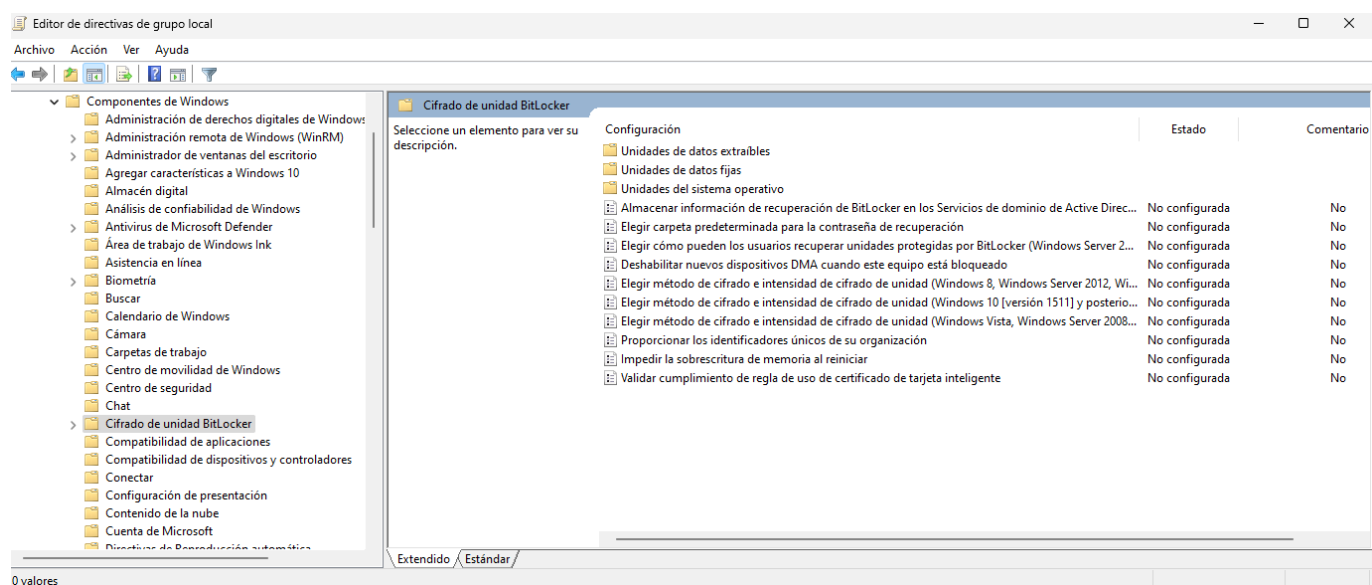


[FORT] Práctica 9: Fortificación de la información y auditoría de Windows 11

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

Elegir carpeta predeterminada para la contraseña de recuperación

Elegir carpeta predeterminada para la contraseña de recuperación

Valor anterior

Valor siguiente

☐ No configurada

☒ Habilitada

☐ Deshabilitada

Comentario:

Compatible con:

Al menos Windows Vista

Opciones:

Ayuda:

Configurar la ruta de acceso predeterminada de carpetas:

Especifique una ruta de acceso completa o incluya las variables de entorno del equipo en la ruta de acceso.

Por ejemplo, escriba
"\\servidor\carpetaDeCopiaDeSeguridad", o "%variableDeEntornoDeUnidadSegura%\carpetaDeCopiaDeSeguridad"

Nota: en todos los casos, el usuario podrá seleccionar otras carpetas donde guardar la contraseña de recuperación.

Esta configuración de directiva permite especificar la ruta de acceso predeterminada que se muestra cuando el asistente para la instalación del Cifrado de unidad BitLocker solicita al usuario que escriba la ubicación de una carpeta donde se guardará la contraseña de recuperación. Esta configuración de directiva se aplica al activar BitLocker.

Si habilita esta configuración de directiva, puede especificar la ruta que se usará como ubicación de carpeta predeterminada cuando el usuario seleccione la opción de guardar la contraseña de recuperación en una carpeta. Puede especificar una ruta de acceso completa o incluir en la ruta las variables del entorno del equipo de destino. Si la ruta de acceso no es válida, el asistente para la instalación de BitLocker mostrará la vista de carpetas de nivel superior del equipo.

Si deshabilita o no establece esta configuración de directiva, el asistente para la instalación de BitLocker mostrará la vista de carpetas de nivel superior del equipo cuando el usuario seleccione la opción de guardar la contraseña de recuperación en una carpeta.

Aceptar

Cancelar

Aplicar

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.

Almacenar información de recuperación de BitLocker en los Servicios de dominio de Active Directory (Windows Serv...

Almacenar información de recuperación de BitLocker en los Servicios de dominio de Active Directory (Windows Server 2008 y Windows Vista)

Valor anterior Valor siguiente

☐ No configurada ☒ Habilitada ☐ Deshabilitada

Comentario:

Compatible con: Windows Server 2008 y Windows Vista

Opciones:

☒ Requerir copia de seguridad de BitLocker en AD DS

Si se selecciona, no se podrá activar BitLocker si la copia de seguridad no se realiza correctamente (valor predeterminado recomendado).

Si no se selecciona, se podrá activar BitLocker aunque la copia de seguridad no se realice correctamente. No se vuelve a intentar realizar la copia de seguridad automáticamente.

Seleccionar la información de recuperación de BitLocker que debe almacenarse:

Contraseñas de recuperación y paquetes de claves

Una contraseña de recuperación es un número de 48

Ayuda:

Esta configuración de directiva permite administrar la copia de seguridad de los Servicios de dominio de Active Directory (AD DS) de la información de recuperación del Cifrado de unidad BitLocker. Esto proporciona un método administrativo de recuperación de datos cifrados por BitLocker con el fin de evitar la pérdida de datos debida a la falta de información sobre la clave. Esta configuración de directiva se aplica solo a equipos que ejecutan Windows Server 2008 o Windows Vista.

Si habilita esta configuración de directiva, se realizará una copia de seguridad de la información de recuperación del BitLocker en AD DS, de forma automática y sin notificaciones, cuando BitLocker se active en un equipo. Esta configuración de directiva se aplica al activar BitLocker.

Nota: para que la copia de seguridad de AD DS se realice correctamente, es probable que deba configurar primero extensiones de esquema adecuadas y la configuración de control de acceso en el dominio. En Microsoft TechNet, encontrará más información sobre configuración de una copia de seguridad en AD DS para BitLocker.

Aceptar Cancelar Aplicar

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:

Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y poste...

Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y posteriores)

Valor anterior Valor siguiente

☐ No configurada Comentario:

☒ Habilitada

☐ Deshabilitada

Compatible con: Se requiere al menos Windows Server 2016 o Windows 10

Opciones:

Ayuda:

Selecciona el método de cifrado de las unidades del sistema operativo:

XTS-AES de 128 bits (predeterminado)

Selecciona el método de cifrado de las unidades de datos fijas:

XTS-AES de 128 bits (predeterminado)

Selecciona el método de cifrado de las unidades de datos extraíbles:

AES-CBC de 128 bits (predeterminado)

Esta configuración de directiva te permite configurar el algoritmo y la intensidad del cifrado que se usan en el Cifrado de unidad BitLocker. Esta configuración de directiva se aplica al activar BitLocker. El cambio del método de cifrado no tendrá ningún efecto si la unidad ya está cifrada o si el cifrado está en curso.

Si habilitas esta configuración de directiva para configurar un algoritmo de cifrado y la intensidad de cifrado de clave de unidades de datos fijas, unidades del sistema operativo y unidades de datos extraíbles de manera individual. Para unidades del sistema operativo y unidades fijas, se recomienda usar el algoritmo XTS-AES. Para unidades extraíbles, usa el cifrado AES-CBC de 128 bits o AES-CBC de 256 bits si la unidad se usará en otros dispositivos que no ejecuten Windows 10 (versión 1511).

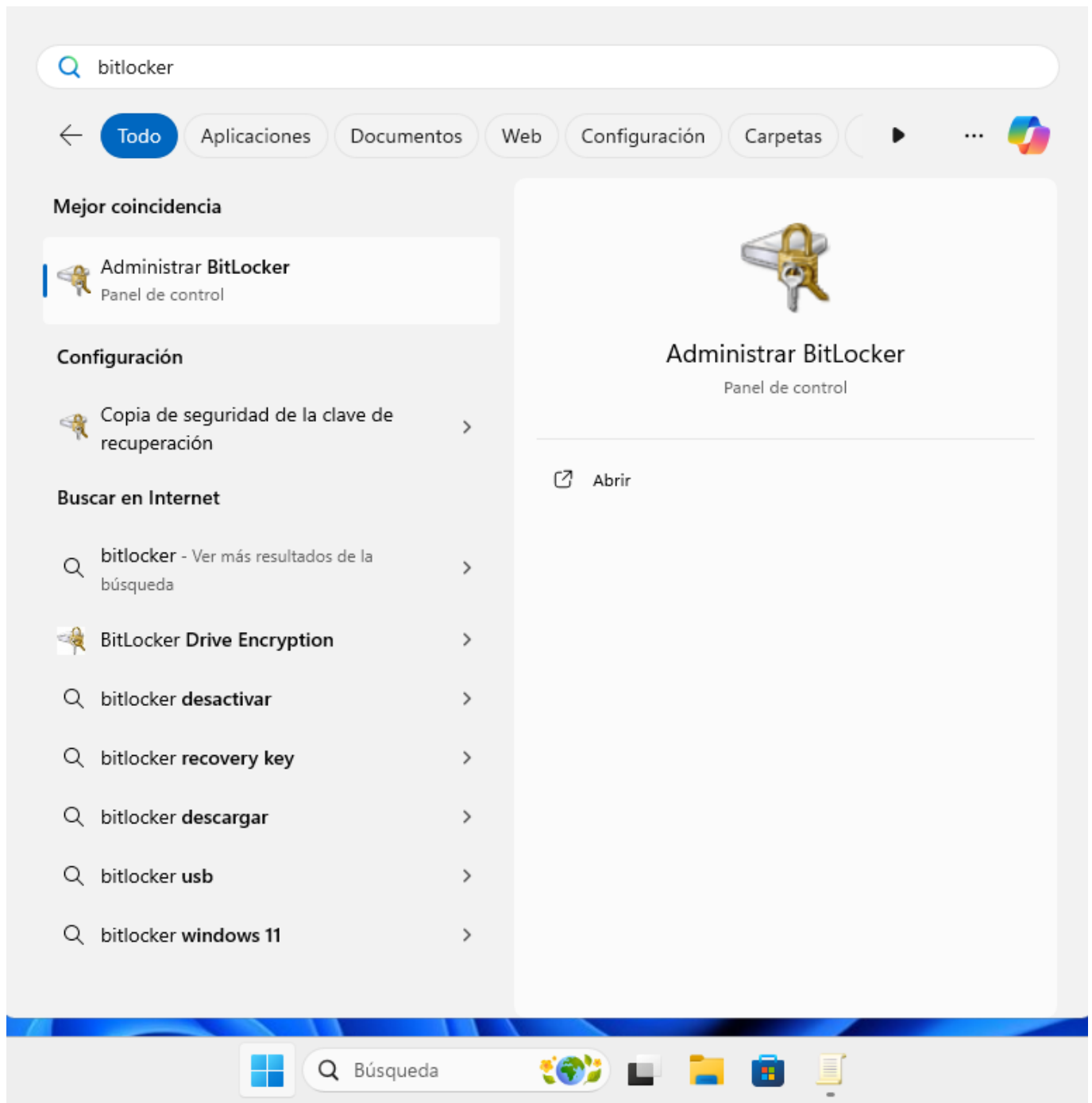
Si deshabilitas o no estableces esta configuración de directiva, BitLocker usará AES con la misma intensidad de bits (128 bits o 256 bits) que la configuración de directiva "Elegir método de cifrado e intensidad de cifrado de unidad (Windows Vista

