Manual

tecni Solutions

ENCRIPTACIÓN

Verycript en el aula

Pasos previos:

- Trabajo ideal (nube).
- Crear un archivo discreto.
- Crear una contraseña lo más compleja y fácil de recordar. (Mayúsculas y minúsculas, cifras y caracteres) Puedes usar Keeper (https://www.keepersecurity.com/es_ES/)
- Determinar lo que se puede y no transportar.
- Medios de transporte de datos.

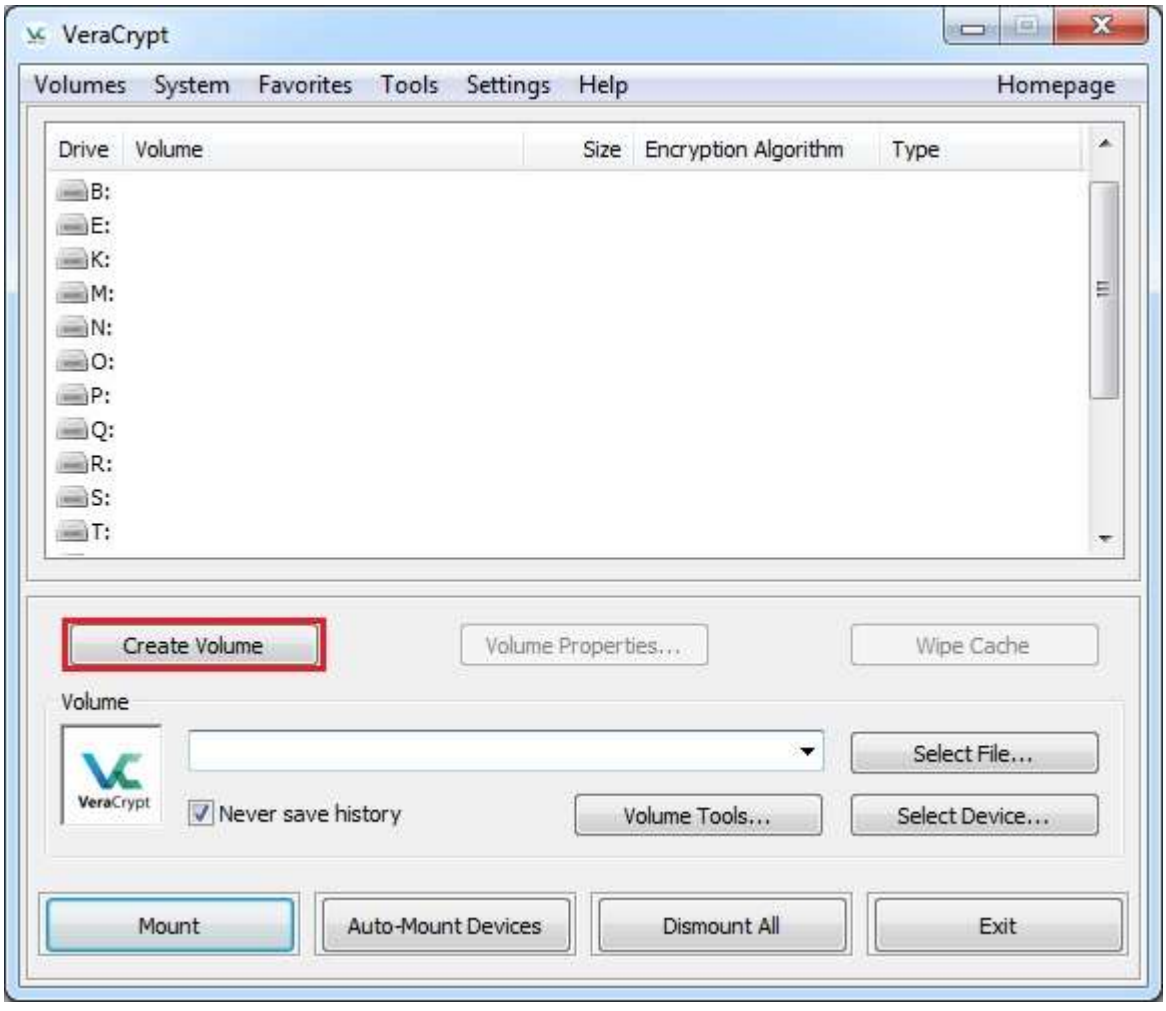
Cómo crear y usar un contenedor VeraCrypt

Este capítulo contiene instrucciones paso a paso sobre cómo crear, montar y usar un volumen VeraCrypt. Le recomendamos encarecidamente que también lea las otras secciones de este manual, ya que contienen información importante.

PASO 1:

Si no lo ha hecho, descargue e instale VeraCrypt (tecnisolutions.es/programas 2 programa ENCRIPTACIÓN) Inicie VeraCrypt haciendo doble clic en el archivo VeraCrypt.exe o haciendo clic en el acceso directo VeraCrypt en el menú Inicio de Windows.

PASO 2:



La ventana principal de VeraCrypt debería aparecer. Haga clic en **Crear volumen** (marcado con un rectángulo rojo para mayor claridad).

PASO 3:

Debería aparecer la ventana del Asistente de creación de volumen de VeraCrypt.

En este paso, debe elegir dónde desea que se cree el volumen VeraCrypt. Un volumen VeraCrypt puede residir en un archivo, que también se llama contenedor, en una partición o unidad. En este tutorial, elegiremos la primera opción y crearemos un volumen VeraCrypt dentro de un archivo.

Como la opción está seleccionada de forma predeterminada, puede hacer clic en **Siguiente** .

Nota: En los siguientes pasos, las capturas de pantalla mostrarán solo la parte derecha de la ventana del asistente.

ETAPA 4:

En este paso, debe elegir si desea crear un volumen VeraCrypt estándar u oculto. En este tutorial, elegiremos la primera opción y crearemos un volumen estándar de VeraCrypt.

Como la opción está seleccionada de forma predeterminada, puede hacer clic en **Siguiente** .

