CONFIGURACIÓN DE HERRAMIENTAS DE CIFRADO

CONEXO

Esta obra está bajo una Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional.

Última actualización: Abril 2024

VERACRYPT

Características:

- Es un software de código abierto que sirve para cifrar:
  - Volúmenes de un disco.
  - Unidades completas de almacenamiento (como una unidad flash USB o un disco duro externo).
- Ayuda a impedir el acceso de terceros a información sensible.
- Está disponible para Microsoft Windows, Mac OS X y GNU/Linux.

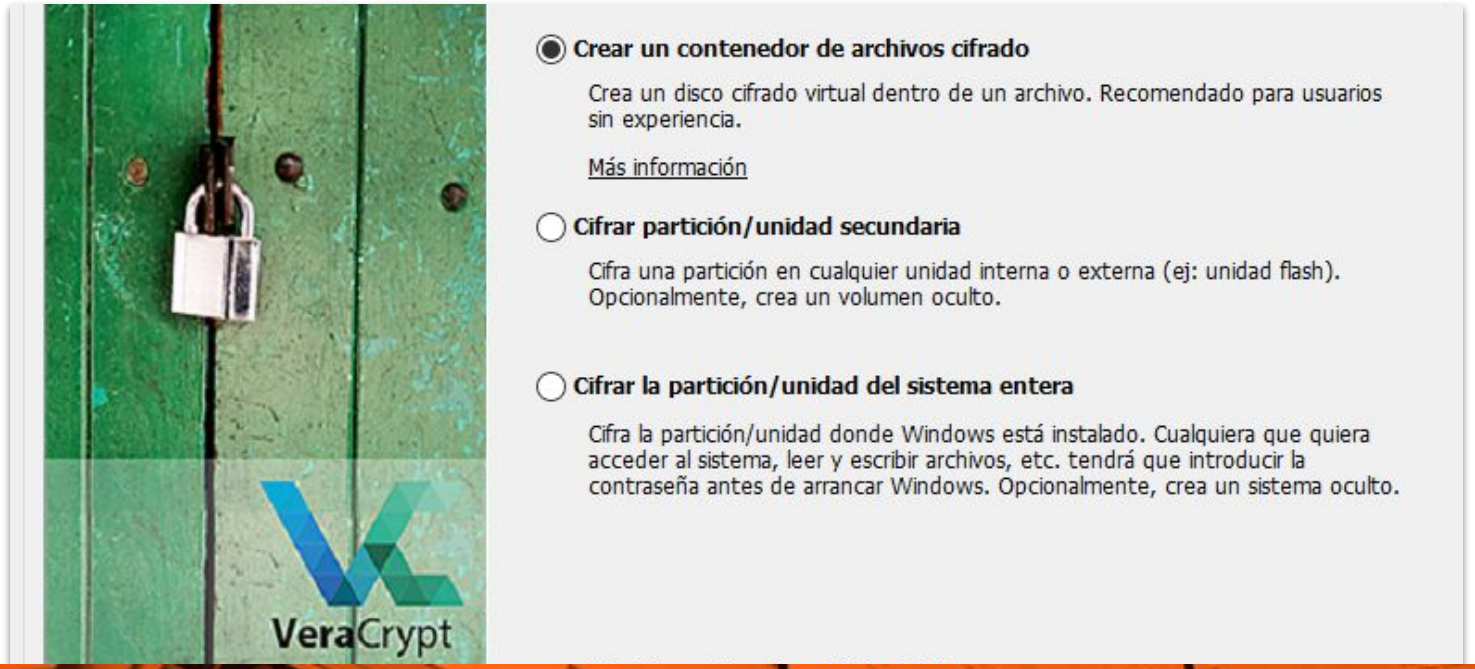
VeraCrypt

https://www.veracrypt.fr/



VERACRYPT

Características. VeraCrypt te permite cifrar:



VeraCrypt

https://www.veracrypt.fr/



ÍNDICE

CONFIGURACIÓN DE HERRAMIENTAS DE CIFRADO

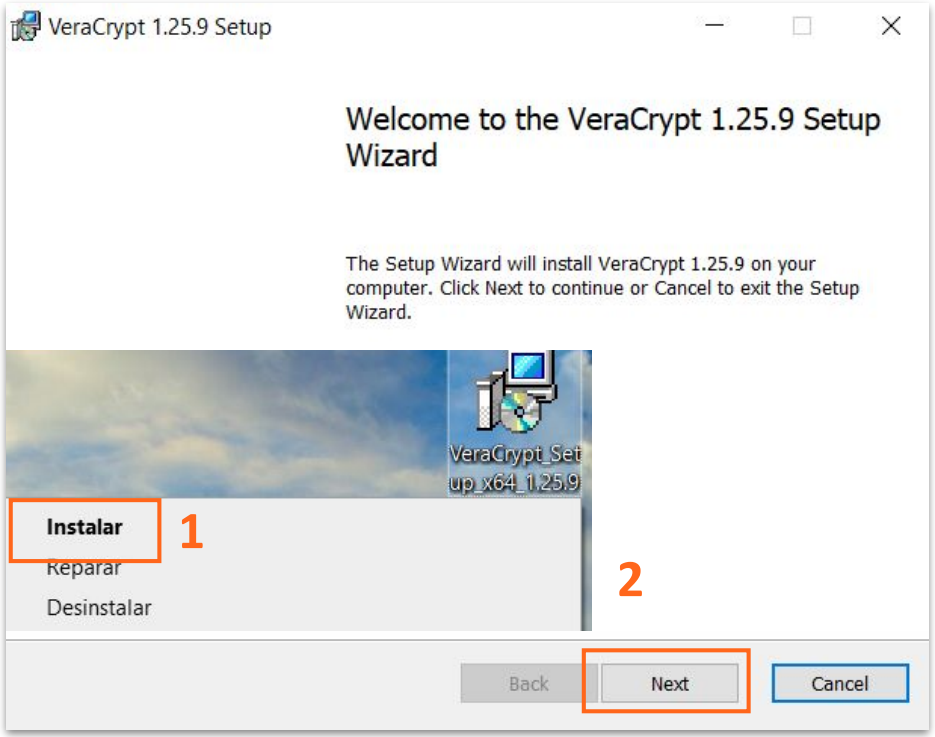
1. Instala VeraCrypt
2. Crea un volumen estándar
3. Usa tu volumen estándar VeraCrypt
   3.1 Montar un volumen estándar
   3.2 Desmontar un volumen estándar
4. Crea un volumen oculto
5. Usa tu volumen oculto VeraCrypt
   5.1 Montar un volumen oculto
   5.2 Desmontar un volumen oculto
   5.3 Proteger un volumen oculto
6. Cambia la(s) contraseña(s) de tu volumen(es) en VeraCrypt
7. BitLocker
8. FileVault

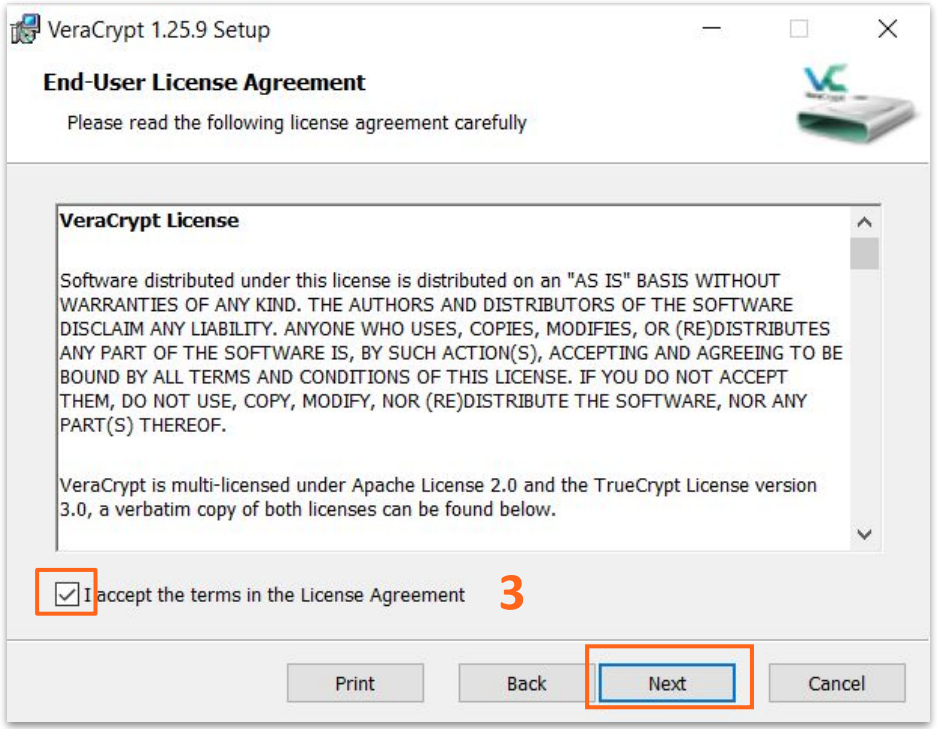
CONEXO

INSTALACIÓN

1. Instala VeraCrypt

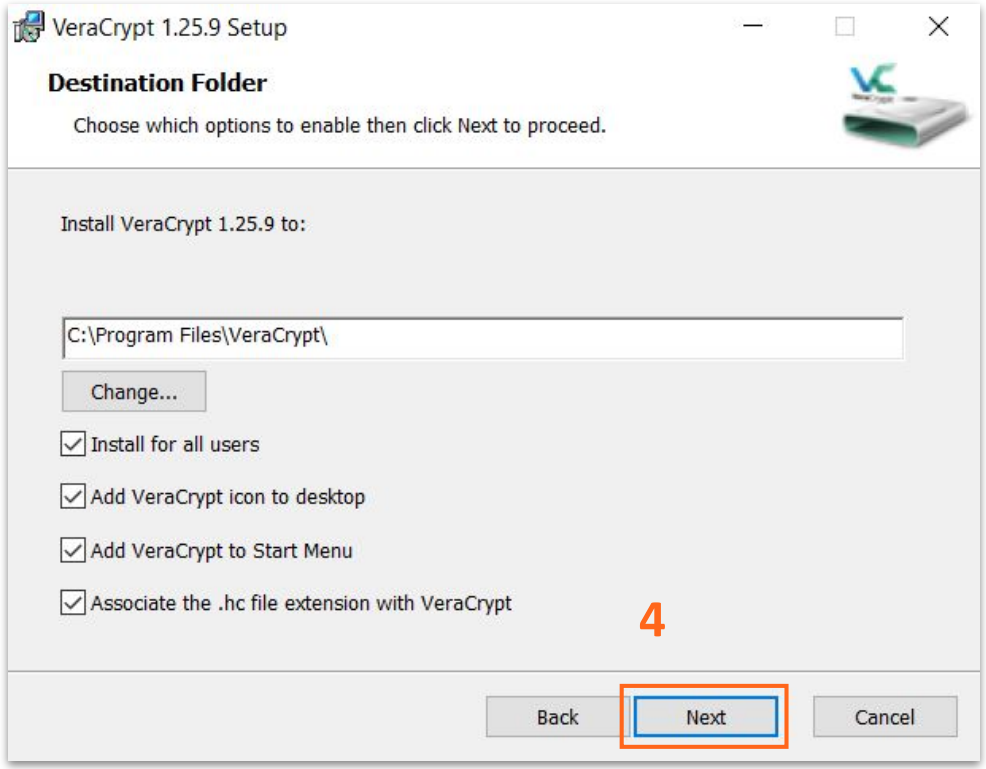
- ➔ Ingresa en: https://www.veracrypt.fr/en/Downloads.html y descarga la versión que se adapte a tu sistema operativo (Microsoft Windows, Mac OS X o GNU/Linux.
- ➔ Haz doble clic en el archivo de instalación llamado "**VeraCrypt_Setup**" y habilita los permisos para que se ejecute el instalador del programa.
- ➔ Acepta los "**términos de la licencia**" y continúa con el proceso de instalación hasta que finalice y puedas ver el botón de acceso directo a VeraCrypt en tu escritorio.



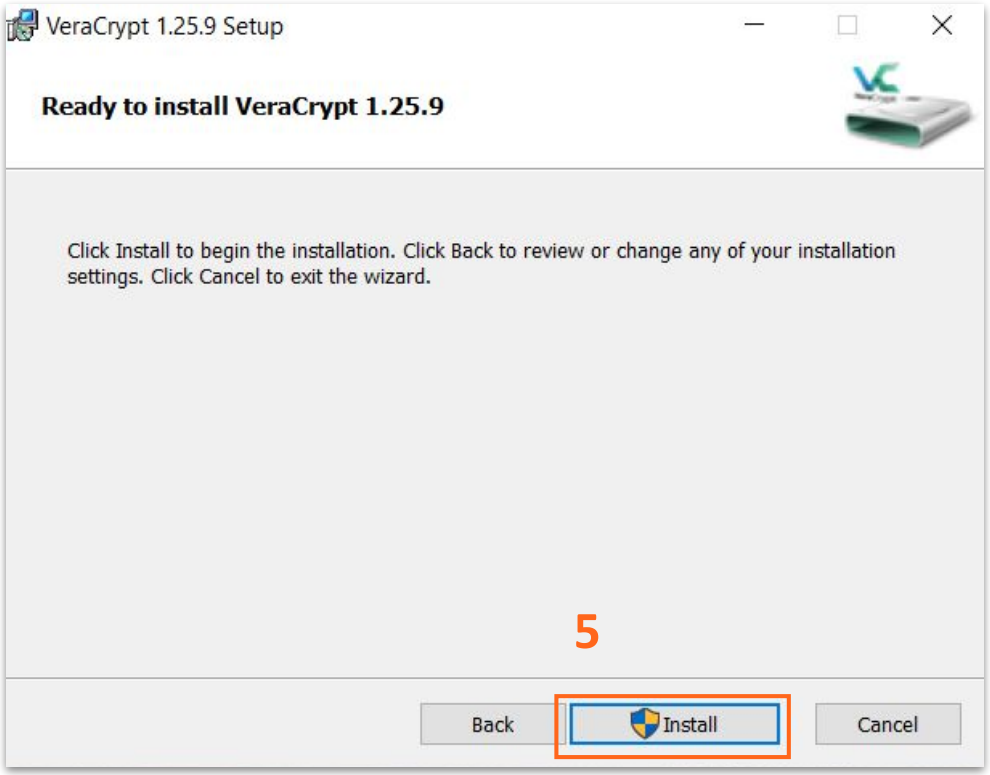


INSTALACIÓN

1. Instala VeraCrypt



➔ Elige dónde quieres instalar VeraCrypt y haz clic en "**Siguiente**"

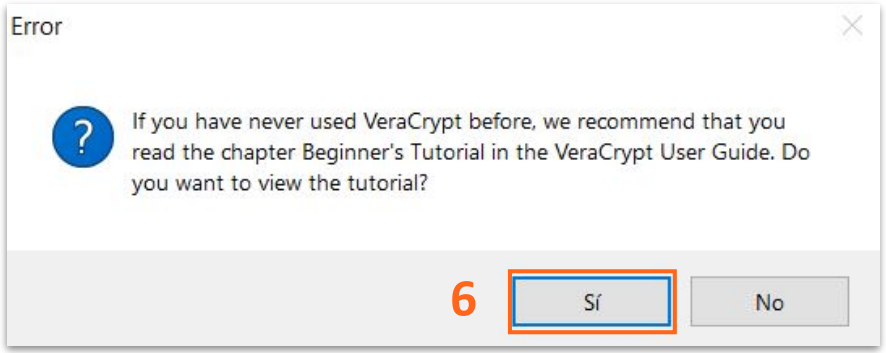


➔ Haz clic en "**Instalar**" y espera a que se culmine la instalación del programa

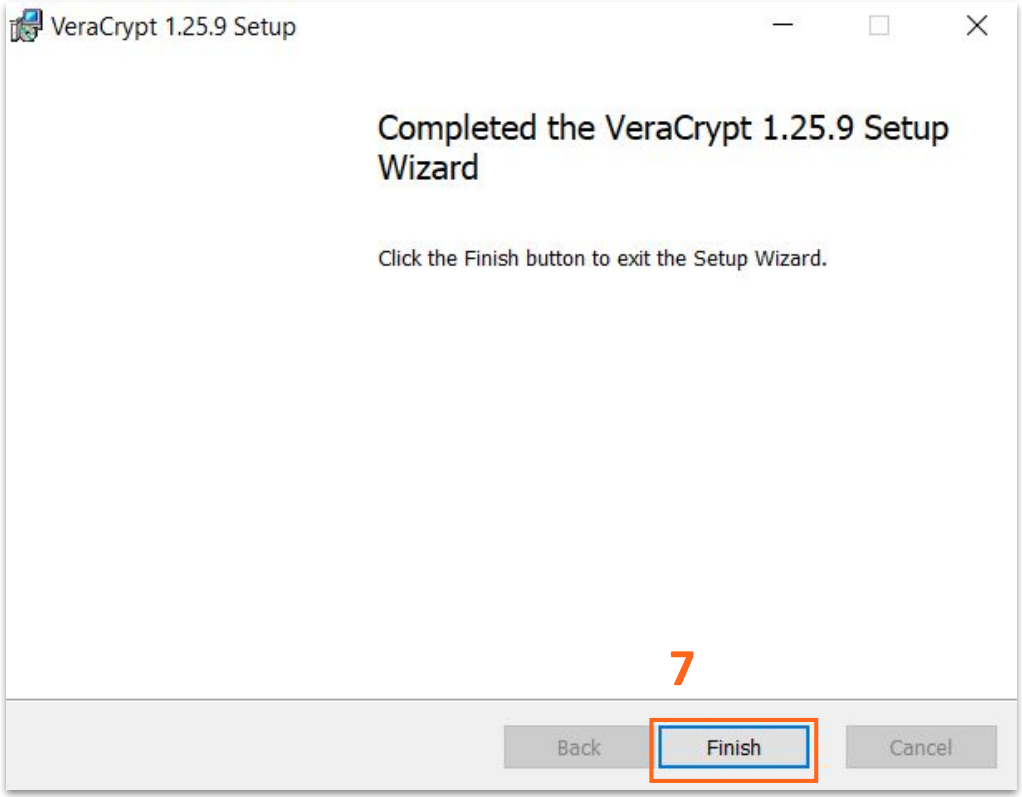


INSTALACIÓN

1. Instala VeraCrypt







➔ Al finalizar la instalación, te saldrá una notificación para visualizar el "**Tutorial para principiantes de VeraCrypt**". Opcionalmente haz clic en "**Sí**" y explora la información.