Aceptar Cancelar Aplicar

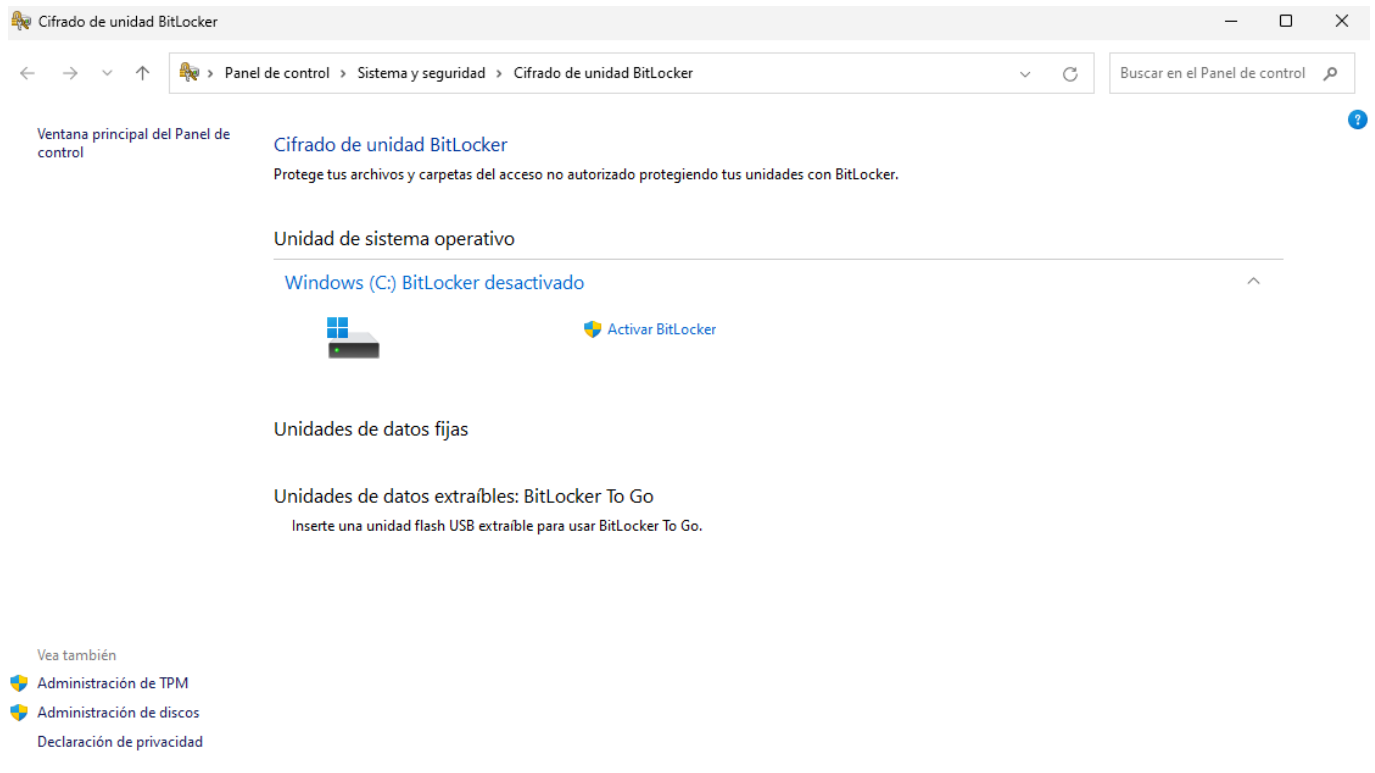
b) Realiza la activación de firado Bitlocker sobre C:\

i. Indica los pasos a seguir para realizar dicho cifrado

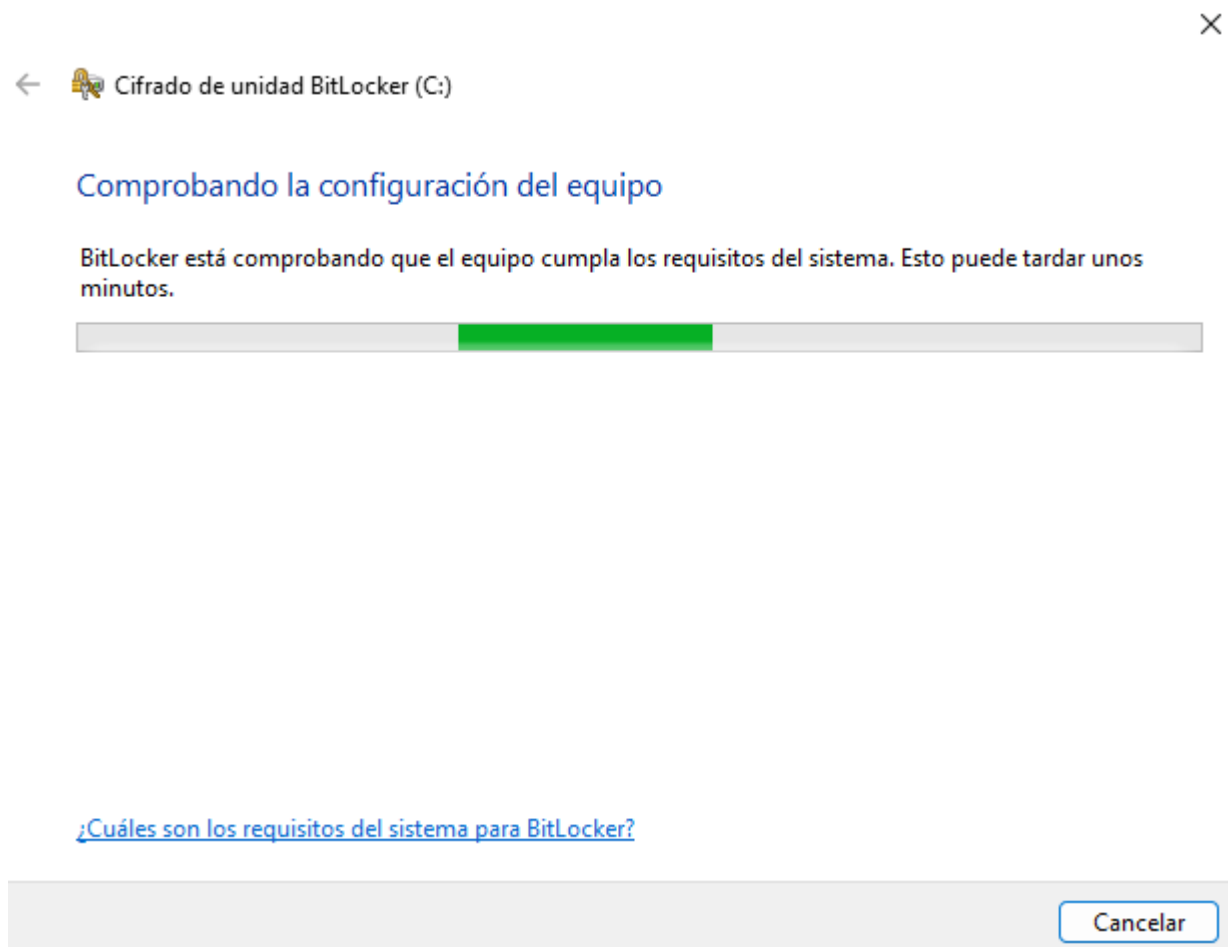
La forma más simple de realizar el cifrado del disco mediante bitlocker es pulsar el botón windows y buscar bitlocker:



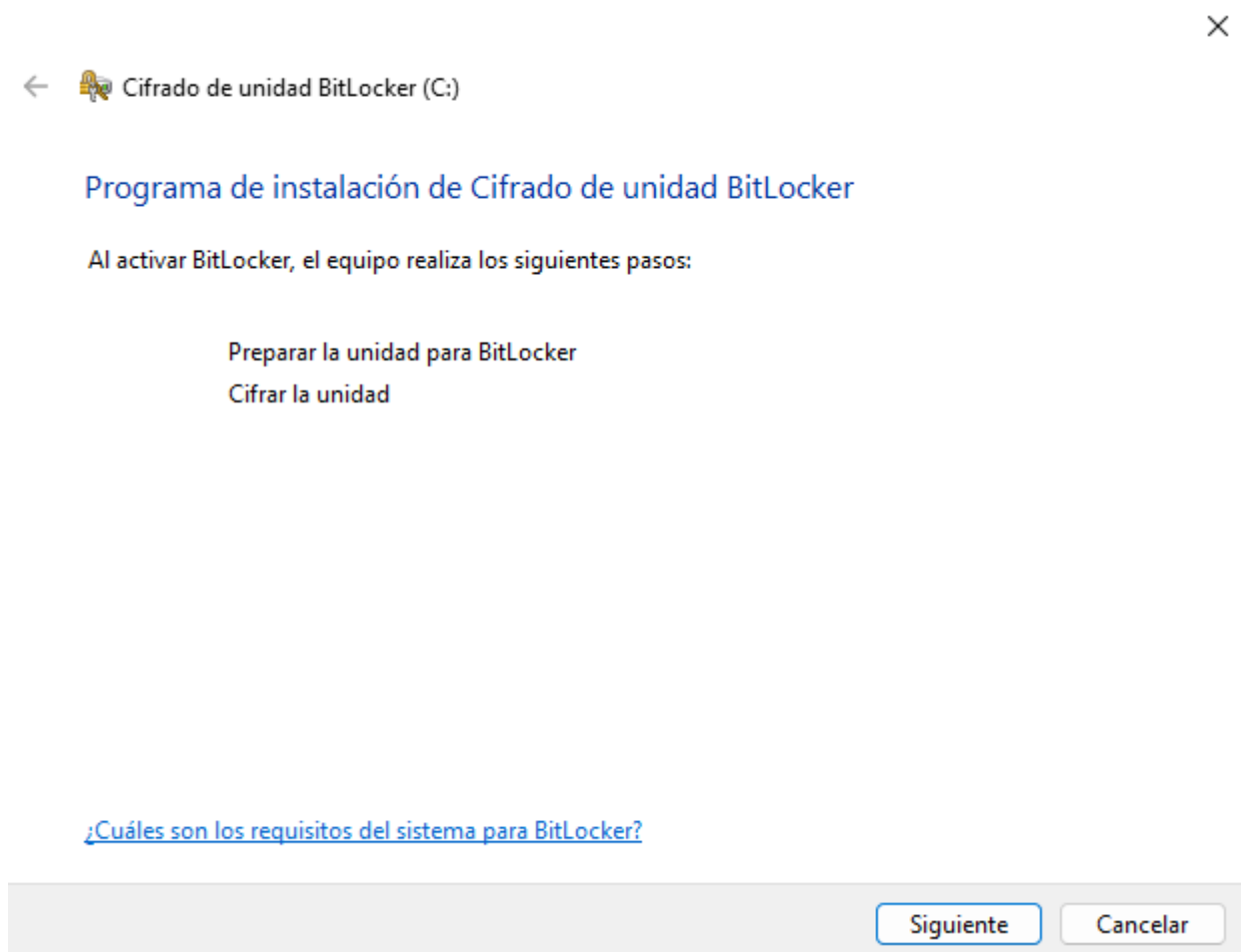
Una vez dentro de del administrador de cifrado de bitlocker se verá una ventana como esta:



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:




←  Cifrado de unidad BitLocker (C:)


Preparación de la unidad para BitLocker

Se usará una unidad existente o espacio disponible sin asignar en la unidad de disco duro para activar BitLocker.

▼ Detalles

Precaución:

 Se recomienda hacer una copia de seguridad de los archivos y datos imprescindibles antes de continuar.
[Usar el historial de archivos para realizar una copia de seguridad](#)


 Este proceso puede tardar unos minutos, según el tamaño y el contenido de la unidad.

Siguiente

Cancelar

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



←  Cifrado de unidad BitLocker (C:)

Programa de instalación de Cifrado de unidad BitLocker

✗ Ya no podrá usar el Entorno de recuperación de Windows a menos que se habilite manualmente y se mueva a la unidad del sistema.

Al activar BitLocker, el equipo realiza los siguientes pasos:

- ✓ Preparar la unidad para BitLocker
- Cifrar la unidad

[¿Cuáles son los requisitos del sistema para BitLocker?](#)

Siguiente

Cancelar

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



← Cifrado de unidad BitLocker (C:)

¿Cómo desea realizar la copia de seguridad de la clave de recuperación?

i El administrador del sistema administra ciertas configuraciones.

Se puede usar una clave de recuperación para acceder a los archivos y carpetas si tiene problemas para desbloquear su PC. Se recomienda tener más de una y conservarlas en un lugar seguro fuera de su PC.

→ Guardar en la cuenta Microsoft

→ Guardar en un archivo

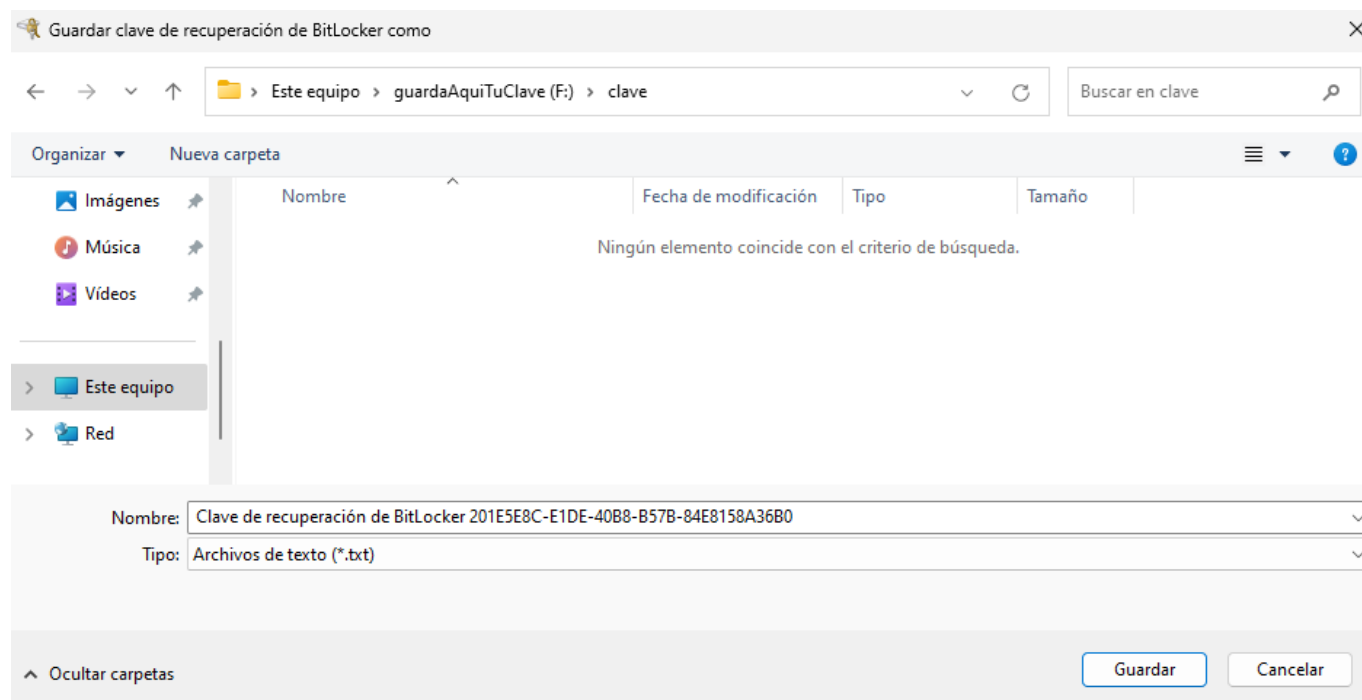
→ Imprimir la clave de recuperación

[¿Cómo puedo encontrar después mi clave de recuperación?](#)

Siguiente


Cancelar

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:



←  Cifrado de unidad BitLocker (C:)

Elegir qué cantidad de la unidad desea cifrar

Si está instalando BitLocker en una unidad nueva o un equipo nuevo, solo es necesario cifrar la parte de la unidad que se está usando actualmente. BitLocker cifrará los datos nuevos automáticamente conforme los agregue.

Si están instalando BitLocker en un equipo o una unidad que ya se está usando, entonces cifre la unidad completa. Al cifrar la unidad completa, se asegura de que todos los datos están protegidos, incluso datos que haya podido eliminar pero que aún puedan contener información recuperable.


- ☒ Cifrar solo el espacio en disco utilizado (mejor y más rápido para unidades y equipos nuevos)
- ☐ Cifrar la unidad entera (más lento, pero mejor para unidades y PCs que ya se encuentran en uso)

Siguiente

Cancelar

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



←  Cifrado de unidad BitLocker (C:)

Elección del modo de cifrado que se usará

La actualización de Windows 10 (versión 1511) introduce un nuevo modo de cifrado de disco (XTS-AES). Este modo ofrece soporte de integridad adicional, pero no es compatible con las versiones anteriores de Windows.

Si se trata de una unidad extraíble que usarás con una versión anterior de Windows, elige el modo Compatible.

Si es una unidad fija o si solo se utilizará en dispositivos con la actualización de Windows 10 (versión 1511) o versiones posteriores, elige el nuevo modo de cifrado.

- ☒ Modo de cifrado nuevo (recomendado para las unidades fijas en este dispositivo)
- ☐ Modo Compatible (recomendado para las unidades que se puedan mover de este dispositivo)

Siguiente

Cancelar

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



← Cifrado de unidad BitLocker (C:)

¿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.