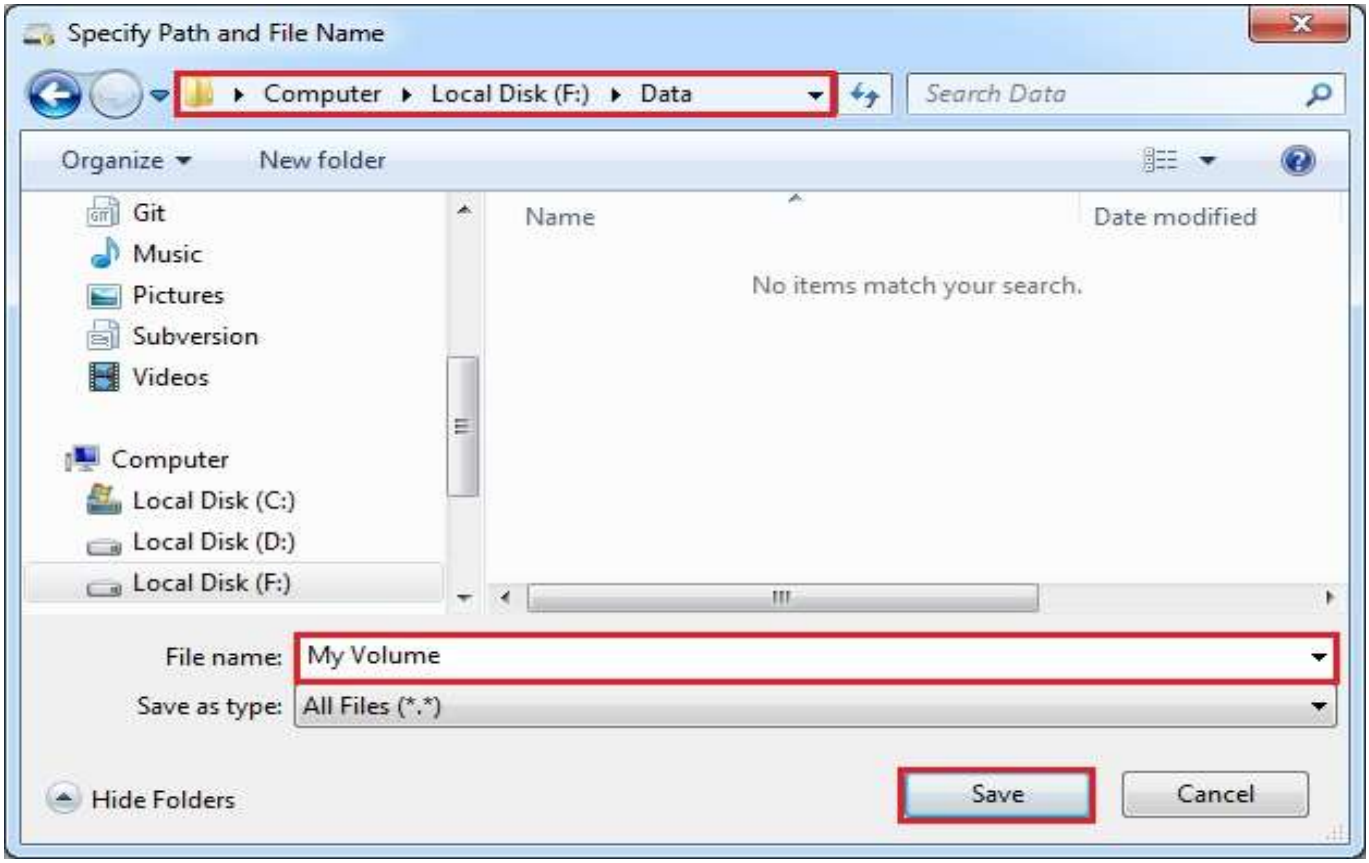
PASO 5:

En este paso, debe especificar dónde desea que se cree el volumen VeraCrypt (contenedor de archivos). Tenga en cuenta que un contenedor VeraCrypt es como cualquier archivo normal. Puede, por ejemplo, moverse o eliminarse como cualquier archivo normal. También necesita un nombre de archivo, que elegirá en el siguiente paso.

Haga clic en **Seleccionar archivo** .

El selector de archivos estándar de Windows debería aparecer (mientras la ventana del Asistente de creación de volumen de VeraCrypt permanece abierta en segundo plano).

PASO 6:



En este tutorial, crearemos nuestro volumen VeraCrypt en la carpeta F *:* \ *Data* \ y el nombre de archivo del volumen (contenedor) será *Mi volumen* (como se puede ver en la captura de pantalla anterior). Por supuesto, puede elegir cualquier otro nombre de archivo y ubicación que desee (por ejemplo, en una memoria USB). Tenga en cuenta que el archivo *Mi volumen* aún no existe: VeraCrypt lo creará.

IMPORTANTE: Tenga en cuenta que VeraCrypt *no* cifrará ningún archivo existente (al crear un contenedor de archivos VeraCrypt). Si selecciona un archivo existente en este paso, se sobrescribirá y se reemplazará por el volumen recién creado (por lo que el archivo sobrescrito

se *perderá* , *no se* cifrará). Podrá cifrar archivos existentes (más adelante) moviéndolos al volumen VeraCrypt que estamos creando ahora. *

Seleccione la ruta deseada (donde desea que se cree el contenedor) en el selector de archivos. Escriba el nombre del archivo contenedor deseado en el cuadro **Nombre** de **archivo** .

