

[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:

Configuración	Estado	Comentario
Unidades de datos extraibles	No configurada	No
Unidades de datos fijas	No configurada	No
Unidades del sistema operativo	No configurada	No
Almacenar información de recuperación de BitLocker en los Servicios de dominio de Active Direc...	No configurada	No
Elegir carpeta predeterminada para la contraseña de recuperación	No configurada	No
Elegir cómo pueden los usuarios recuperar unidades protegidas por BitLocker (Windows Server 2...	No configurada	No
Deshabilitar nuevos dispositivos DMA cuando este equipo está bloqueado	No configurada	No
Elegir método de cifrado e intensidad de cifrado de unidad (Windows 8, Windows Server 2012, Wi...	No configurada	No
Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y posterio...	No configurada	No
Elegir método de cifrado e intensidad de cifrado de unidad (Windows Vista, Windows Server 2008...	No configurada	No
Proporcionar los identificadores únicos de su organización	No configurada	No
Impedir la sobreescritura de memoria al reiniciar	No configurada	No
Validar cumplimiento de regla de uso de certificado de tarjeta inteligente	No configurada	No

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

No configurada Comentario:

Habilitada

Deshabilitada Compatible con:

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.

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 Comentario:

Habilitada

Deshabilitada Compatible con: Windows Server 2008 y Windows Vista

Opciones: Ayuda:

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

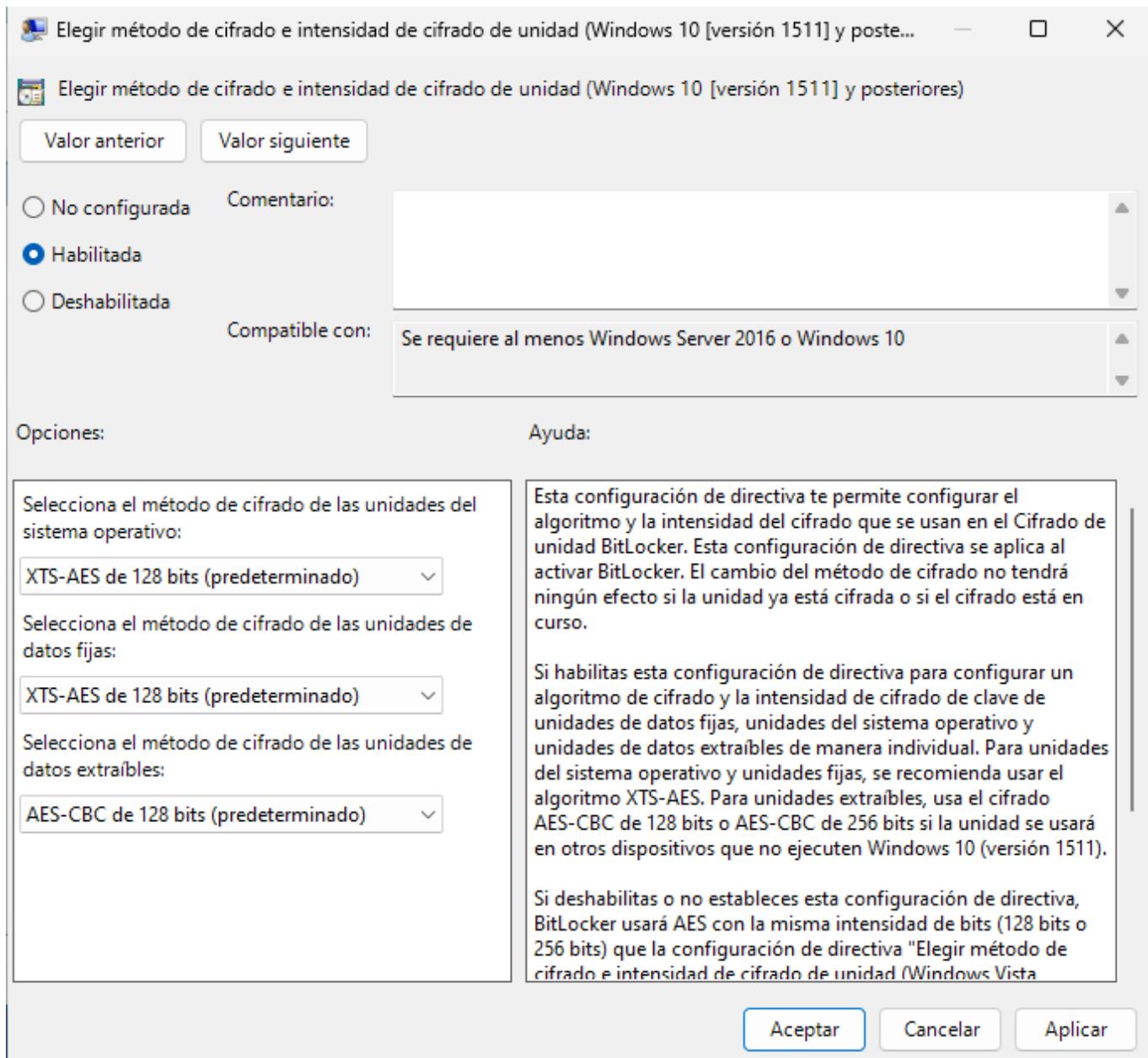
Esta configuración de directiva permite administrar la copia de seguridad de los Servicios de dominio de Active Directory (AD DS) de la información de recuperación del Cifrado de unidad BitLocker. Esto proporciona un método administrativo de recuperación de datos cifrados por BitLocker con el fin de 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

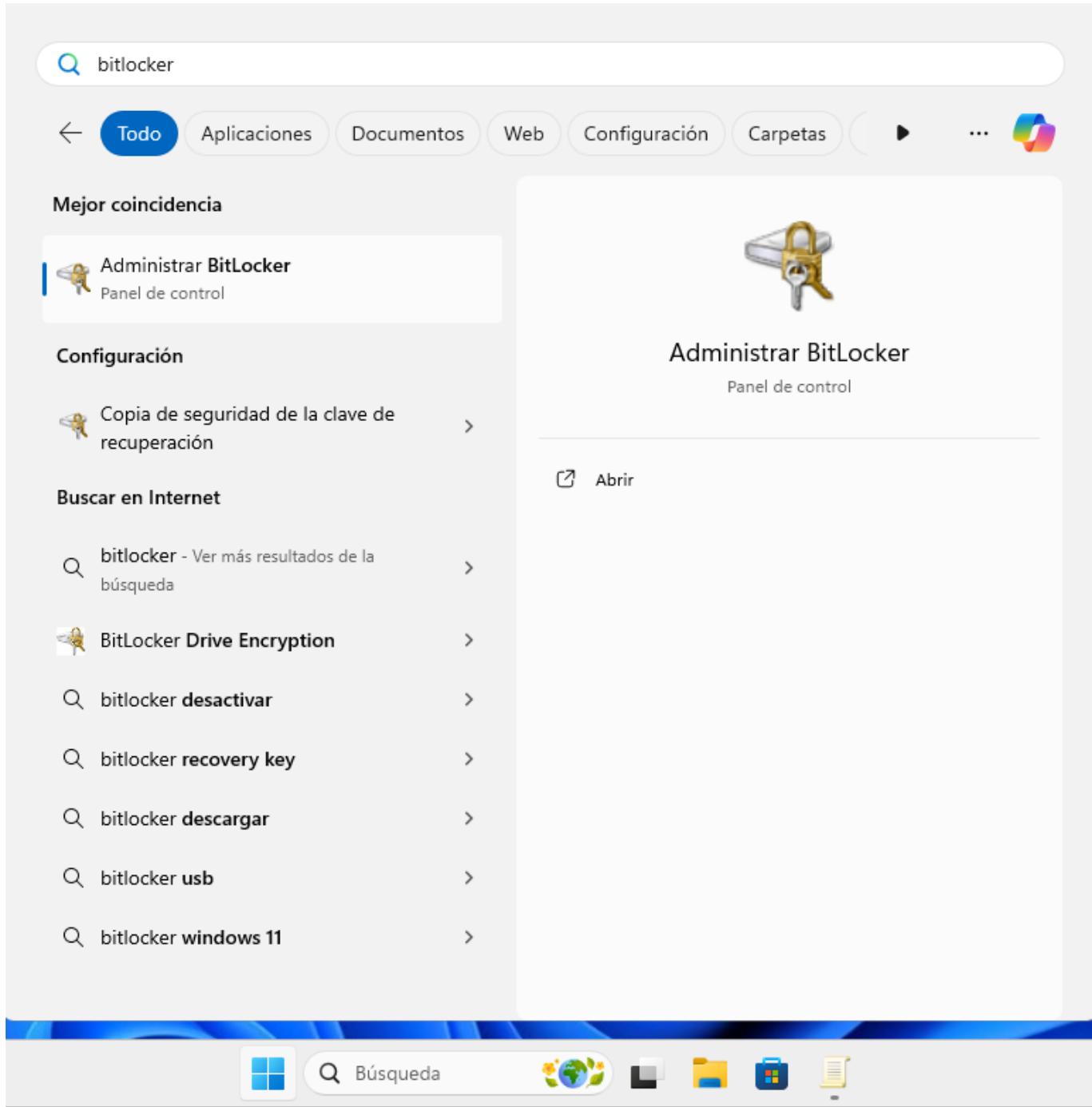
Para mejorar el cifrado podemos modificar la política de “Elegir método de cifrado e intensidad de cifrado de unidad” para sistemas de Windows 10 en adelante:



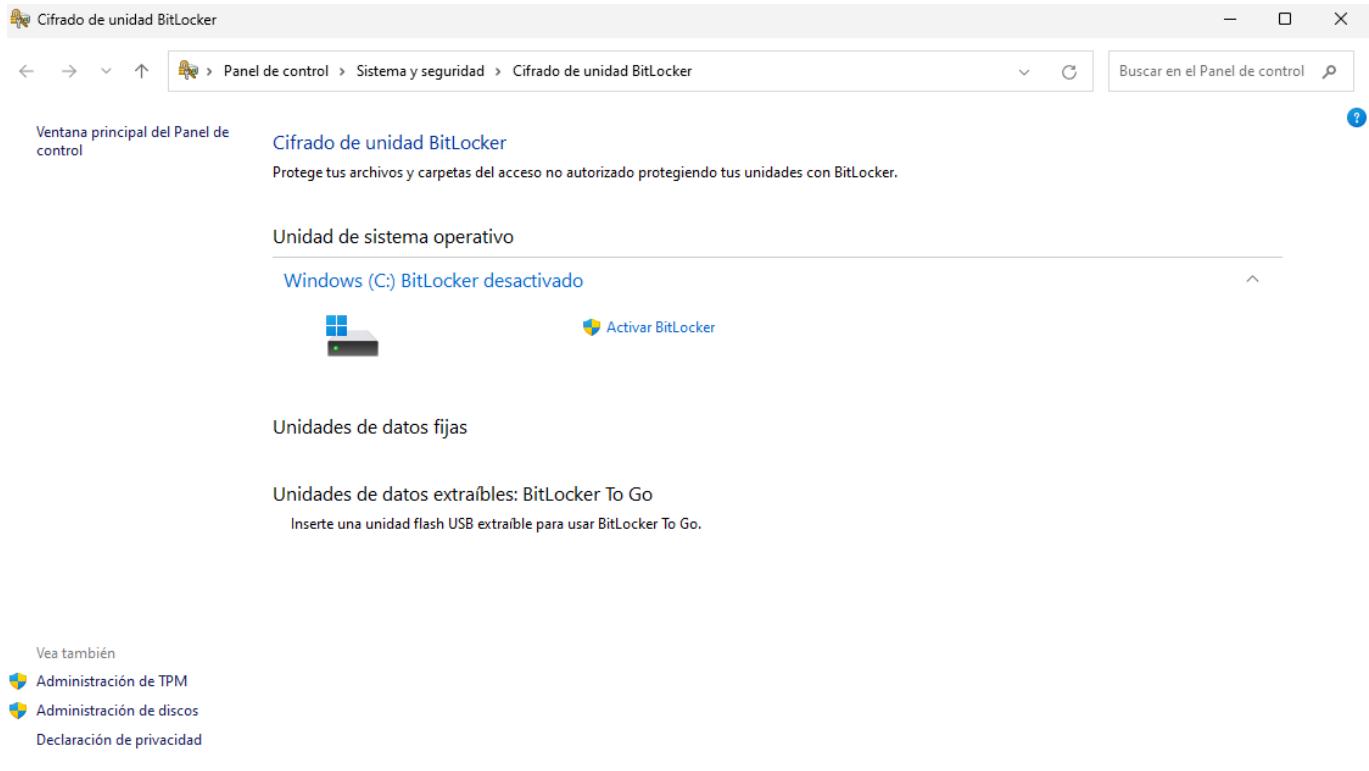
b) Realiza la activación de cifrado Bitlocker sobre C:\

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:

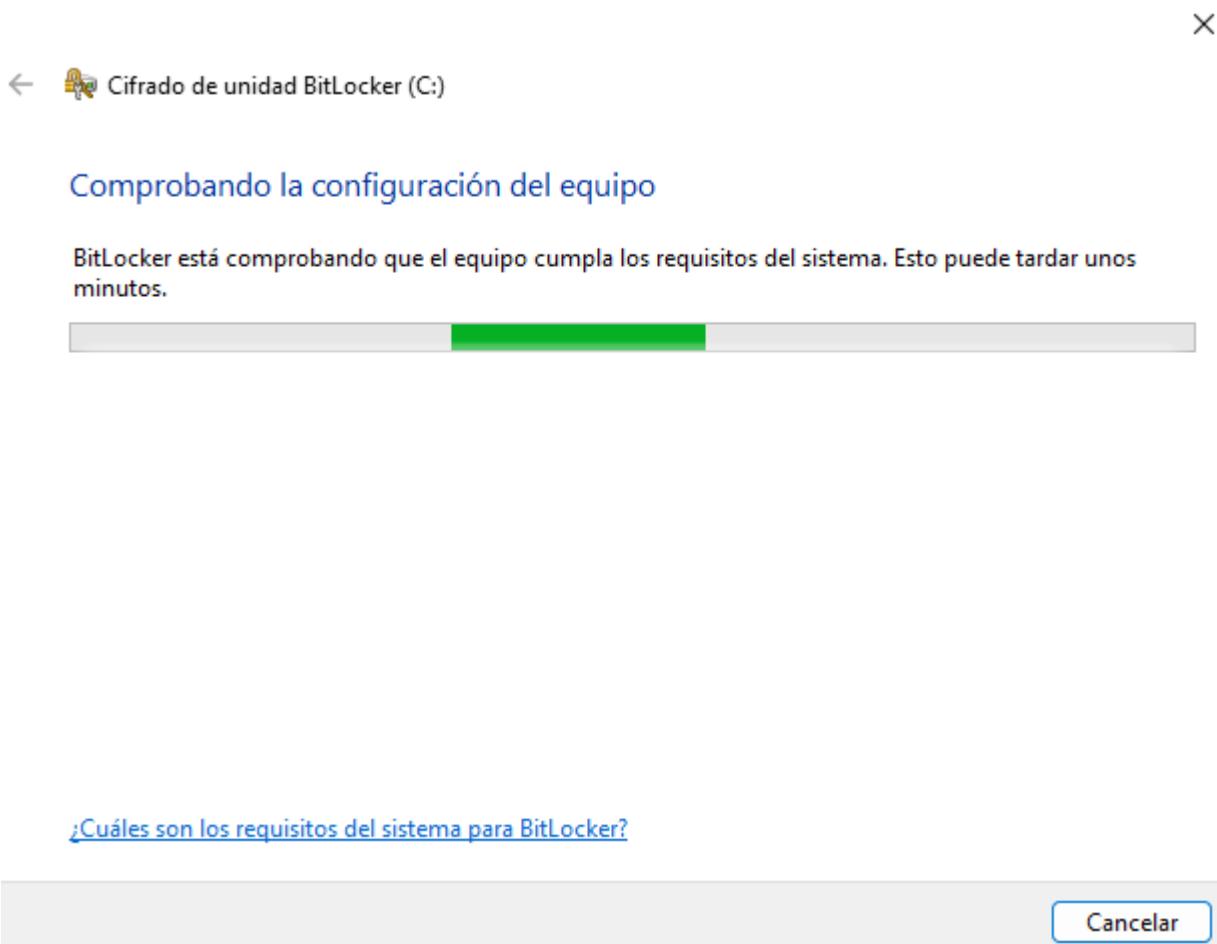


Una vez dentro de del administrador de cifrado de bitlocker se verá una ventana como esta:



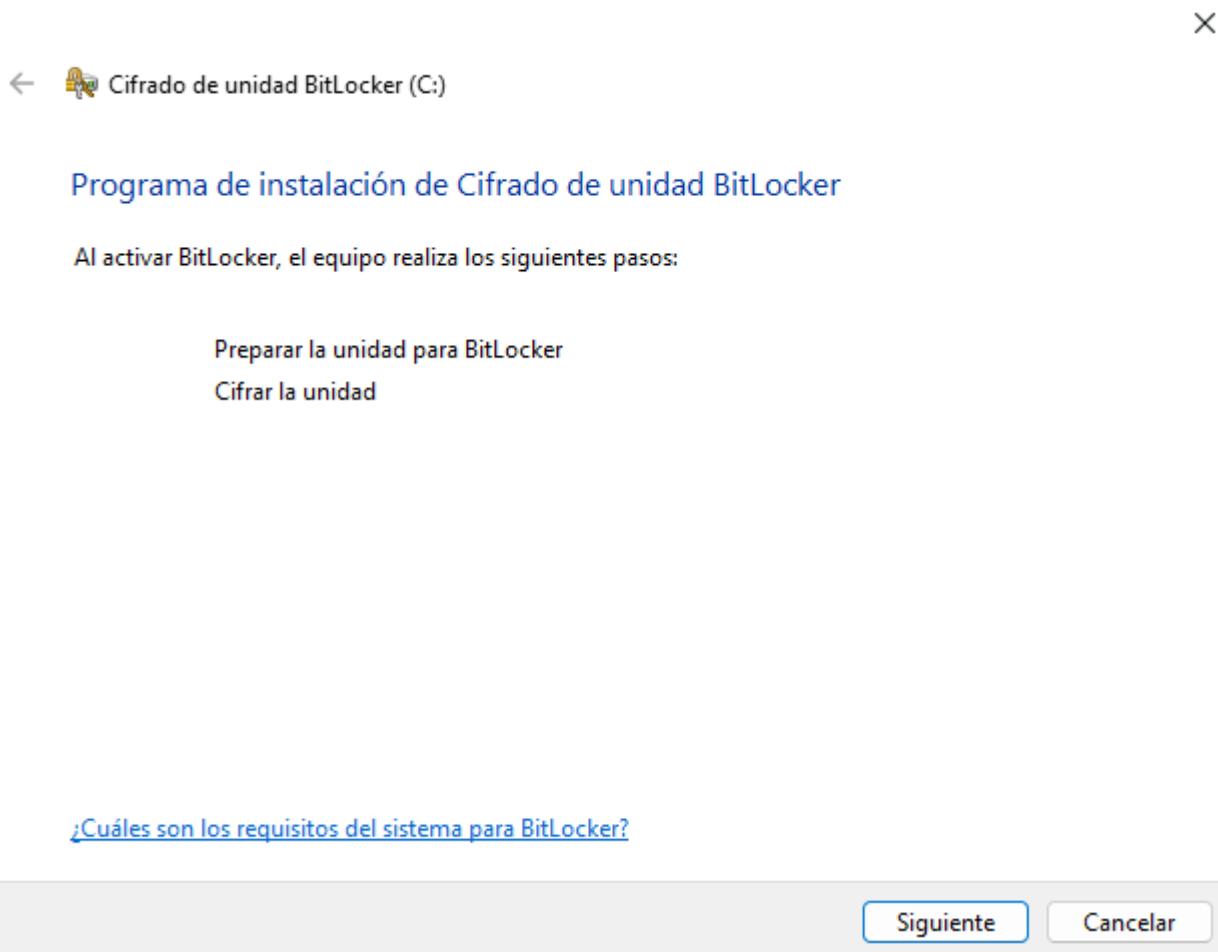
The screenshot shows the 'Cifrado de unidad BitLocker' (BitLocker Drive Encryption) page in the Windows Control Panel. At the top, there's a breadcrumb navigation: 'Panel de control > Sistema y seguridad > Cifrado de unidad BitLocker'. Below the title 'Cifrado de unidad BitLocker' and a subtitle 'Protege tus archivos y carpetas del acceso no autorizado protegiendo tus unidades con BitLocker.', there's a section for 'Unidad de sistema operativo' (Operating System Volume) labeled 'Windows (C:) BitLocker desactivado' (BitLocker disabled). It shows a small icon of a drive and a 'Activar BitLocker' (Enable BitLocker) button. Below this, there's a section for 'Unidades de datos fijas' (Fixed Data Drives) and 'Unidades de datos extraíbles: BitLocker To Go' (Removable Data Drives: BitLocker To Go), with a note to insert a USB drive. At the bottom, there's a 'Vea también' (See also) section with links to 'Administración de TPM', 'Administración de discos', and 'Declaración de privacidad'.

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



The screenshot shows a progress dialog box for BitLocker setup. The title bar says 'Cifrado de unidad BitLocker (C:)'. The main text says 'Comprobando la configuración del equipo' (Checking the system configuration) and 'BitLocker está comprobando que el equipo cumpla los requisitos del sistema. Esto puede tardar unos minutos.' (BitLocker is checking that the computer meets the system requirements. This may take a few minutes.). A progress bar is shown, with a significant portion filled in green. At the bottom, there's a link '¿Cuáles son los requisitos del sistema para BitLocker?' (What are the system requirements for BitLocker?) and a 'Cancelar' (Cancel) button.

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:

X

←  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:

X

←  Cifrado de unidad BitLocker (C:)

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

 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**

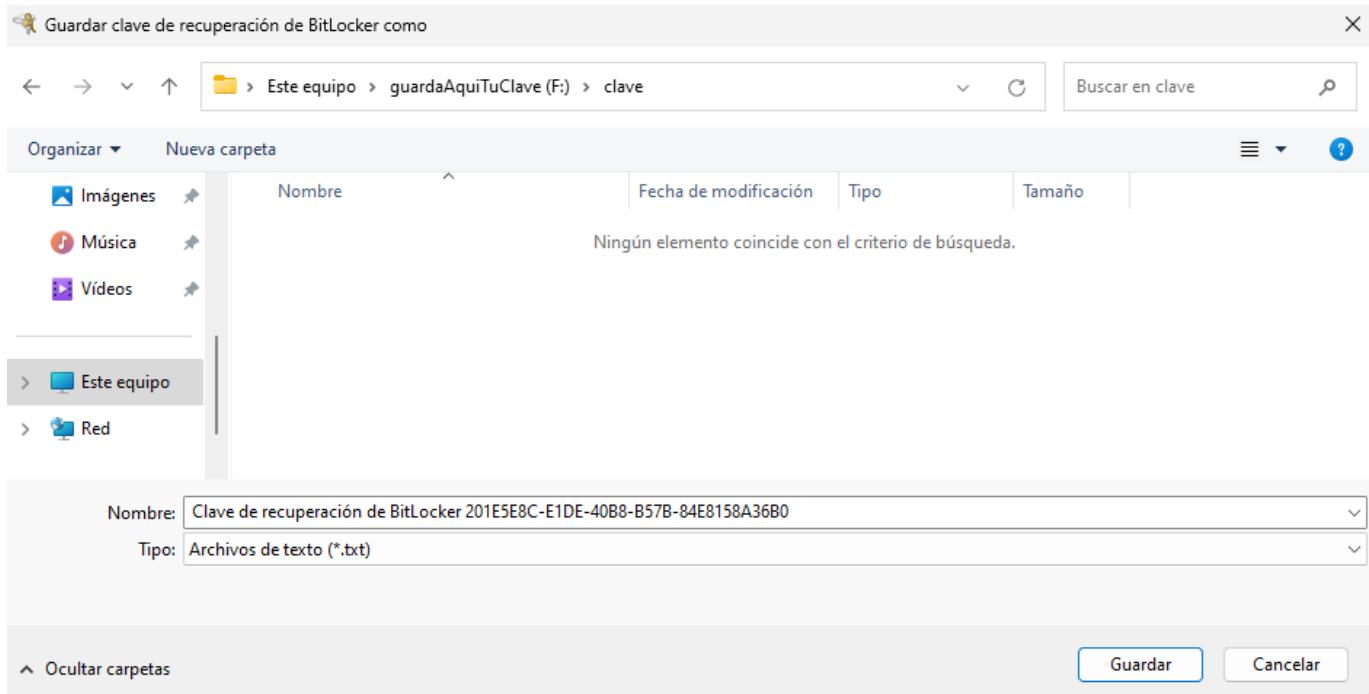
→ **Imprimir la clave de recuperación**

¿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:

X

 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:

X

←  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.

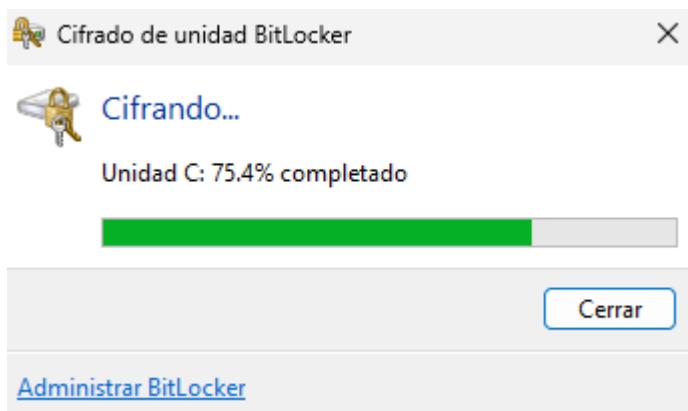
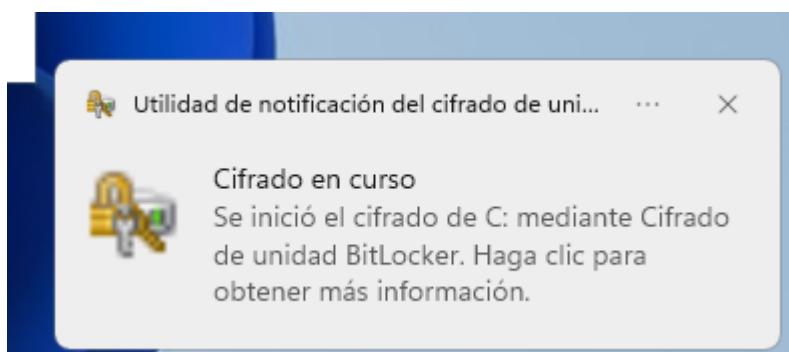
BitLocker reiniciará el equipo antes de iniciar el cifrado.