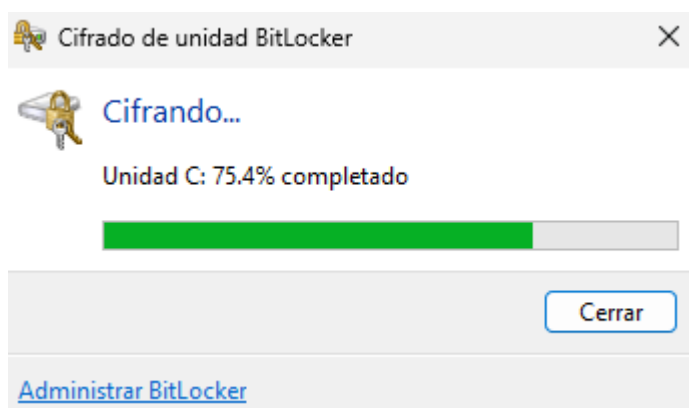
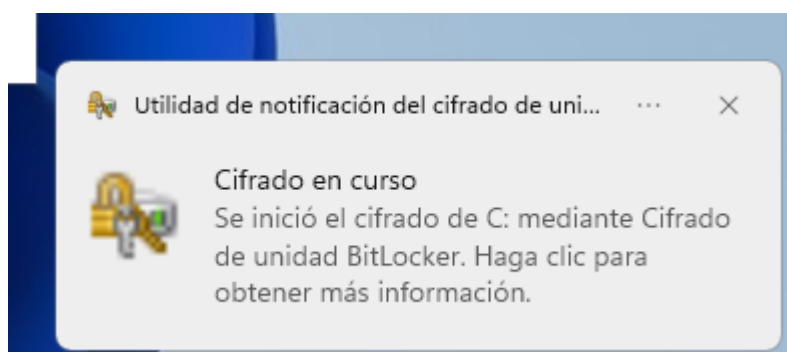
BitLocker reiniciará el equipo antes de iniciar el cifrado.

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

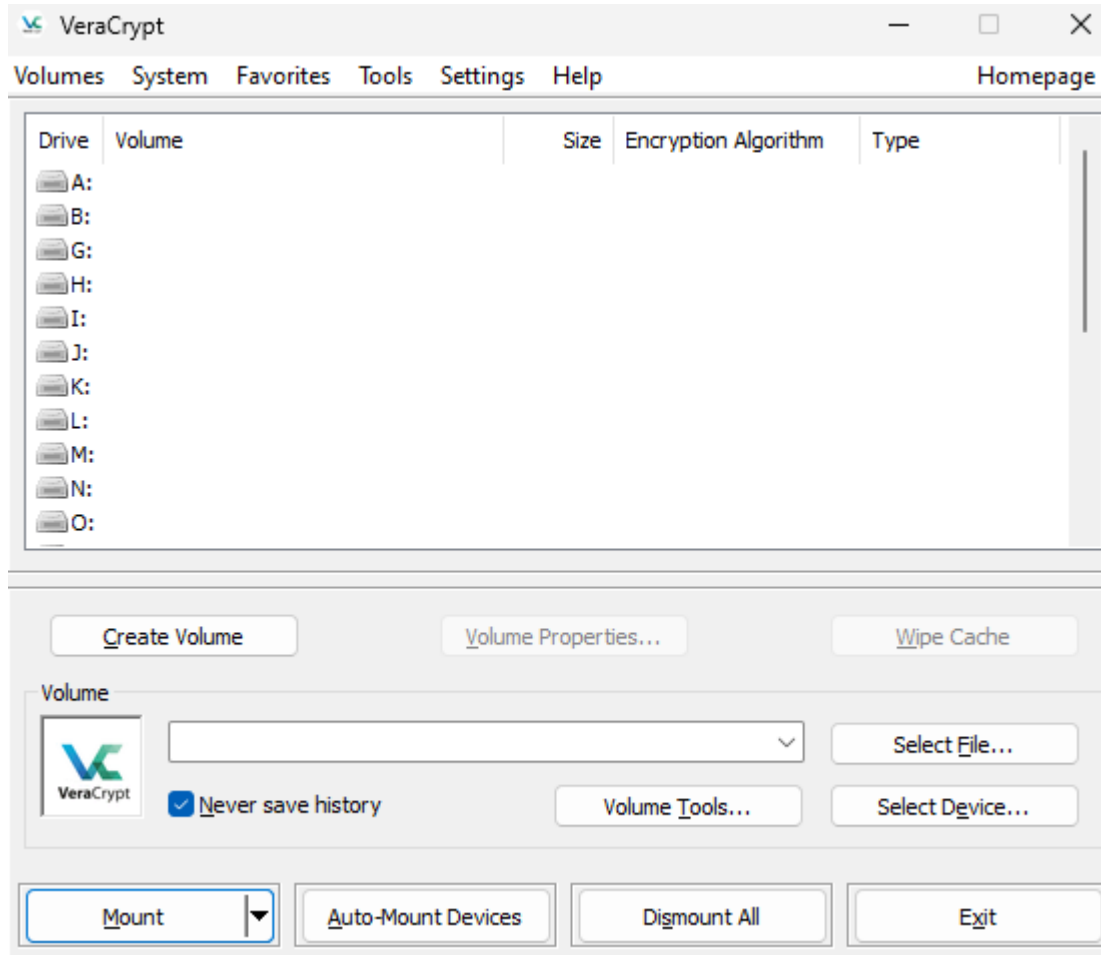
Cancelar

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

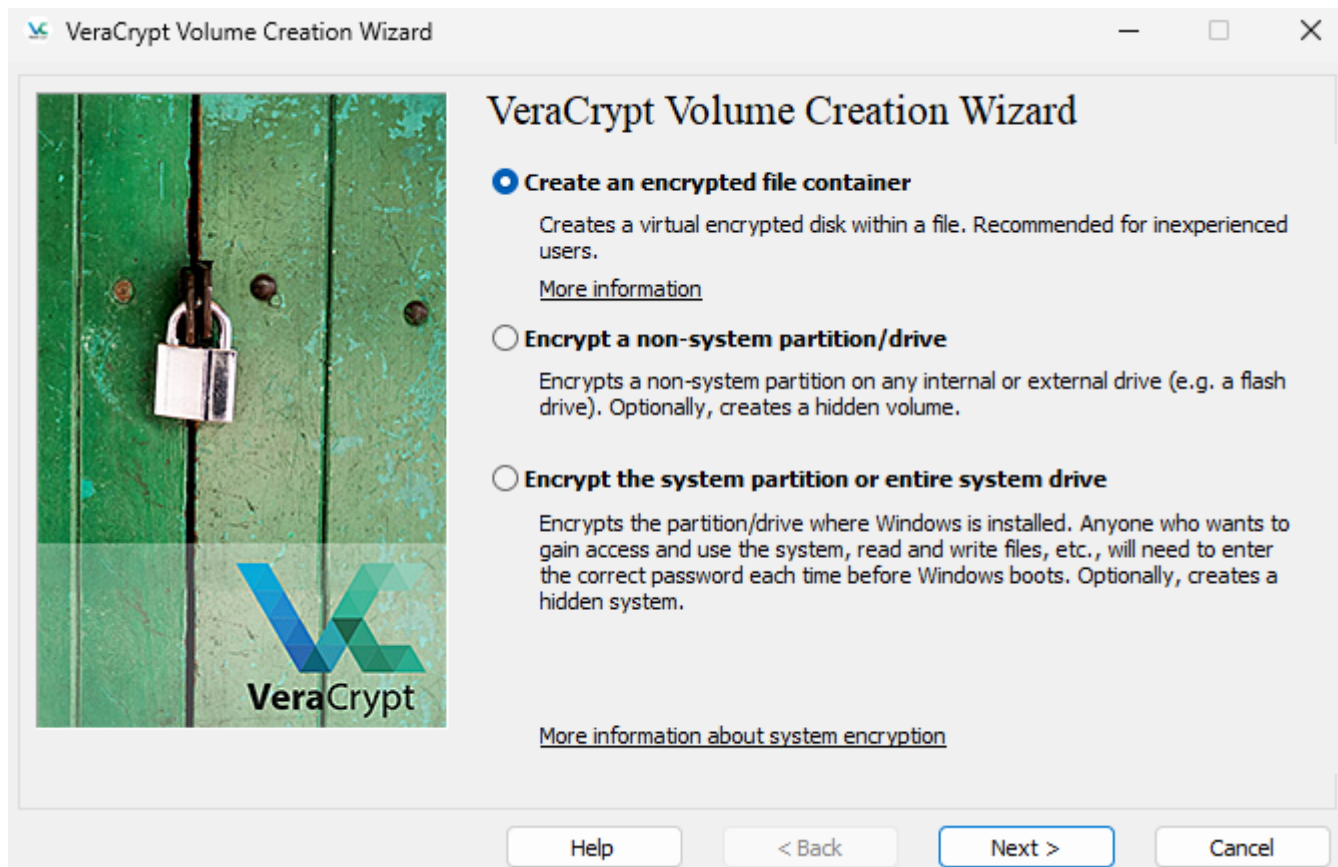


c) Usa Veracrypt para crear un contenedor cifrado para el usuario dentro de su perfil