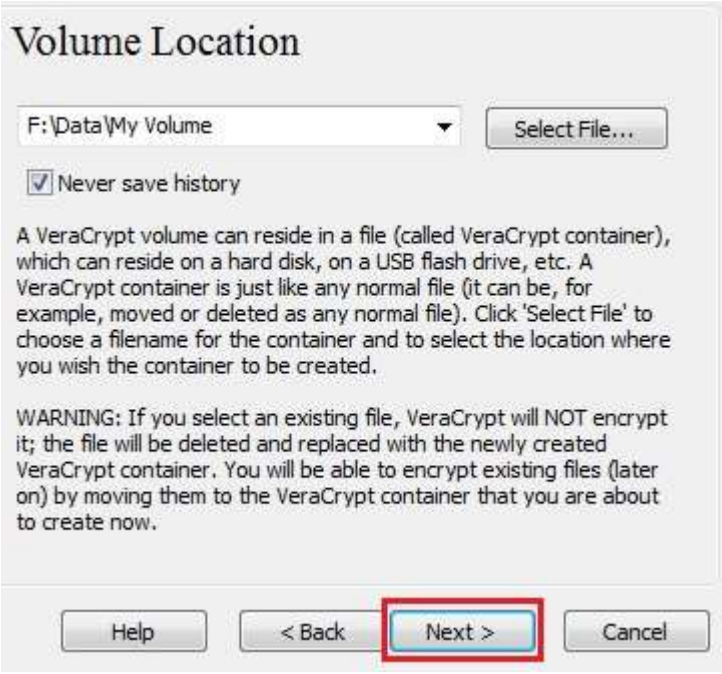
Haz clic en **Guardar** .

La ventana del selector de archivos debería desaparecer.

En los siguientes pasos, volveremos al Asistente de creación de volúmenes de VeraCrypt.

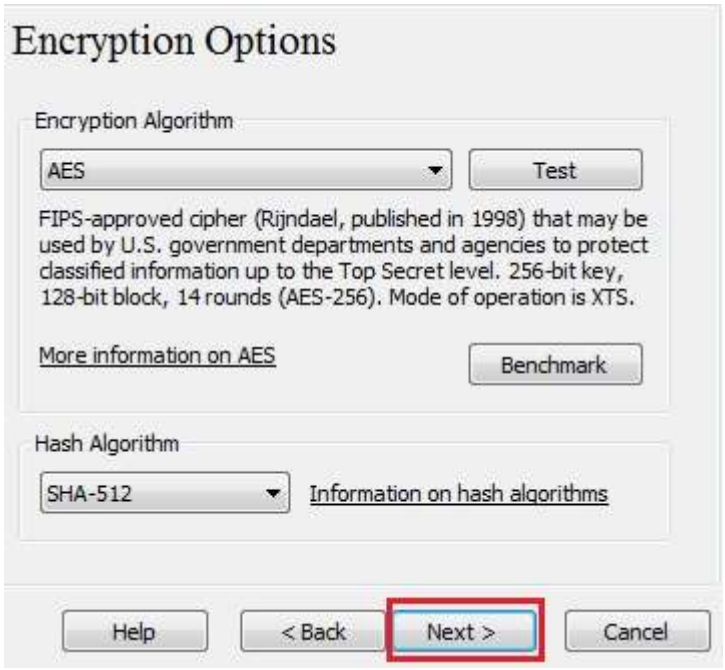
* Tenga en cuenta que después de copiar los archivos no cifrados existentes en un volumen VeraCrypt, debe borrar (borrar) de forma segura los archivos no cifrados originales. Existen herramientas de software que pueden usarse con el propósito de borrar de forma segura (muchas de ellas son gratuitas).

PASO 7:



En la ventana del Asistente de creación de volumen, haga clic en **Siguiente** .

PASO 8:



Aquí puede elegir un algoritmo de cifrado y un algoritmo hash para el volumen. Si no está seguro de qué seleccionar aquí, puede usar la configuración predeterminada y hacer clic en **Siguiente** (para obtener más información, consulte los capítulos *Algoritmos de cifrado* y *Algoritmos hash*).

PASO 9:

Aquí especificamos que deseamos que el tamaño de nuestro contenedor VeraCrypt sea de 250 megabytes. Por supuesto, puede especificar un tamaño diferente. Después de escribir el tamaño deseado en el campo de entrada (marcado con un rectángulo rojo), haga clic en **Siguiente** .

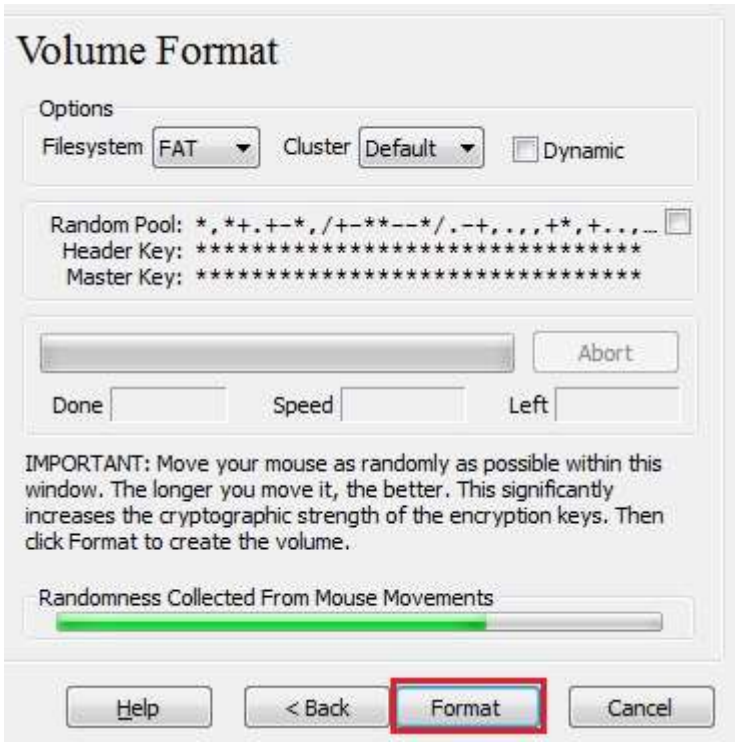
PASO 10:

Este es uno de los pasos más importantes. Aquí tienes que elegir una buena contraseña de volumen. Lea atentamente la información que se muestra en la ventana del asistente sobre lo que se considera una buena contraseña.

Después de elegir una buena contraseña, escríbala en el primer campo de entrada. Luego vuelva a escribirlo en el campo de entrada debajo del primero y haga clic en **Siguiente** .

Nota: El botón **Siguiente** se desactivará hasta que las contraseñas en ambos campos de entrada sean las mismas.

