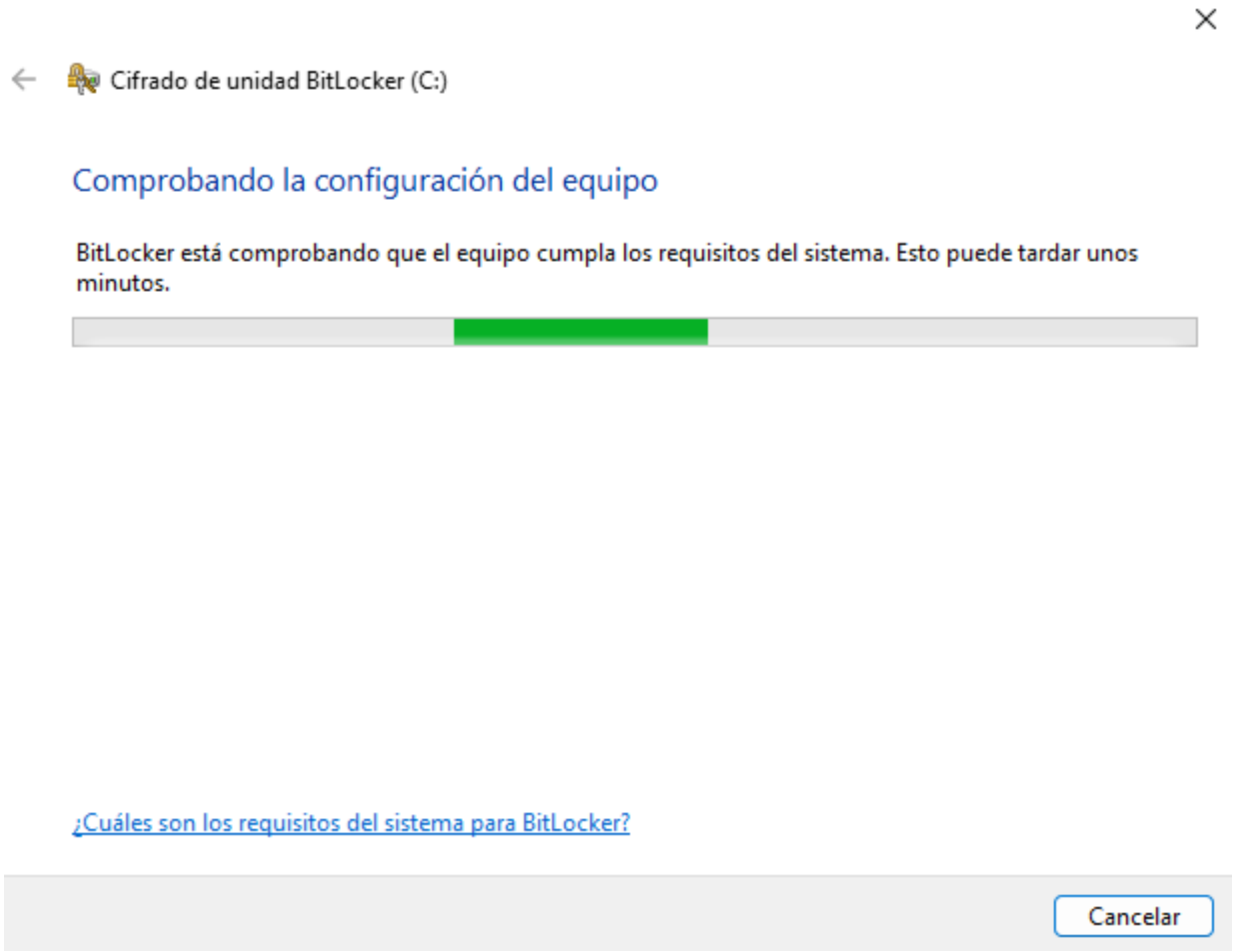
La forma más simple de realizar el cifrado del disco mediante bitlocker es pulsar el botón windows y buscar bitlocker:



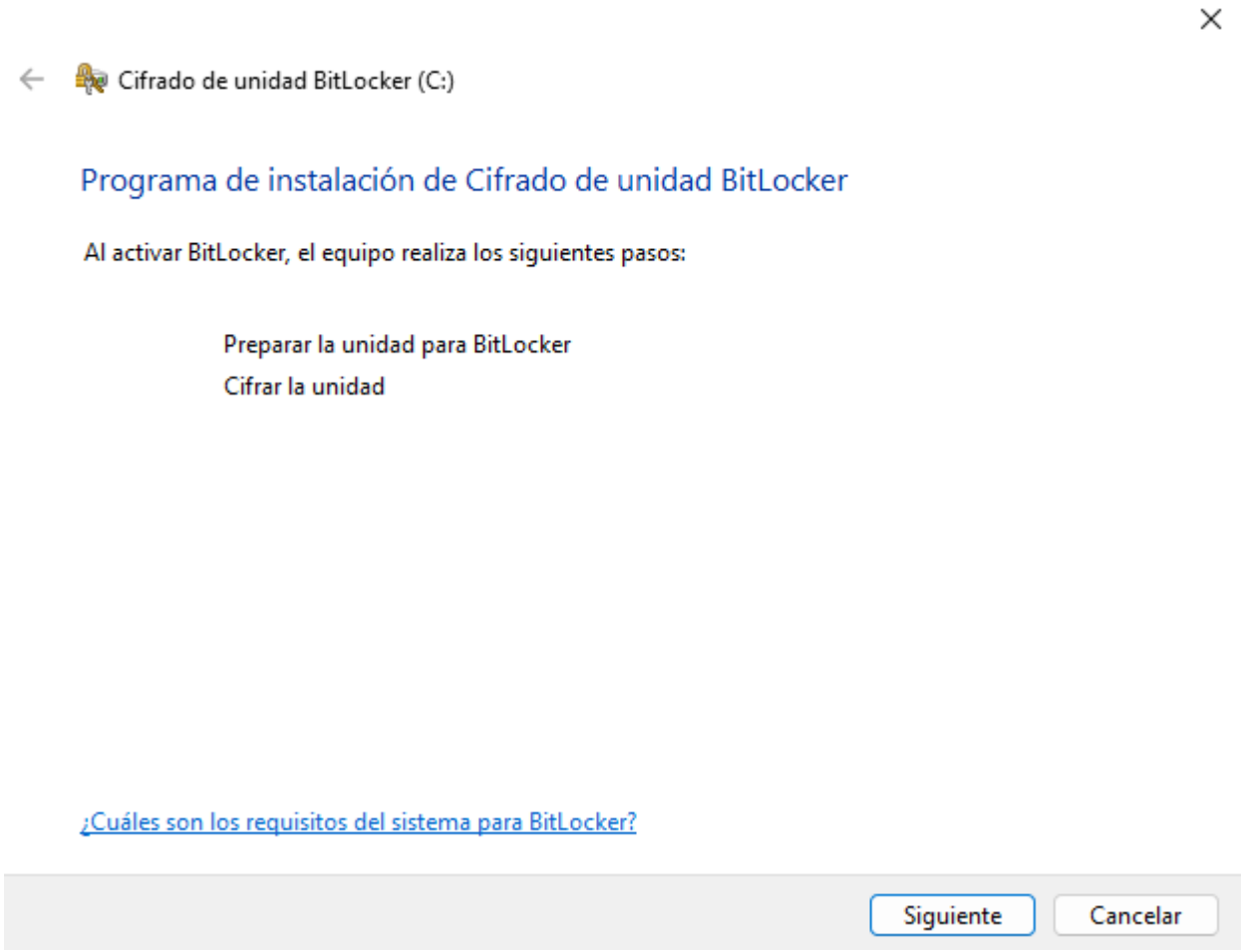
Una vez dentro de del administrador de cifrado de bitlocker se verá una ventana como esta:



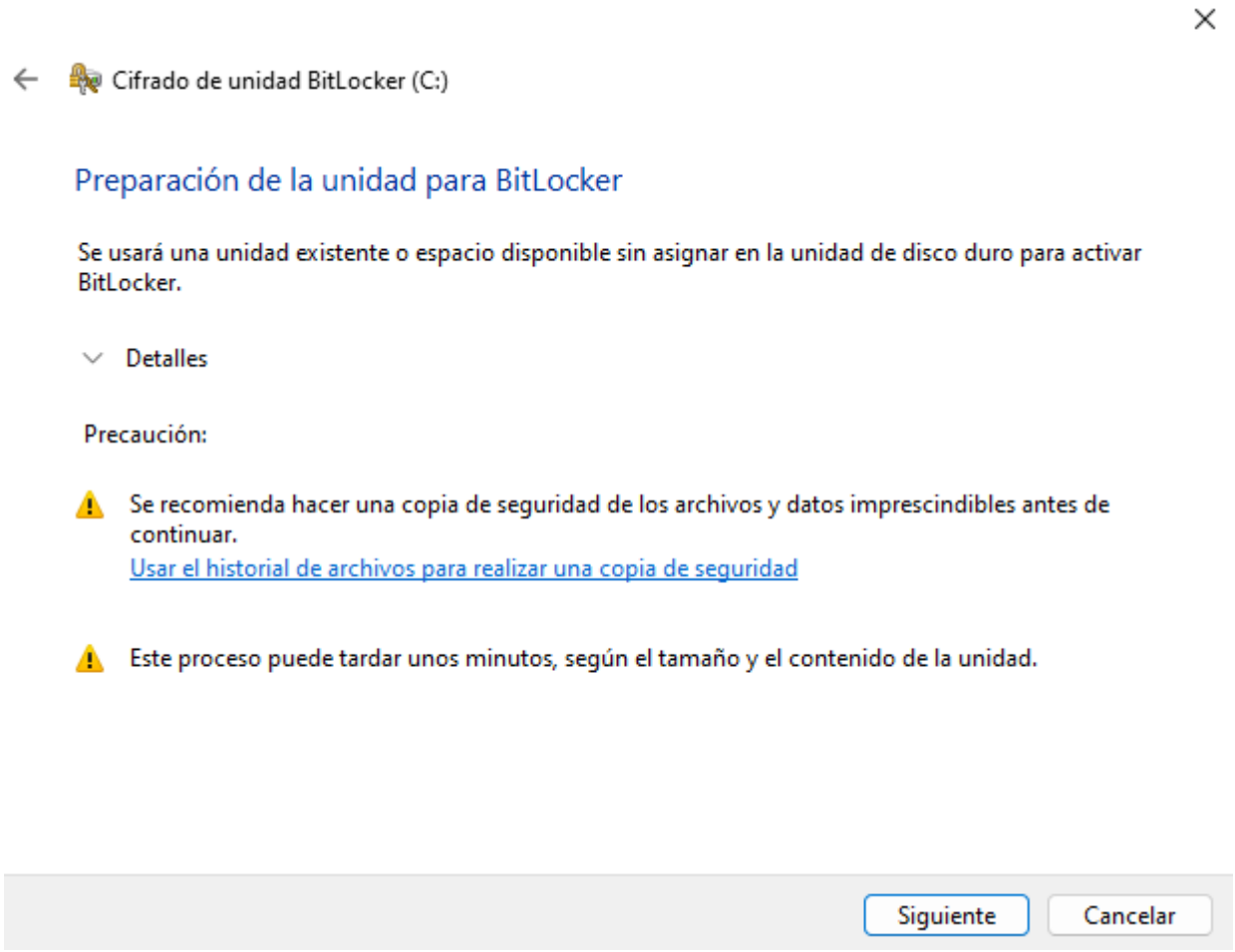
Para activar Bitlocker simplemente debemos pulsar en donde pone “Activar Bitlocker”