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

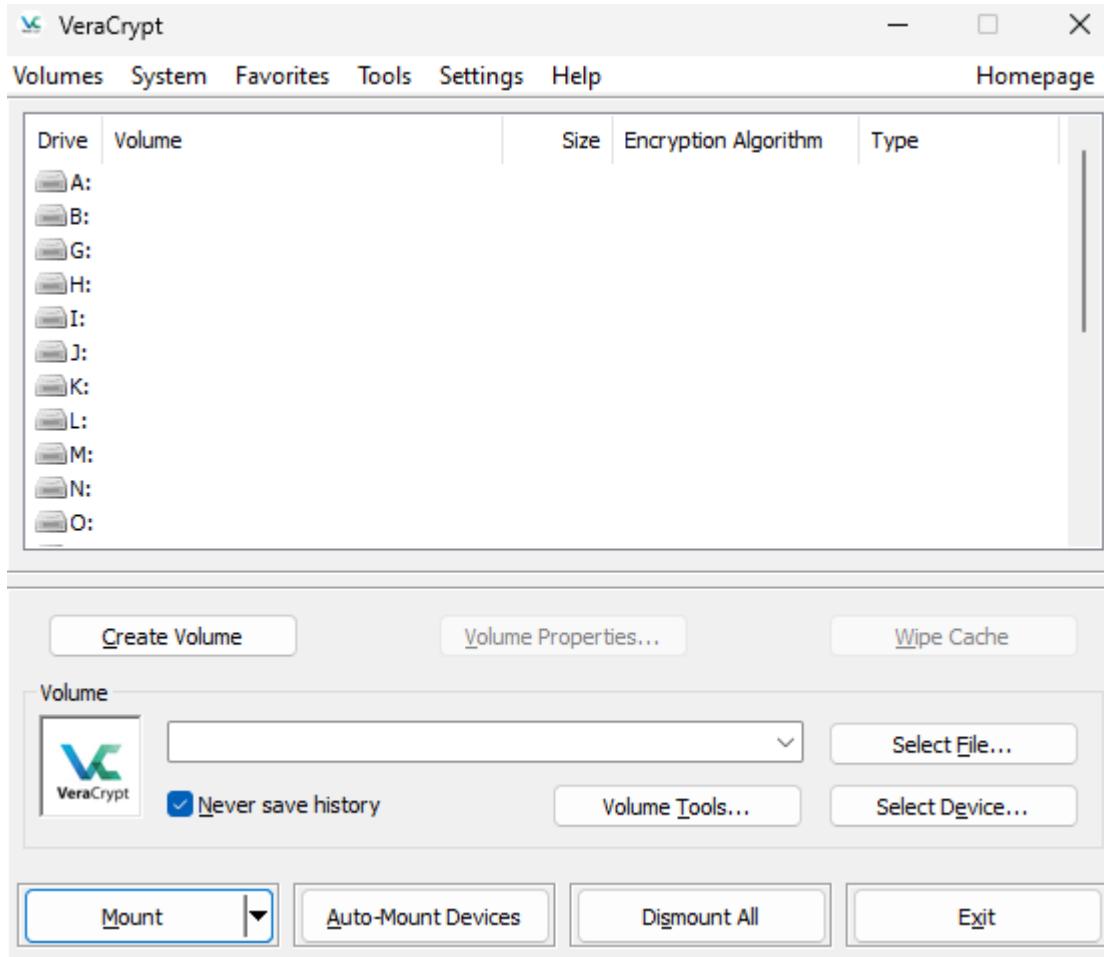
Cancelar

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

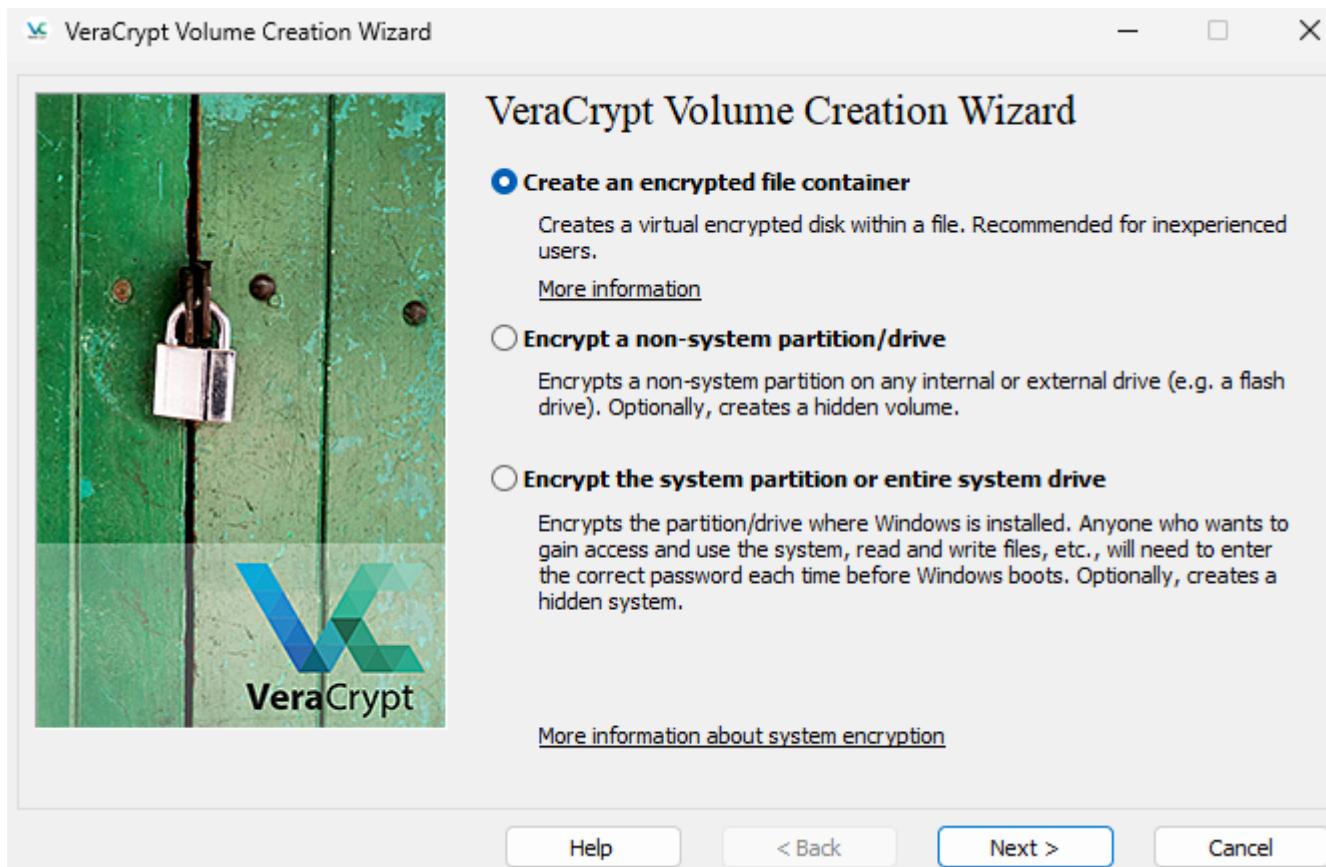


c) Usa Veracrypt para crear un contenedor cifrado para el usuario dentro de su perfil