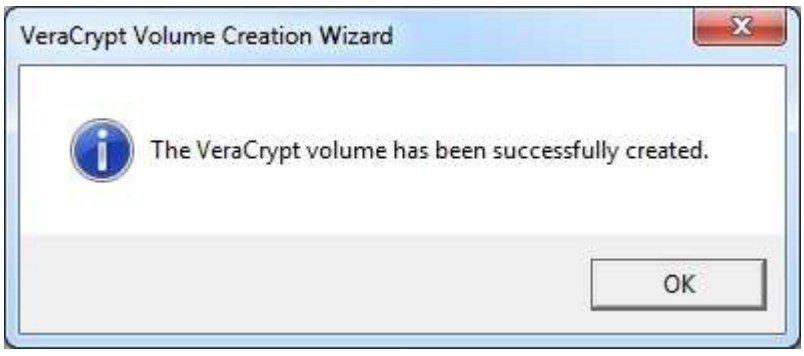
PASO 11:



Mueva el mouse lo más al azar posible dentro de la ventana del Asistente de creación de volumen al menos hasta que el indicador de aleatoriedad se vuelva verde. Cuanto más tiempo mueva el mouse, mejor (se recomienda mover el mouse durante al menos 30 segundos). Esto aumenta significativamente la fuerza criptográfica de las claves de cifrado (lo que aumenta la seguridad).

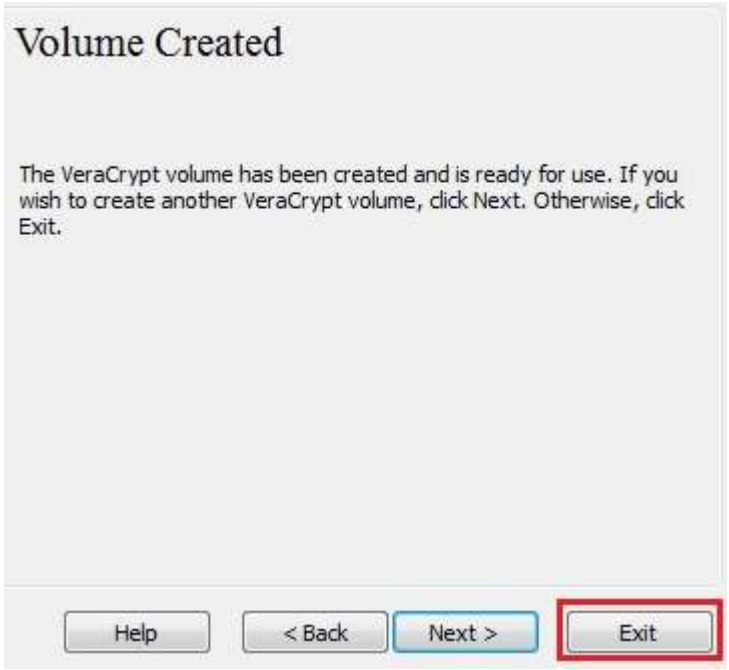
Haga clic en **formato** .

La creación del volumen debe comenzar. VeraCrypt ahora creará un archivo llamado *My Volume* en la carpeta F *:* \ *Data* \ (como especificamos en el Paso 6). Este archivo será un contenedor VeraCrypt (contendrá el volumen cifrado de VeraCrypt). Dependiendo del tamaño del volumen, la creación del volumen puede llevar mucho tiempo. Después de que termine, aparecerá el siguiente cuadro de diálogo:



Haga clic en**Aceptar** para cerrar el cuadro de diálogo.

PASO 12:

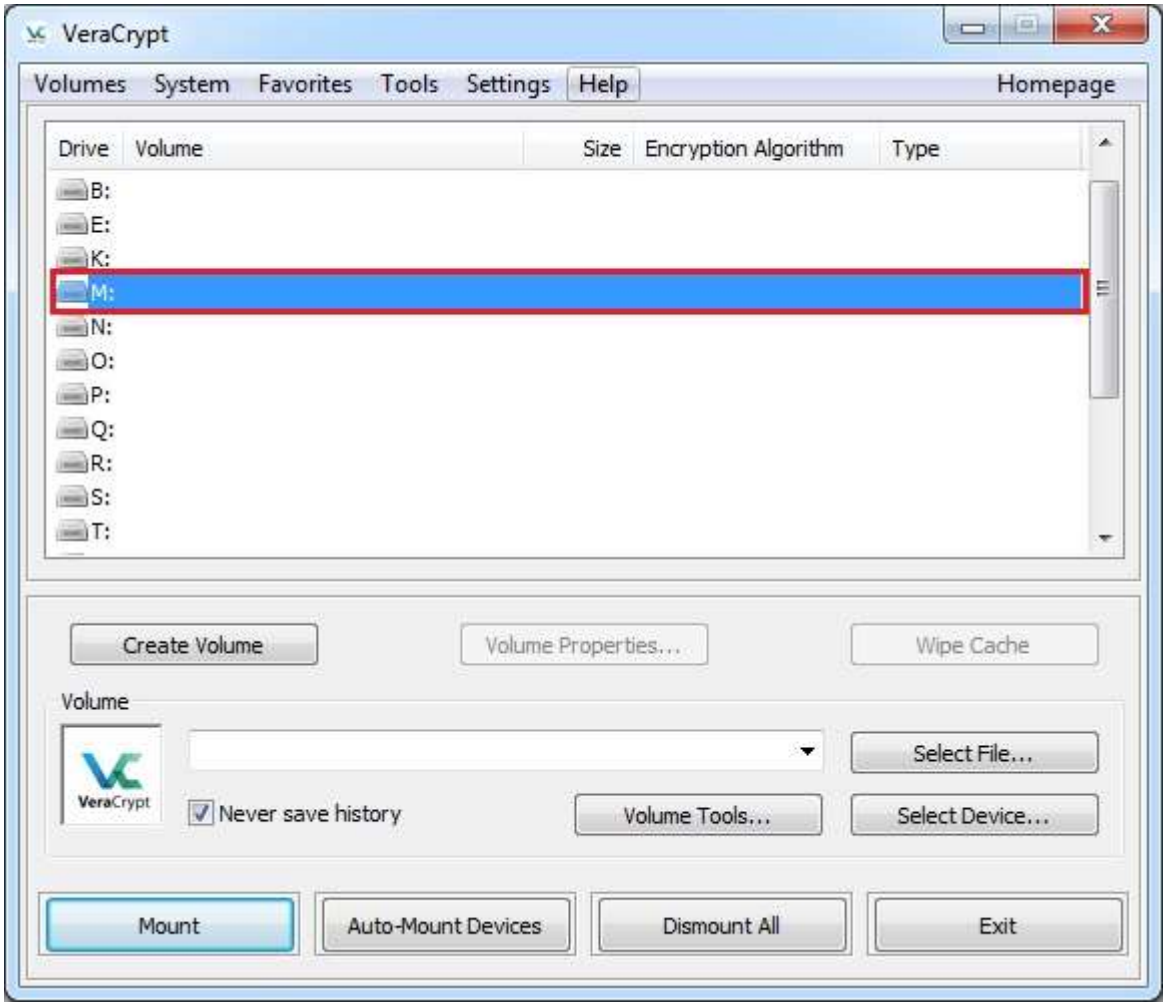


Acabamos de crear con éxito un volumen VeraCrypt (contenedor de archivos). En la ventana del Asistente de creación de volumen de VeraCrypt, haga clic en **Salir** .

La ventana del asistente debería desaparecer.

En los pasos restantes, montaremos el volumen que acabamos de crear. Volveremos a la ventana principal de VeraCrypt (que aún debería estar abierta, pero si no lo está, repita el Paso 1 para iniciar VeraCrypt y luego continúe desde el Paso 13).

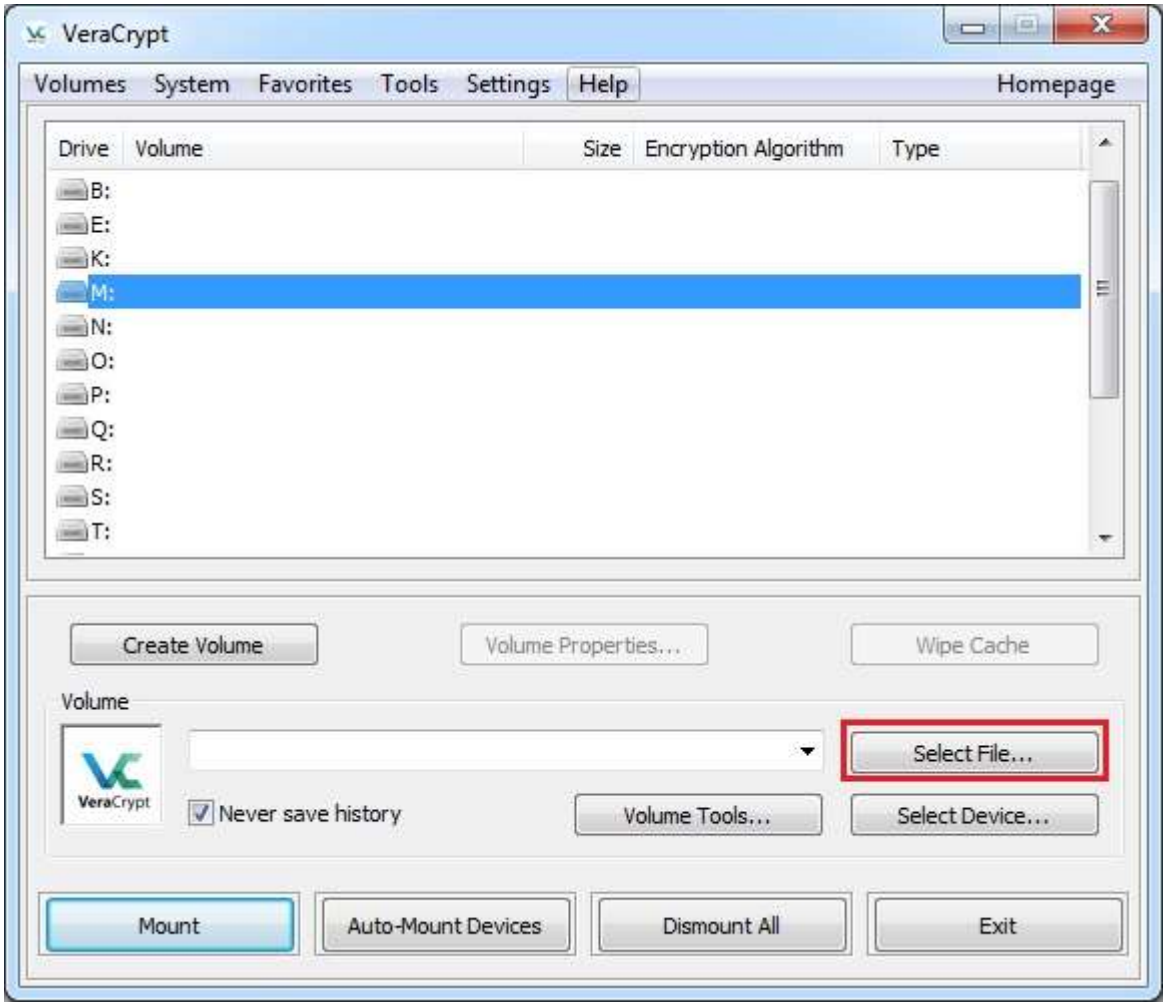
PASO 13:



Seleccione una letra de unidad de la lista (marcada con un rectángulo rojo). Esta será la letra de unidad en la que se montará el contenedor VeraCrypt.

Nota: En este tutorial, elegimos la letra de unidad M, pero, por supuesto, puede elegir cualquier otra letra de unidad disponible.

PASO 14:



Haga clic en **Seleccionar archivo** .

La ventana del selector de archivos estándar debería aparecer.