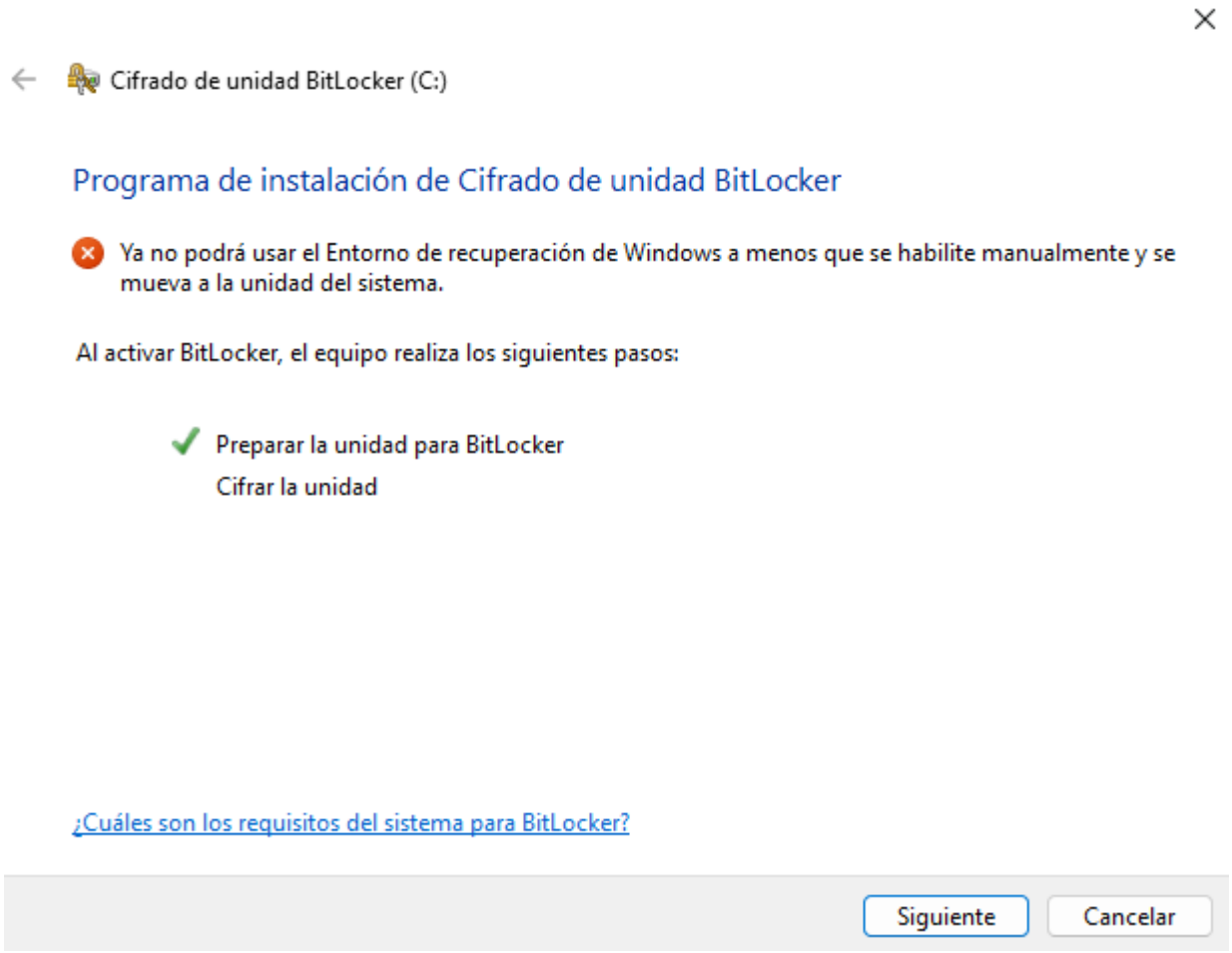
El sistema realizará una comprobación y si el sistema puede aplicar bitlocker veremos una ventana como esta:



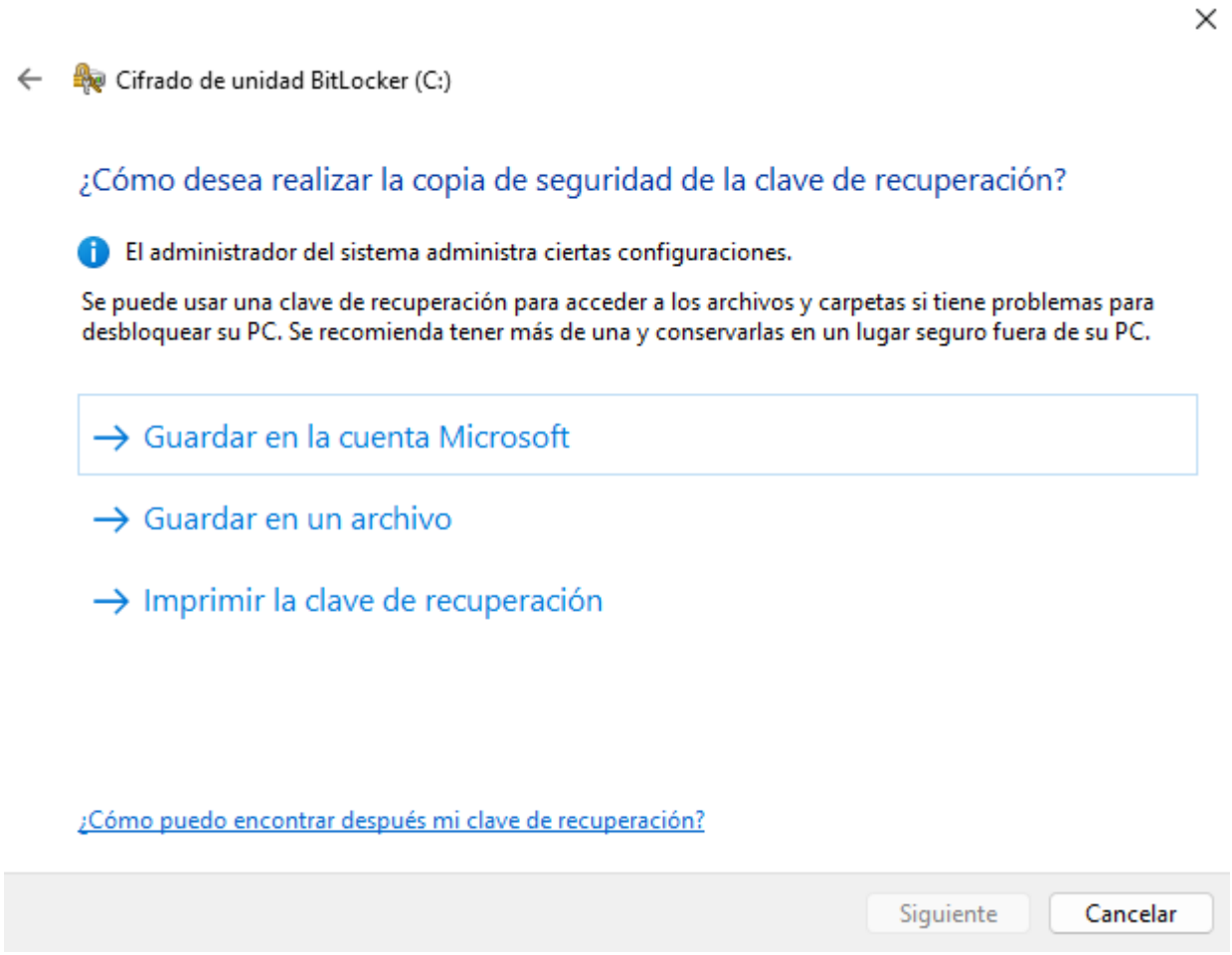
Para proceder presionaremos en el botón de siguiente y nos aparecerá este aviso:



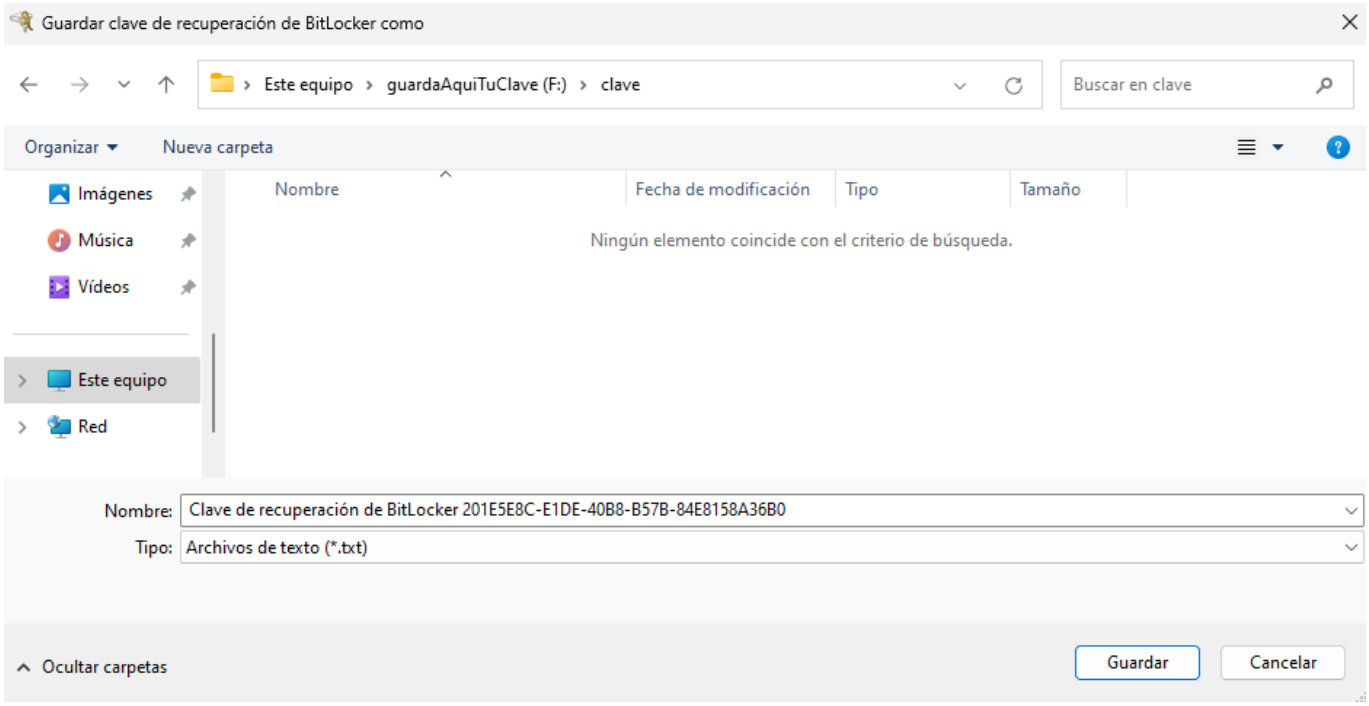
Presionaremos en siguiente, el sistema procederá a preparar el disco para su cifrado y tras eso aparecerá una ventana como la siguiente:



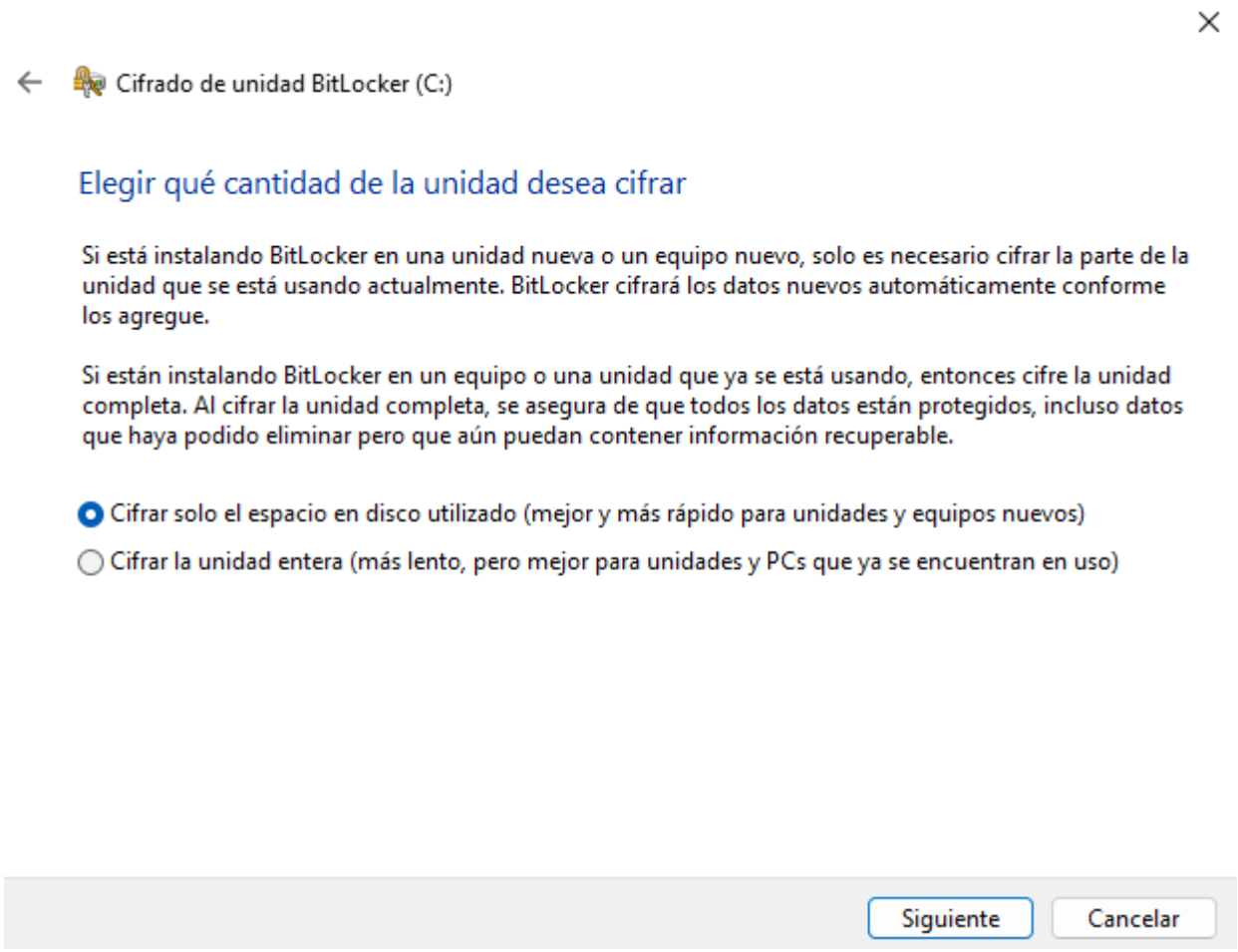
Se presiona en siguiente y se nos preguntará como queremos guardar la clave de recuperación:



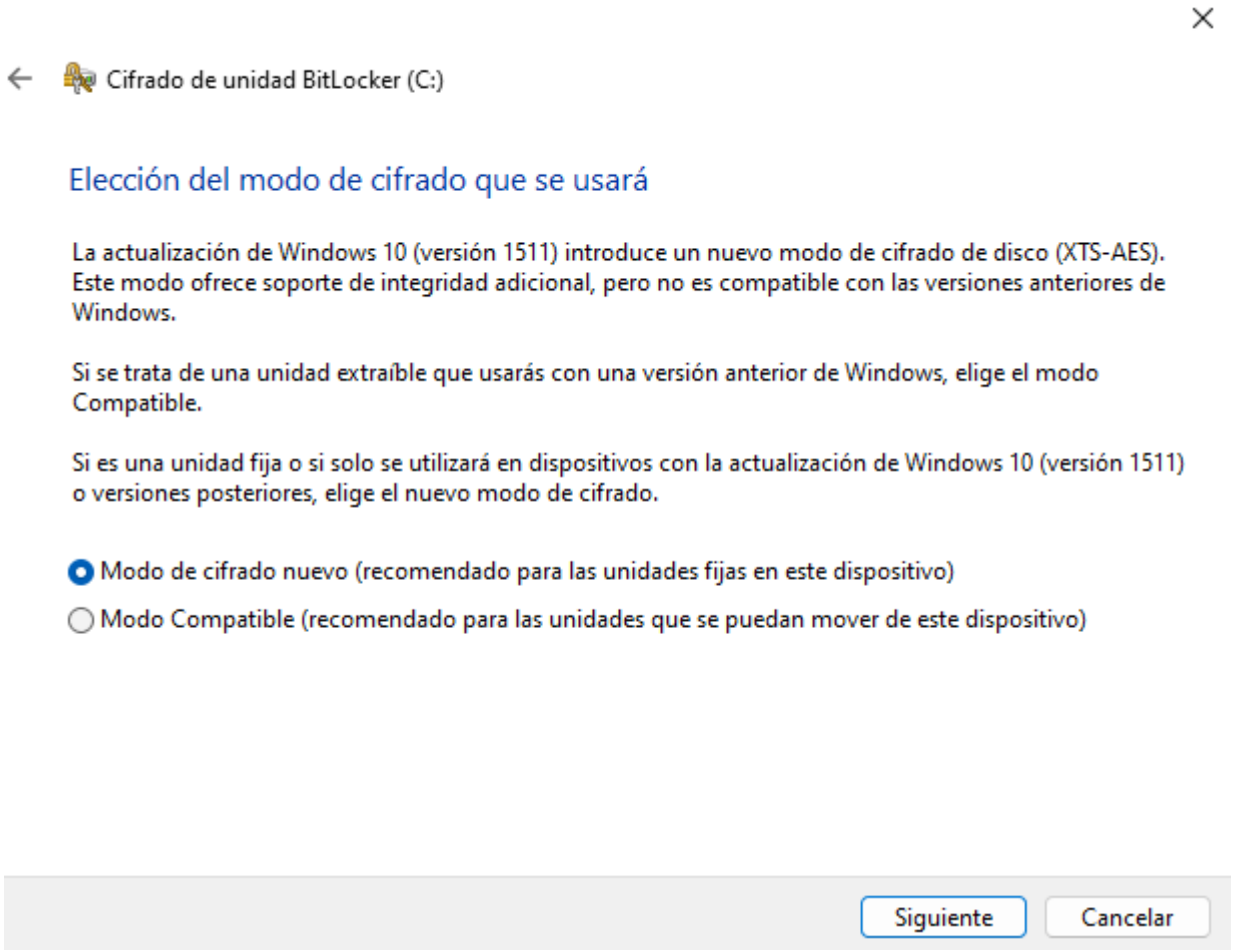
Como no tenemos cuenta microsoft, en este caso se guardará la clave de recuperación en un archivo:



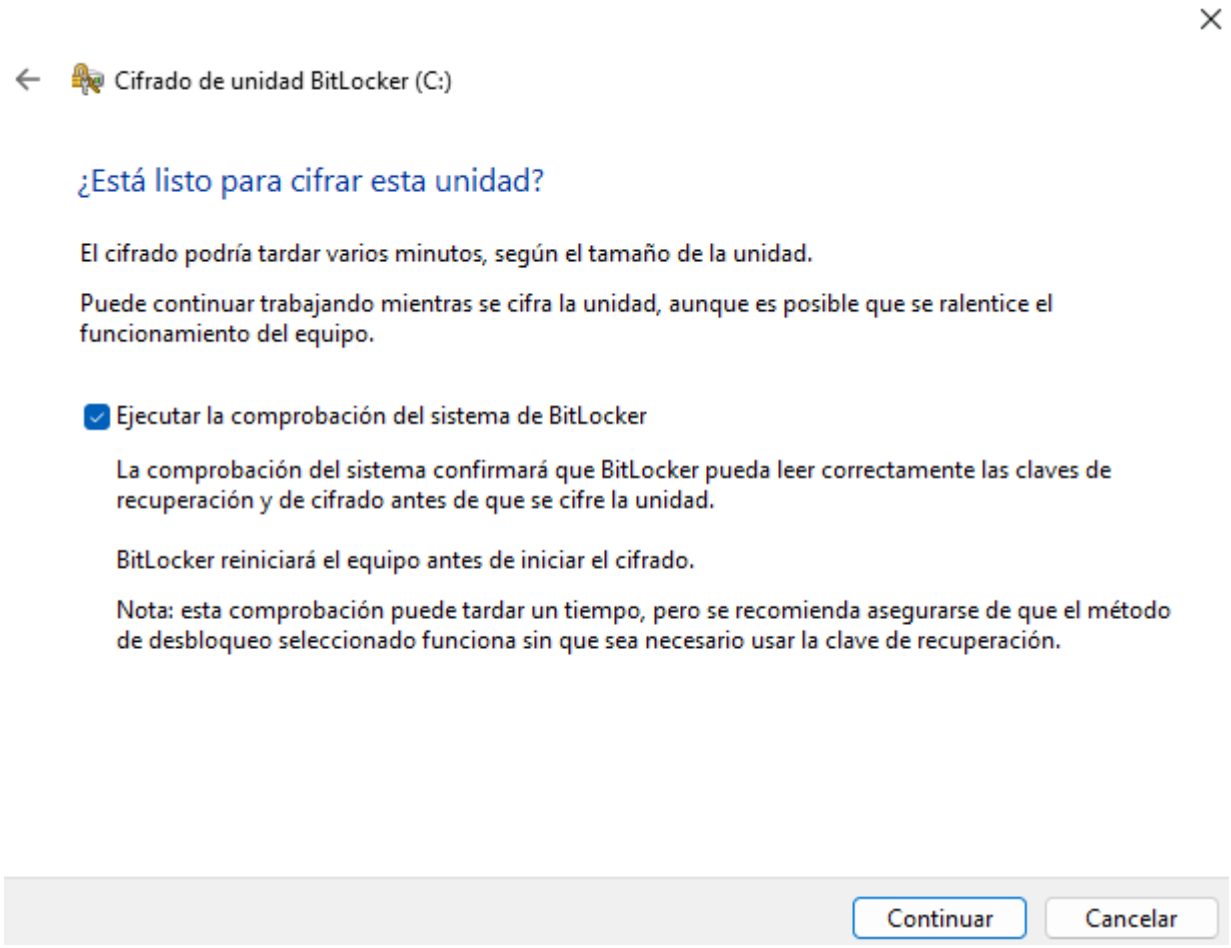
Una vez guardada la clave se puede proceder a pulsar en siguiente y se selecciona la opción de cifrar el espacio usado para que no lleve demasiado el proceso de cifrado de la unidad:



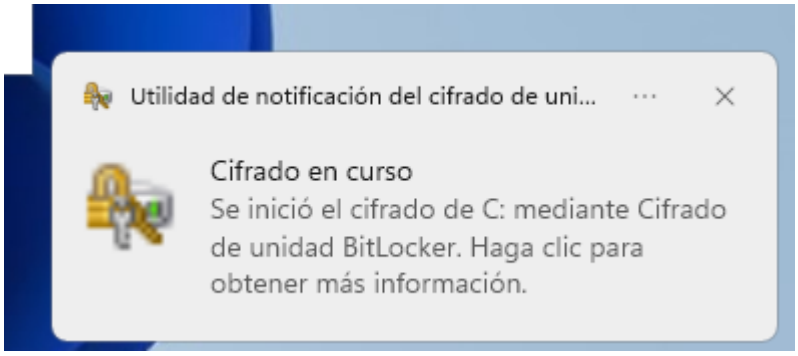
Tras eso le damos a siguiente y seleccionamos la opción de Modo de cifrado nuevo:

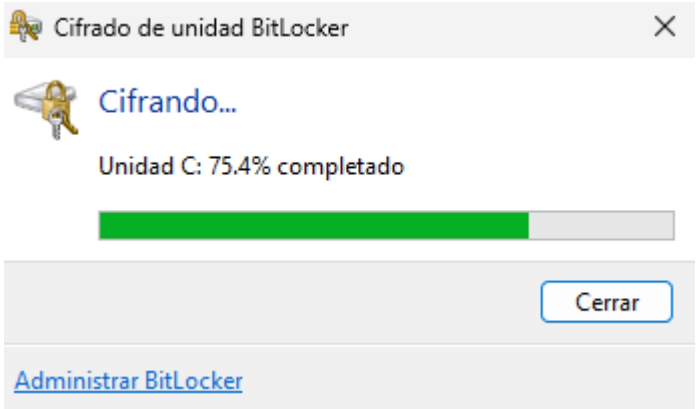


Finalmente nos permitirá iniciar el cifrado, se recomienda marcar la casilla de ejecutar la comprobación del sistema de bitlocker:



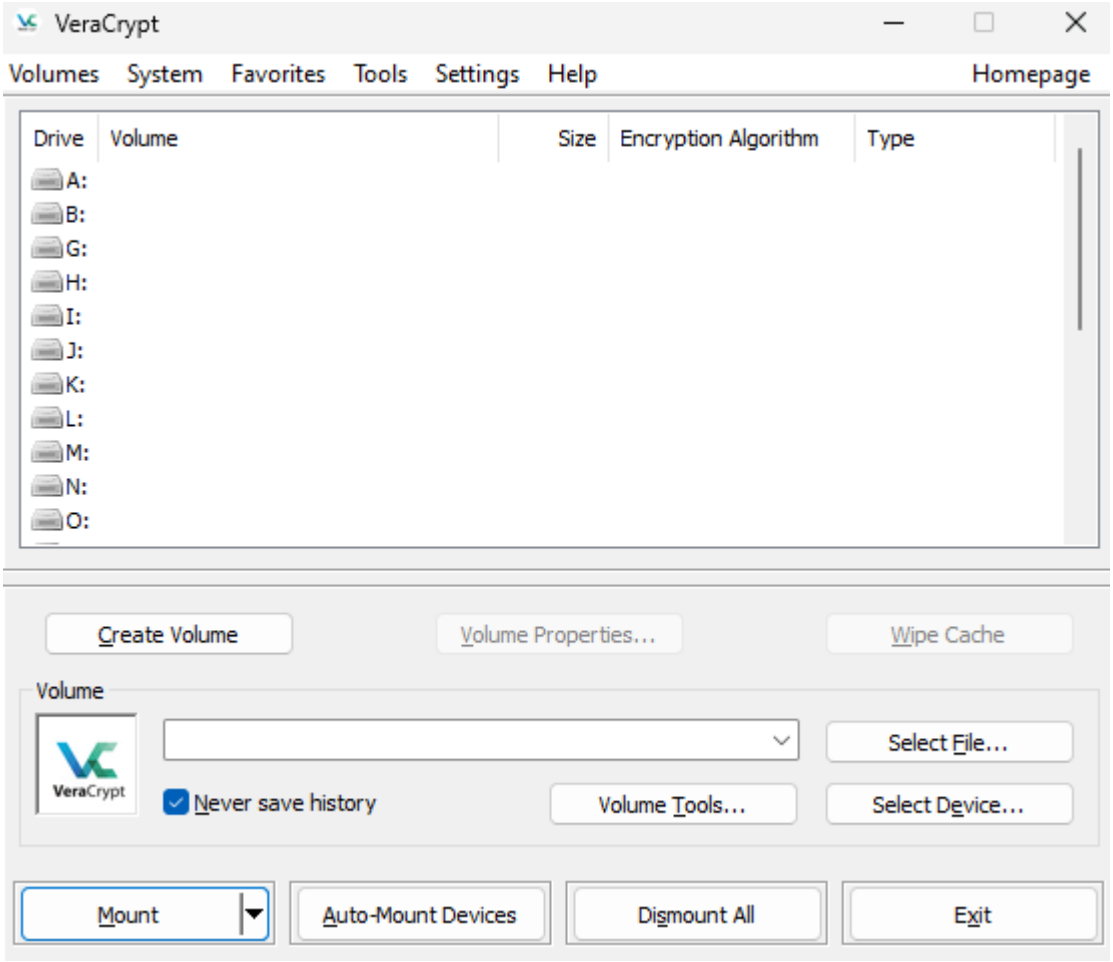
Una vez le demos a iniciar cifrado aparecerá una notificación indicando que se ha iniciado el cifrado y este se realizará en segundo plano:



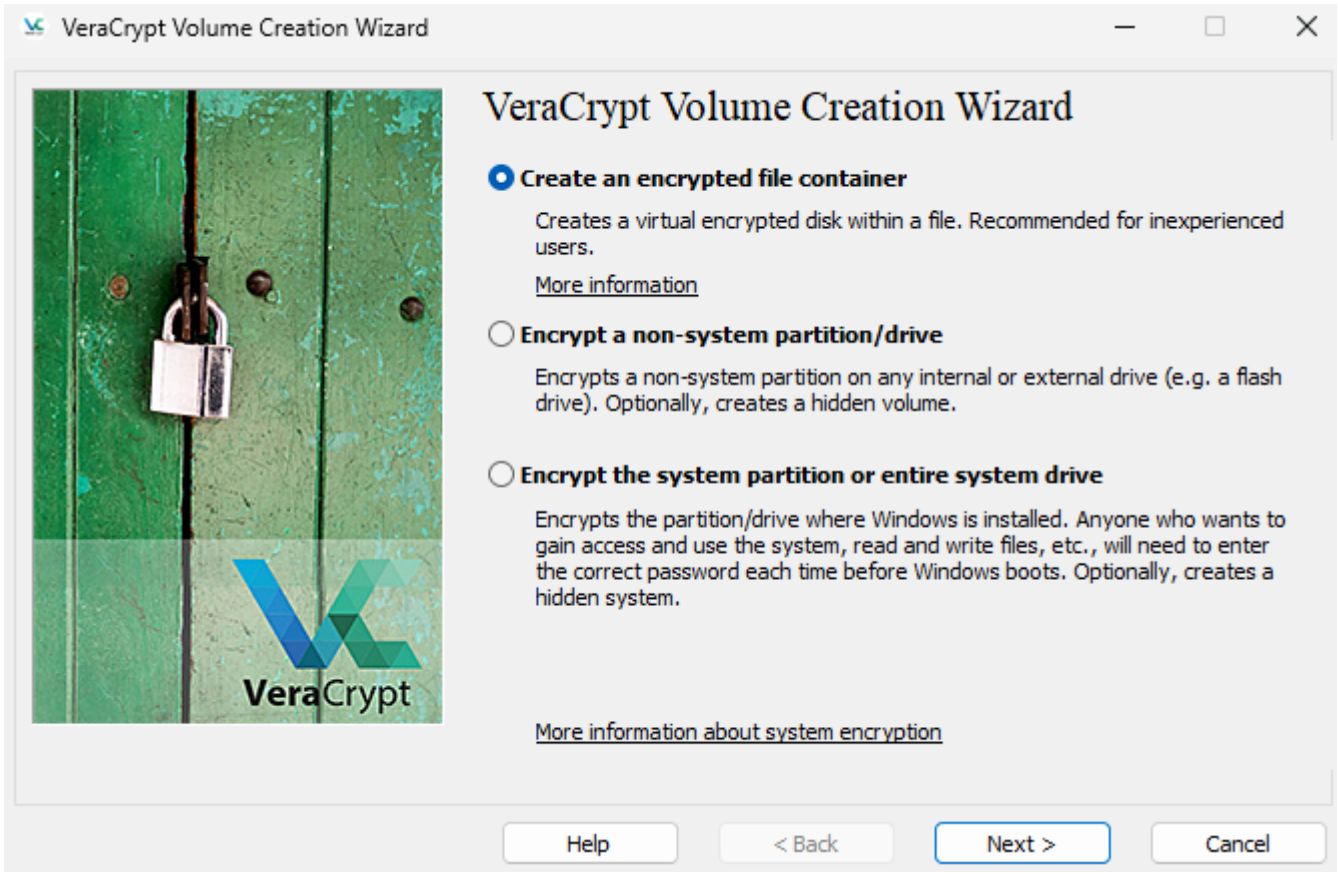


c) Usa Veracrypt para crear un contenedor cifrado para el usuario dentro de su perfil