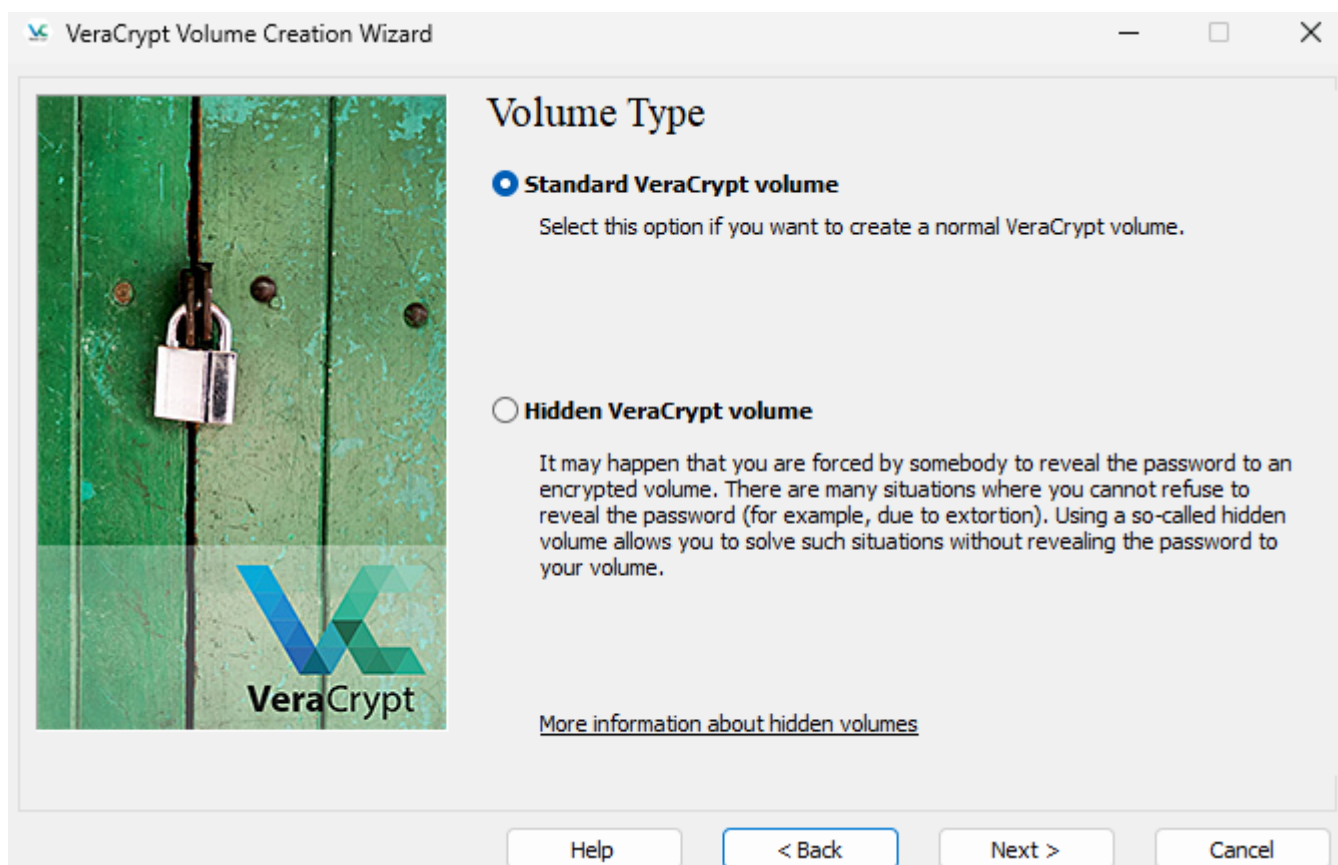
Para crear un contenedor cifrado primero debemos descargar e instalar veracrypt en nuestra máquina con windows 11. Tras eso se procede a abrir veracrypt:



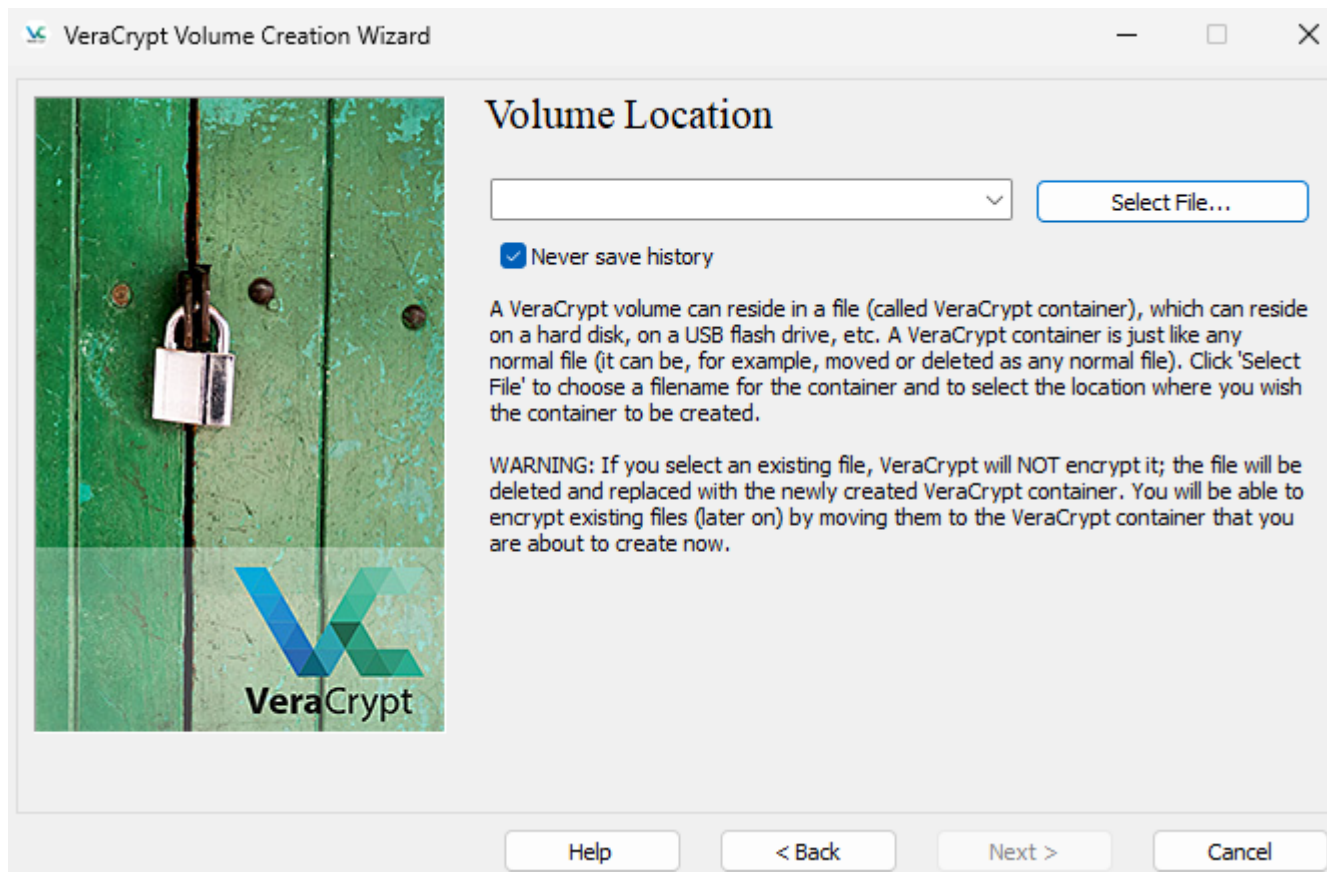
Lo primero que se debe hacer es presionar en “Create Volume”:



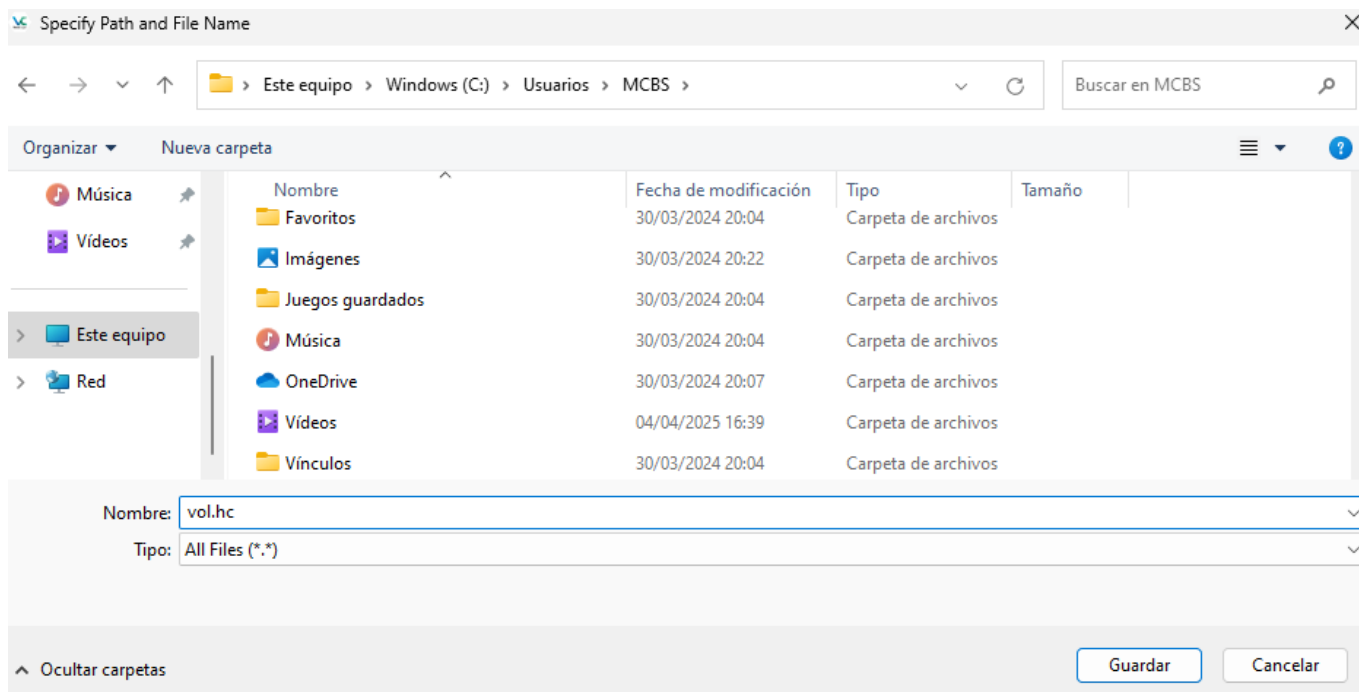
En la ventana que aparece seleccionamos "Create an encrypted container" y pulsamos en Next:



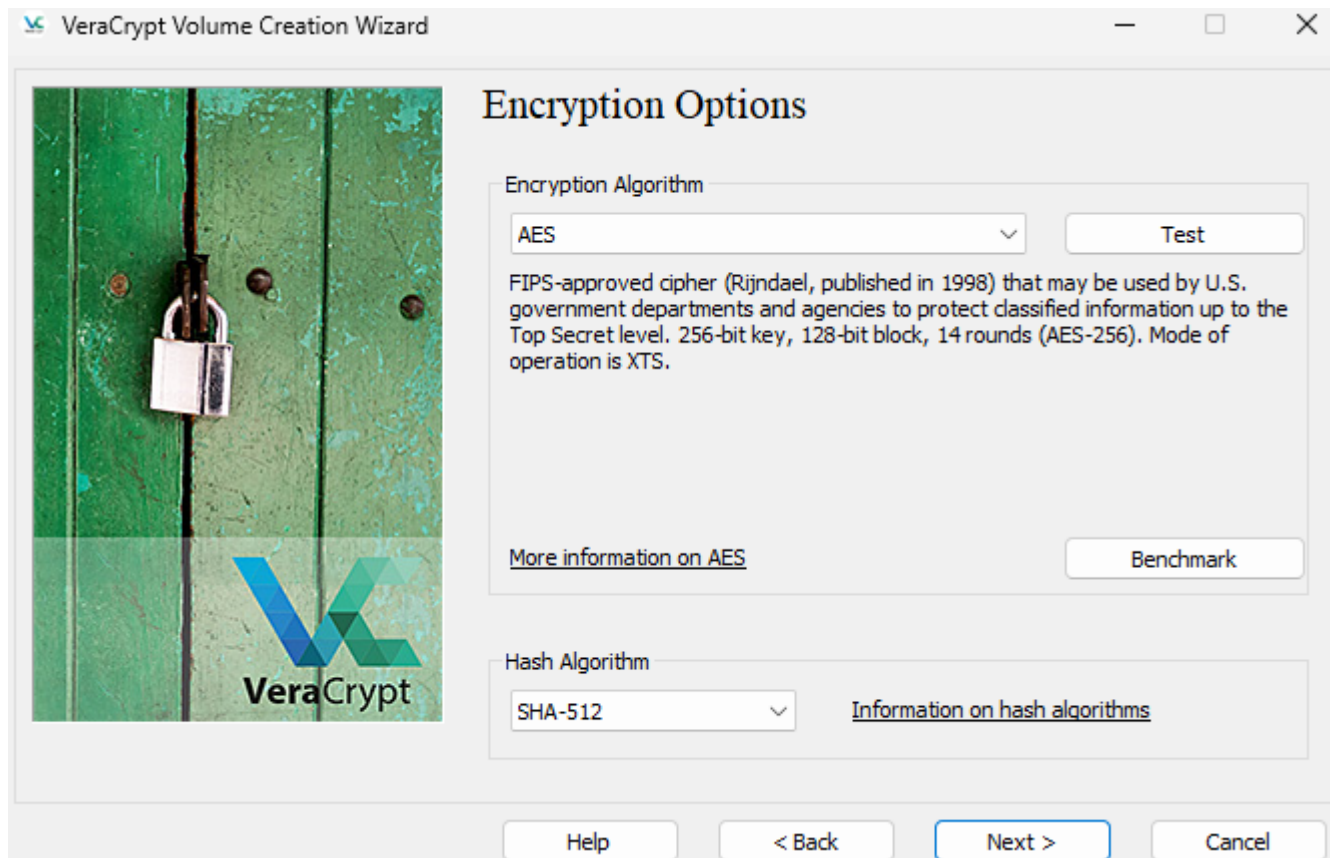
Seleccionamos Standard VeraCrypt Volume y le damos a next:



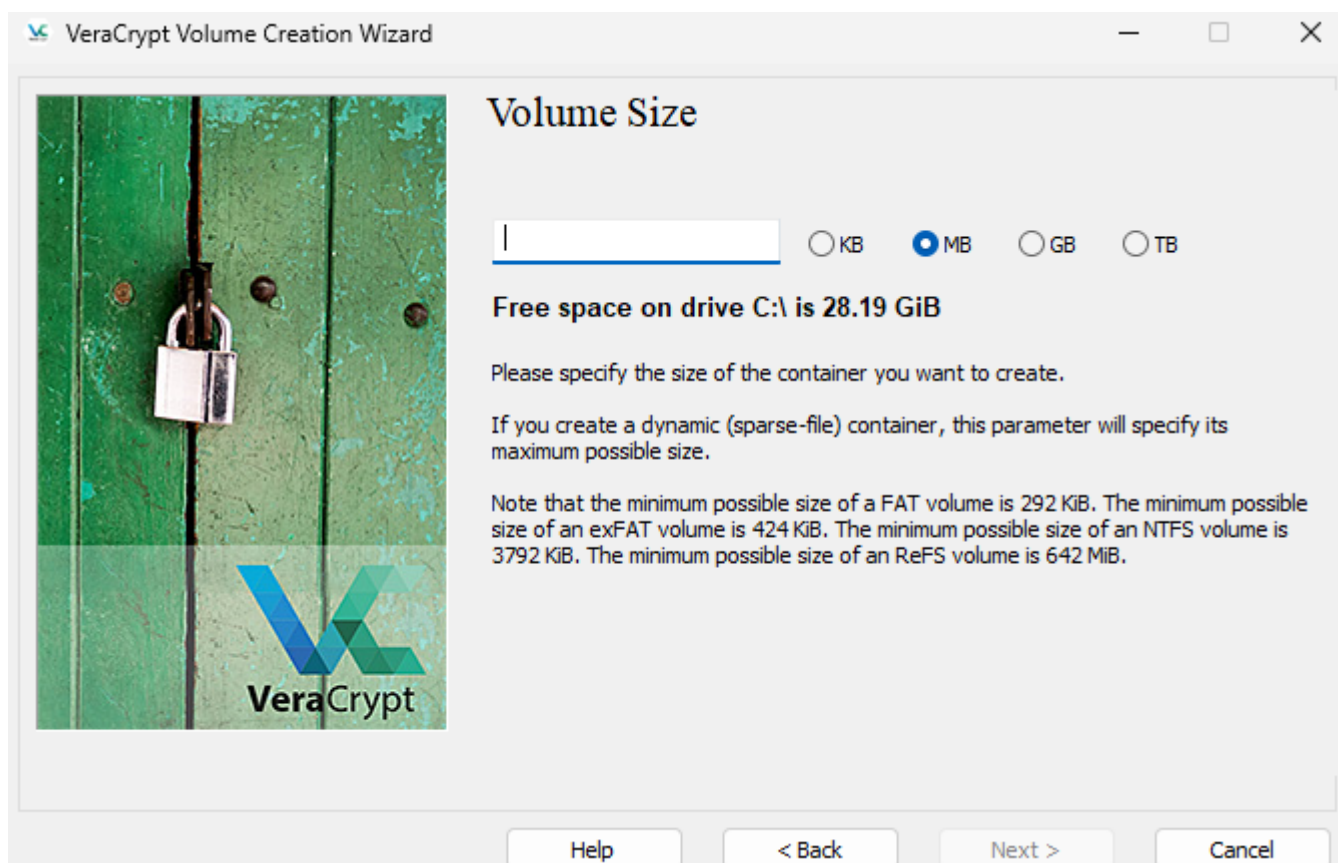
Para almacenar el volúmen seleccionamos la carpeta de nuestro usuario:



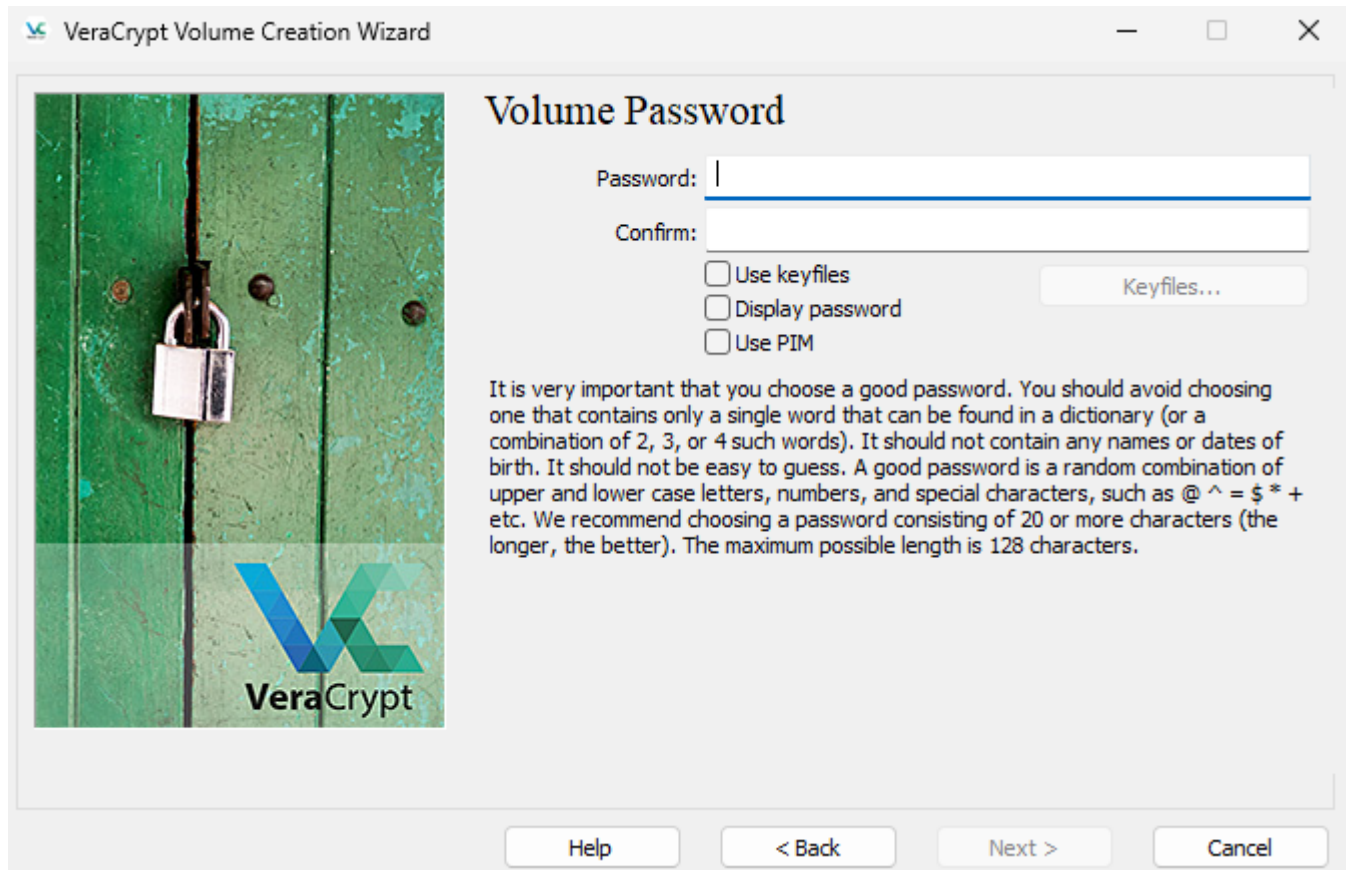
Una vez seleccionada la ubicación le damos a next:



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:



The screenshot shows the 'Volume Password' window of the VeraCrypt Volume Creation Wizard. On the left is a green wooden door with a silver padlock and the VeraCrypt logo. The main area contains the title 'Volume Password', two input fields for 'Password' and 'Confirm', and three checkboxes: 'Use keyfiles', 'Display password', and 'Use PIM'. A 'Keyfiles...' button is next to the 'Use keyfiles' checkbox. Below these is a paragraph of advice on choosing a strong password. At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

Volume Password

Password:

Confirm:

☐ Use keyfiles Keyfiles...