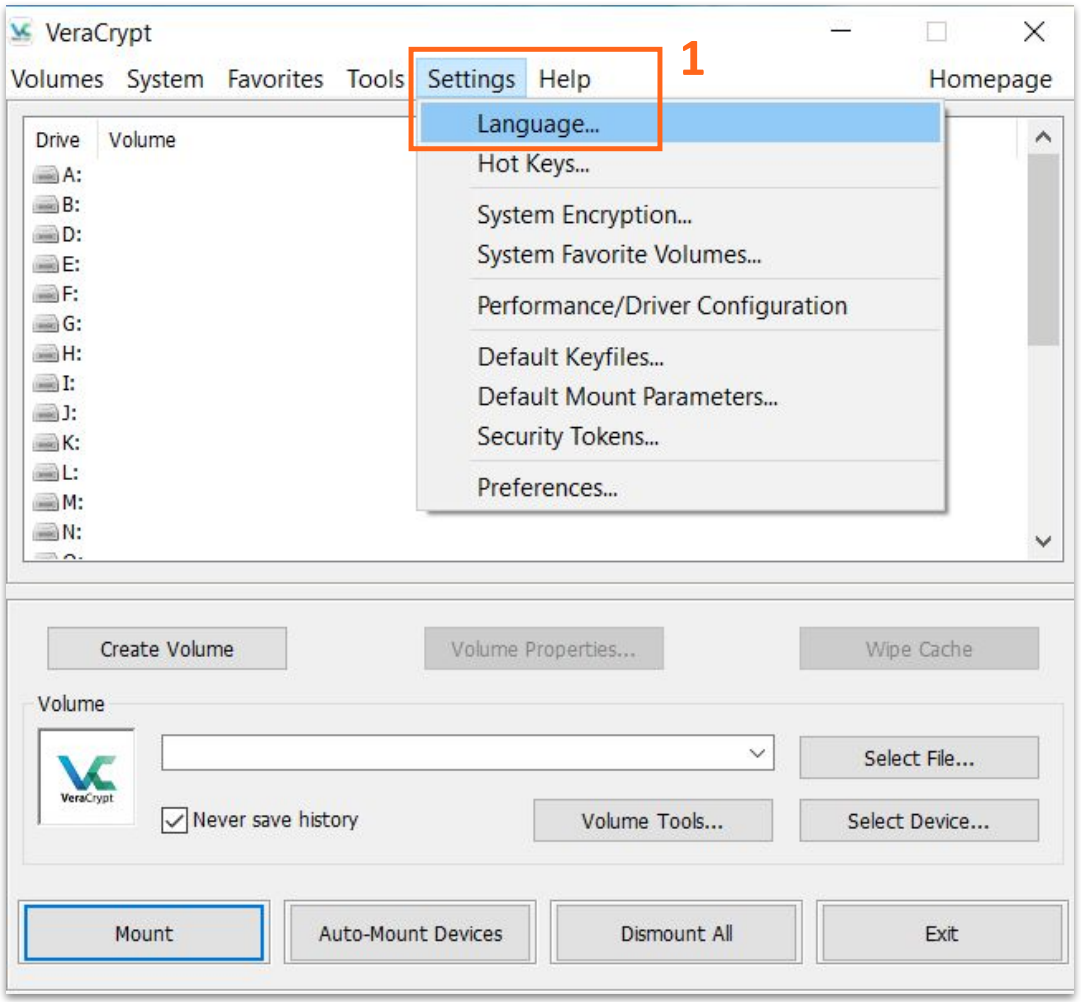
➔ Haz clic en "**Finalizar**" y busca el botón de acceso directo a VeraCrypt en tu escritorio para comenzar a utilizarlo.

Nota: Si no quieres hacer evidente el hecho de que posiblemente tengas archivos encriptados en tu computadora, tal vez prefieras borrar este acceso directo.

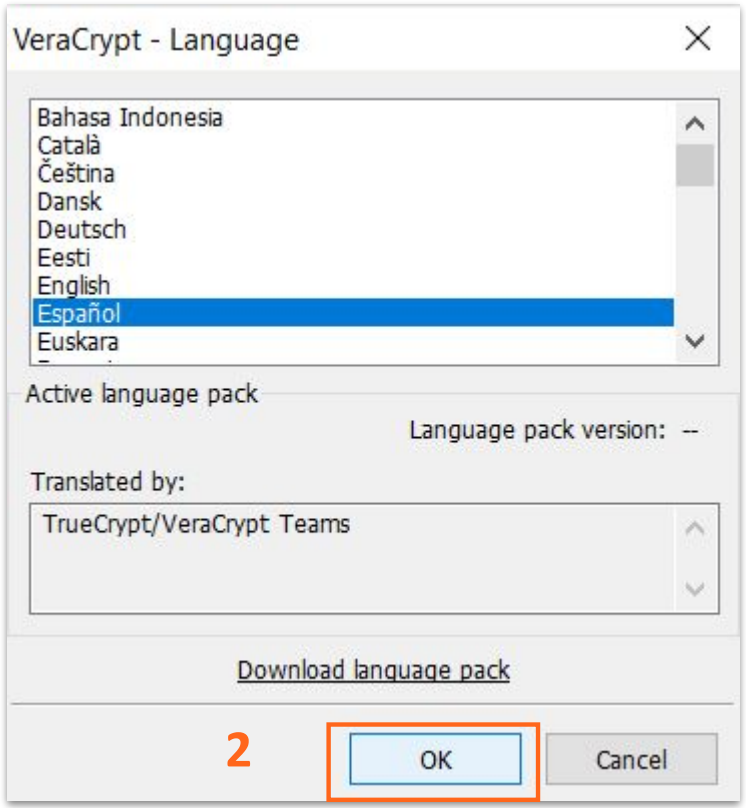


INSTALACIÓN

1. Instala VeraCrypt
1.1 Configura el lenguaje de preferencia



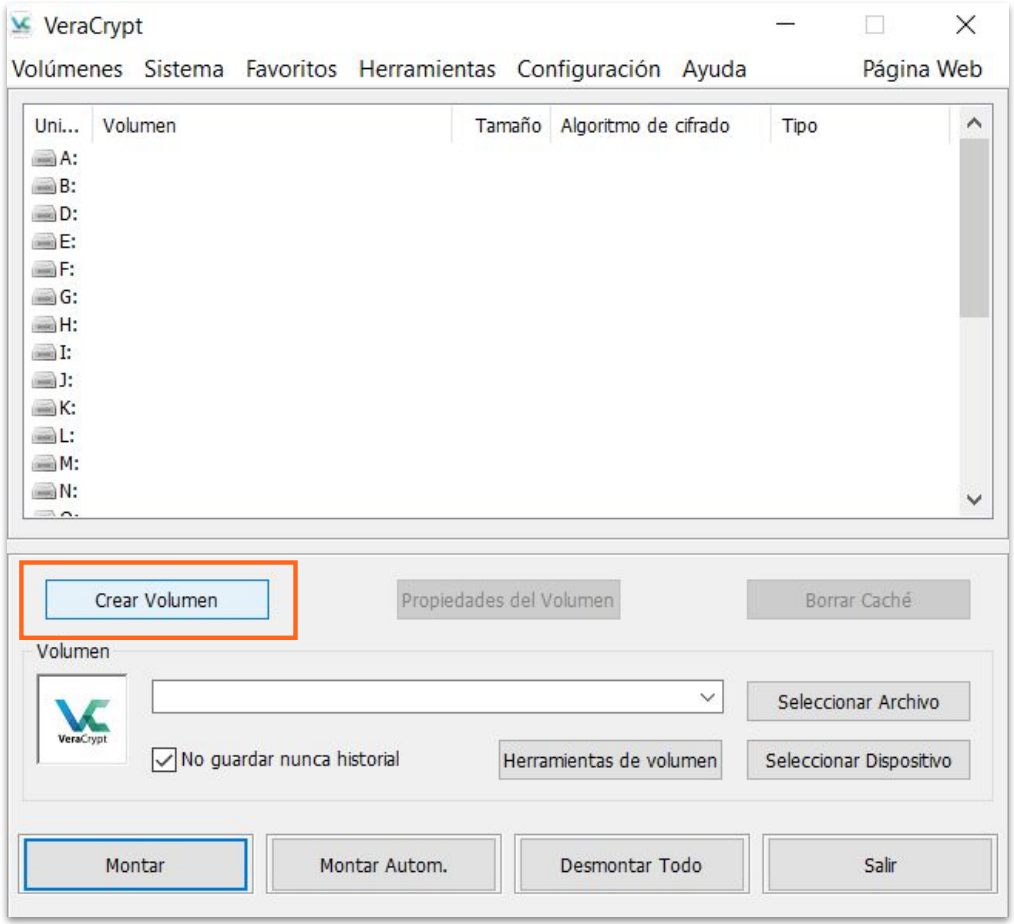
➔ Abre el programa y haz clic en "**Settings**" > "**Language**" y selecciona el lenguaje de tu preferencia. Luego haz clic en "**OK**"



VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar

➔ Abre VeraCrypt para acceder a la página inicial de la aplicación y haz clic en **“Crear Volumen”** para activar el *“Asistente de creación de volumen de VeraCrypt”*



Los volúmenes estándar protegen tus archivos encriptándolos con una contraseña que se debe ingresar para poder de acceder a ellos. **Estos volúmenes no están ocultos.**

VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar



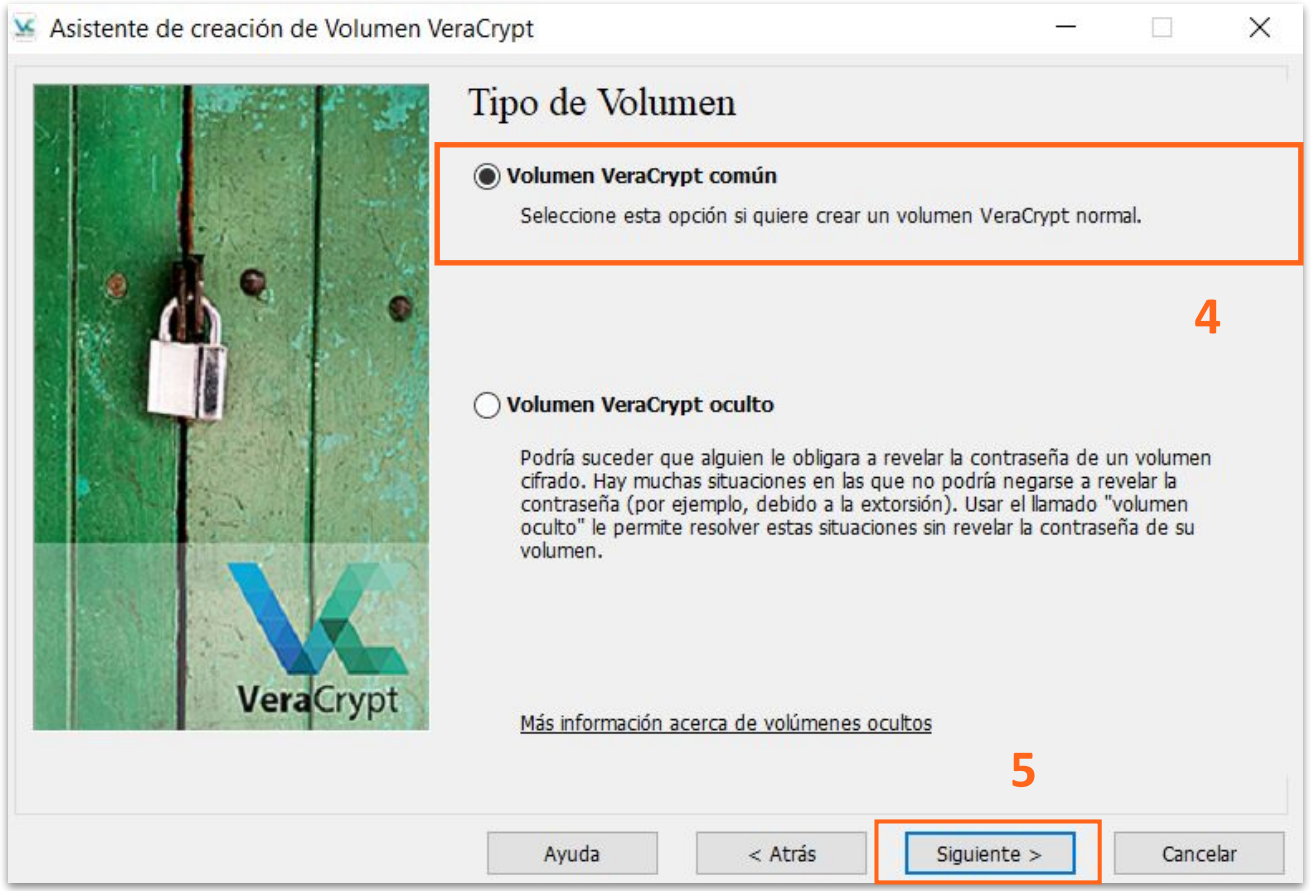
➔ Haz clic en "**Crear un contenedor de archivos cifrado**": En este caso, crearemos un **disco cifrado virtual dentro de un archivo**, llamado **"Contenedor".**

➔ Haz clic en "**Siguiente**" para elegir el tipo de volumen que quieres crear

VOLUMEN ESTÁNDAR

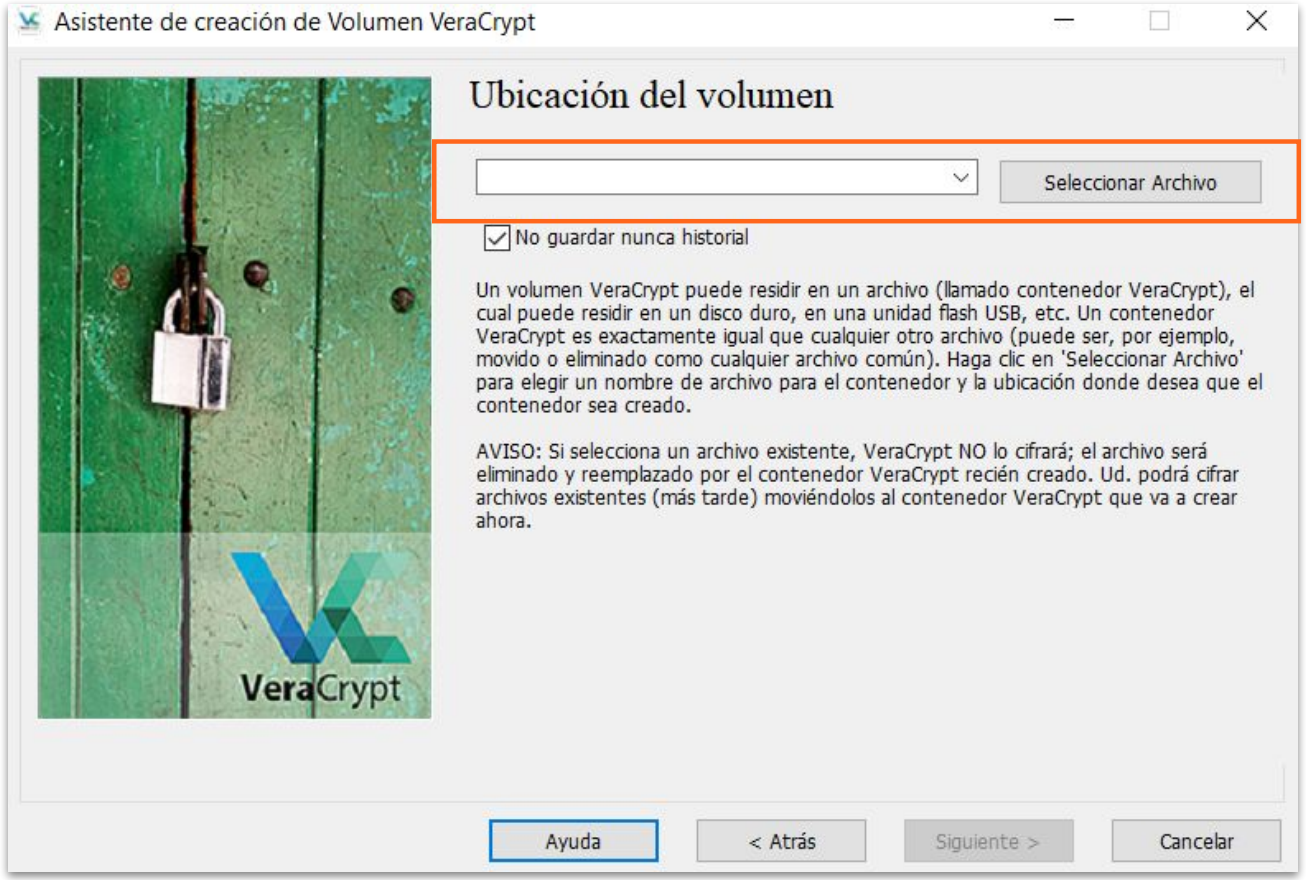
2. Crea un Volumen Estándar

- ➔ Selecciona el **“Volumen VeraCrypt común”**, que se refiere a un volumen estándar.
- ➔ Haz clic en “**Siguiente**” para elegir un nombre y ubicación para el archivo contenedor de VeraCrypt.



VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar



6

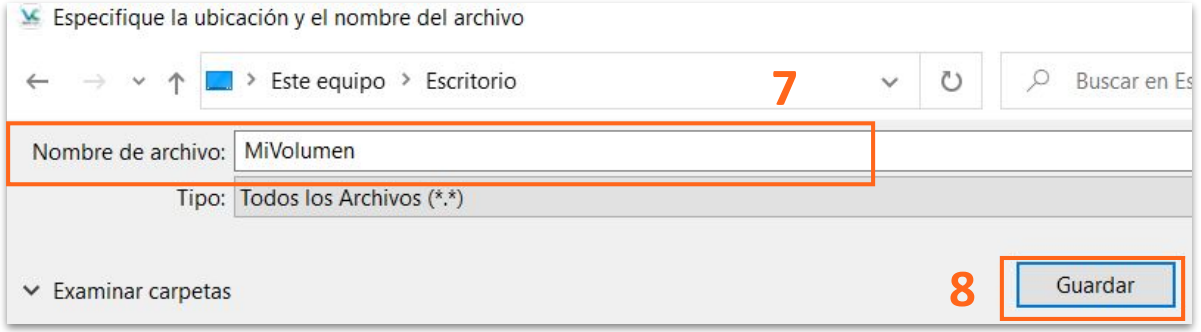
➔ Haz clic en "**Seleccionar Archivo"** para elegir la ubicación en donde vas a guardar tu archivo contenedor de VeraCrypt

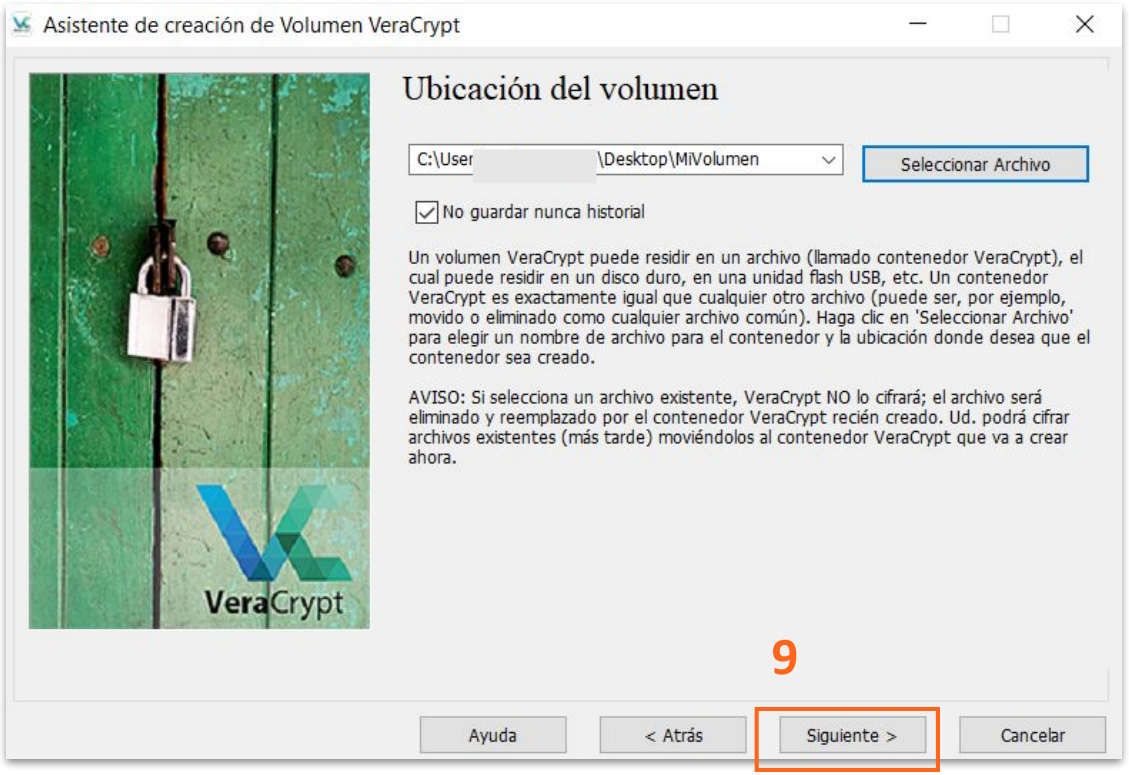
VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar

En esta sección, crearemos nuestro contenedor en el **Escritorio** y lo llamaremos **“Mi Volumen”:**

- ➔ Elige una ubicación y **especifica un nombre** para el archivo contenedor de VeraCrypt que estás a punto de crear.
- ➔ Haz clic en “**Guardar**” para volver al **“Asistente de creación de volumen”**
- ➔ Haz clic en “**Siguiente**” para acceder a la ventana de **“Opciones de encriptación”**





Nota: Puedes usar cualquier nombre de archivo o extensión de archivo para tu contenedor. Por ejemplo, “recetas.doc”, con la esperanza de que un observador casual piense que es un documento Microsoft Word

VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar



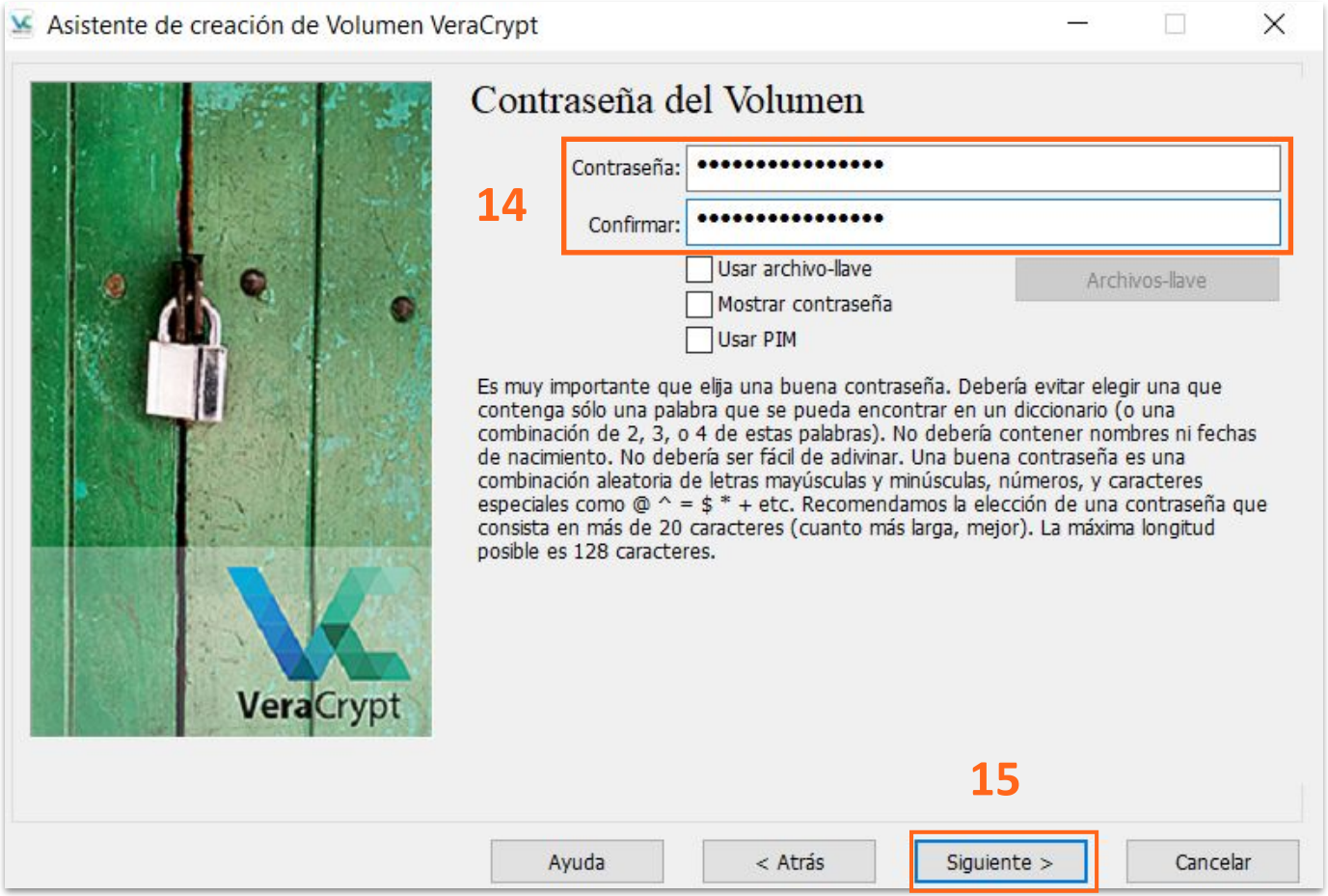


- ➔ Selecciona en la lista desplegable un método específico (o algoritmo) a usar cuando cifres y descifres los archivos almacenados dentro de tu contenedor VeraCrypt. **Las opciones por defecto se consideran seguras, así que probablemente deberías dejarlas tal como están.**

- ➔ Haz clic en "**Siguiente**" para determinar el tamaño que tendrá tu volumen encriptado estándar
- ➔ Escribe el tamaño del volumen que quieres crear. Asegúrate de elegir el valor correcto para KB (kilobytes), MB (megabytes), GB (gigabytes) o TB (terabytes).
- ➔ Haz clic en "**Siguiente**" para elegir una contraseña.

VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar



- ➔ Escribe tu contraseña y luego vuelve a escribirla en el campo "**Confirmar**" para activar el botón "**Siguiente**".
- ➔ Haz clic en "**Siguiente**" para elegir el formato del volumen.

Nota: Tu contraseña debe seguir las recomendaciones para que sea segura. **VeraCrypt te recomienda que sean contraseñas de 20 caracteres o más.** Utilizar una contraseña segura es uno de los pasos más importantes para proteger tu volumen de VeraCrypt. Te recomendamos almacenarla en un lugar seguro como tu administrador de contraseñas



VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar



- ➔ Dependiendo del tamaño que le asignes al volumen esta pantalla podría aparecer
- ➔ Si tus archivos pueden ser mayores a 4 GB selecciona **sí**, en caso contrario selecciona **no**
- ➔ Haz clic en "**Siguiente**" para elegir el formato del volumen.

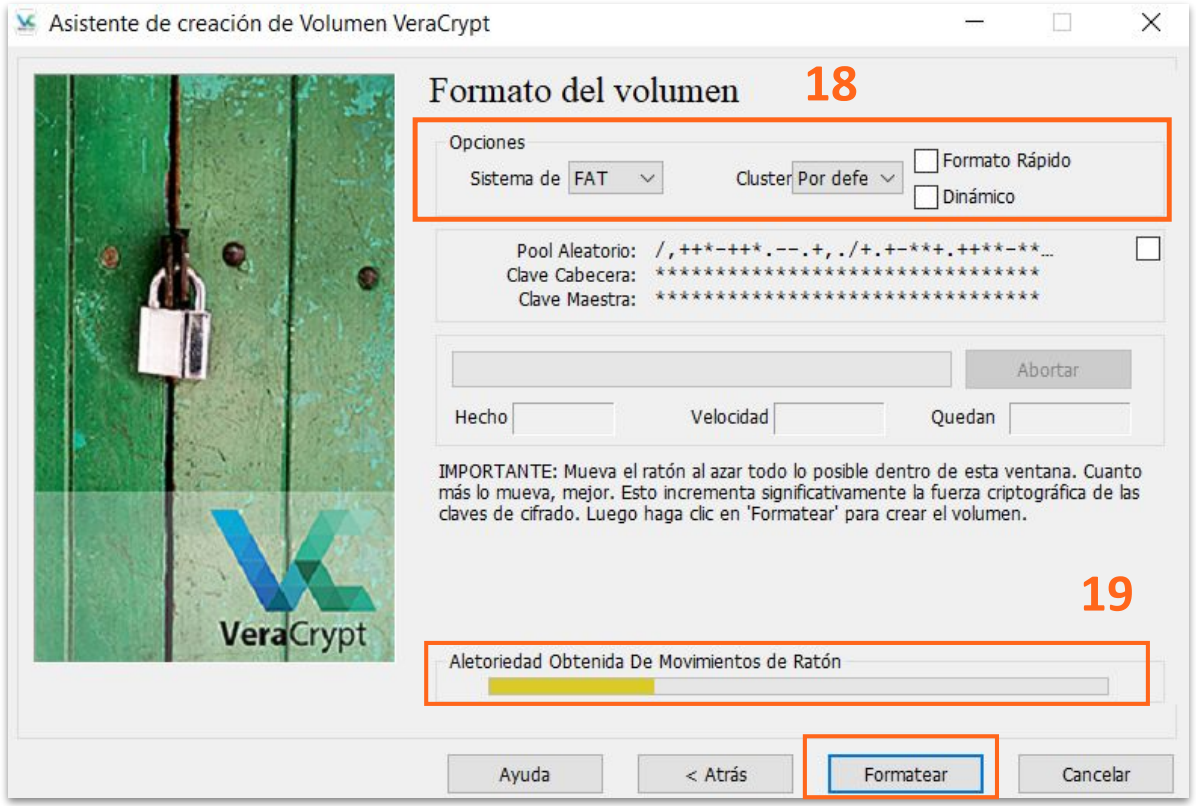
Nota: VeraCrypt hace esta pregunta para saber que tipo de formato colocará por defecto en la siguiente pantalla FAT o exFAT



VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar

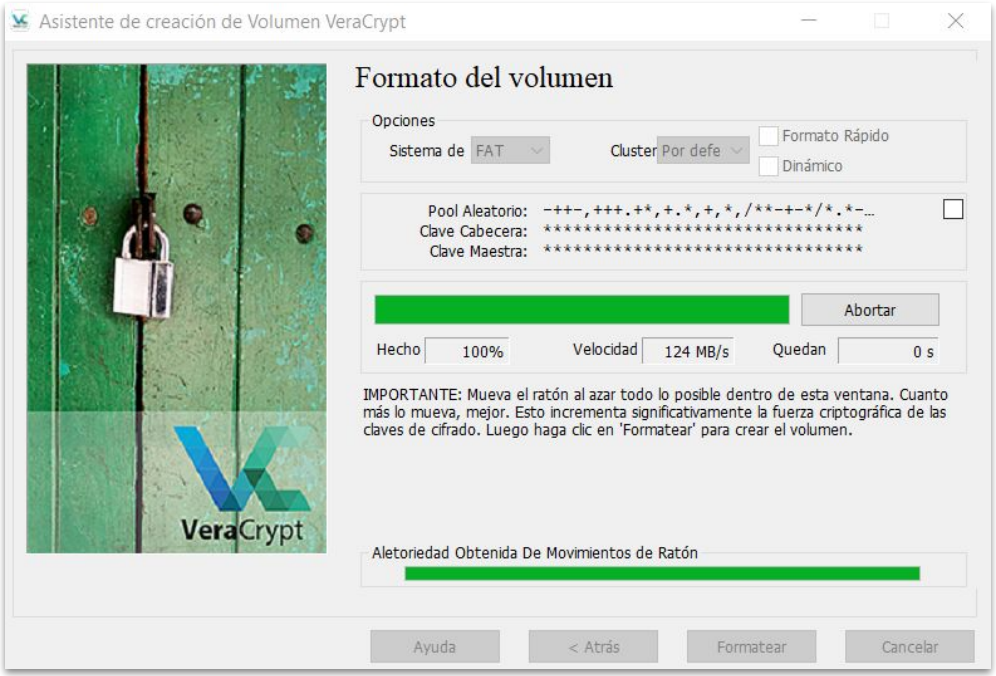
- ➔ Selecciona las opciones de formato que se requieran
- ➔ Mueve el ratón al azar dentro de la ventana para aumentar la fuerza criptográfica de las claves de cifrado **(hasta que la barra se coloque en verde)**
- ➔ Haz clic en "**Formatear**" para empezar a crear tu volumen estándar

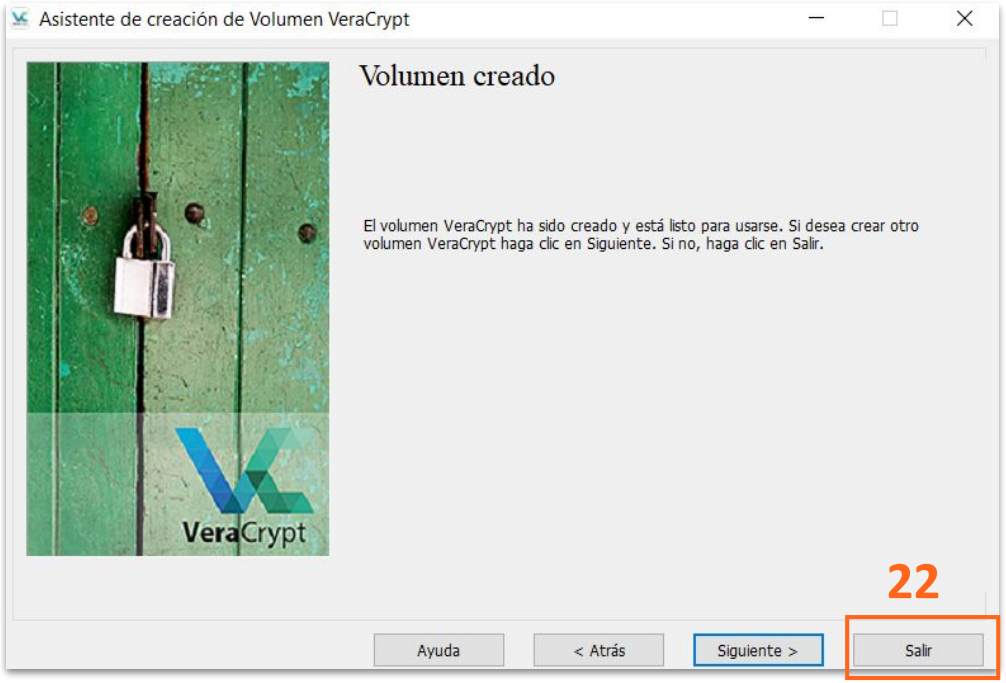


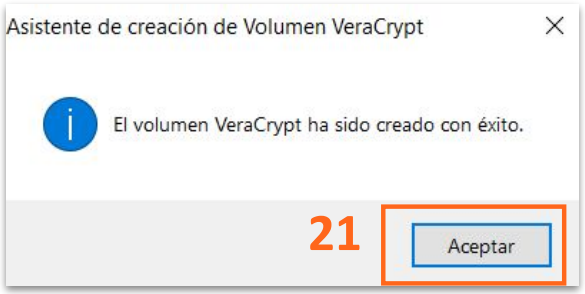
Nota: El valor por defecto ("FAT") funcionará para la mayoría de los usuarios y es compatible con computadoras Windows, Mac OS X y Linux. sólo podrás guardar archivos menores a 4G

VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar





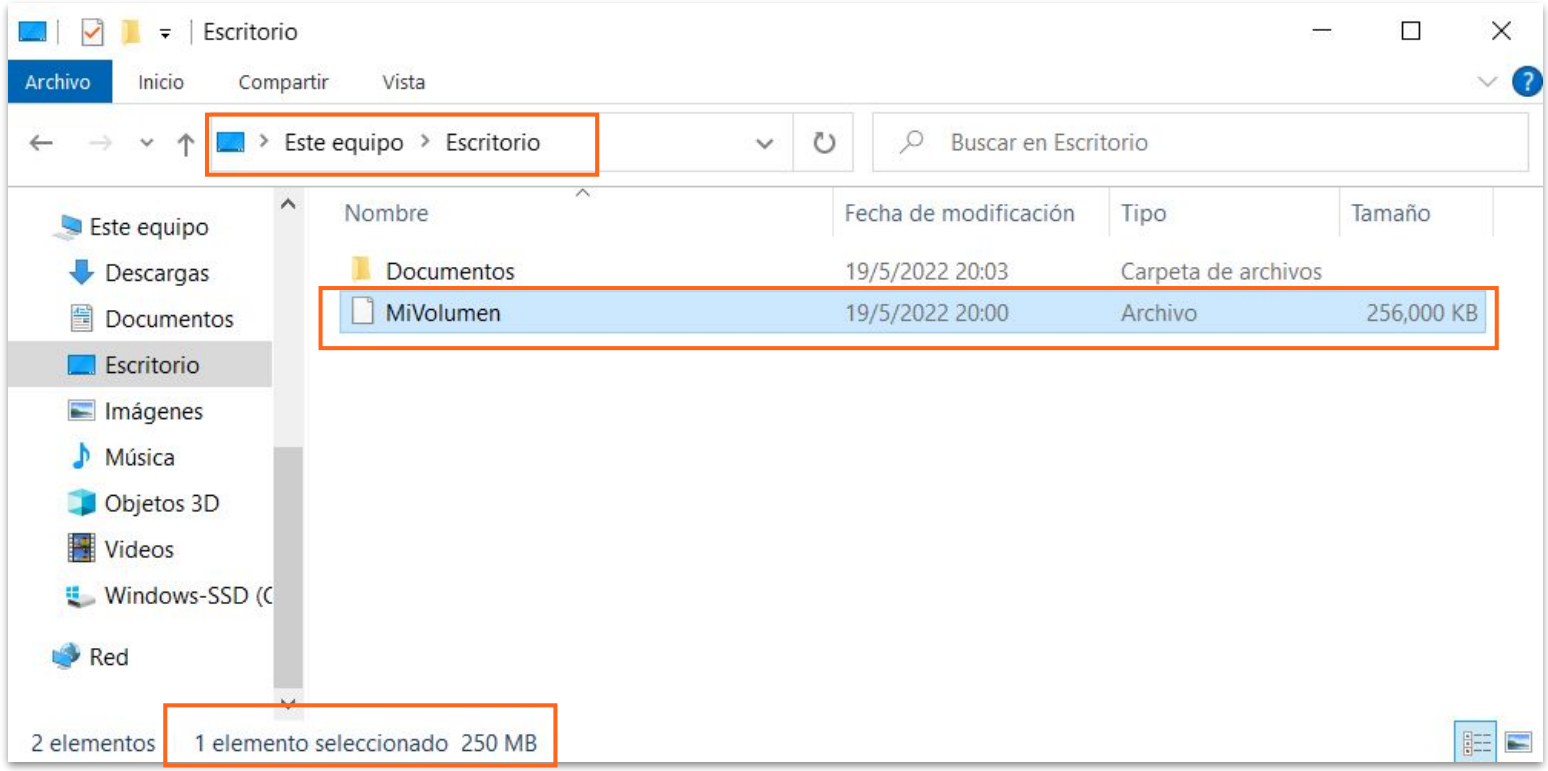


- ➔ VeraCrypt te avisará cuando el volumen haya sido creado con éxito
- ➔ Haz Clic en "**Aceptar**" para continuar
- ➔ Haz Clic en "**Salir**" para volver a la página inicial

VOLUMEN ESTÁNDAR

2. Crea un Volumen Estándar

➔ Ahora puedes ver un archivo llamado **“Mi Volumen”** en el Escritorio, como se especifica arriba. Este archivo tendrá un contenedor de volumen estándar VeraCrypt de 250 MB, el cual puedes usar para almacenar tus archivos de una forma más segura.



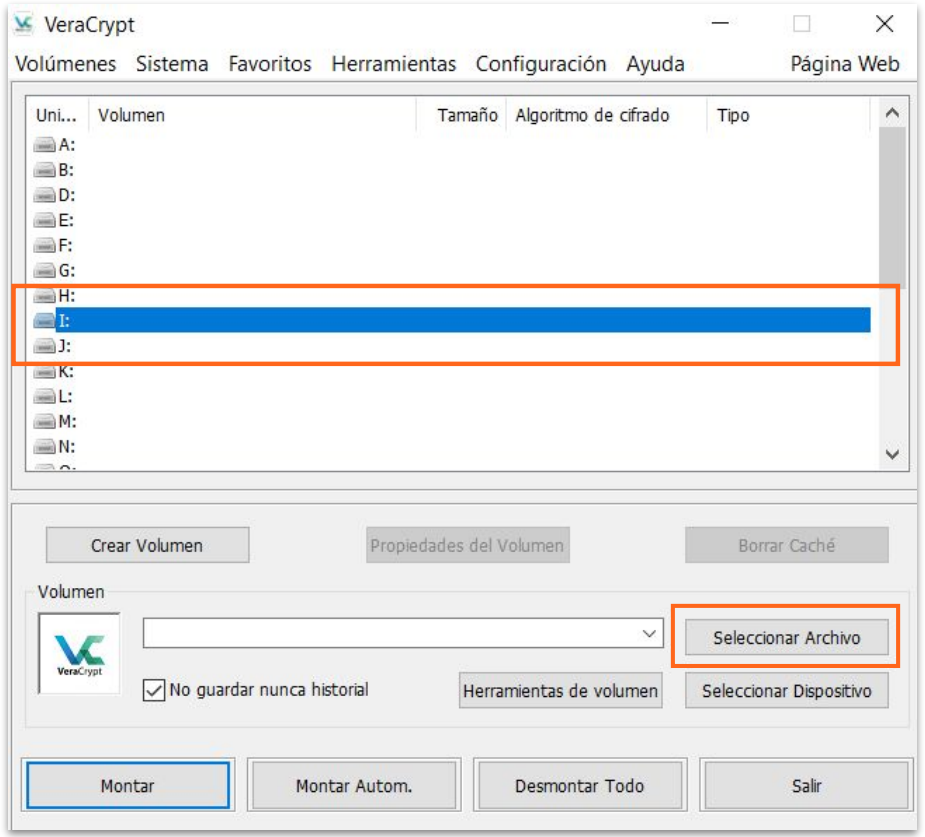
USAR TU VOLUMEN

Se denomina "**montar**" a la acción de integrar un sistema de archivos alojado en un determinado dispositivo dentro del árbol de directorios de un sistema operativo.

3. Usa tu volumen estándar VeraCrypt

3.1 Montar un volumen estándar (para abrirlo):

En VeraCrypt, montar un volumen es hacerlo disponible para uso. Aparece como si hubieras adjuntado una memoria USB a tu computadora. Puedes usar este disco para acceder, crear, modificar o borrar archivos y carpetas. Para montar un volumen sigue los siguientes pasos:



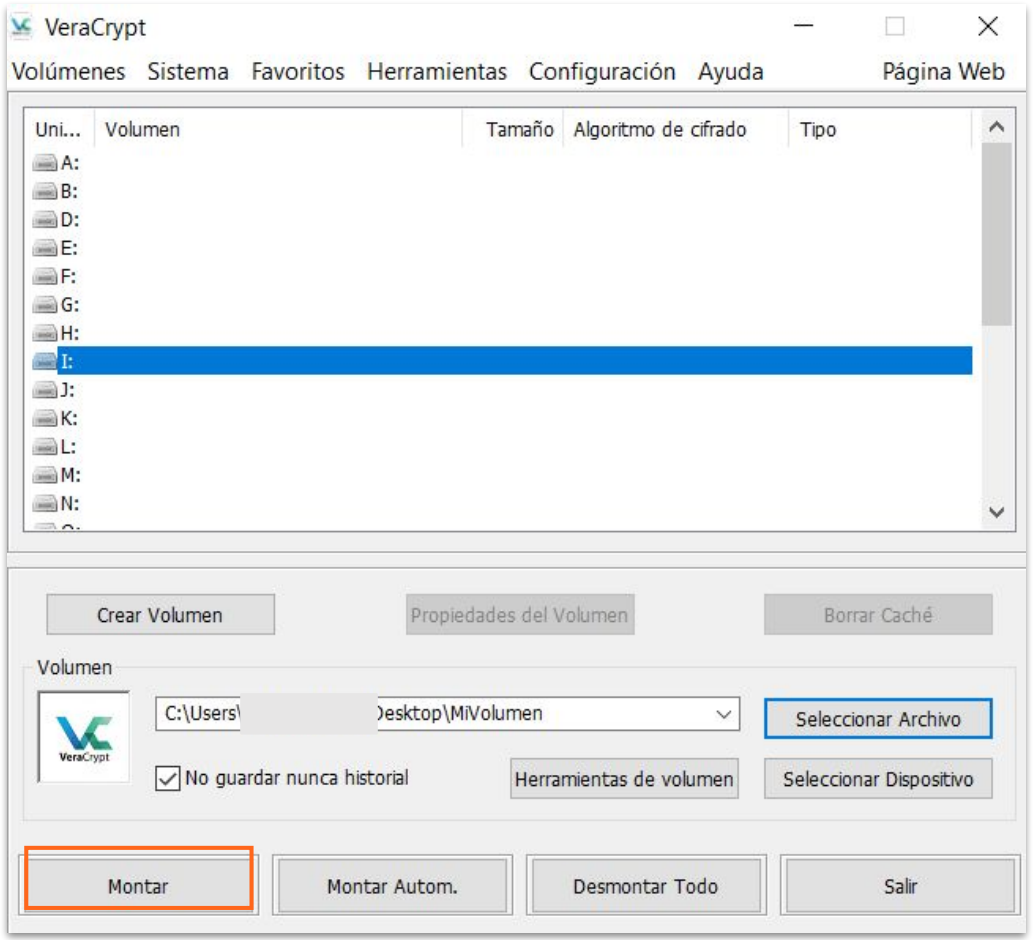
- ➔ Abre VeraCrypt para acceder a la página inicial de la aplicación y elige una de las unidades que existen disponibles.
- ➔ Haz clic en "**Seleccionar Archivo**" para ubicar tu archivo contenedor de VeraCrypt

Nota: Escogimos montar nuestro volumen encriptado en la "Unidad I:" Puedes escoger la letra de cualquiera de las unidades que se muestran.

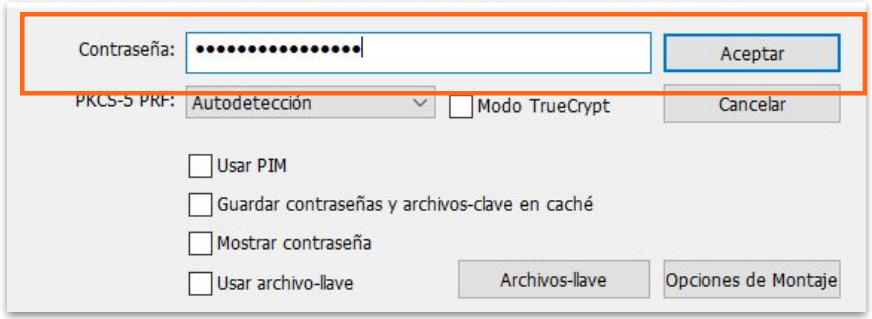
USAR TU VOLUMEN

3. Usa tu volumen estándar VeraCrypt

3.1 Montar un volumen estándar (para abrirlo):



3



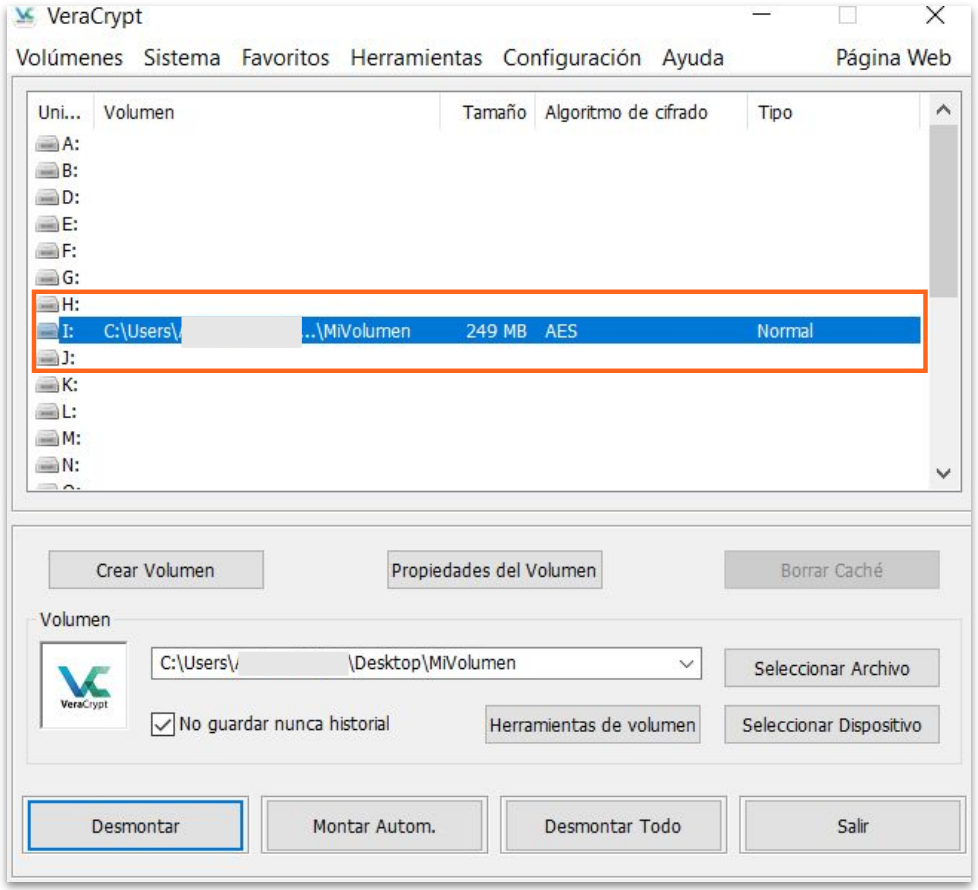
4

- ➔ Haz clic en "**Montar**" para escribir tu contraseña.
- ➔ Escribe la contraseña del volumen estándar.
- ➔ Haz clic en "**Aceptar**" para montar el volumen.

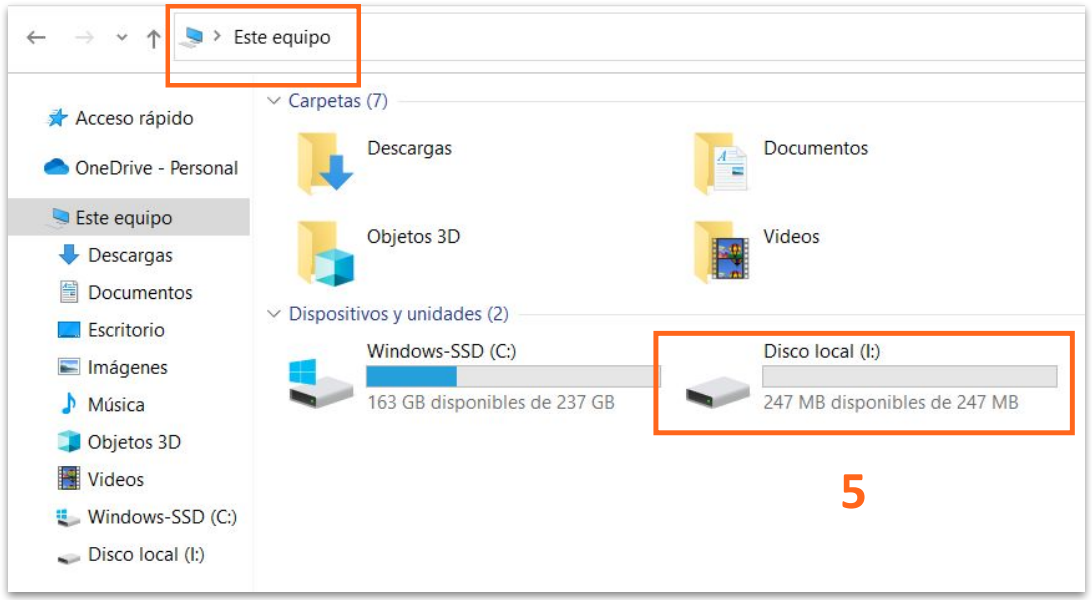
USAR TU VOLUMEN

3. Usa tu volumen estándar VeraCrypt

3.1 Montar un volumen estándar (para abrirlo):



- Luego de montar el volumen, podrás visualizarlo en la aplicación de VeraCrypt en la unidad que seleccionaste. O, puedes visualizarlo como un dispositivo en la lista de unidades de tu equipo.
- Haz doble clic en cualquiera de las dos visualizaciones, para acceder a tu volumen montado.