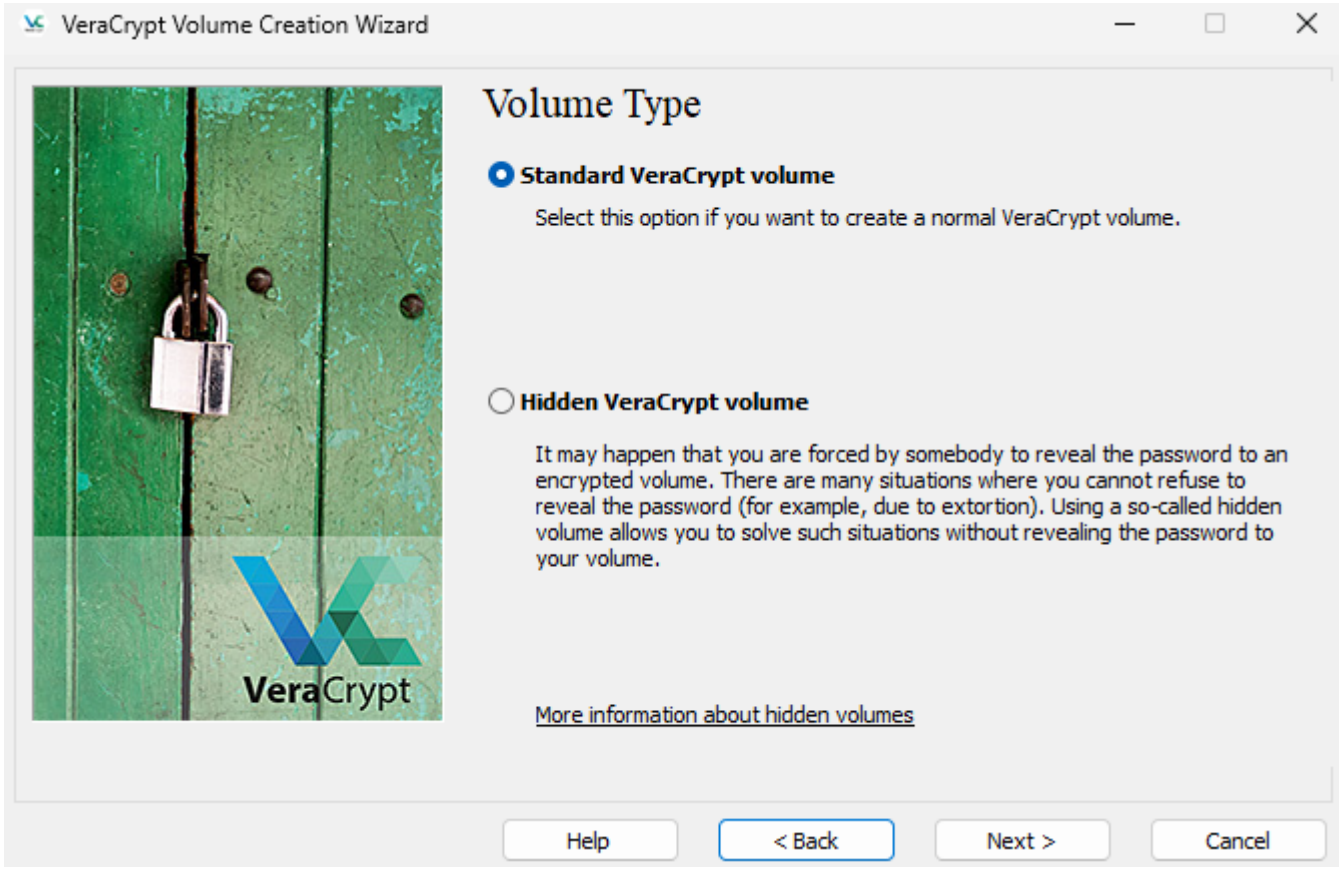
Para crear un contenedor cifrado primero debemos descargar e instalar veracrypt en nuestra máquina con windows 11. Tras eso se procede a abrir veracrypt:



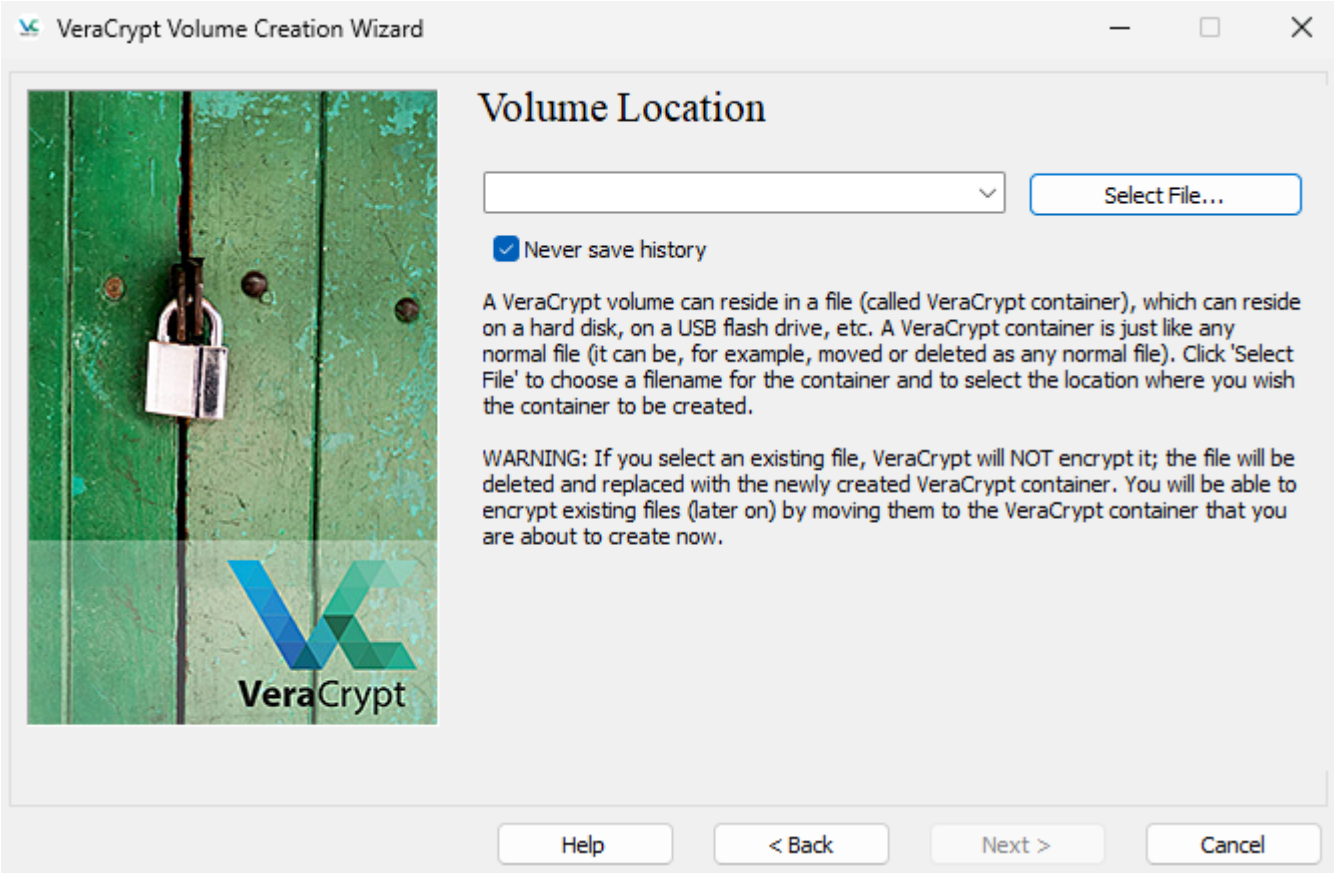
Lo primero que se debe hacer es presionar en “Create Volume”:



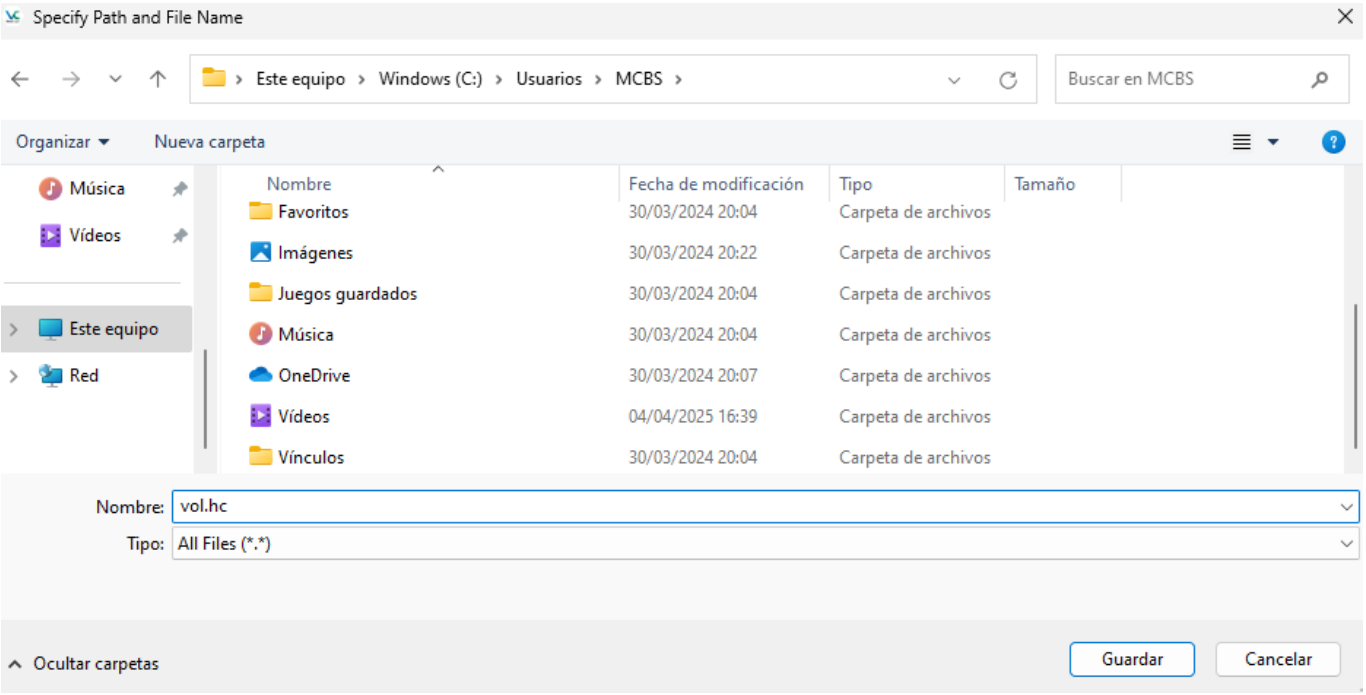
En la ventana que aparece seleccionamos “Create an encrypted container” y pulsamos en Next:



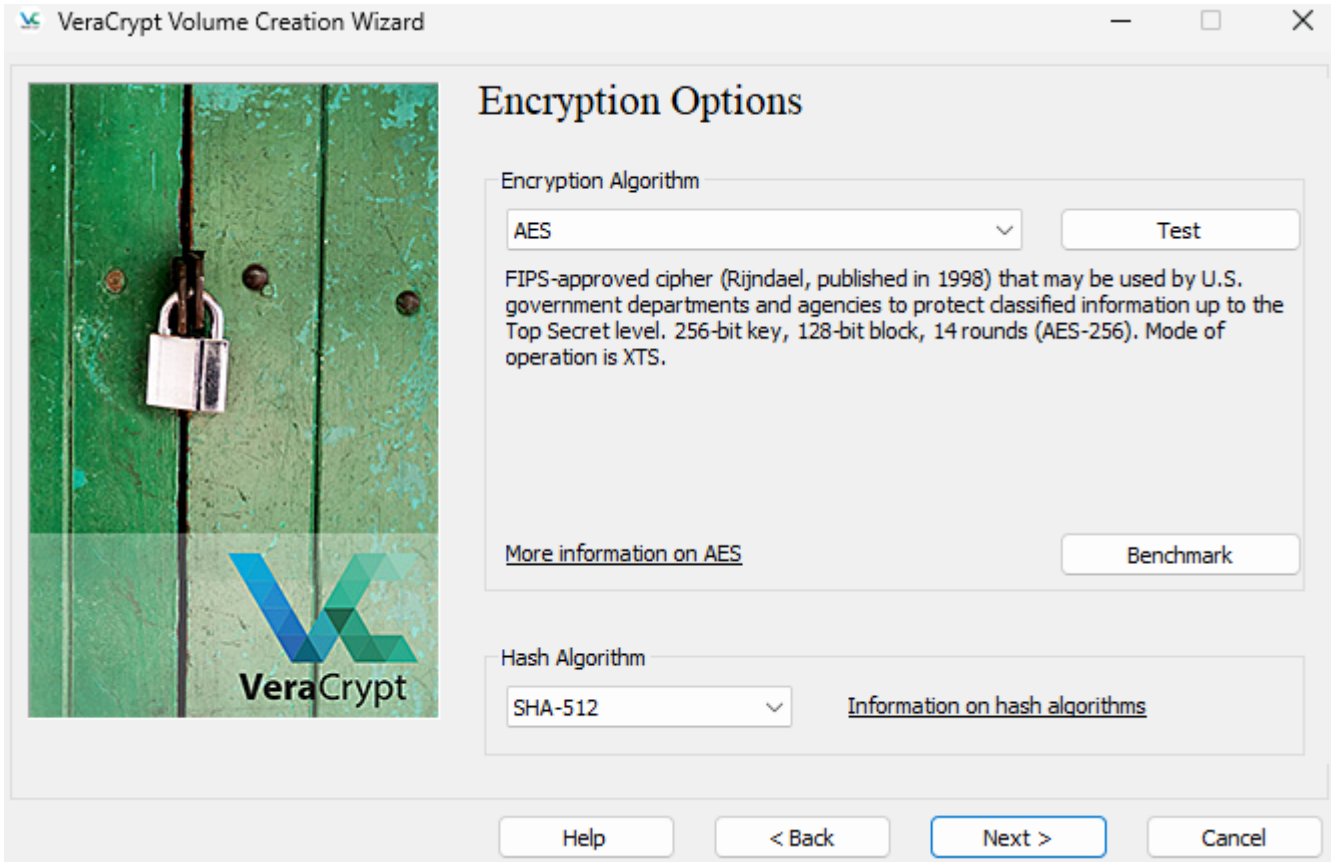
Seleccionamos Standard VeraCrypt Volume y le damos a next:



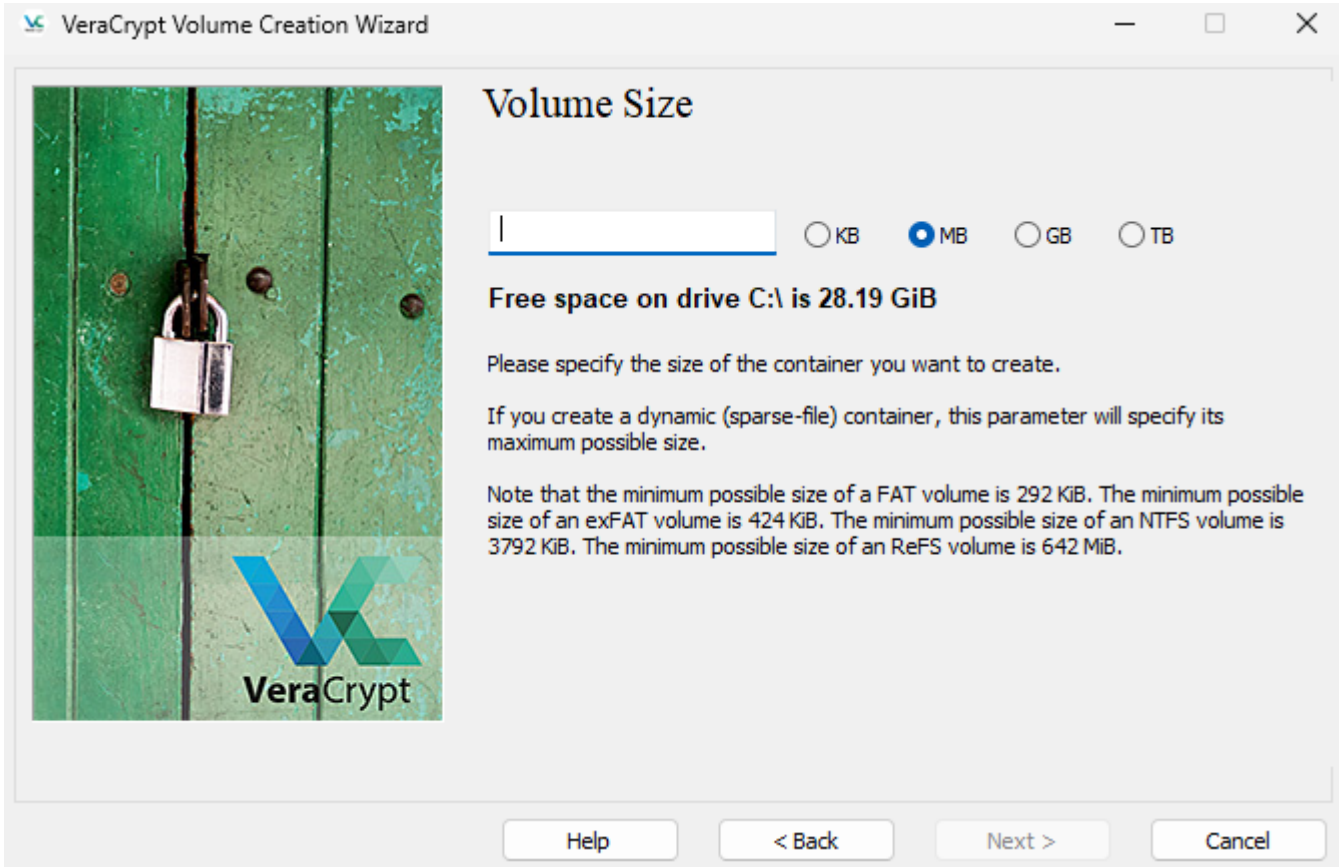
Para almacenar el volúmen seleccionamos la carpeta de nuestro usuario:



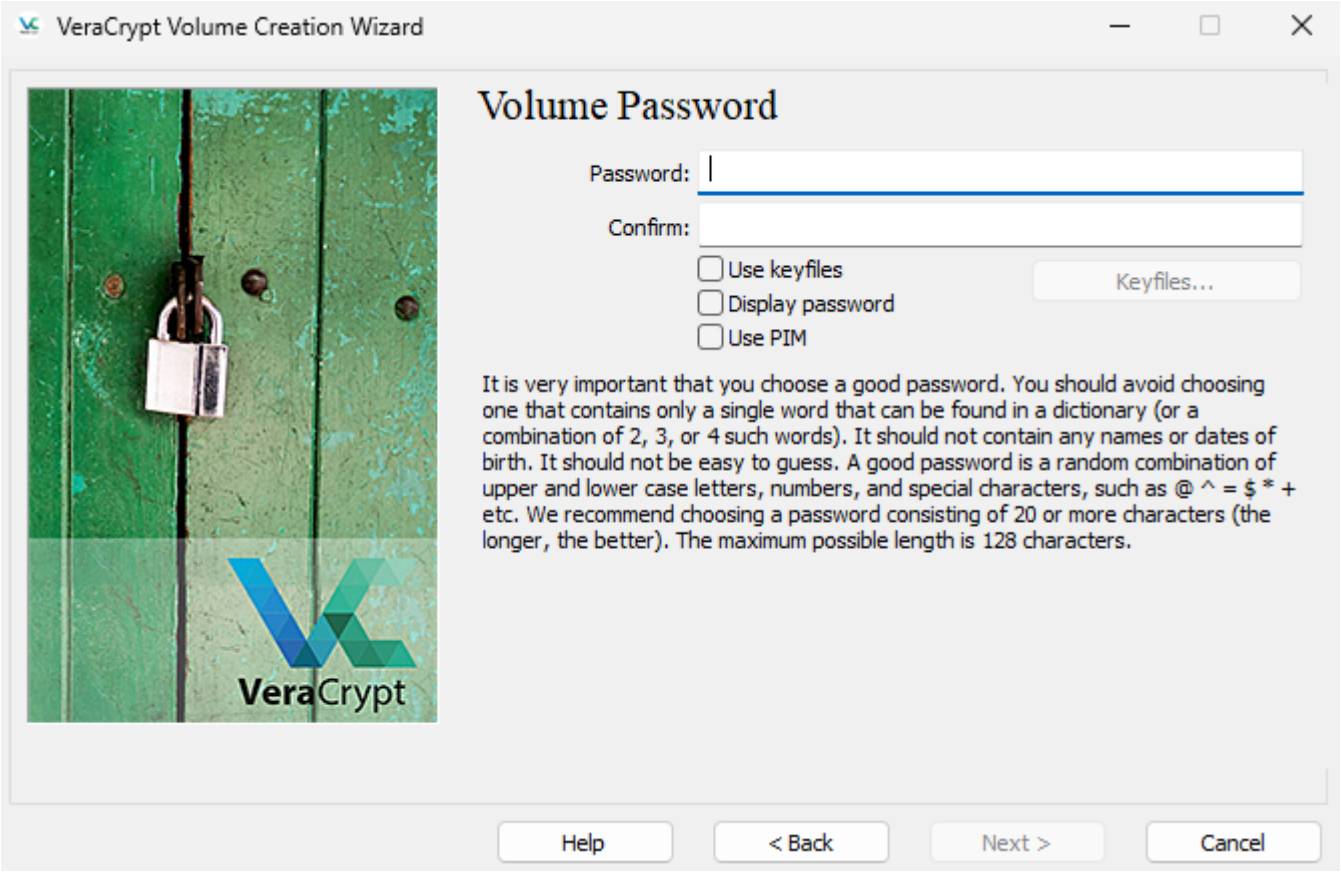
Una vez seleccionada la ubicación le damos a next:



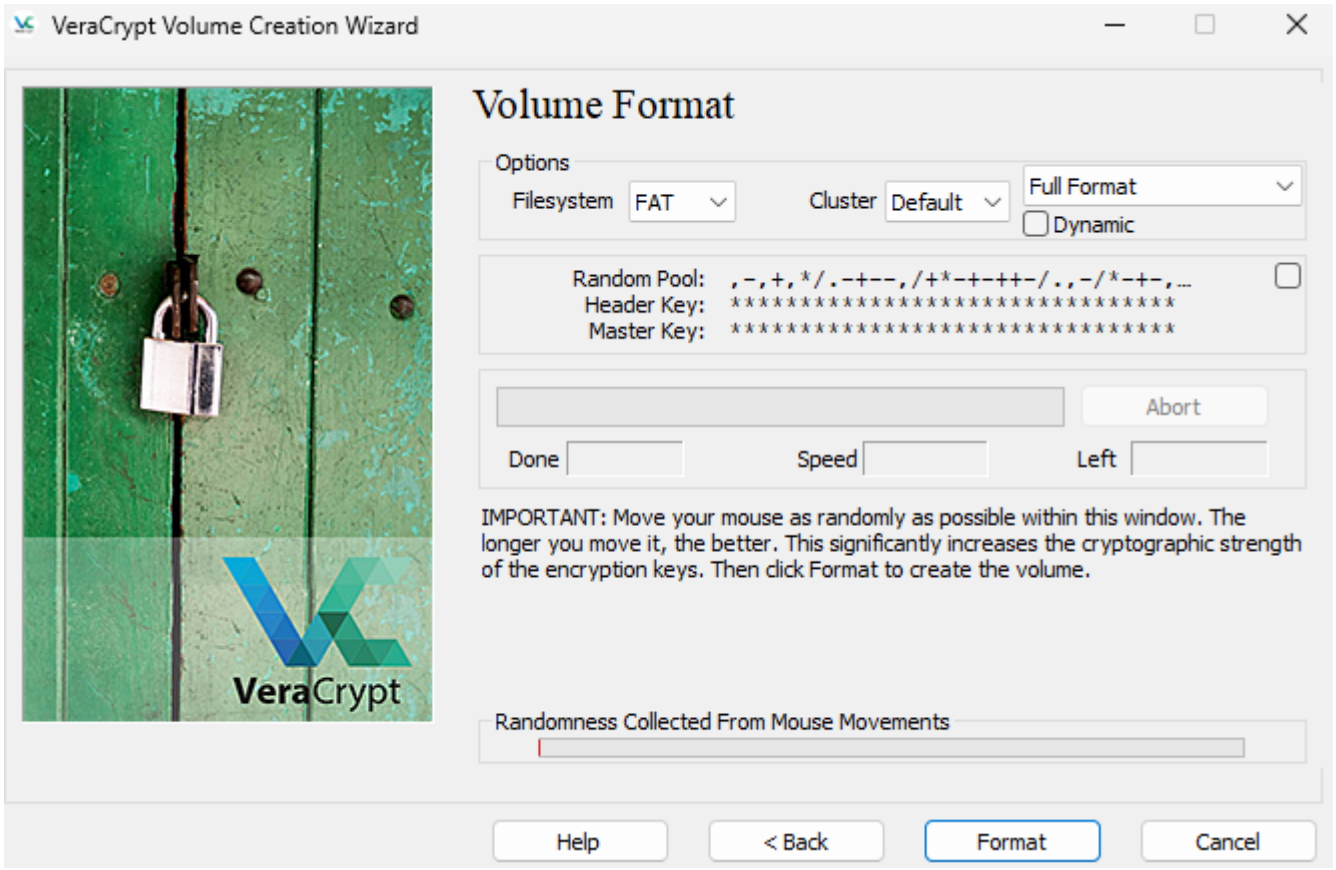
En la ventana que aparece se puede seleccionar el cifrado que se va a aplicar, una vez seleccionado se pulsa en siguiente:



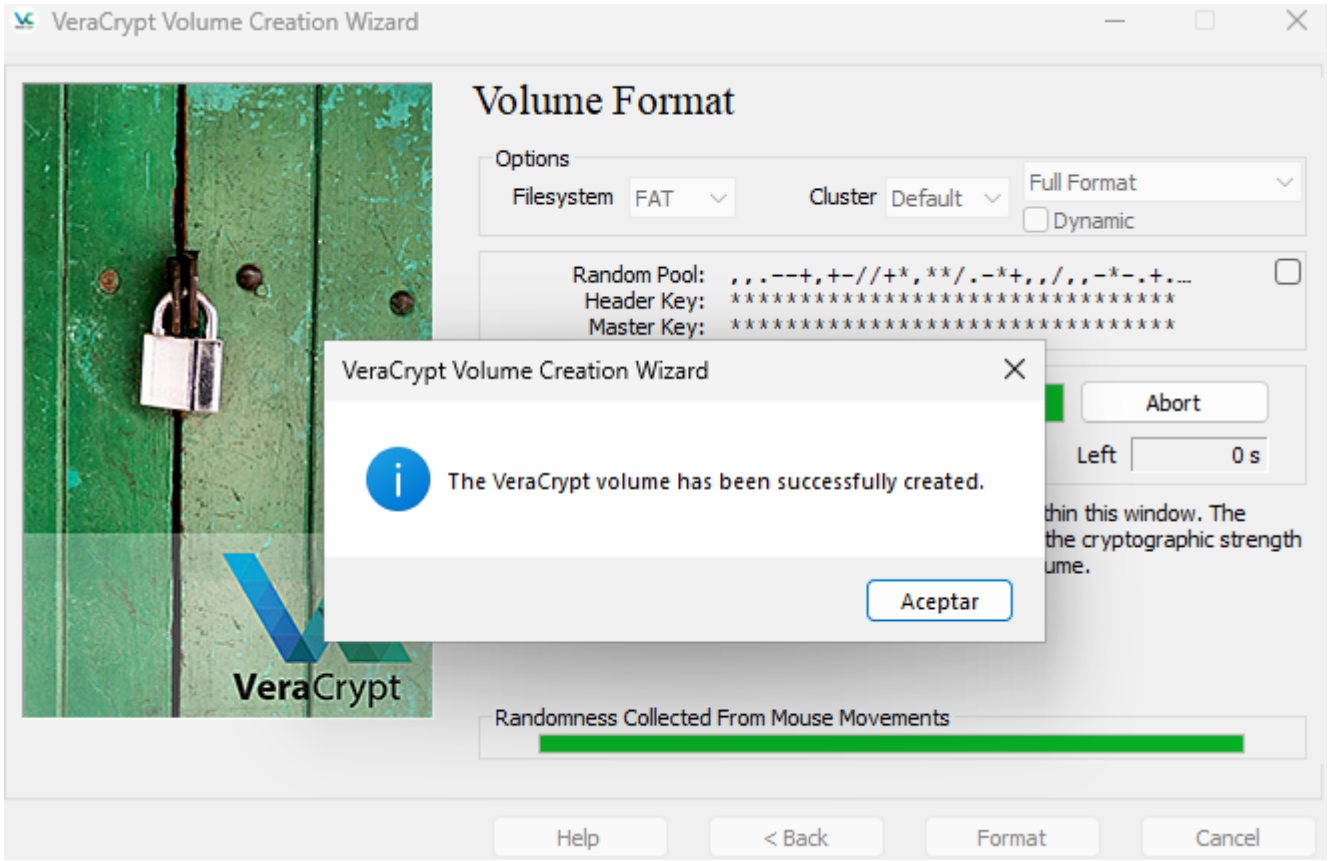
Seleccionaremos el tamaño que va a tener el contanier y pulsaremos en siguiente:



Ahora estableceremos una contraseña y pulsaremos en siguiente:



Finalmente se selecciona el tipo de formateo que va a tener el container y se presiona en “Format”



Como resultado se obtiene un nuevo container de veracrypt.

d) Crea una carpeta con el sistema de cifrado EFS

i. Indica como sería el procedimiento

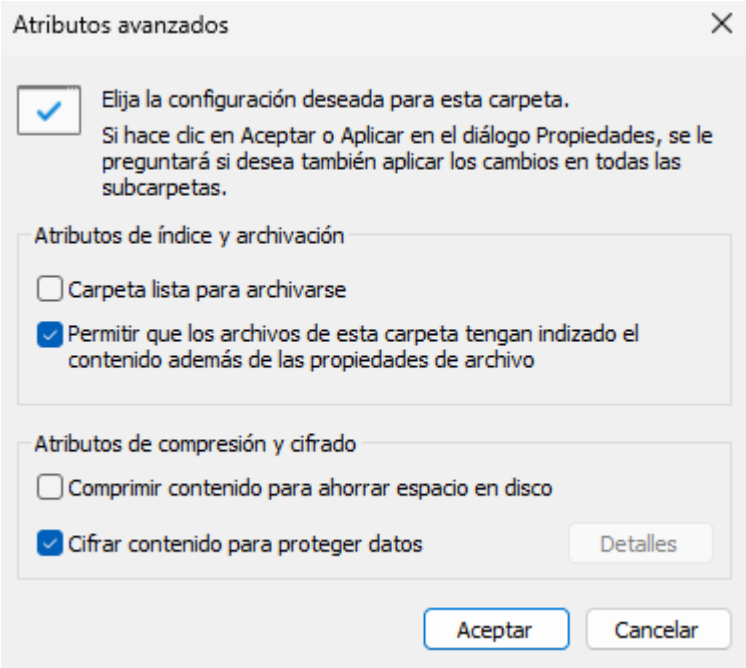
Para realizar un cifrado EFS de una carpeta debemos abrir el CMD como administrador y escribir el siguiente comando:

```
fsutil behavior set disableencryption 0
```

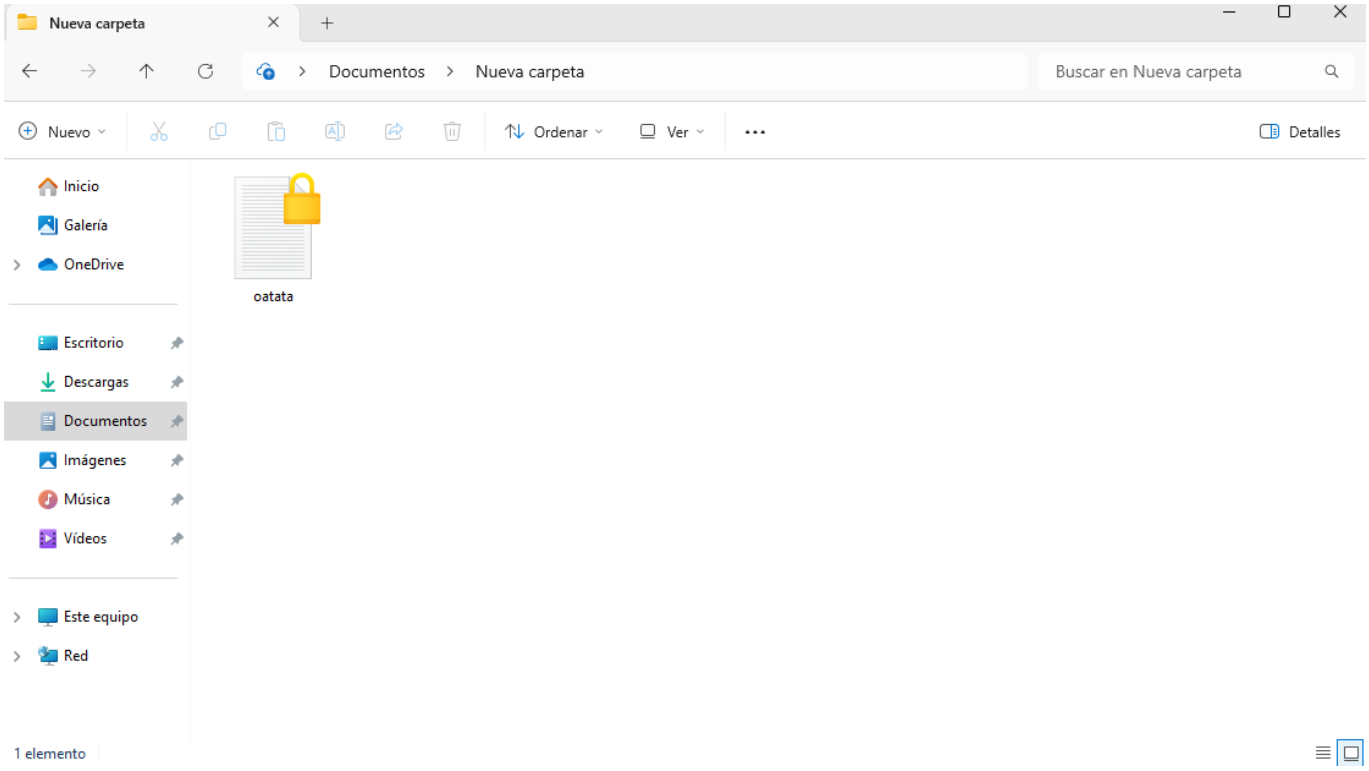
```
C:\Users\MCBS\Documents\Nueva carpeta>fsutil behavior set disableencryption 0
DisableEncryption = 0  (El cifrado está HABILITADO)

Es necesario reiniciar el equipo para aplicar este cambio
```

Otra opción es ir a opciones avanzadas en propiedades de la carpeta y marcar la casilla de cifrar contenido para proteger los datos:



Como se puede observar la carpeta ahora está cifrada:



ii. ¿Puede habilitar este sistema de cifrado un usuario limitado?