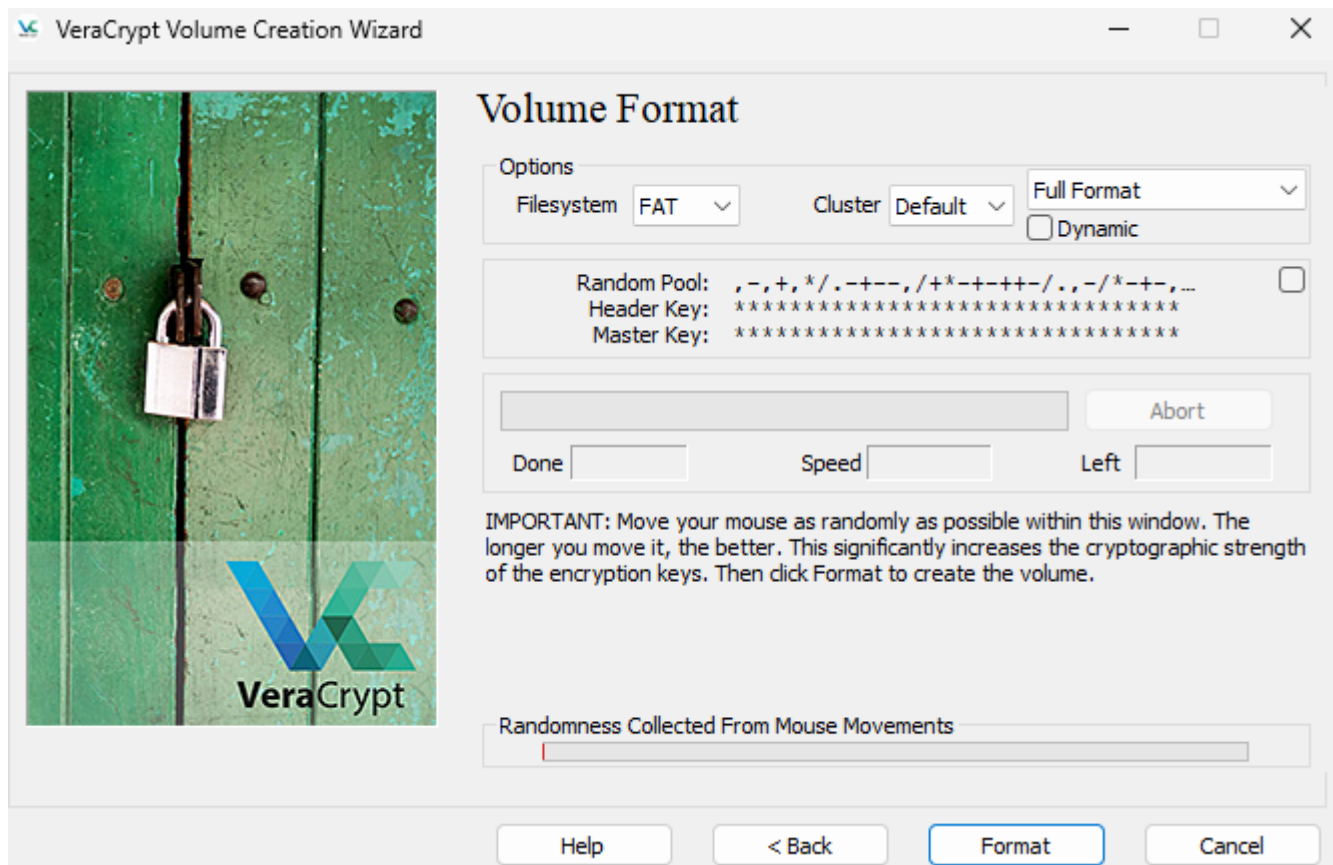
☐ Display password

☐ Use PIM

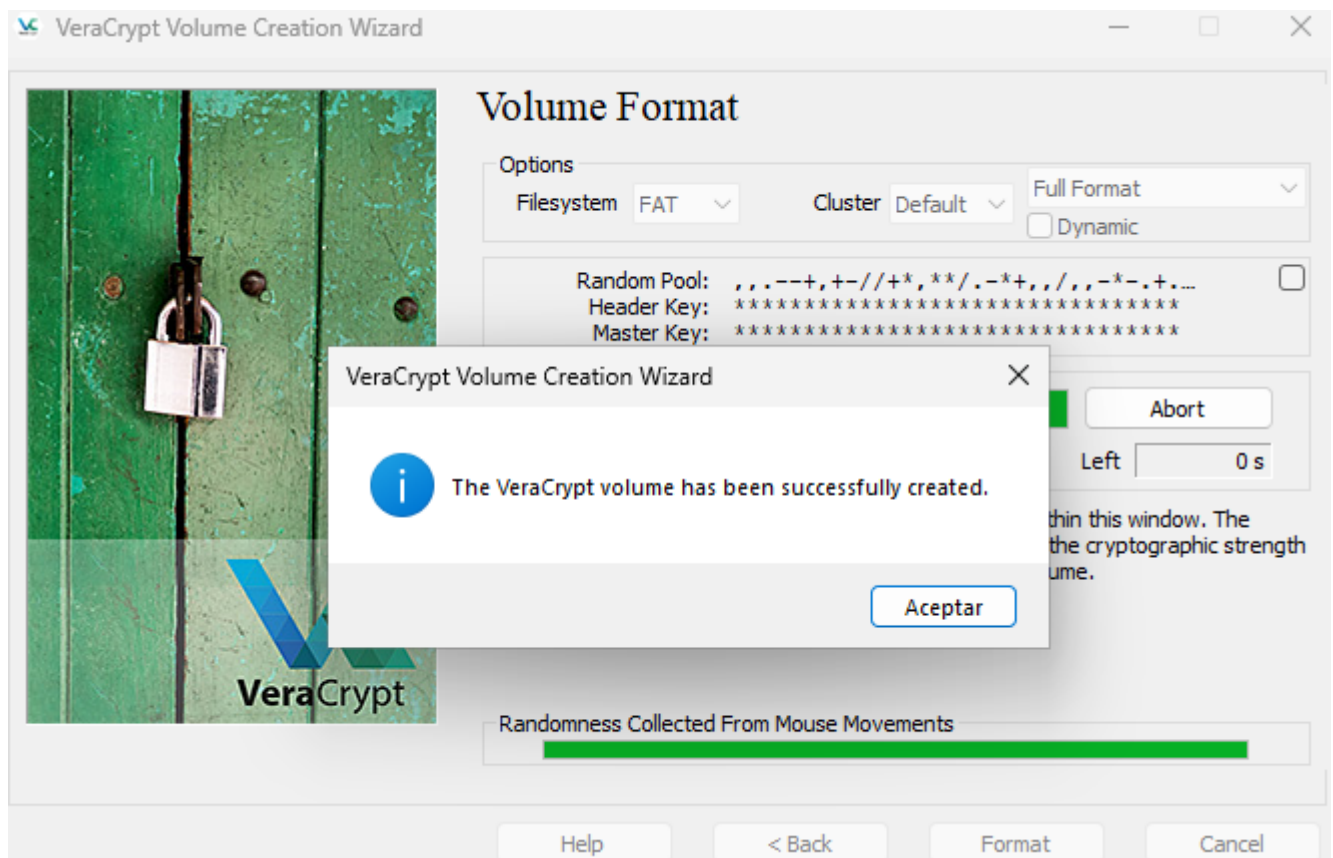
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

Help < Back Next > Cancel

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

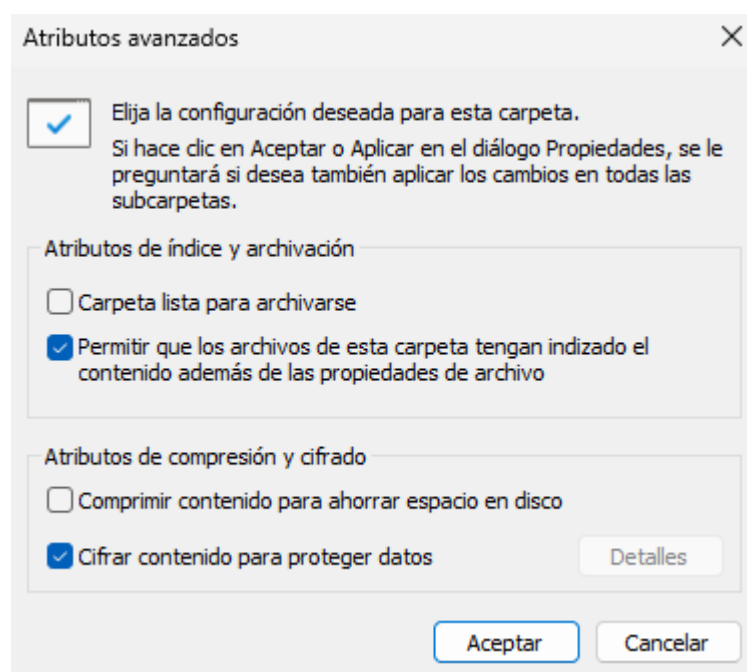
Para realizar un cifrado EFS de una carpeta debemos abrir el CMD como administrador y escribir el siguiente comando:

```
fsutil behavior set disableencryption 0
```