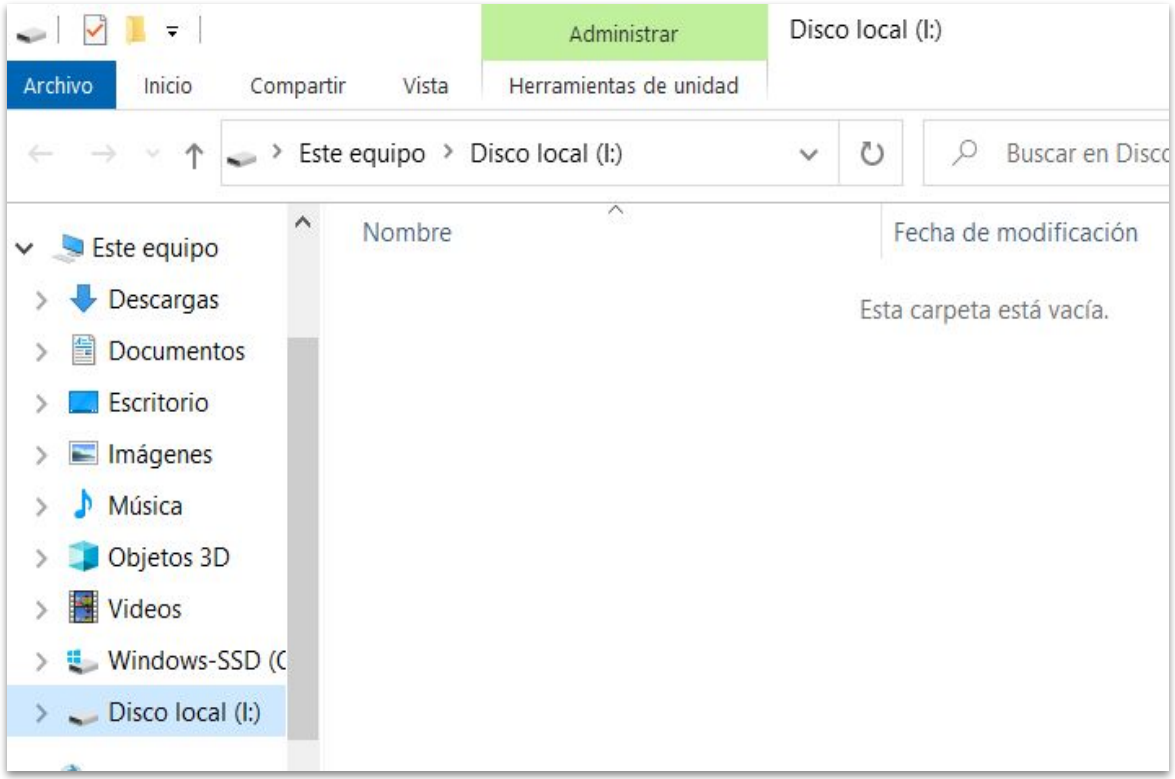


USAR TU VOLUMEN

3. Usa tu volumen estándar VeraCrypt

3.1 Montar un volumen estándar (para abrirlo):

- ➔ Inicialmente, el volumen estará vacío. Cuando hayas guardado los archivos ahí, serán accesibles (y se podrán editar) cada vez que abras el volumen.
- ➔ Este disco virtual funciona como un dispositivo de almacenamiento externo, se pueden copiar archivos hacia y desde el disco tal como se haría con un dispositivo de almacenamiento USB.
- ➔ Mientras tu volumen de VeraCrypt esté montado, los archivos adentro no están protegidos y serán visibles a cualquiera que tenga acceso a tu computadora.



Nota: Para proteger tus archivos sensibles, debes **desmontar** tu volumen de VeraCrypt cuando no lo estés usando. Cerrar simplemente la ventana principal haciendo clic en "**Salir**" no es suficiente para salir completamente de la aplicación y ocultar tu volumen.

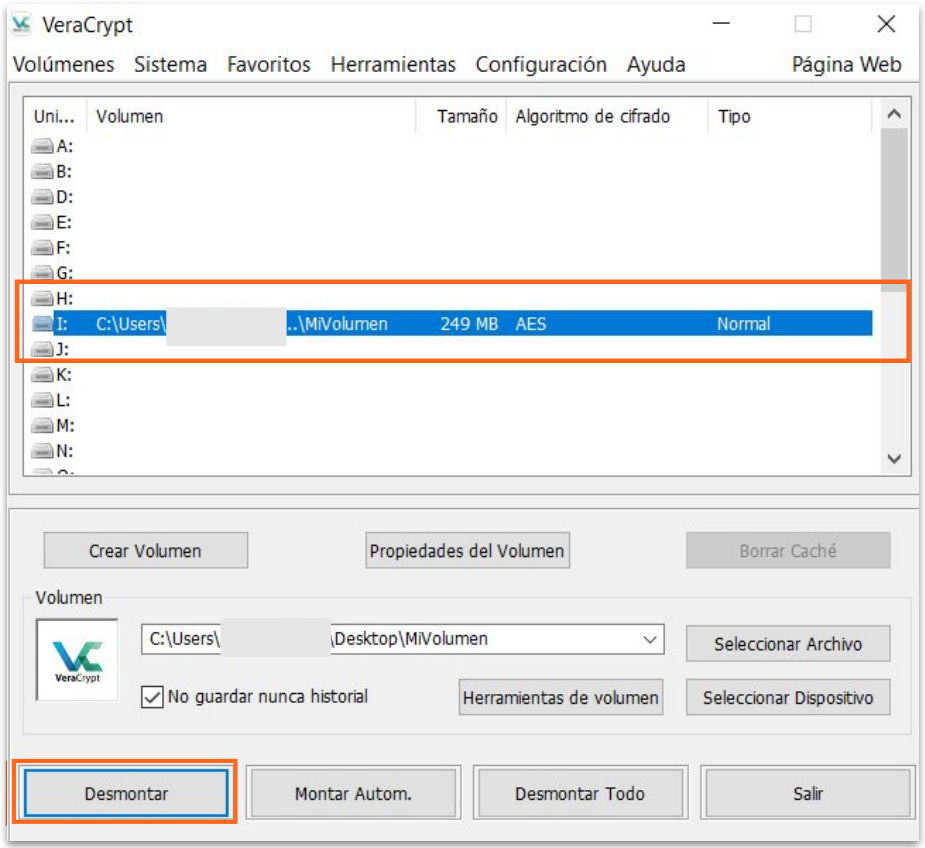
USAR TU VOLUMEN

3. Usa tu volumen estándar VeraCrypt

3.2 Desmontar un volumen estándar (para cerrar):

"**Desmontar**" es la operación inversa a "**montar**", por la cual se desconecta un dispositivo de un árbol de carpetas.

En VeraCrypt, desmontar un volumen es hacer que ya no esté disponible para ser usado.
Para desmontar un volumen y asegurarte de que nadie pueda tener acceso a los archivos a menos que sepan la contraseña apropiada, realiza los siguientes pasos:



1

2

- ➔ Abre VeraCrypt para acceder a la página inicial de la aplicación y seleccionar la unidad en donde se encuentre el volumen que quieres desmontar.
- ➔ Haz clic en "**Desmontar**" para cerrar tu volumen VeraCrypt
- ➔ Sal de VeraCrypt

Nota: Para recuperar un archivo guardado en tu volumen una vez que lo hayas cerrado o desmontado, deberás volver a montarlo.

USAR TU VOLUMEN

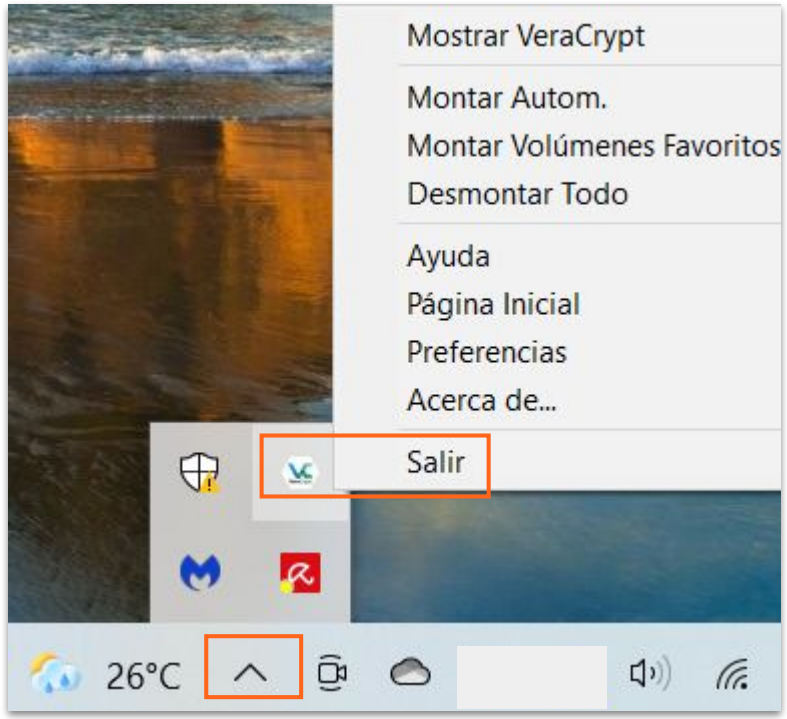
3. Usa tu volumen estándar VeraCrypt

3.2 Desmontar un volumen estándar (para cerrar):

IMPORTANTE: Asegúrate de **desmontar** tu volumen VeraCrypt antes de:

- ➔ Retirar el dispositivo de almacenamiento externo USB en el que tu contenedor está guardado (si has escogido guardarlo en un dispositivo de almacenamiento USB).
- ➔ Poner tu computadora en modo “De espera” o “Hibernación”
- ➔ Dejar tu computadora sin supervisión.
- ➔ Entrar en una situación en donde hay más probabilidades que de costumbre que tu computadora se pierda, la roben o confisquen.

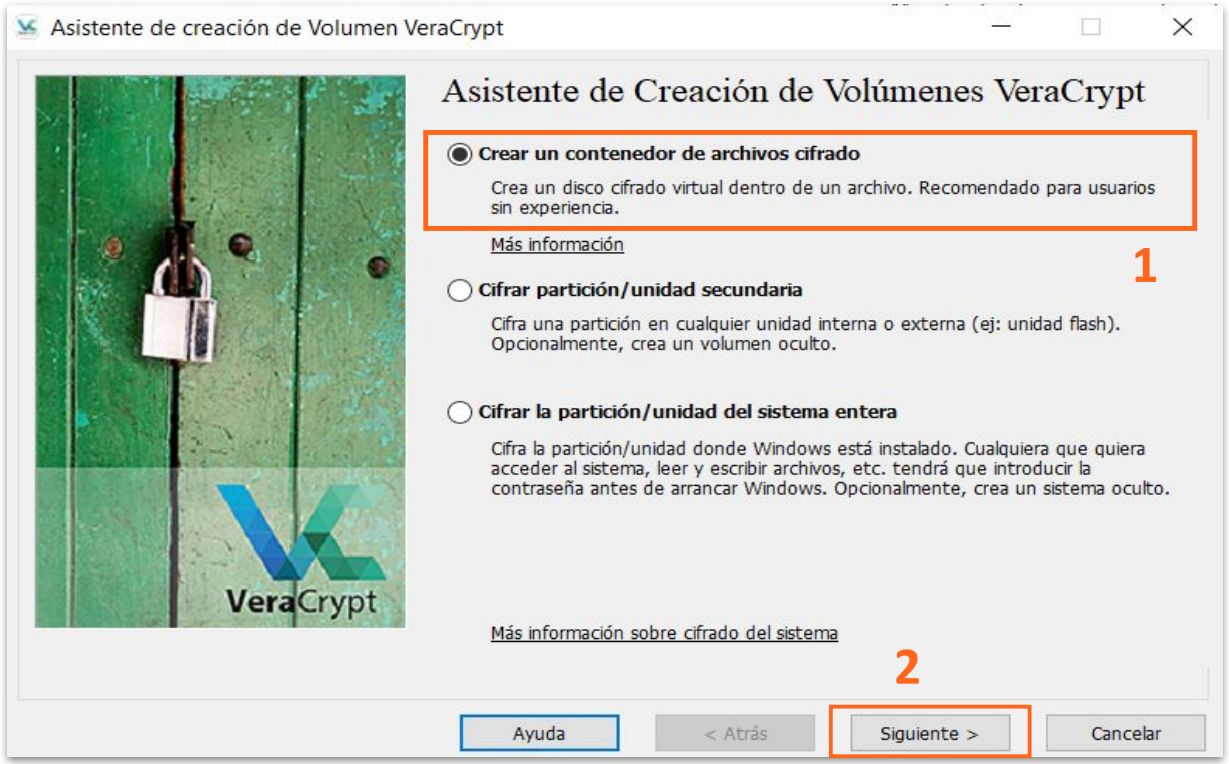
Nota: Para salir completamente de VeraCrypt, debes buscar el icono en la barra de tareas y hacer clic derecho en “Salir”



VOLUMEN OCULTO

4. Crea un Volumen Oculto

- En VeraCrypt, un volumen oculto se almacena dentro de tu volumen estándar encriptado.
- El objetivo de un volumen oculto es esconder su propia existencia, y por tanto, esconder los archivos dentro, aunque te obliguen a revelar la contraseña de tu volumen estándar.
- VeraCrypt te permite crear dos contraseñas separadas: una que abre el volumen estándar exterior (o "señuelo") y una que abre el volumen oculto interior.



Para crear un Volumen Oculto en VeraCrypt sigue los siguientes pasos:

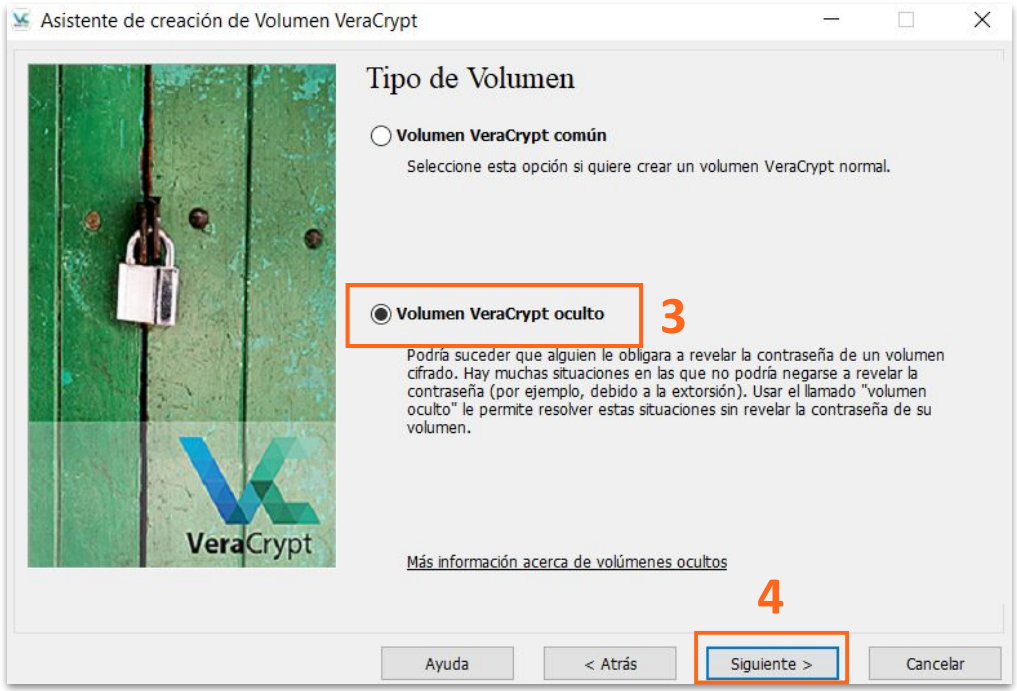
➔ Accede al "**Asistente de creación de volúmenes de VeraCrypt**"
(Abre VeraCrypt > Crear Volumen)

➔ Selecciona "**Crear un contenedor de archivos cifrado**"

➔ Haz clic en "**Siguiente**" para elegir el tipo de volumen, en este caso oculto.

VOLUMEN OCULTO

4. Crea un Volumen Oculto



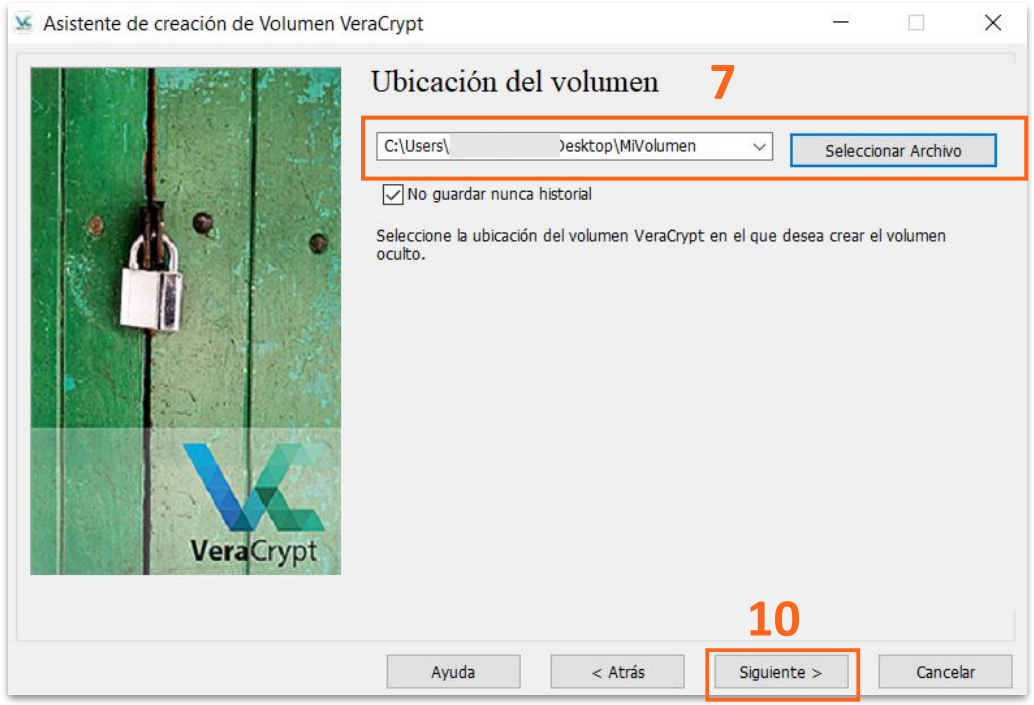


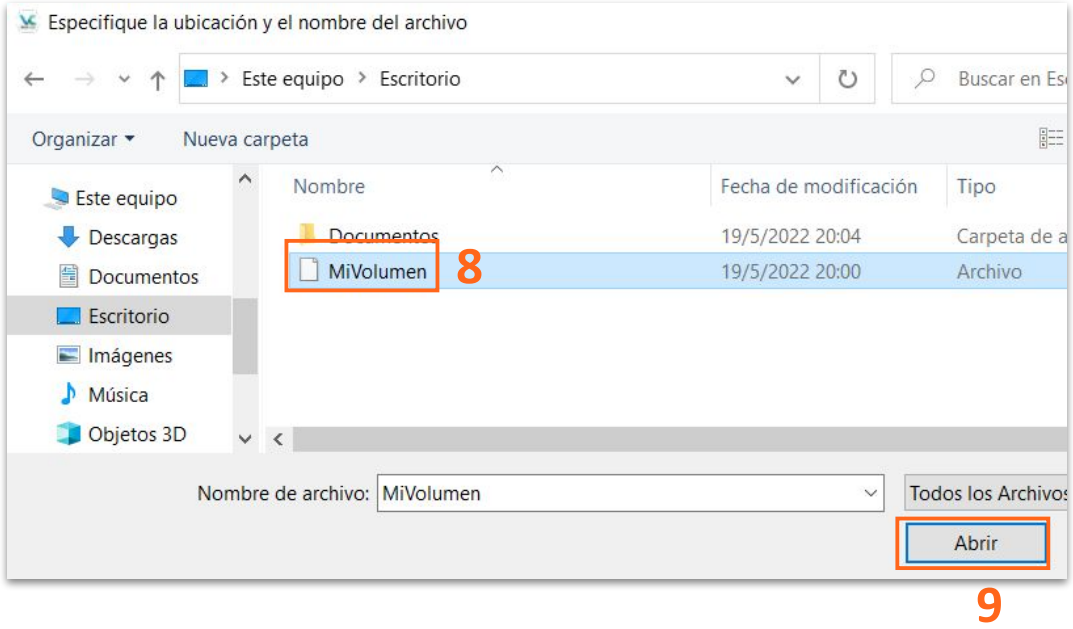
- ➔ Selecciona "**Volumen VeraCrypt oculto**".
- ➔ Haz clic en "**Siguiente**" para elegir el modo en cómo vas a crear el volumen oculto.