No, es necesario tener permisos de administrador para hacerlo

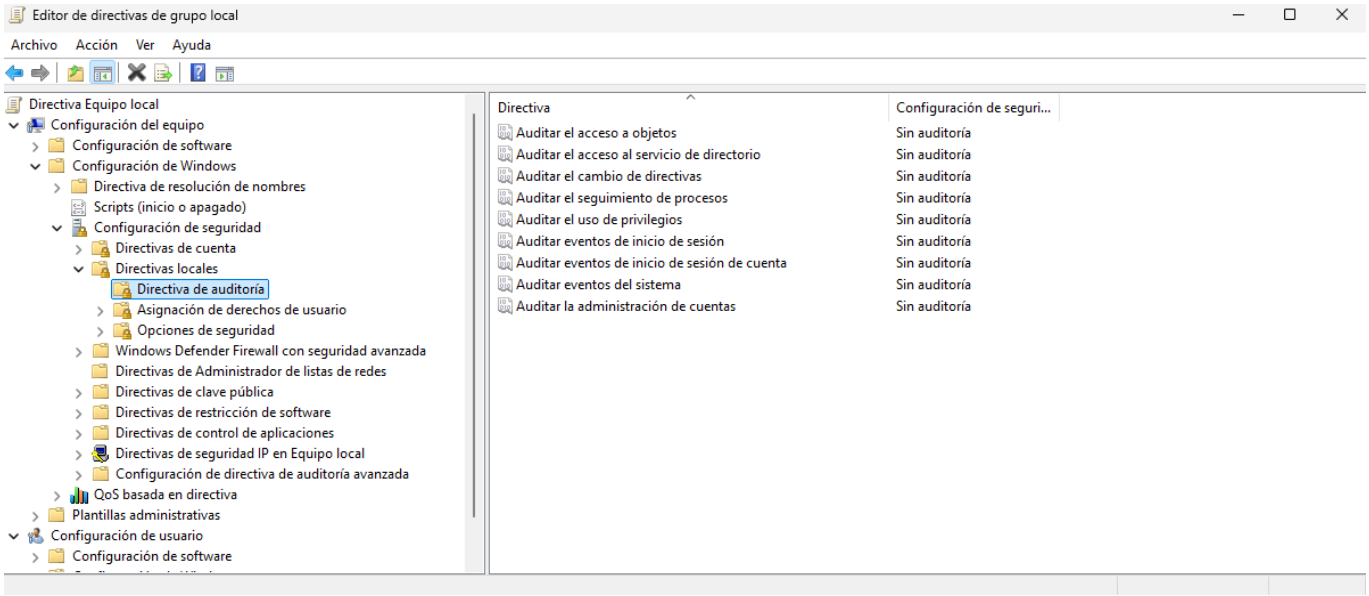
iii. ¿Podrían acceder varios usuarios al mismo fichero/carpeta compartida y crifrada?¿Cual sería el procedimiento?

Si, pero para ello habría que ir de nuevo a las propiedaddes, de la carpeta, opciones avanzadas y presionar en detalles al lado de la casilla de cifrar la carpeta y en la ventana que sale darle a añadir usuario.

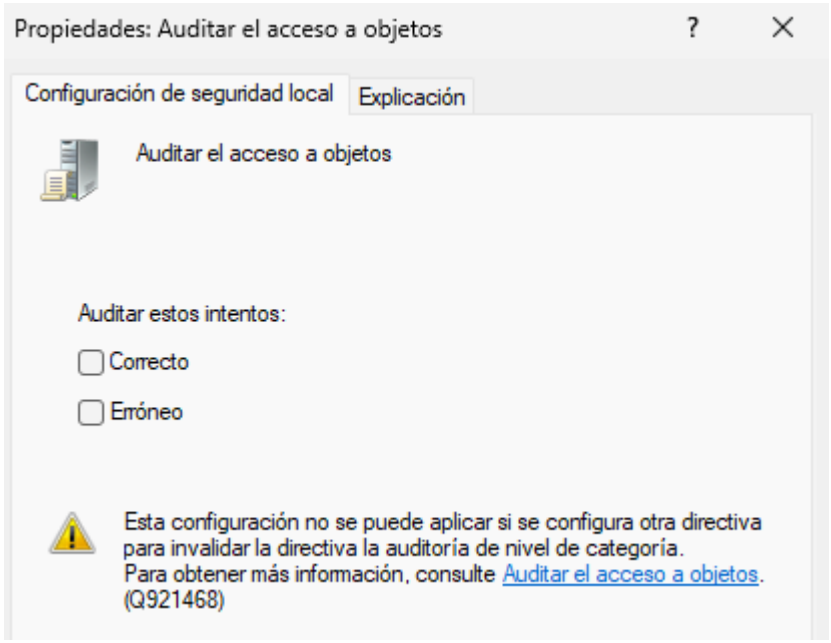
2. Auditoría del sistema

a) ¿Está el sistema de auditoría de windows activado por defecto? ¿Como se puede activar el sistema de auditoría?

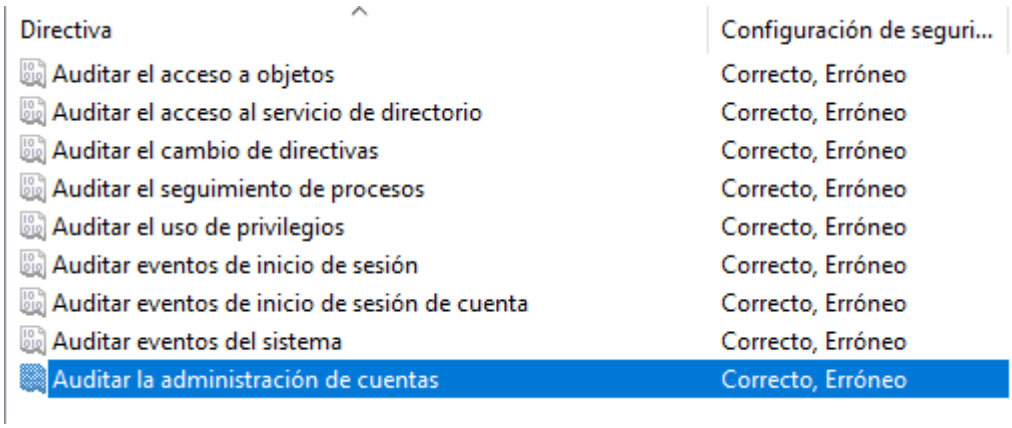
Por defecto la auditoría está desactivada, para activarla habría que ir al editor de directivas de grupo local “Configuración del equipo/Configuración de Windows/Configuración de Seguridad/Directivas Locales/Directivas de auditoría”:



Aquí habría que activar la auditoría para cada elemento, donde podemos elegir que queremos auditar:



En este caso auditaremos los accesos correctos y erróneos para todo:



Directiva	Configuración de seguri...
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso al servicio de directorio	Correcto, Erróneo
Auditar el cambio de directivas	Correcto, Erróneo
Auditar el seguimiento de procesos	Correcto, Erróneo
Auditar el uso de privilegios	Correcto, Erróneo
Auditar eventos de inicio de sesión	Correcto, Erróneo
Auditar eventos de inicio de sesión de cuenta	Correcto, Erróneo
Auditar eventos del sistema	Correcto, Erróneo
Auditar la administración de cuentas	Correcto, Erróneo

b) ¿Qué categorías podemos auditar en un sistema operativo Windows 11?

Como se puede observar en la anterior captura de pantalla se pueden auditar las siguientes categorías:

- Acceso a objetos
- Acceso al servicio de directorio
- Cambio de directivas
- Seguimiento de procesos
- uso de privilegios
- Eventos de inicio de sesión
- Eventos de inicio de sesión de cuenta
- Eventos del sistema
- Administración de cuentas

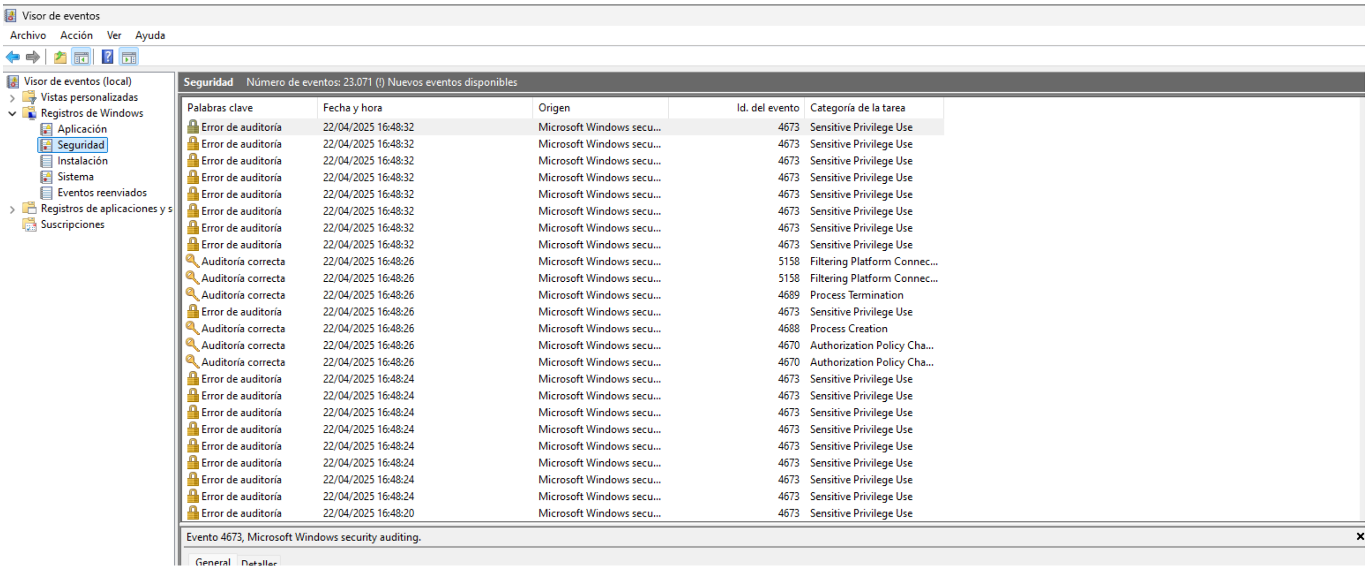
c) ¿Sobre que tipo de objetos podemos aplicar una auditoría de Windows 11?

Se puede aplicar una auditoría de windows a los siguientes obejtos:

- Archivos
- Carpetas
- Servicios

d) ¿Como podemos observar los resultados de una auditoría?

Podemos observarlos desde el Visor de eventos yendo a “Registros de Windows/Seguridad”:



From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:fortificacion:p9

Last update: **2025/04/22 14:49**