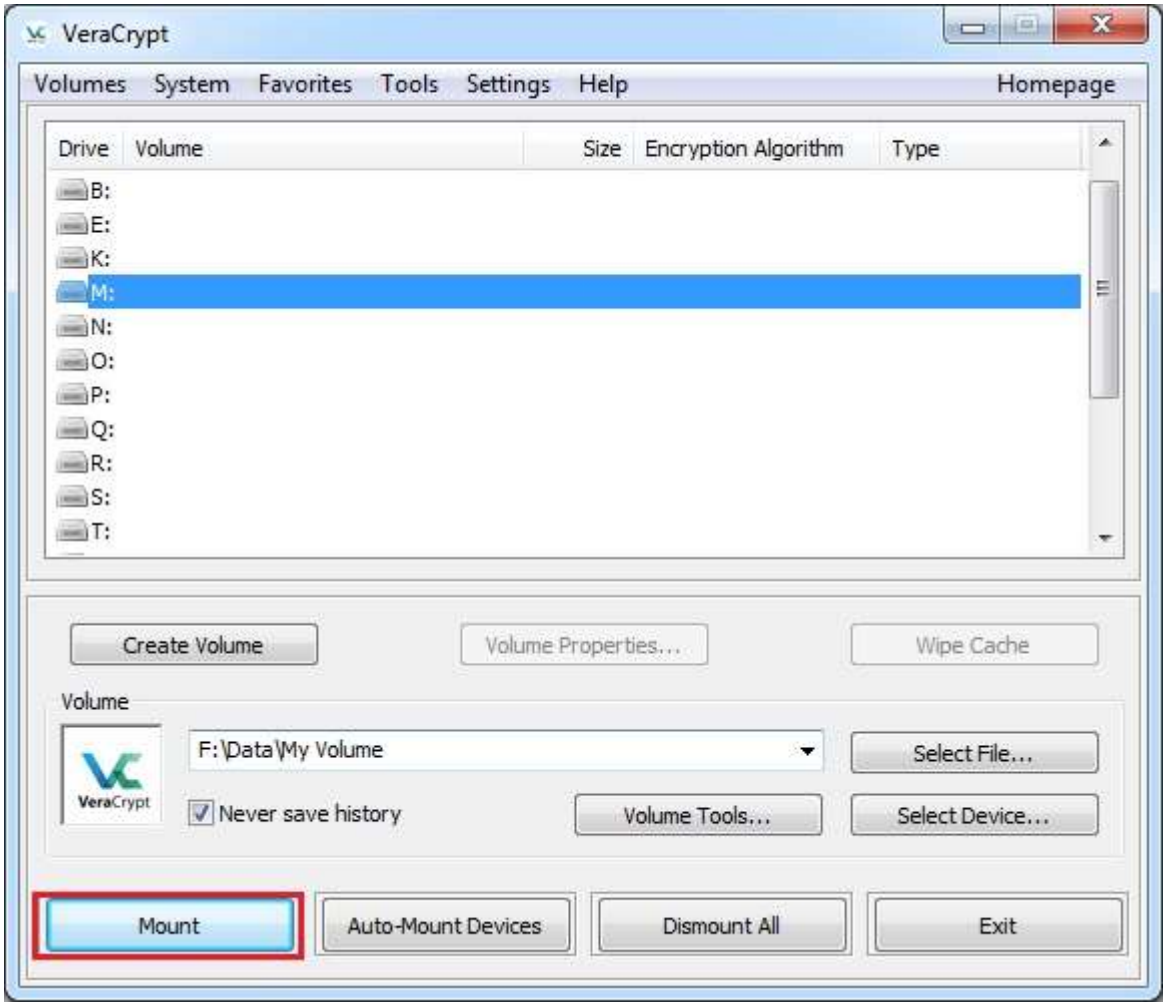
PASO 15:

En el selector de archivos, busque el archivo contenedor (que creamos en los Pasos 6-12) y selecciónelo. Haga clic en **Abrir** (en la ventana del selector de archivos).

La ventana del selector de archivos debería desaparecer.

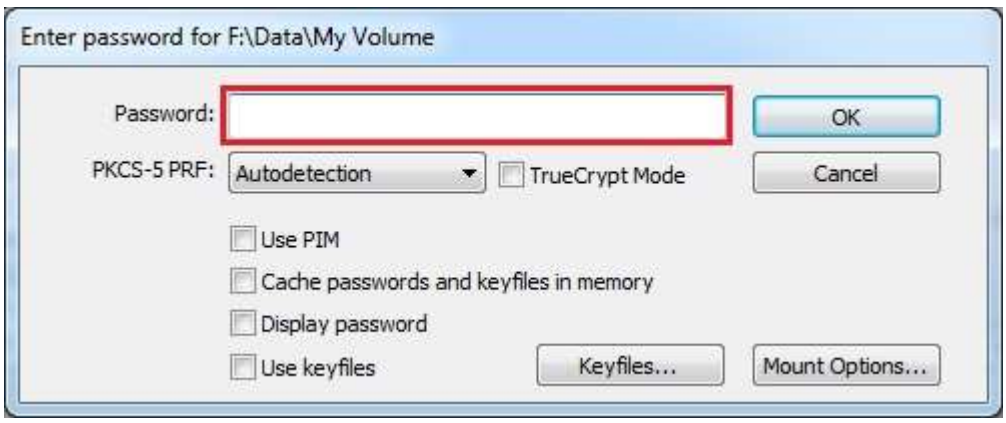
En los siguientes pasos, volveremos a la ventana principal de VeraCrypt.

PASO 16:



En la ventana principal de VeraCrypt, haga clic en **Montar** . Debe aparecer la ventana de diálogo de solicitud de contraseña.