- ➔ Aprovecharemos el volumen estándar creado, selecciona "**Modo Directo**".
- ➔ Haz clic en "**Siguiente**" para elegir el volumen estándar ya existente.

VOLUMEN OCULTO

4. Crea un Volumen Oculto





- ➔ Haz clic en "**Seleccionar Archivo**" y ubica tu archivo contenedor de volumen estándar existente.

  ("Mi Volumen", creado en el apartado anterior y ubicado en Escritorio).

- ➔ Selecciona el archivo contenedor del volumen estándar existente, y haz clic en **"Abrir"**.
- ➔ Haz clic en "**Siguiente**" para ingresar la contraseña de tu volumen estándar existente.

VOLUMEN OCULTO

4. Crea un Volumen Oculto





- ➔ Escribe la contraseña que elegiste al crear el volumen estándar seleccionado.
- ➔ Haz clic en "**Siguiente**" para preparar el volumen estándar y que se le agregue un volumen oculto.
- ➔ Acepta los permisos que solicita el sistema.

- ➔ Luego del análisis, VeraCrypt te avisará cuando esté listo para configurar el volumen oculto.
- ➔ Haz clic en "**Siguiente**" para seleccionar las opciones de encriptación del volumen oculto.

VOLUMEN OCULTO

4. Crea un Volumen Oculto



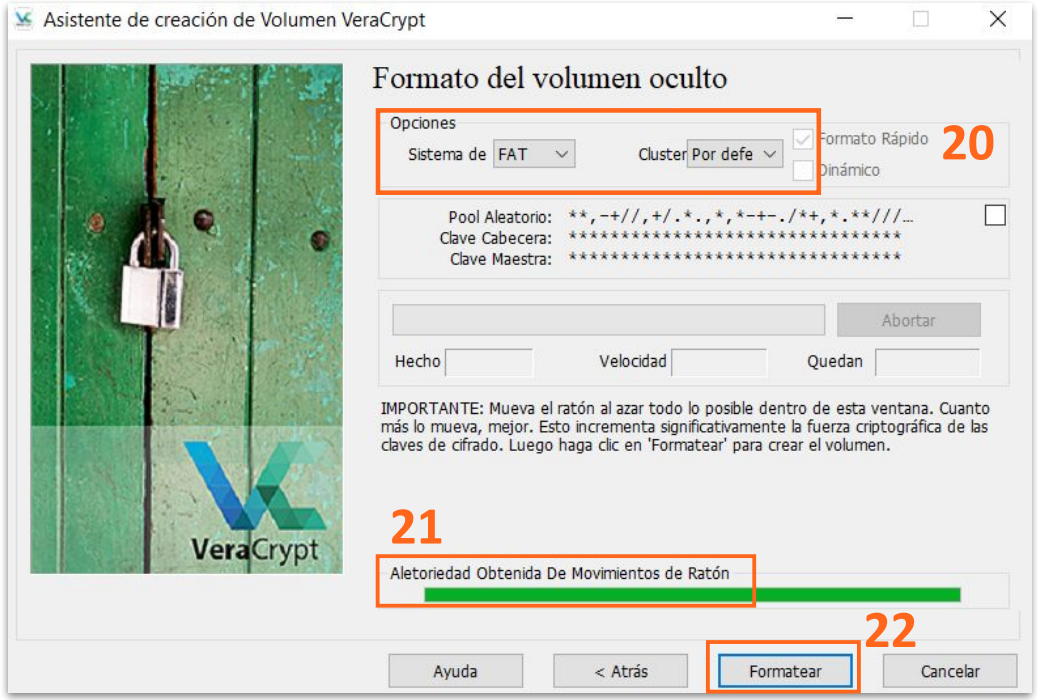


- ➔ Selecciona el método o algoritmo de cifrado. **Las opciones por defecto se consideran seguras en muchos casos, así que podrías dejarlas tal como están.**
- ➔ Haz clic en "**Siguiente**" para determinar el tamaño que tendrá tu volumen oculto.
- ➔ VeraCrypt te avisará cual es el tamaño máximo que puede tener tu volumen oculto, escribe un tamaño más pequeño para que puedas guardar los archivos "señuelo" en tu volumen estándar.
- ➔ Haz clic en "**Siguiente**" para crear una contraseña para tu volumen oculto.

VOLUMEN OCULTO

4. Crea un Volumen Oculto

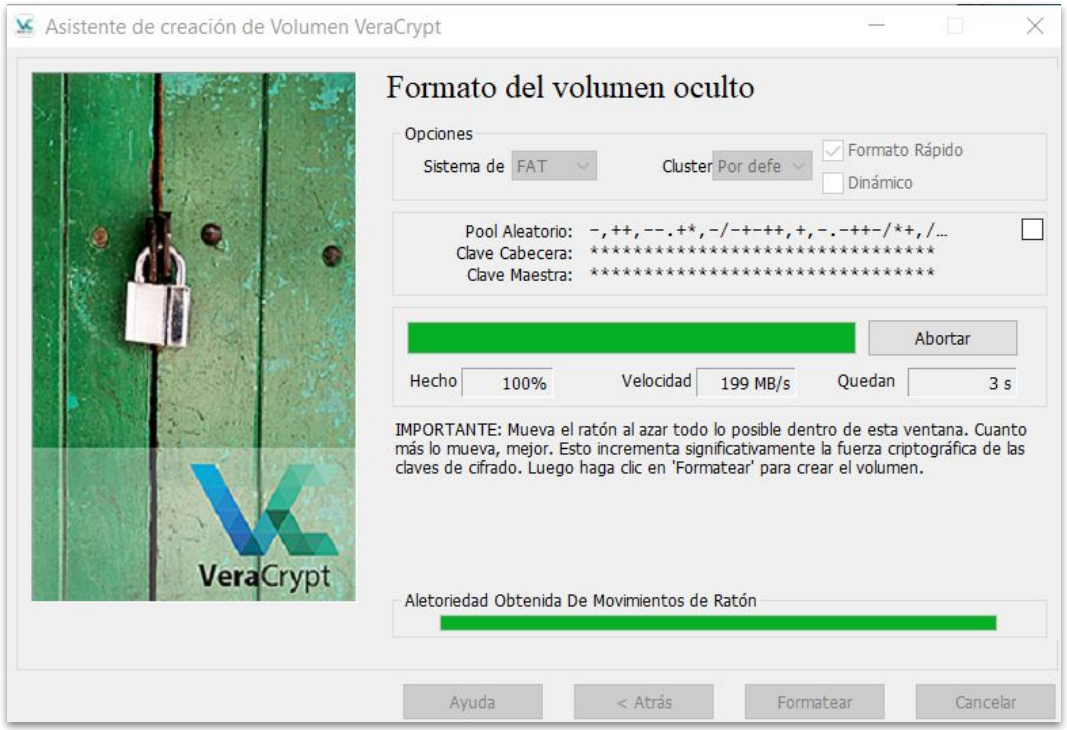




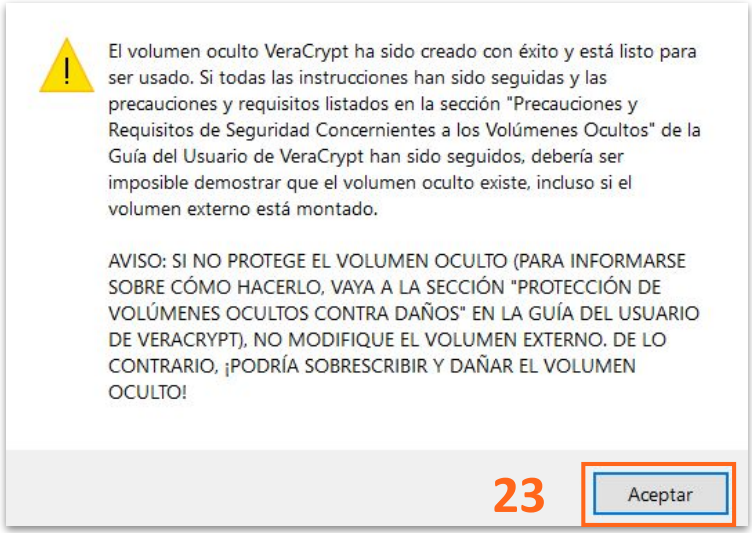
- ➔ Escribe tu contraseña (distinta a la del volumen estándar) y luego vuelve a escribirla en el campo "**Confirmar**" para activar el botón "**Siguiente**". **Recuerda usar una contraseña segura.**
- ➔ Haz clic en "**Siguiente**" para elegir el formato de tu volumen oculto.
- ➔ Selecciona las opciones de formato que se requieran.
- ➔ Mueve el ratón al azar dentro de la ventana para aumentar la fuerza criptográfica de las claves de cifrado. (Hasta que la barra sea verde)
- ➔ Haz clic en "**Formatear**" para empezar a crear tu volumen oculto.

VOLUMEN OCULTO

4. Crea un Volumen Oculto



- VeraCrypt te avisará cuando el volumen oculto haya sido creado con éxito y te mostrará una **advertencia** sobre proteger los archivos en tu volumen oculto cuando agregues contenido a tu volumen estándar.
- Haz clic en “Aceptar” para terminar de crear tu volumen oculto.



- Esta advertencia se relaciona con la forma en que VeraCrypt oculta la existencia de tu volumen oculto.
- Si tratas de copiar archivos en tu volumen estándar (externo), cuyo tamaño sea mayor al espacio libre disponible (del volumen externo) corromperás o borrarás los archivos del volumen oculto.
- VeraCrypt no te advertirá sobre esto, para evitar que algún observador note la existencia del volumen oculto

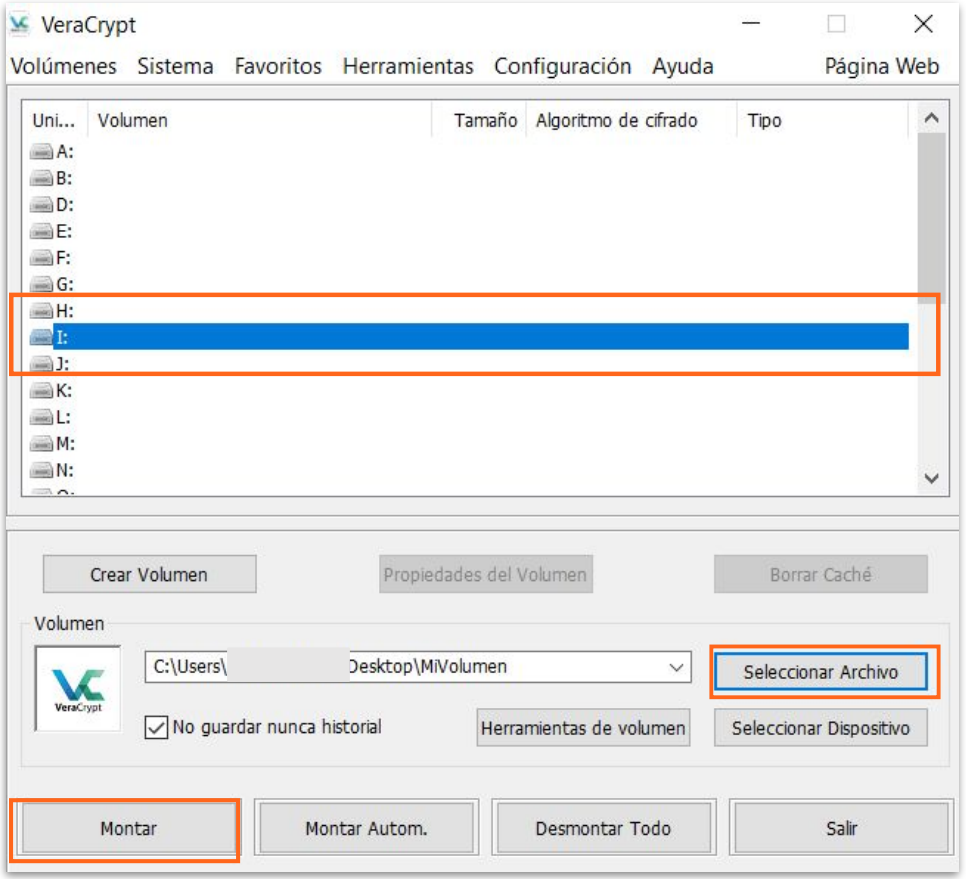
Más adelante te explicaremos cómo proteger contra escritura tu volumen oculto.

VOLUMEN OCULTO

5. Usa tu volumen oculto VeraCrypt

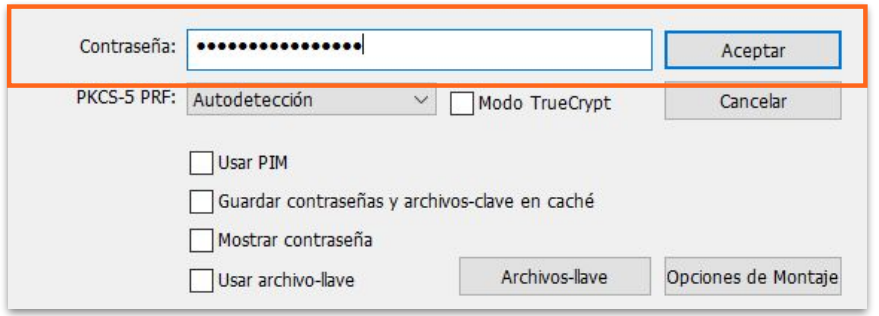
5.1 Montar un volumen oculto

Montar (para abrir) un volumen oculto es similar a montar un volumen estándar, solo debes introducir la contraseña correspondiente a tu volumen oculto. Para hacerlo sigue estos pasos:



➔ Selecciona el archivo contenedor del volumen estándar que contiene tu volumen oculto. (Abre VeraCrypt > Elige una unidad > Selecciona tu archivo contenedor)

➔ Haz clic en "**Montar**" para escribir la contraseña de tu volumen oculto



➔ Haz clic en "**Aceptar**" para montar el volumen

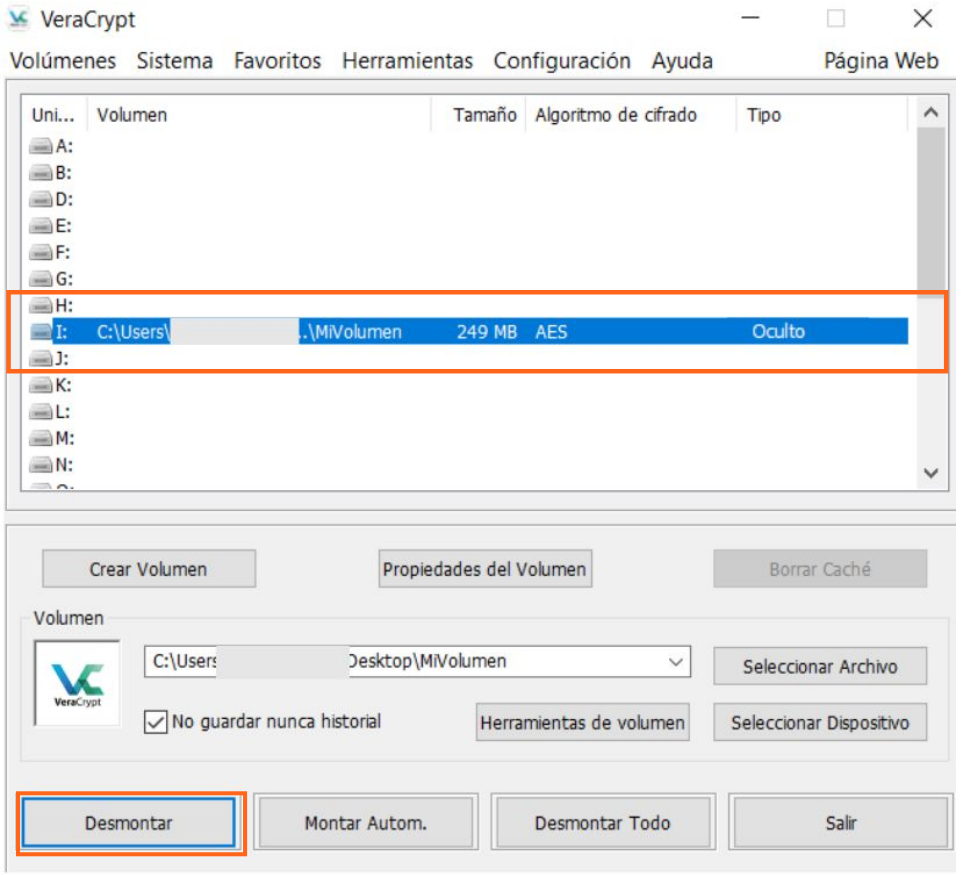
➔ Accede a tu volumen y comienza a añadir/editar información.

VOLUMEN OCULTO

5. Usa tu volumen oculto VeraCrypt

5.2. Desmontar un volumen oculto

Desmontar (para cerrar) un volumen oculto es similar a desmontar un volumen estándar, para hacerlo sigue estos pasos:



- ➔ En VeraCrypt selecciona la unidad en donde se encuentre el volumen que quieres desmontar.
- ➔ Haz clic en "**Desmontar**" para cerrar tu volumen VeraCrypt.
- ➔ Sal de VeraCrypt.