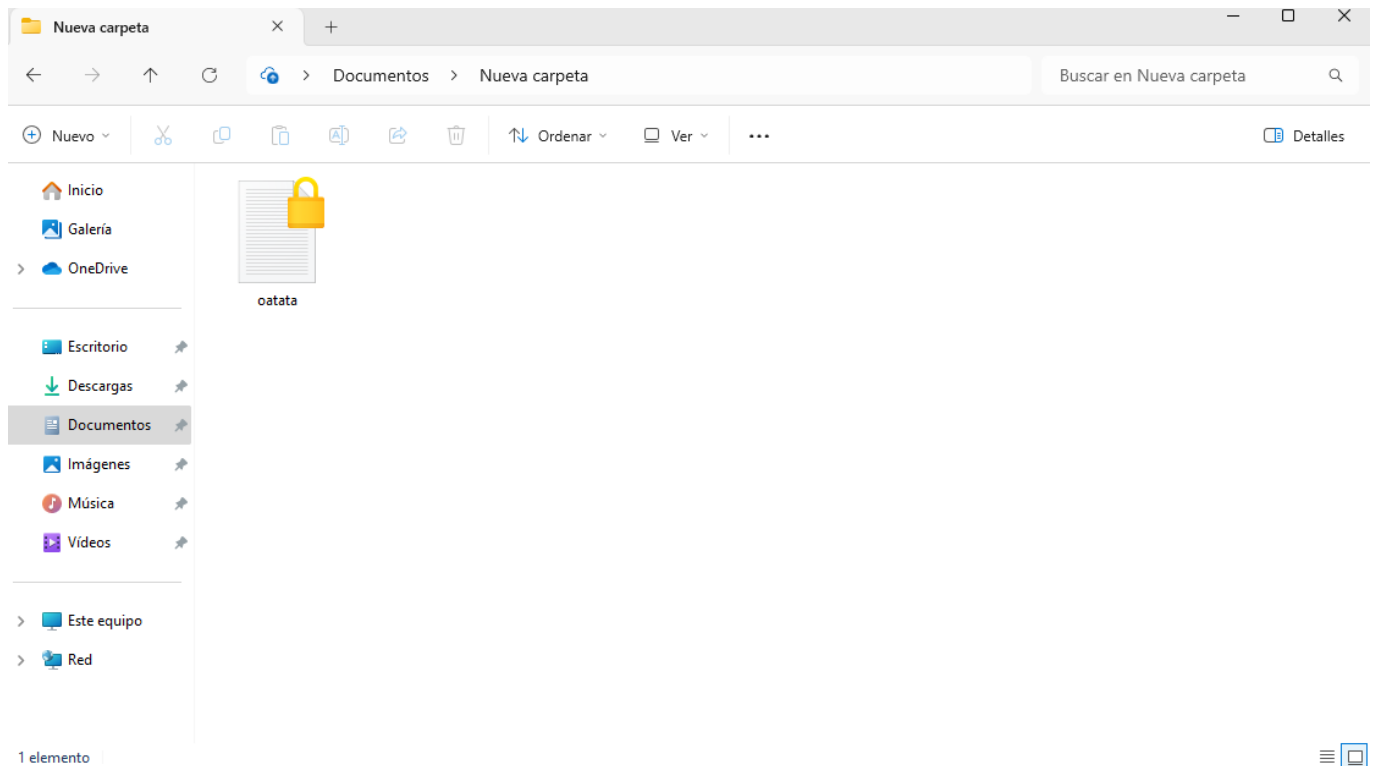
```
C:\Users\MCBS\Documents\Nueva carpeta>fsutil behavior set disableencryption 0
DisableEncryption = 0 (El cifrado está HABILITADO)

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

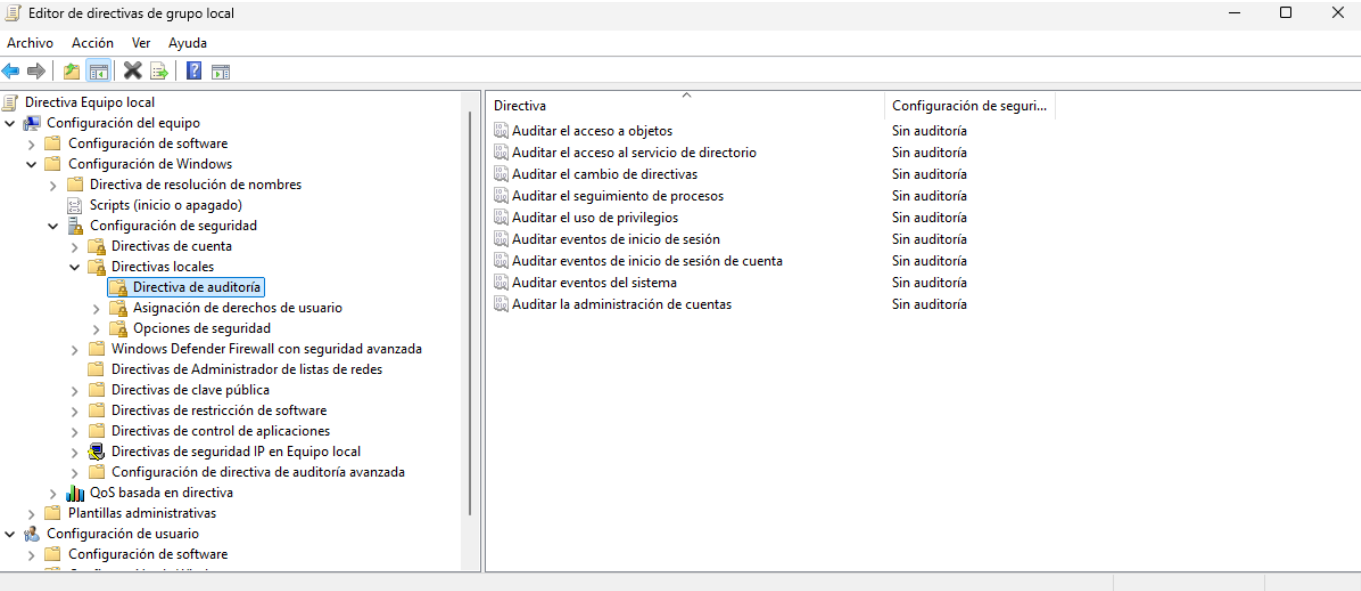
iii. ¿Podrían acceder varios usuarios al mismo fichero/carpeta compartida y crifrada? ¿Cual sería el procedimiento?

Si, pero para ello habría que ir de nuevo a las propiedades, 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.

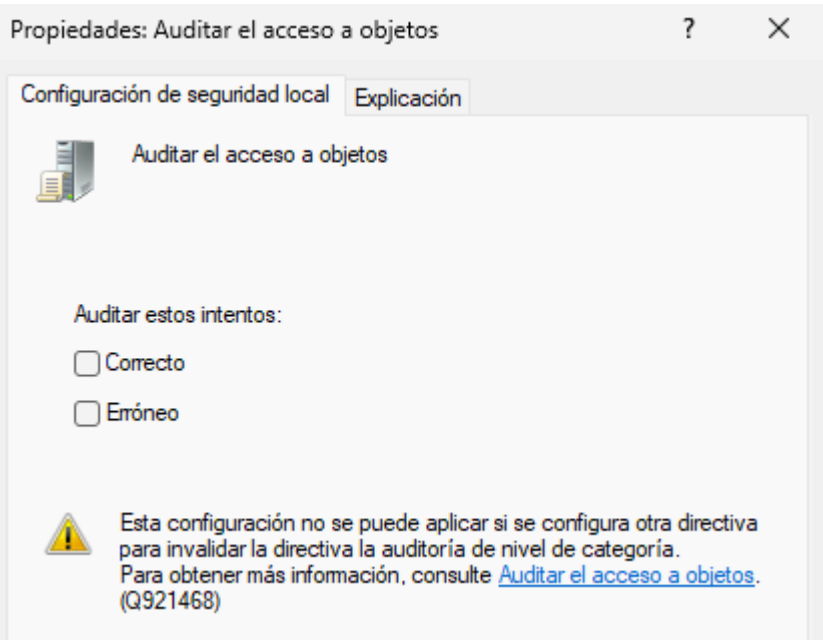
2. Auditoría del sistema

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 obeitos:

- 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”:

Visor de eventos

ArchivoAcciónVerAyuda

Visor de eventos (local)

Vistas personalizadas

Registros de Windows

Aplicación

Seguridad

Instalación

Sistema

Eventos reinviados

Registros de aplicaciones y s

Suscripciones

| Seguridad Número de eventos: 23.071 (1) Nuevos eventos disponibles | | | | |
|---|---------------------|---------------------------|----------------|------------------------------|
| Palabras clave | Fecha y hora | Origen | Id. del evento | Categoría de la tarea |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:32 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Auditoría correcta | 22/04/2025 16:48:26 | Microsoft Windows secu... | 5158 | Filtering Platform Connec... |
| Auditoría correcta | 22/04/2025 16:48:26 | Microsoft Windows secu... | 5158 | Filtering Platform Connec... |
| Auditoría correcta | 22/04/2025 16:48:26 | Microsoft Windows secu... | 4689 | Process Termination |
| Error de auditoría | 22/04/2025 16:48:26 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Auditoría correcta | 22/04/2025 16:48:26 | Microsoft Windows secu... | 4688 | Process Creation |
| Auditoría correcta | 22/04/2025 16:48:26 | Microsoft Windows secu... | 4670 | Authorization Policy Cha... |
| Auditoría correcta | 22/04/2025 16:48:26 | Microsoft Windows secu... | 4670 | Authorization Policy Cha... |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:24 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |
| Error de auditoría | 22/04/2025 16:48:20 | Microsoft Windows secu... | 4673 | Sensitive Privilege Use |

Evento 4673, Microsoft Windows security auditing.

General

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

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

Last update:

2025/04/22 14:49