PASO 17:



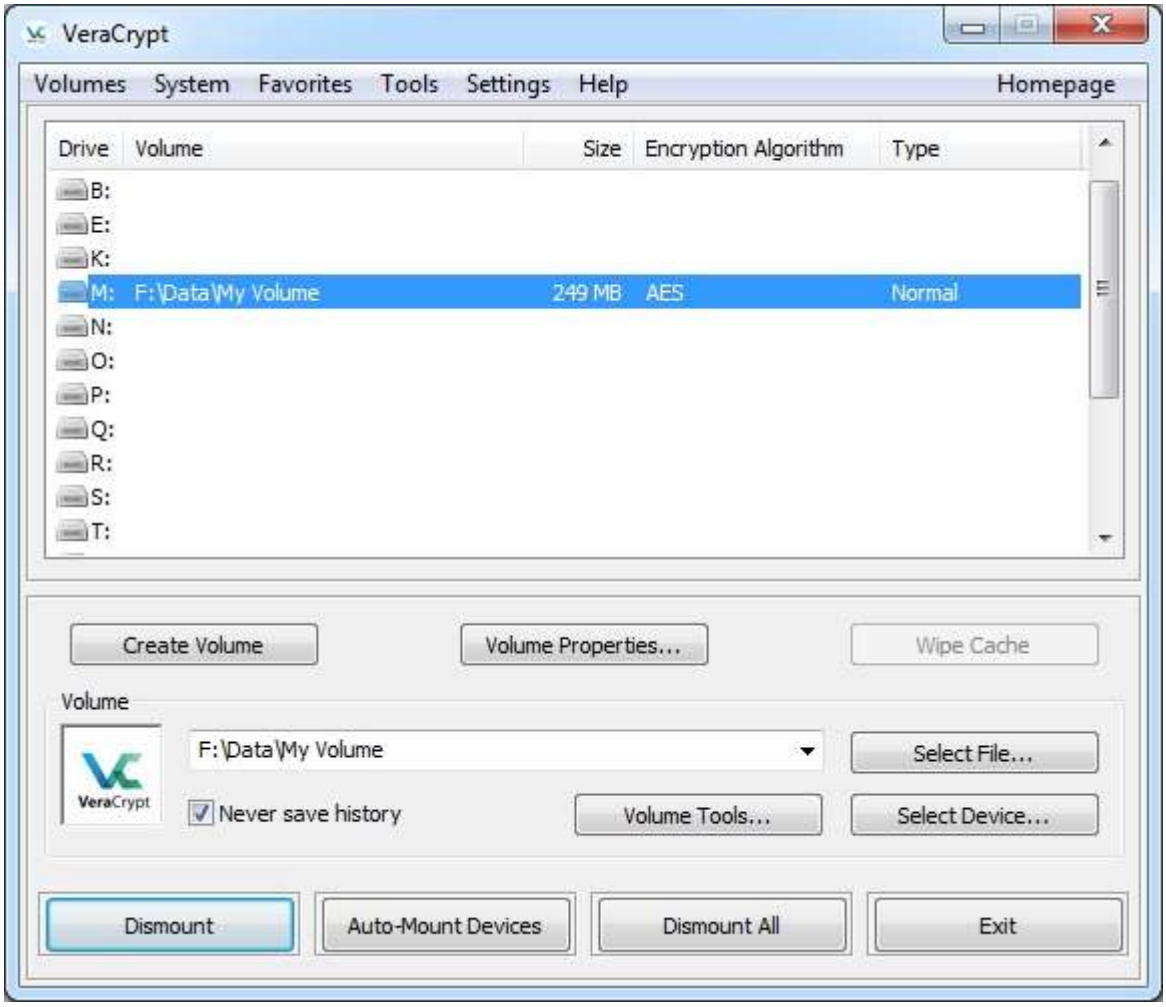
Escriba la contraseña (que especificó en el Paso 10) en el campo de entrada de contraseña (marcado con un rectángulo rojo).

PASO 18:

Seleccione el algoritmo PRF que se utilizó durante la creación del volumen (SHA-512 es el PRF predeterminado utilizado por VeraCrypt). Si no recuerda qué PRF se usó, simplemente déjelo configurado en "autodetección", pero el proceso de montaje tomará más tiempo. Haga clic en **Aceptar** después de ingresar la contraseña.

VeraCrypt ahora intentará subir el volumen. Si la contraseña es incorrecta (por ejemplo, si la escribió incorrectamente), VeraCrypt le notificará y deberá repetir el paso anterior (vuelva a escribir la contraseña y haga **clic** en **Aceptar**). Si la contraseña es correcta, se montará el volumen.

ÚLTIMO PASO:



Acabamos de montar con éxito el contenedor como un disco virtual M:

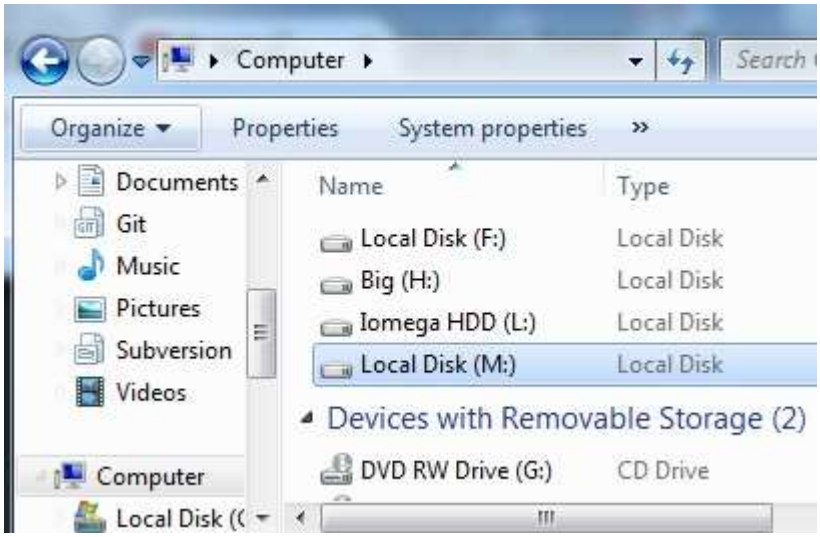
el disco virtual está completamente encriptado (incluidos los nombres de archivo, las tablas de asignación, el espacio libre, etc.) y se comporta como un disco real. Puede guardar (o copiar, mover, etc.) archivos en este disco virtual y se cifrarán sobre la marcha a medida que se escriben.

Si abre un archivo almacenado en un volumen VeraCrypt, por ejemplo, en un reproductor multimedia, el archivo se descifrará automáticamente en la RAM (memoria) sobre la marcha mientras se lee.

Importante: Tenga en cuenta que cuando abra un archivo almacenado en un volumen VeraCrypt (o cuando escriba / copie un archivo en / desde el volumen VeraCrypt) no se le pedirá que ingrese la contraseña nuevamente. Debe ingresar la contraseña correcta solo cuando monte el volumen.