VOLUMEN OCULTO



Recomendaciones

IMPORTANTE: Los volúmenes ocultos se crean para almacenar información sensible, por lo general solo tú sabes de su existencia, lo ideal es apoyarse en el volumen estándar para confundir la existencia del volumen oculto (utilizando archivos señuelo). Te recomendamos lo siguiente para un mejor manejo de tus volúmenes ocultos:

- ➔ **Bajo un contexto de riesgo,** si existe un tercero que te observa o te obliga a abrir la contraseña de tu volumen VeraCrypt, utiliza la contraseña de tu volumen estándar en donde se supone que tienes archivos “señuelo”. Así evitas que sepan de la existencia de tu volumen oculto, en dónde realmente almacenas la información sensible. **Recuerda: toma el hábito de (sólo en privado), introducir la contraseña de tu volumen oculto para añadir/editar información.**
- ➔ Para abrir un volumen estándar en un contenedor que tiene un volumen oculto (con la finalidad de modificar tus archivos "señuelo" y asumiendo que no te están observando), activa la función de “**Proteger tu volumen oculto al modificar los contenidos de tu volumen exterior**” (Ver siguiente lámina).

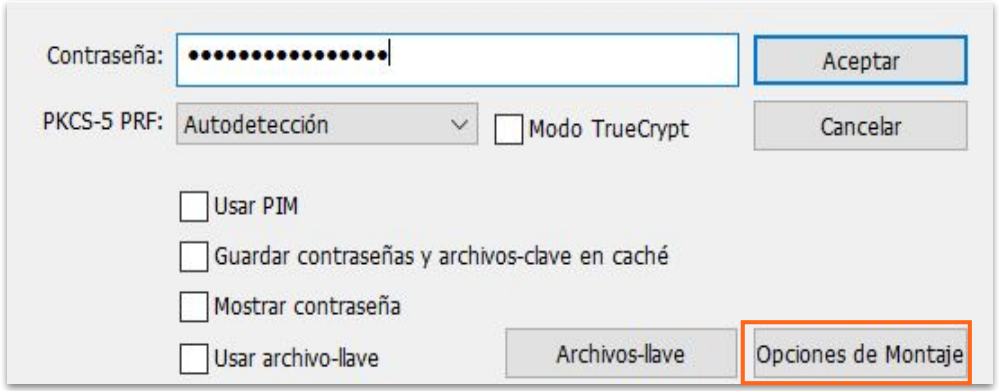


VOLUMEN OCULTO

5. Usa tu volumen oculto VeraCrypt

5.3. Proteger un volumen oculto (contra daños por escritura en el volumen externo)

Esta función te permite agregar nuevos archivos "**señuelo**" a tu volumen estándar sin el riesgo de borrar o corromper accidentalmente los contenidos de tu volumen oculto. Estos son los pasos para activarla:



- ➔ Sigue los pasos para montar tu volumen estándar que tiene un volumen oculto, hasta el punto donde debes ingresar tu contraseña
  (Abre VeraCrypt > Elige una unidad > Selecciona tu archivo contenedor > Haz clic en "Montar").
- ➔ Escribe la contraseña de tu volumen exterior.
- ➔ Haz clic en "**Opciones de Montaje**".
- ➔ Cuando actualices tus archivos señuelo en privado, siempre deberías habilitar esta función.

Nota: No debes activar esta función cuando trates de ocultar la existencia de tu volumen oculto a alguien que te obligue a escribir tu contraseña señuelo; porque hacerlo requiere que escribas tus dos contraseñas.

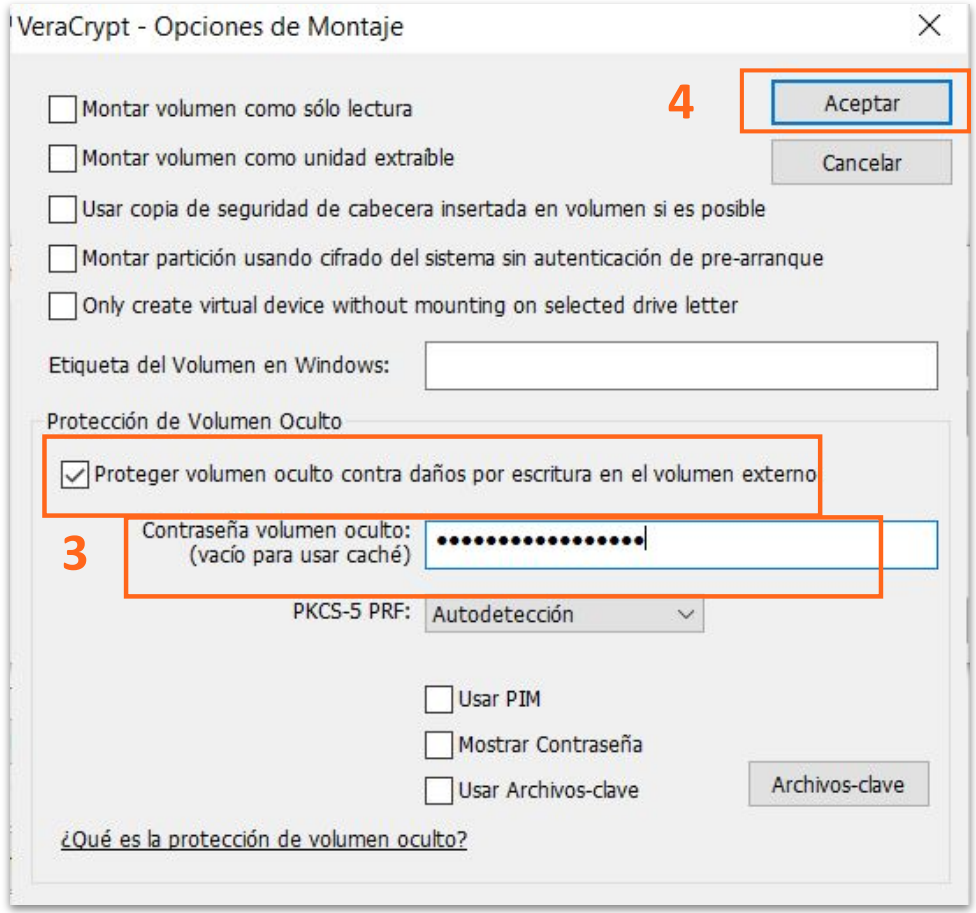


VOLUMEN OCULTO

5. Usa tu volumen oculto VeraCrypt

5.3. Proteger un volumen oculto (contra daños por escritura en el volumen externo)

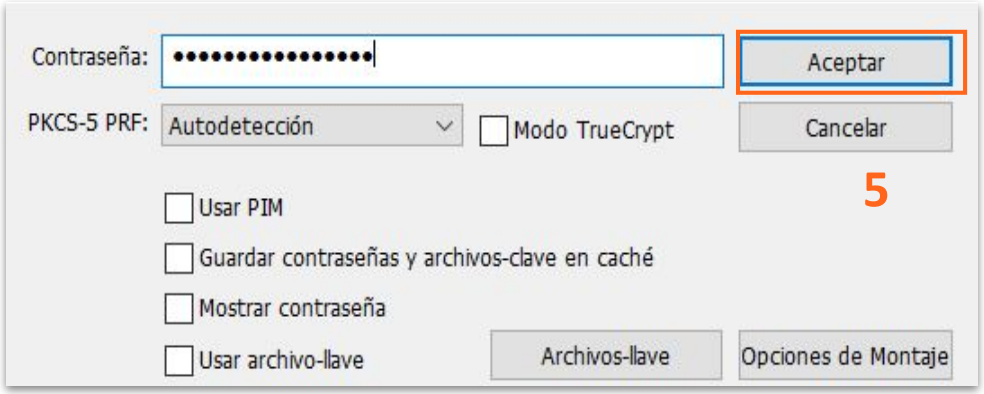
- ➔ Selecciona la opción "**Proteger volumen oculto contra daños por escritura en el volumen externo**"
- ➔ Escribe la contraseña de tu volumen oculto
- ➔ Haz clic en "**Aceptar**" para regresar a la pantalla de contraseña

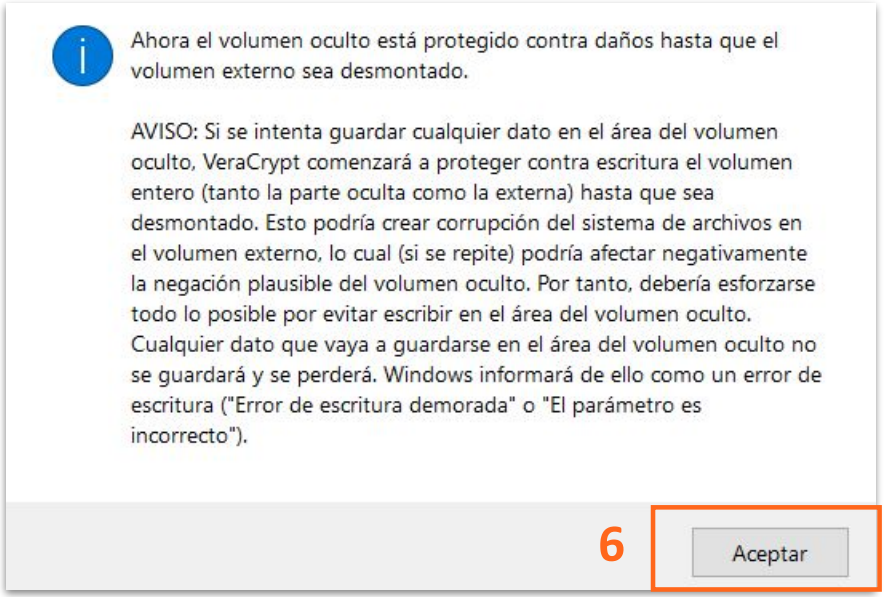


VOLUMEN OCULTO

5. Usa tu volumen oculto VeraCrypt

5.3. Proteger un volumen oculto (contra daños por escritura en el volumen externo)



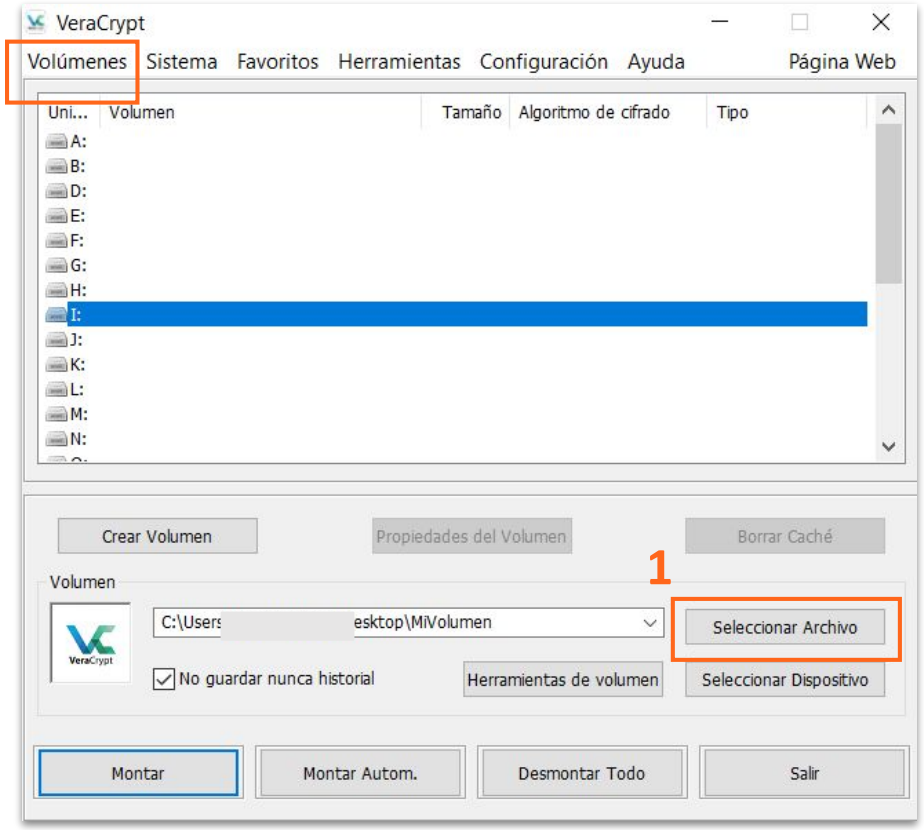


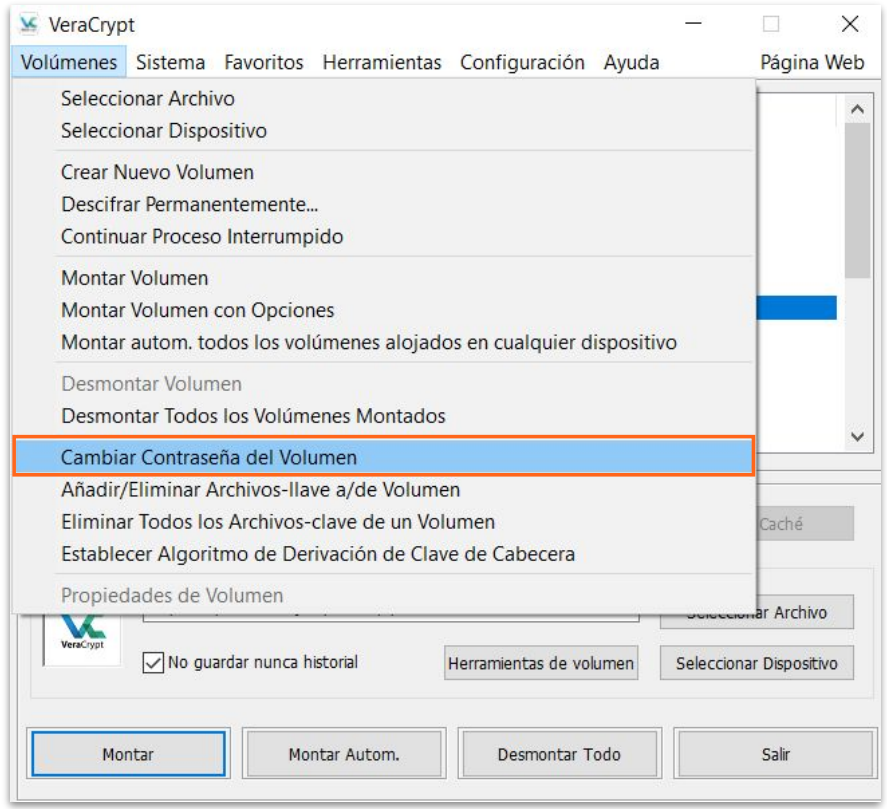
- ➔ Haz clic en "**Aceptar**" para montar tu volumen estándar mientras proteges tu volumen oculto de daño accidental. VeraCrypt te dirá cuando esté hecho.
- ➔ Haz clic en "**Aceptar**" para comenzar a modificar tus archivos "señuelo" y volver a la pantalla inicial de VeraCrypt.
- ➔ Cuando hayas terminado de modificar los contenidos de tu volumen estándar, lo puedes desmontar siguiendo los pasos habituales,

Nota: la próxima vez que montes tu volumen, la marca en el recuadro "Protege el volumen oculto contra daño causado por escribir en el volumen exterior" se retirará por defecto; por lo que no dejará rastros que indiquen que existe un volumen oculto. Por consecuencia, **cada vez que vayas a modificar archivos dentro del volumen oculto, debes activar esta función.**

CONTRASEÑAS

6. Cambia la(s) contraseña(s) de tu volumen(es) en VeraCrypt



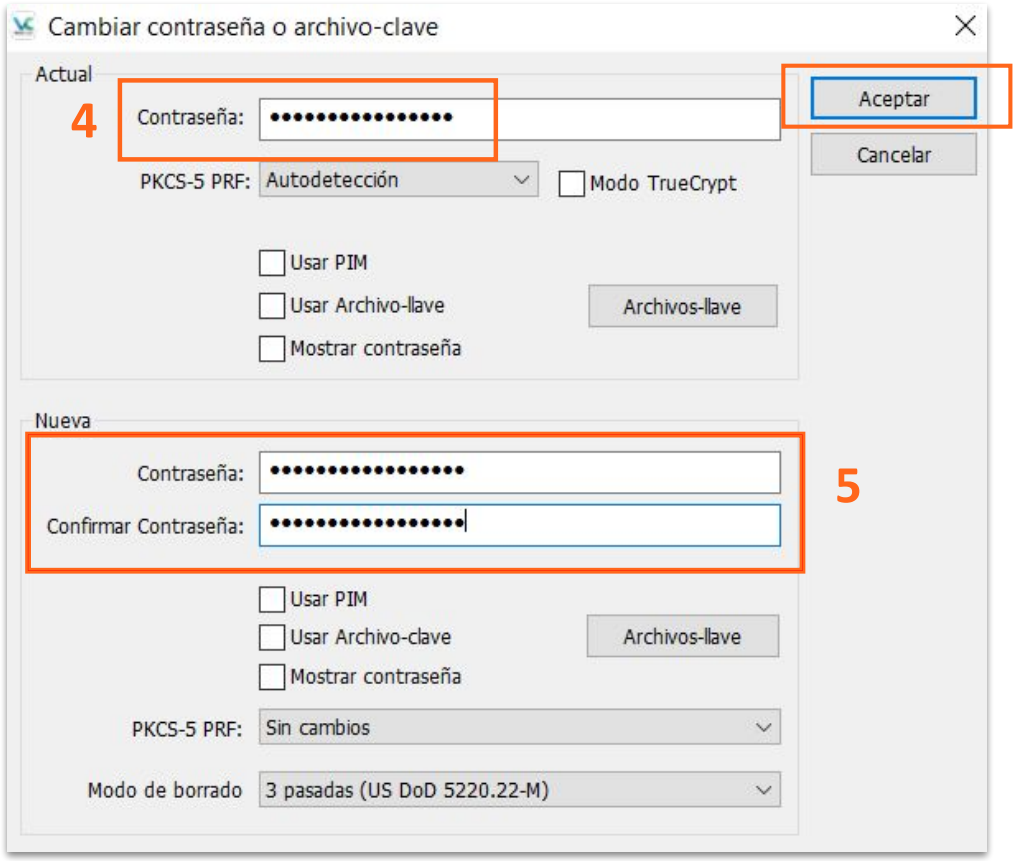


- ➔ Sigue los pasos para seleccionar el volumen al que quieres cambiar su contraseña (Abre VeraCrypt > Elige una unidad > Selecciona tu archivo contenedor)

- ➔ Haz clic en "**Volúmenes**"
- ➔ Elige "**Cambiar la contraseña del volumen"**, esto activará la pantalla de "Cambiar contraseñas"

CONTRASEÑAS

6. Cambia la(s) contraseña(s) de tu volumen(es) en VeraCrypt



- ➔ Escribe la contraseña actual del volumen al que quieres modificar su contraseña (el estándar o el oculto)
- ➔ Escribe la nueva contraseña dos veces
- ➔ Haz clic en "**Aceptar**" para generar la nueva clave

Nota: Si tienes tanto el volumen estándar como el volumen oculto en este contenedor, VeraCrypt determinará automáticamente cuál contraseña cambiar dependiendo de lo que hayas escrito en el campo "Contraseña actual". Si quieres cambiar ambas contraseñas, deberás pasar dos veces por este proceso.