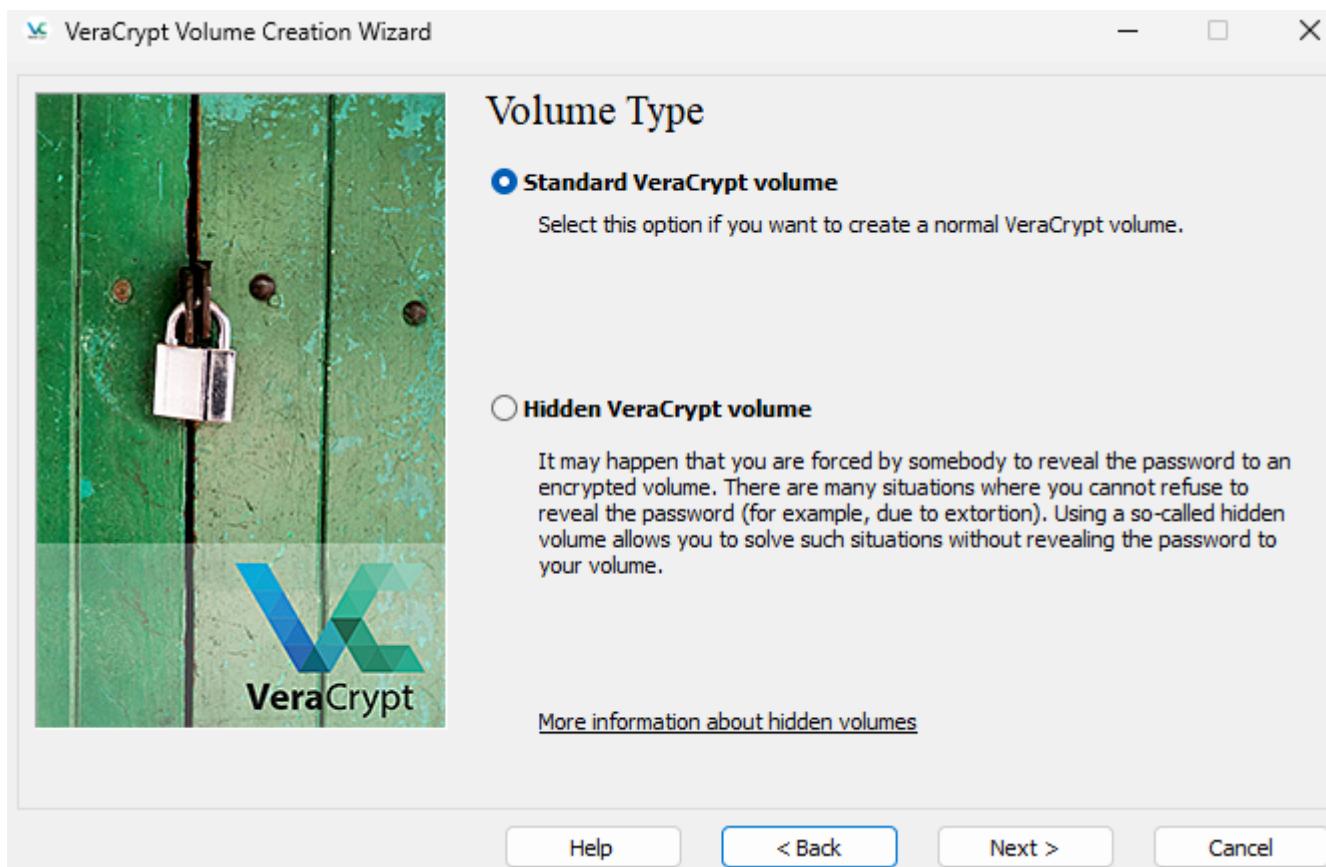
Para crear un contenedor cifrado primero debemos descargar e instalar veracrypt en nuestra máquina con windows 11. Tras eso se procede a abrir veracrypt:



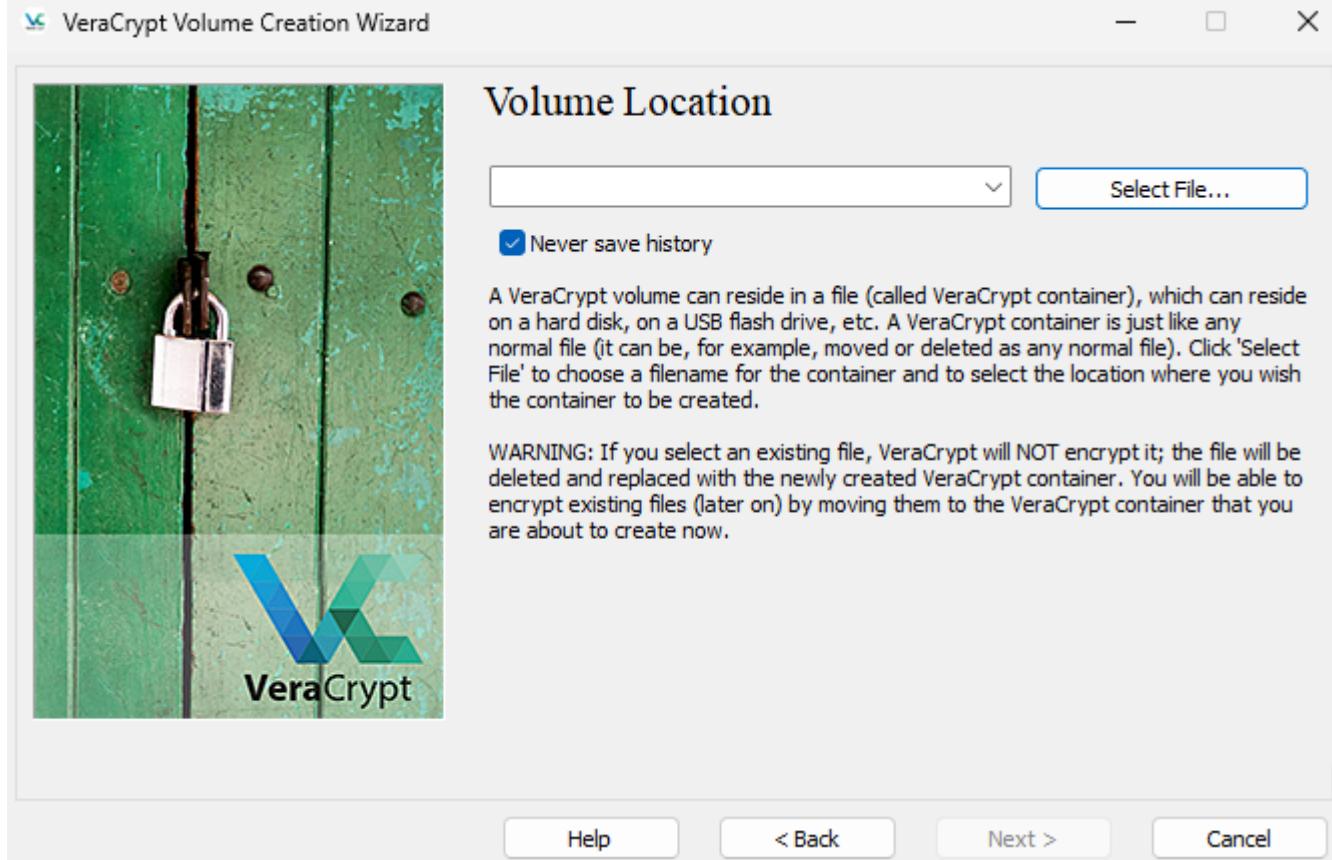
Lo primero que se debe hacer es presionar en “Create Volume”:



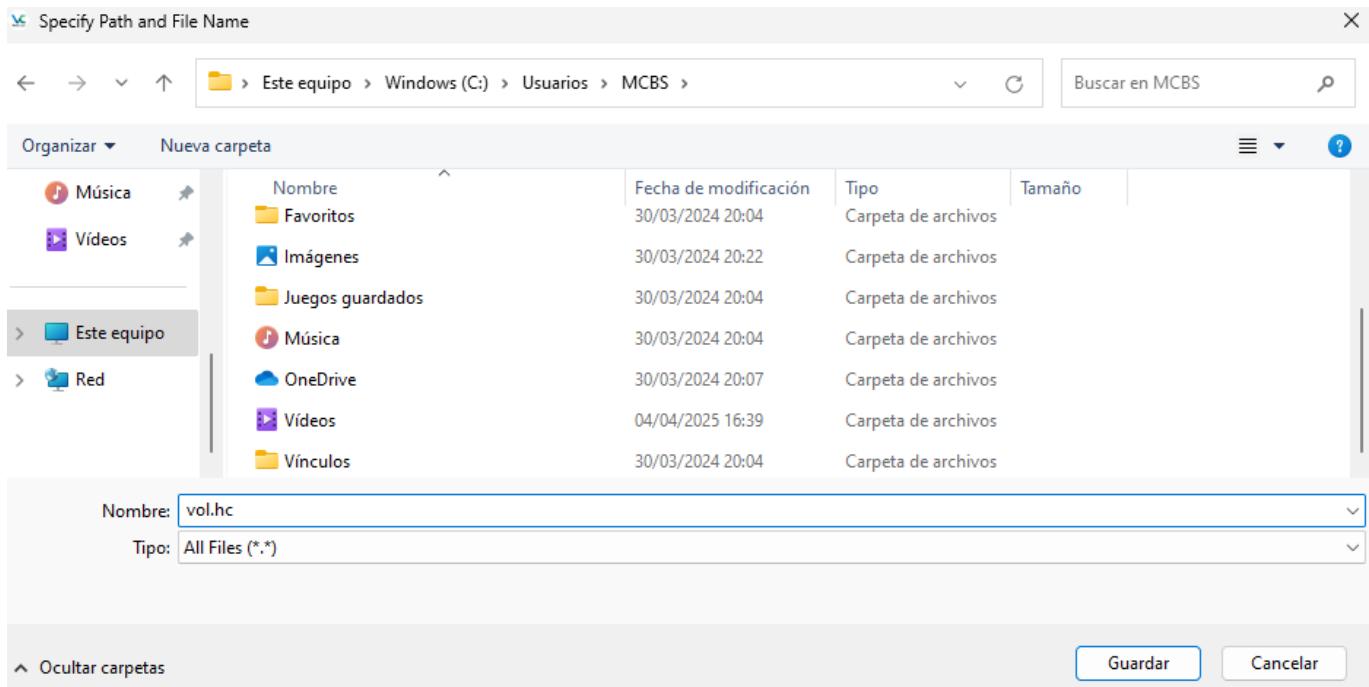
En la ventana que aparece seleccionamos “Create an encrypted container” y pulsamos en Next:



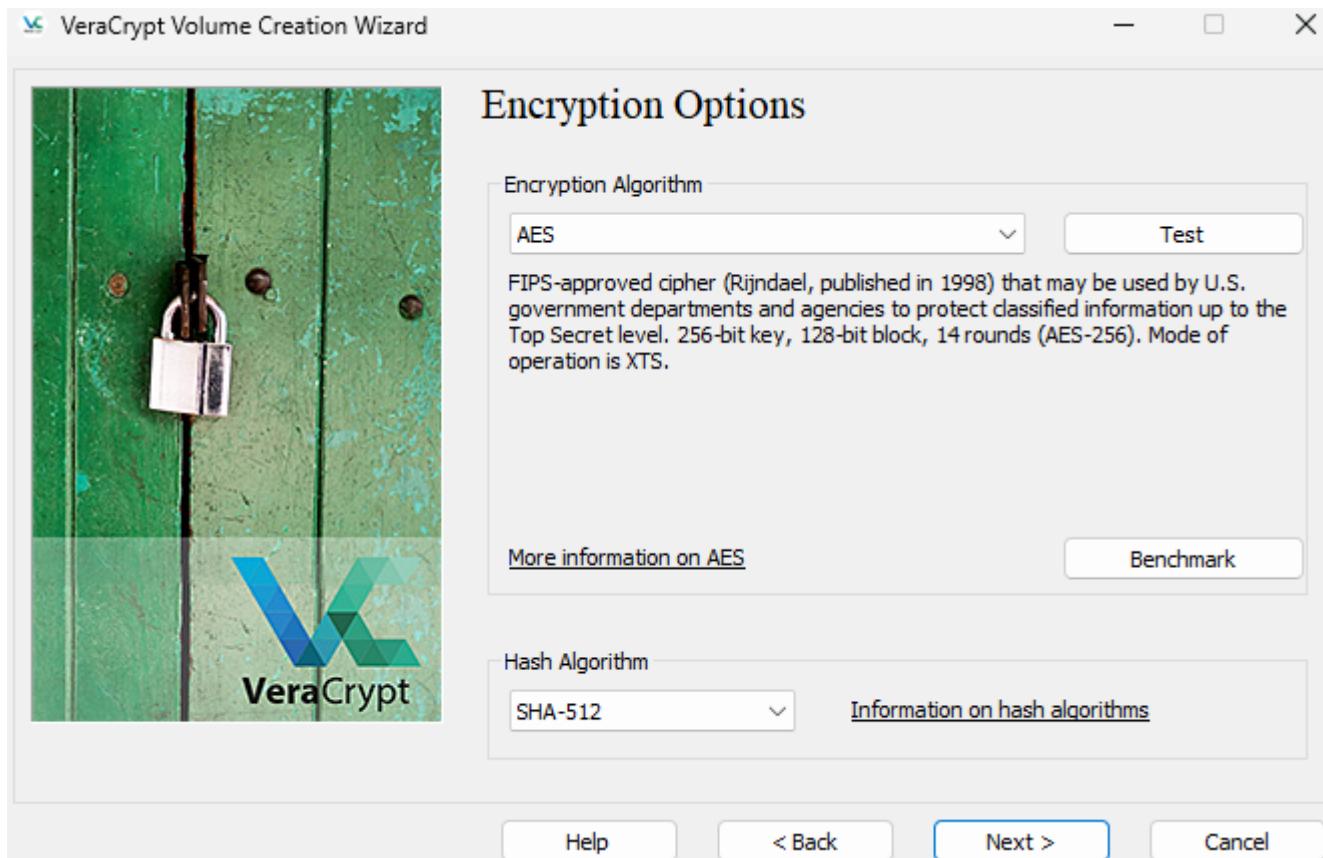
Seleccionamos Standard VeraCrypt Volume y le damos a next:



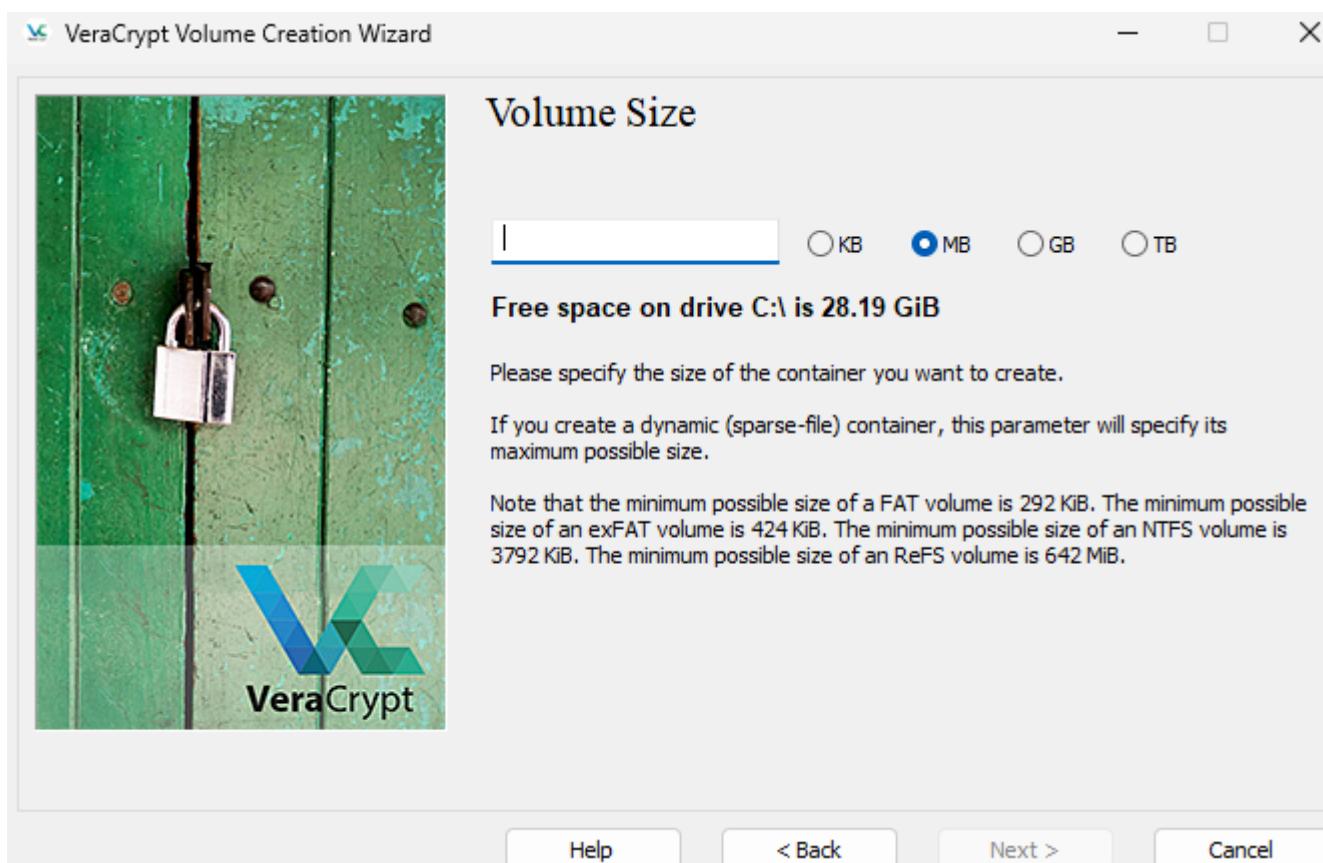
Para almacenar el volúmen seleccionamos la carpeta de nuestro usuario:



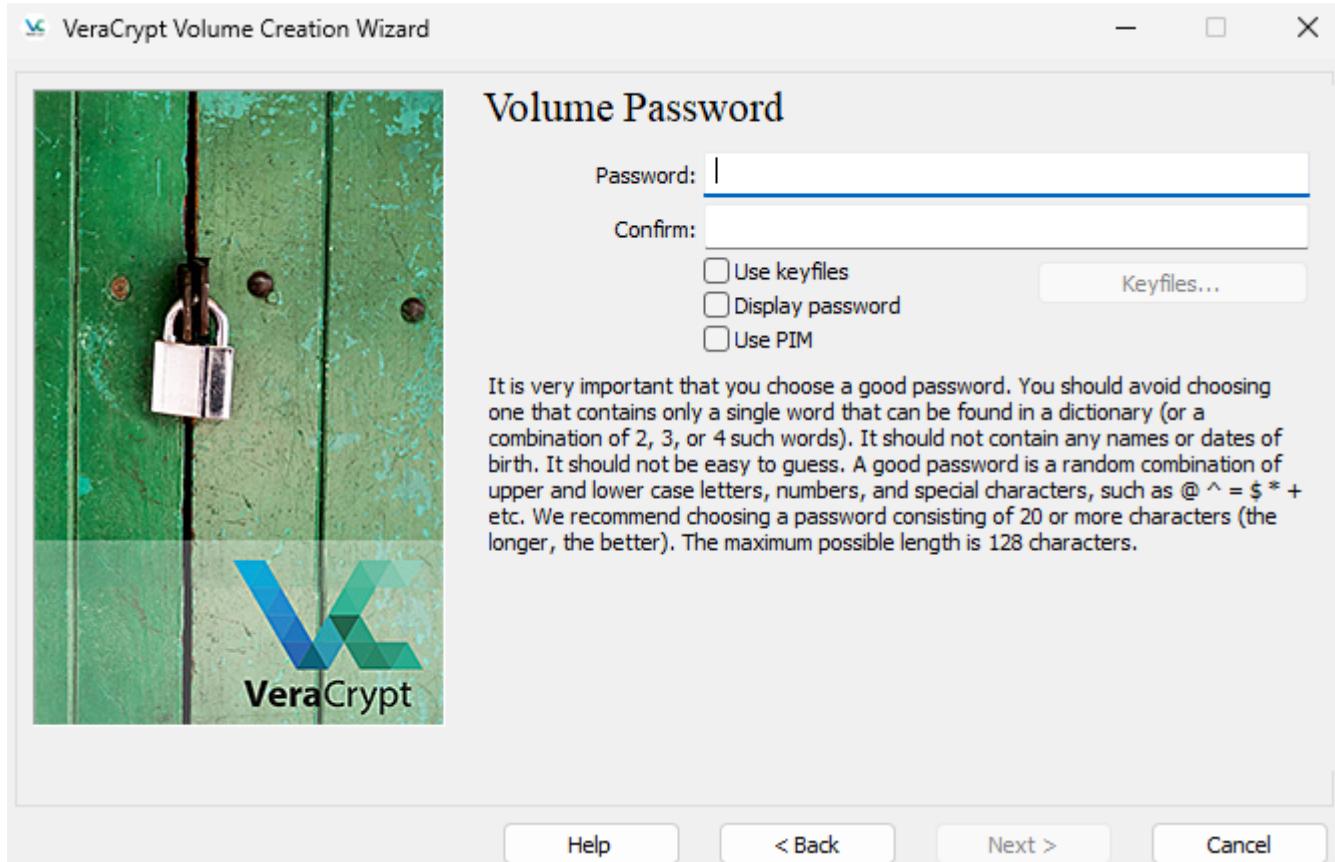
Una vez seleccionada la ubicación le damos a next:



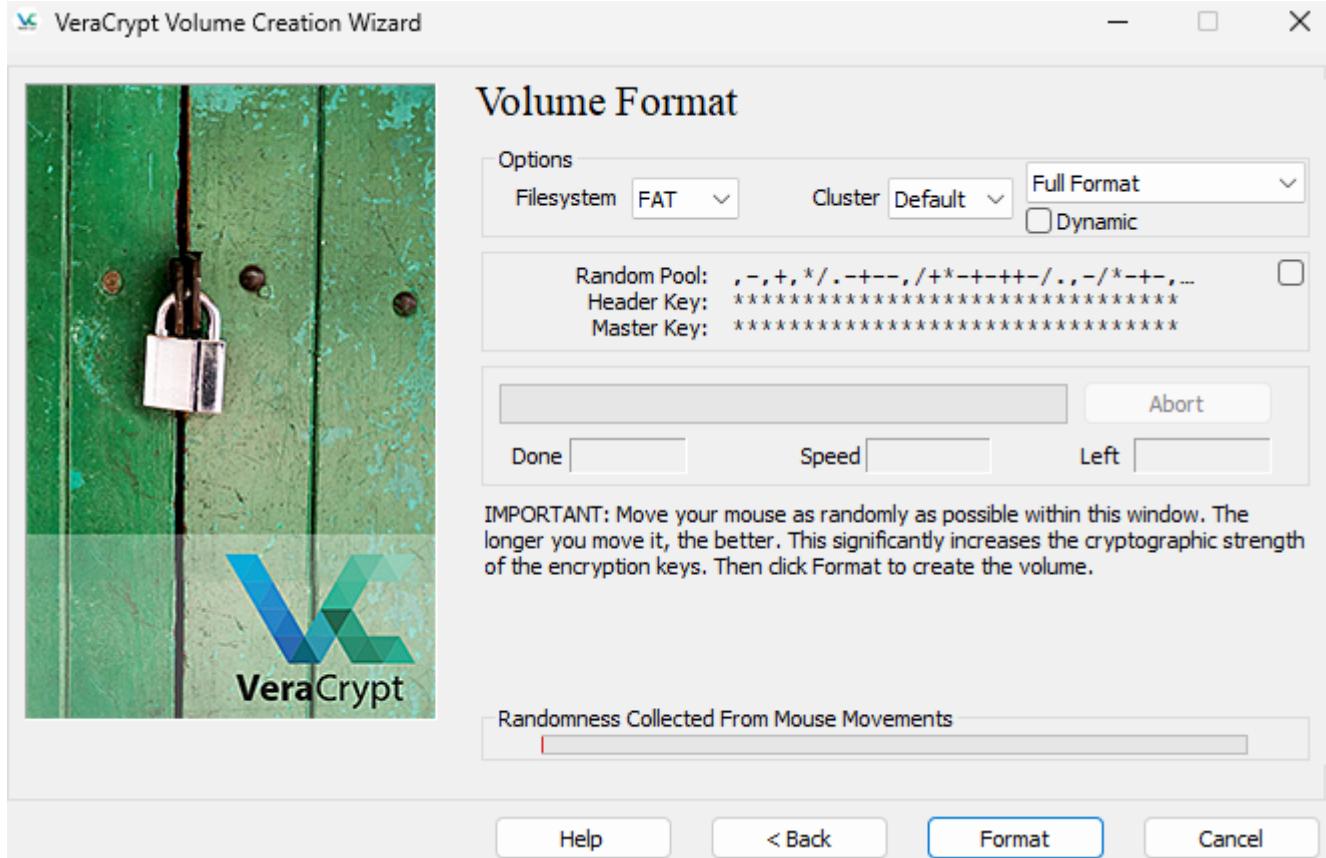
En la ventana que aparece se puede seleccionar el cifrado que se va a aplicar, una vez seleccionado se pulsa en siguiente:



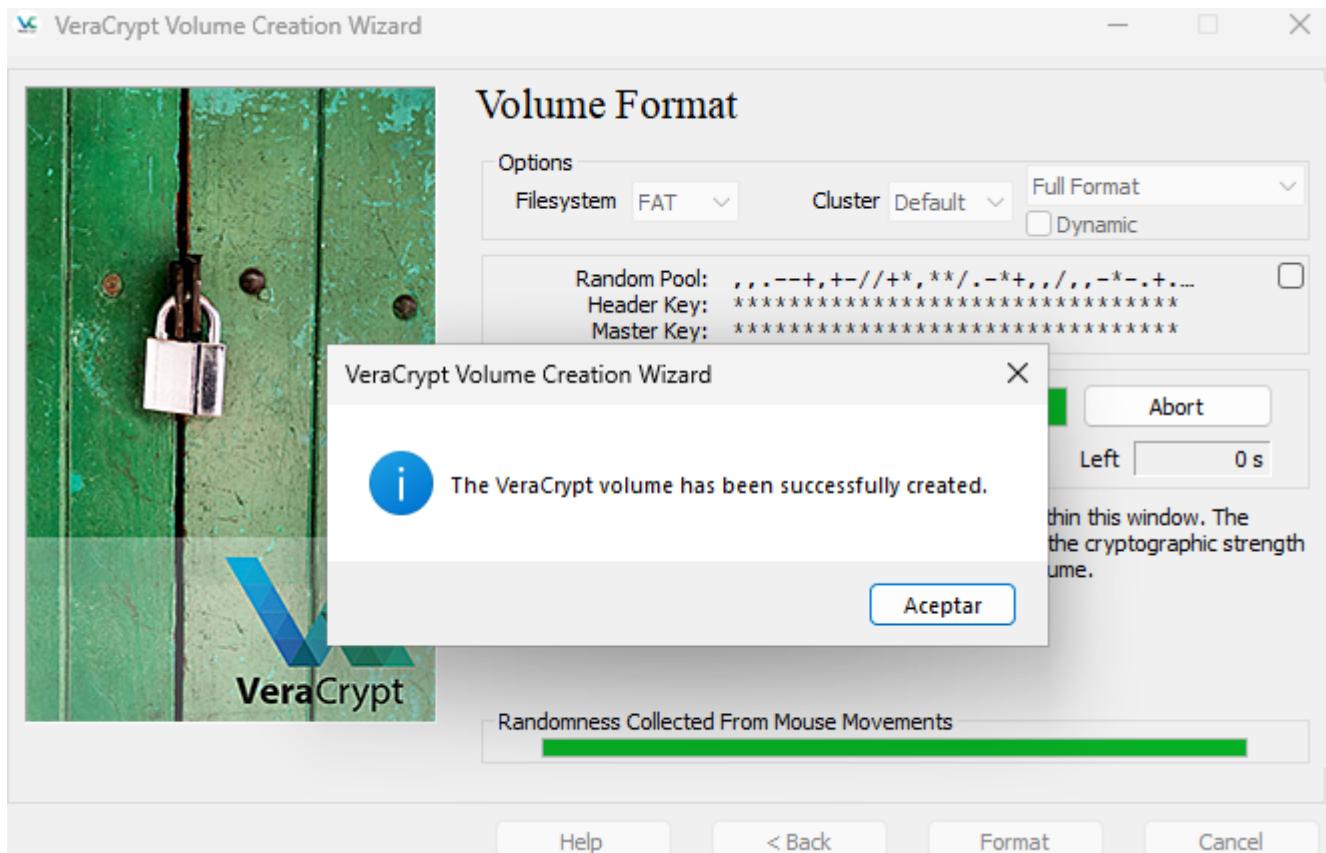
Seleccionaremos el tamaño que va a tener el container y pulsaremos en siguiente:



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

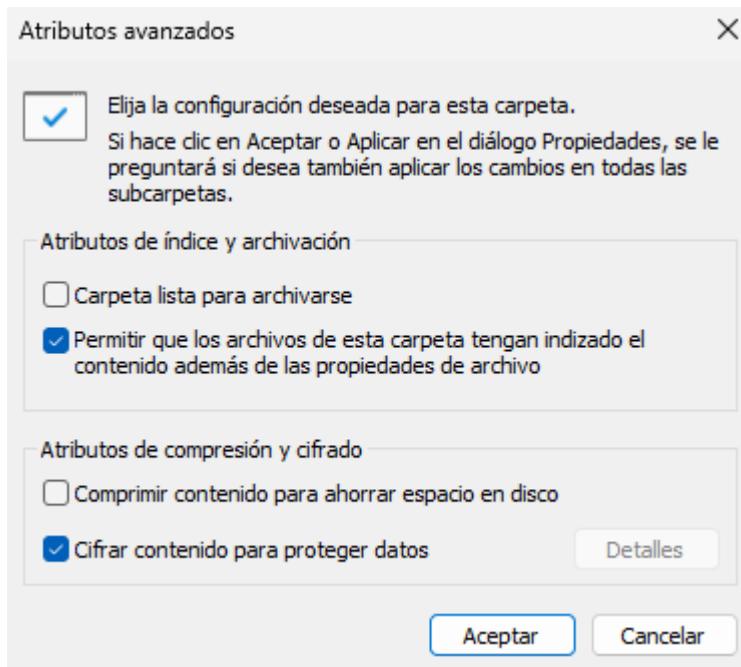
Para realizar un cifrado EFS de una carpeta debemos abrir el CMD como administrador y escribir el siguiente comando:

```
fsutil behavior set disableencryption 0
```

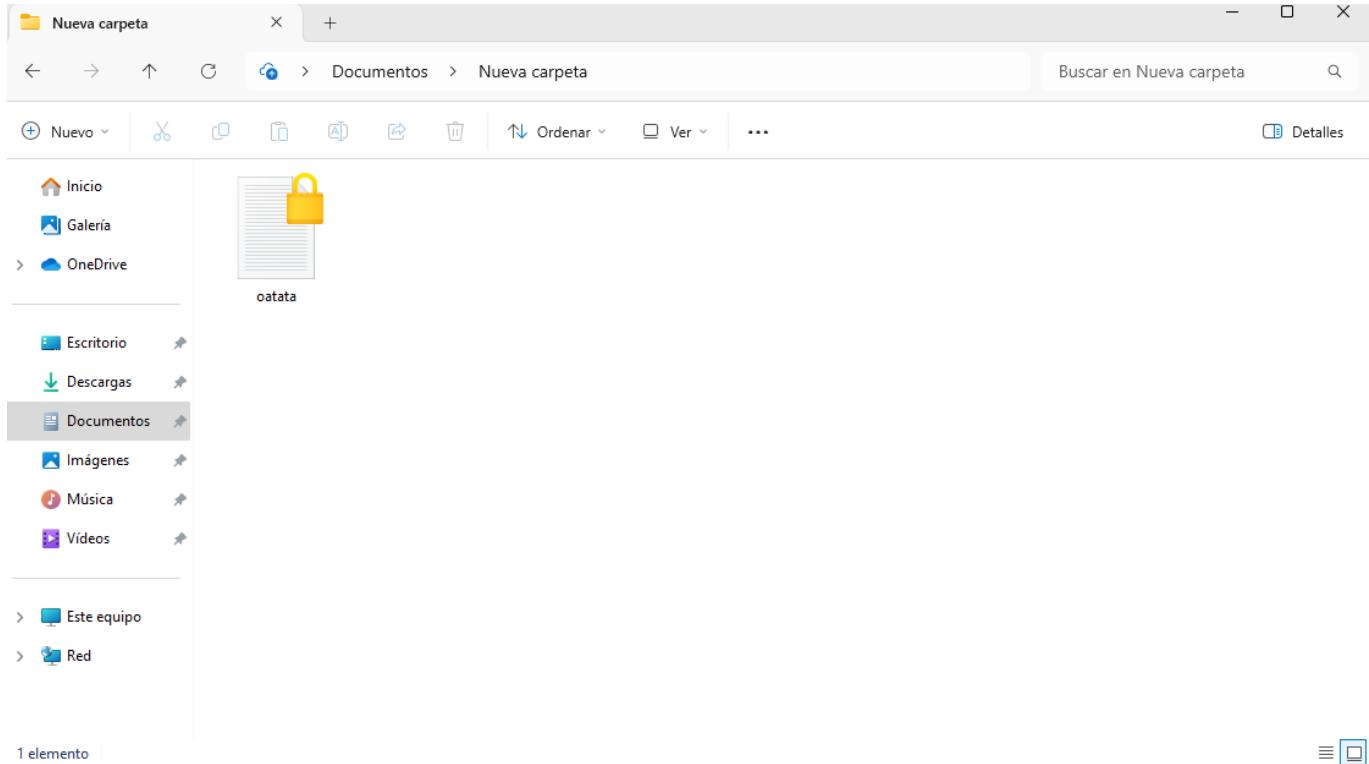
```
C:\Users\MCBS\Documents\Nueva carpeta>fsutil behavior set disableencryption 0
DisableEncryption = 0 (El cifrado está HABILITADO)

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 cifrada? ¿Cuál 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? ¿Cómo 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”:

Directiva	Configuración de seguridad...
Auditar el acceso a objetos	Sin auditoría
Auditar el acceso al servicio de directorio	Sin auditoría
Auditar el cambio de directivas	Sin auditoría
Auditar el seguimiento de procesos	Sin auditoría
Auditar el uso de privilegios	Sin auditoría
Auditar eventos de inicio de sesión	Sin auditoría
Auditar eventos de inicio de sesión de cuenta	Sin auditoría
Auditar eventos del sistema	Sin auditoría
Auditar la administración de cuentas	Sin auditoría

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

Propiedades: Auditar el acceso a objetos

Configuración de seguridad local Explicación

Auditar el acceso a objetos

Auditar estos intentos:

Correcto

Erróneo

Esta configuración no se puede aplicar si se configura otra directiva para invalidar la directiva la auditoría de nivel de categoría.
Para obtener más información, consulte [Auditar el acceso a objetos.](#) (Q921468)

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 qué 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”:

Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

Vistas personalizadas

Registros de Windows

Aplicación

Seguridad

Instalación

Sistema

Eventos reenviados

Registros de aplicaciones y sistema

Suscripciones

Seguridad Número de eventos: 23.071 () 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
>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
>Error de auditoría	22/04/2025 16:48:32	Microsoft Windows secu...	4673	Sensitive Privilege Use
>Error de auditoría	22/04/2025 16:48:26	Microsoft Windows secu...	5158	Filtering Platform Connec...
>Error de auditoría	22/04/2025 16:48:26	Microsoft Windows secu...	5158	Filtering Platform Connec...
>Error de auditoría	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
>Error de auditoría	22/04/2025 16:48:26	Microsoft Windows secu...	4688	Process Creation
>Error de auditoría	22/04/2025 16:48:26	Microsoft Windows secu...	4670	Authorization Policy Cha...
>Error de auditoría	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 16:48:24	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

From:

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

Permanent link:

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

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