Puede abrir el volumen montado, por ejemplo, seleccionándolo en la lista como se muestra en la captura de pantalla anterior (selección azul) y luego haciendo doble clic en el elemento seleccionado.

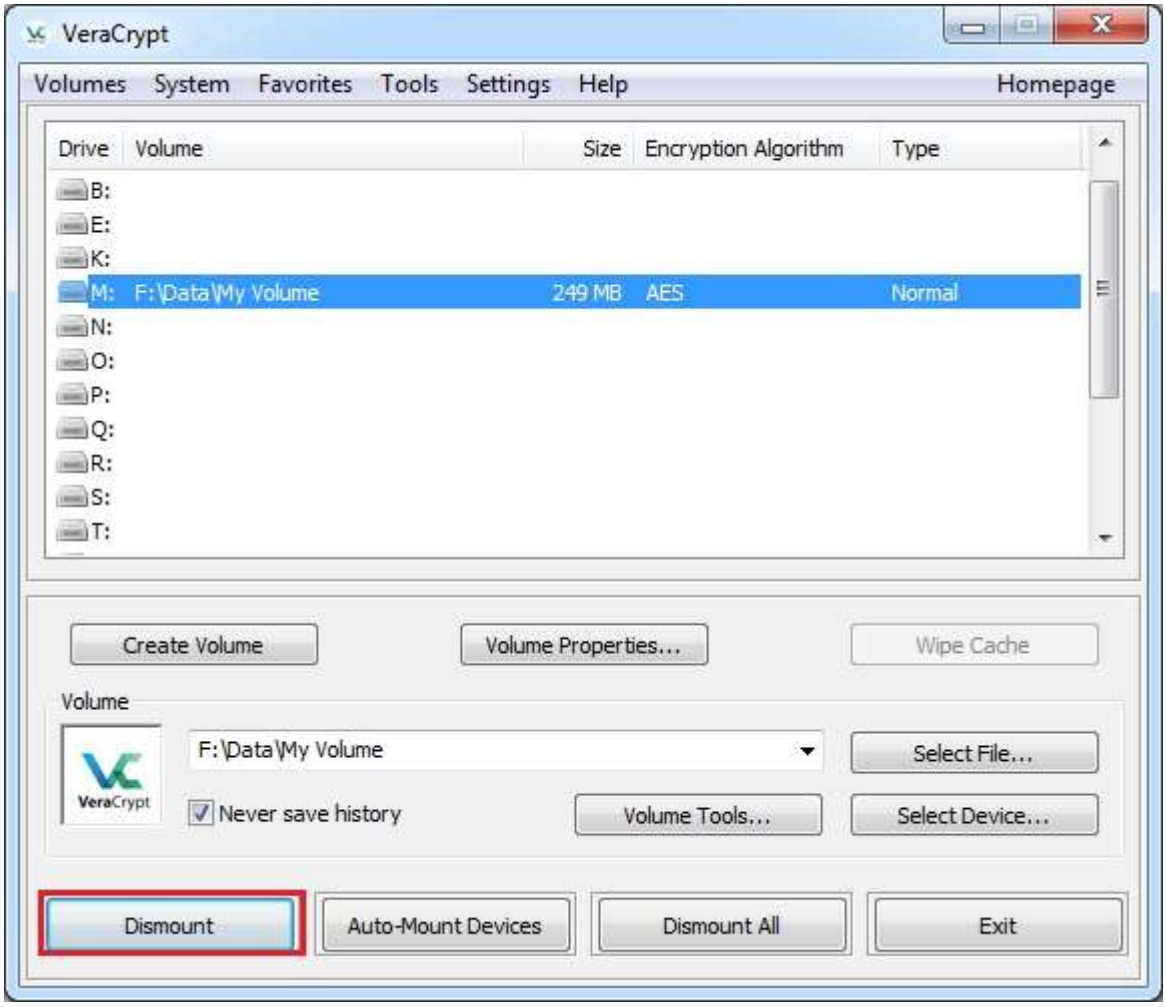
También puede buscar el volumen montado de la forma en que normalmente busca cualquier otro tipo de volumen. Por ejemplo, al abrir la lista ' *Computadora* ' (o ' *Mi PC* ') y hacer doble clic en la letra de unidad correspondiente (en este caso, es la letra M).



Puede copiar archivos (o carpetas) desde y hacia el volumen de VeraCrypt tal como lo haría en cualquier disco normal (por ejemplo, con simples operaciones de arrastrar y soltar). Los archivos que se leen o copian del volumen cifrado de VeraCrypt se descifran automáticamente en la memoria RAM (memoria). Del mismo modo, los archivos que se escriben o copian en el volumen VeraCrypt se cifran automáticamente en la memoria RAM (justo antes de que se escriban en el disco).

Tenga en cuenta que VeraCrypt nunca guarda los datos descifrados en un disco, solo los almacena temporalmente en la RAM (memoria). Incluso cuando el volumen está montado, los datos almacenados en el volumen todavía están encriptados. Cuando reinicie Windows o apague su computadora, el volumen se desmontará y todos los archivos almacenados en él serán inaccesibles (y cifrados). Incluso cuando la fuente de alimentación se interrumpe repentinamente (sin el apagado adecuado del sistema), todos los archivos almacenados en el volumen serán inaccesibles (y encriptados). Para hacerlos accesibles nuevamente, debe montar el volumen. Para hacerlo, repita los pasos 13-18.

Si desea cerrar el volumen y hacer que los archivos almacenados en él sean inaccesibles, reinicie su sistema operativo o desmonte el volumen. Para hacerlo, siga estos pasos:



Seleccione el volumen de la lista de volúmenes montados en la ventana principal de VeraCrypt (marcado con un rectángulo rojo en la captura de pantalla anterior) y luego haga clic en **Desmontar** (también marcado con un rectángulo rojo en la captura de pantalla anterior). Para volver a acceder a los archivos almacenados en el volumen, deberá montar el volumen. Para hacerlo, repita los pasos 13-18.