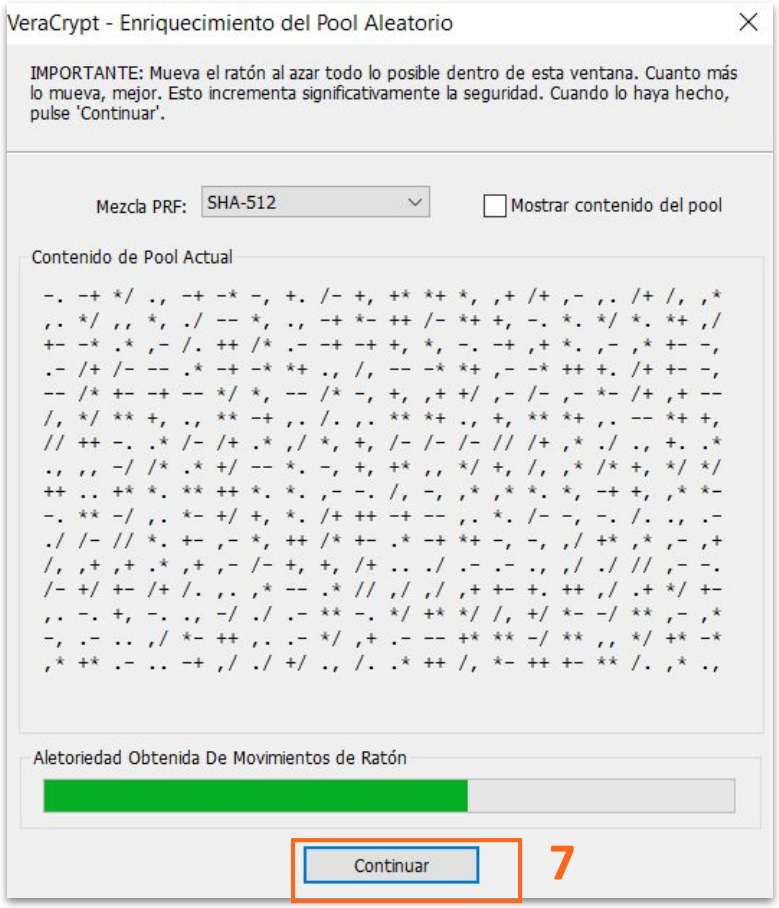


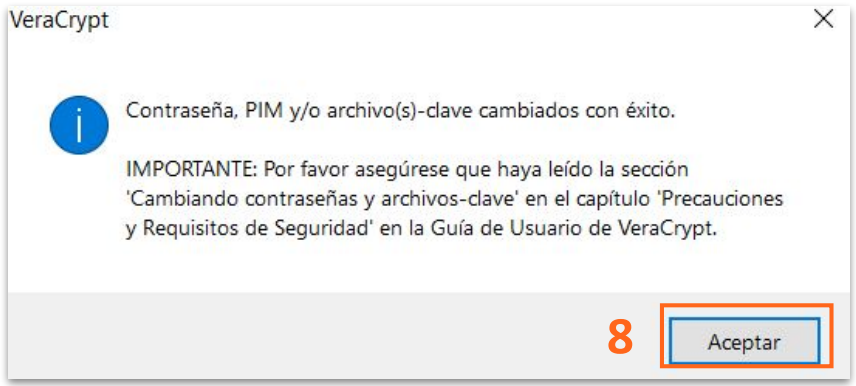
CONTRASEÑAS

Nota: Para más información sobre VeraCrypt, visita la Guía de Usuario en el siguiente link: https://www.veracrypt.fr/en/Documentation.html

6. Cambia la(s) contraseña(s) de tu volumen(es) en VeraCrypt

- ➔ Para continuar, VeraCrypt te mostrará la pantalla de “Pool Aleatorio”
- ➔ Mueve el mouse alrededor de la pantalla para aumentar la fortaleza de encriptación que brinda VeraCrypt.
- ➔ Haz clic en “**Continuar**” para seguir con el proceso de cambio de contraseña.
- ➔ VeraCrypt te dirá cuando haya terminado de generar una nueva clave para tu volumen encriptado. Haz clic en “**Aceptar**”





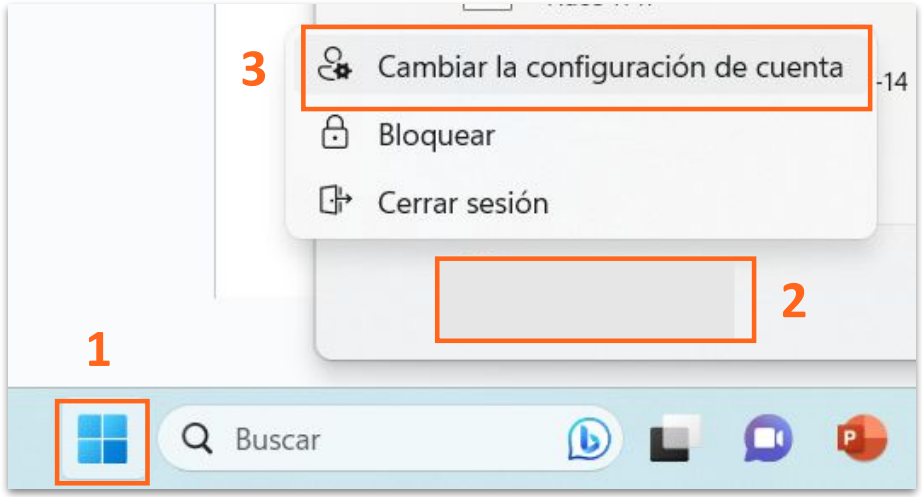
CIFRADO EN DISCO

7. Bitlocker (para usuarios de Windows)

BitLocker es la herramienta de Windows que permite realizar el cifrado del disco completo.



Windows 10
BitLocker

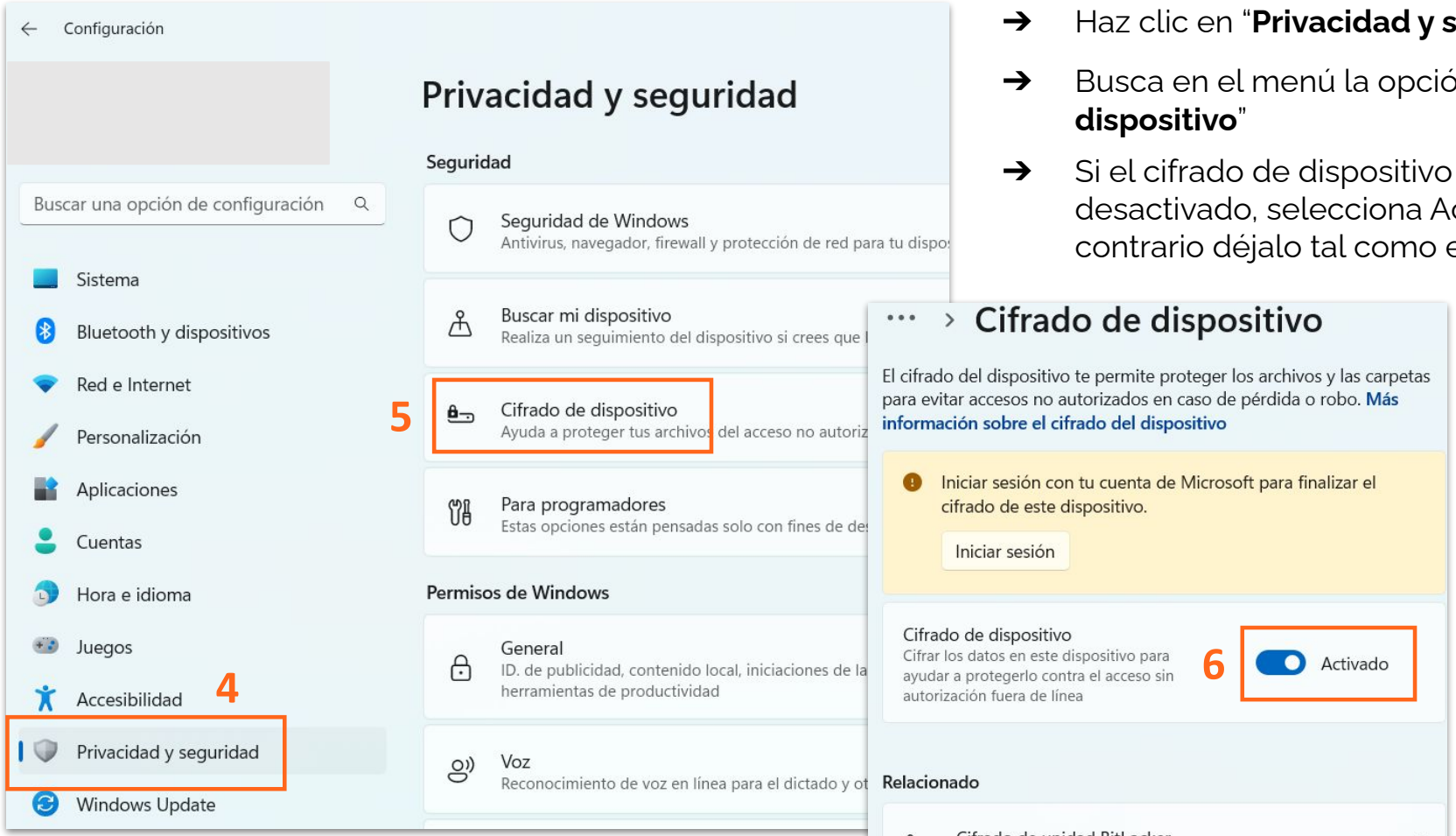


El cifrado de BitLocker está disponible en dispositivos compatibles que ejecutan **Windows 10 u 11 Pro**. Para activarlo sigue los siguientes pasos

➔ En la barra de tareas, selecciona el botón Inicio **>** Selecciona el usuario **>** Haz clic en "**Cambiar la configuración de la cuenta**"

CIFRADO EN DISCO

7. Bitlocker (para usuarios de Windows)



- ➔ Haz clic en "**Privacidad y seguridad**".
- ➔ Busca en el menú la opción "**Cifrado de dispositivo**"
- ➔ Si el cifrado de dispositivo está desactivado, selecciona Activar. De lo contrario déjalo tal como está.

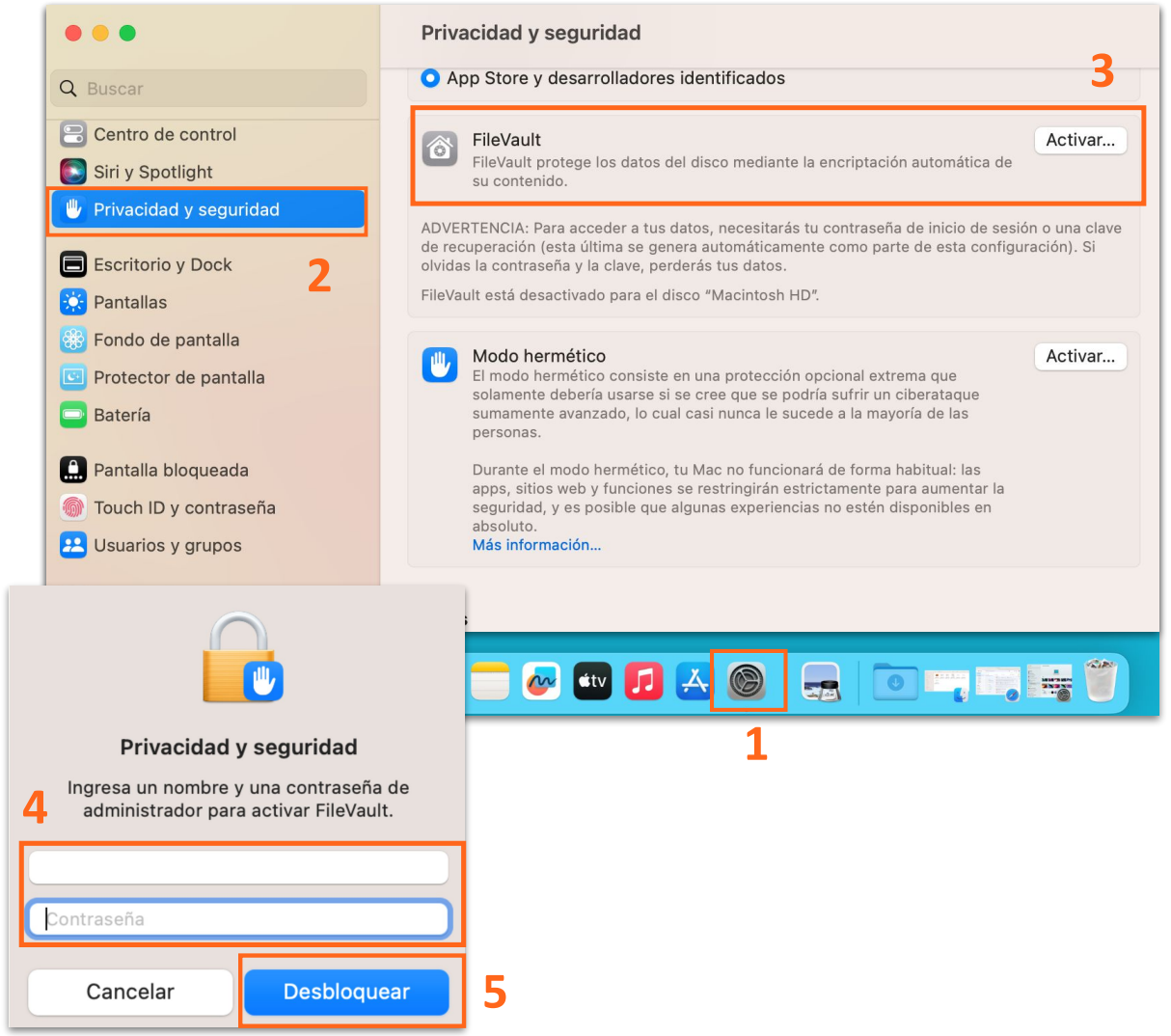
CIFRADO EN DISCO

8. Filevault (para usuarios de MacOS)



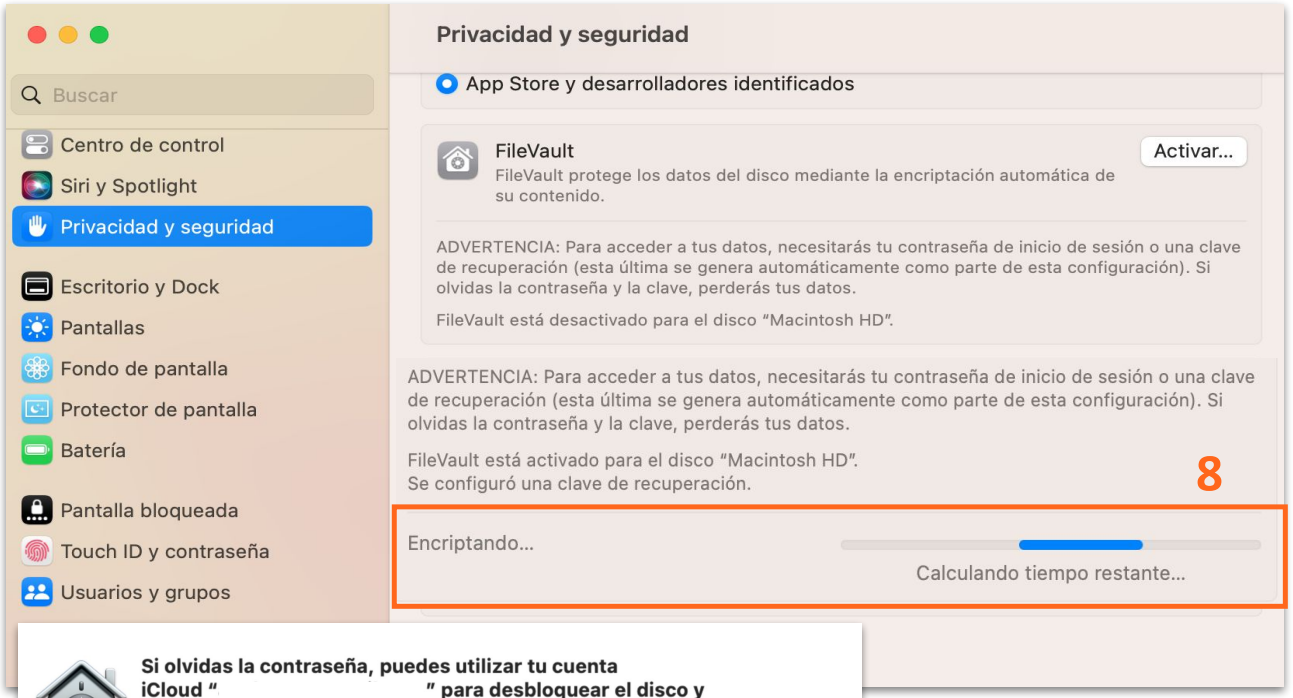
FileVault está disponible en OS X Lion o posterior. Al activar FileVault, la Mac siempre solicita que inicies sesión con la contraseña de tu cuenta.

- ➔ **Configuracion > Seguridad y privacidad > FileVault > Activar**
- ➔ Ingresa tu usuario y contraseña y haz clic en "**Desbloquear**"



CIFRADO EN DISCO

8. Filevault (para usuarios de MacOS)



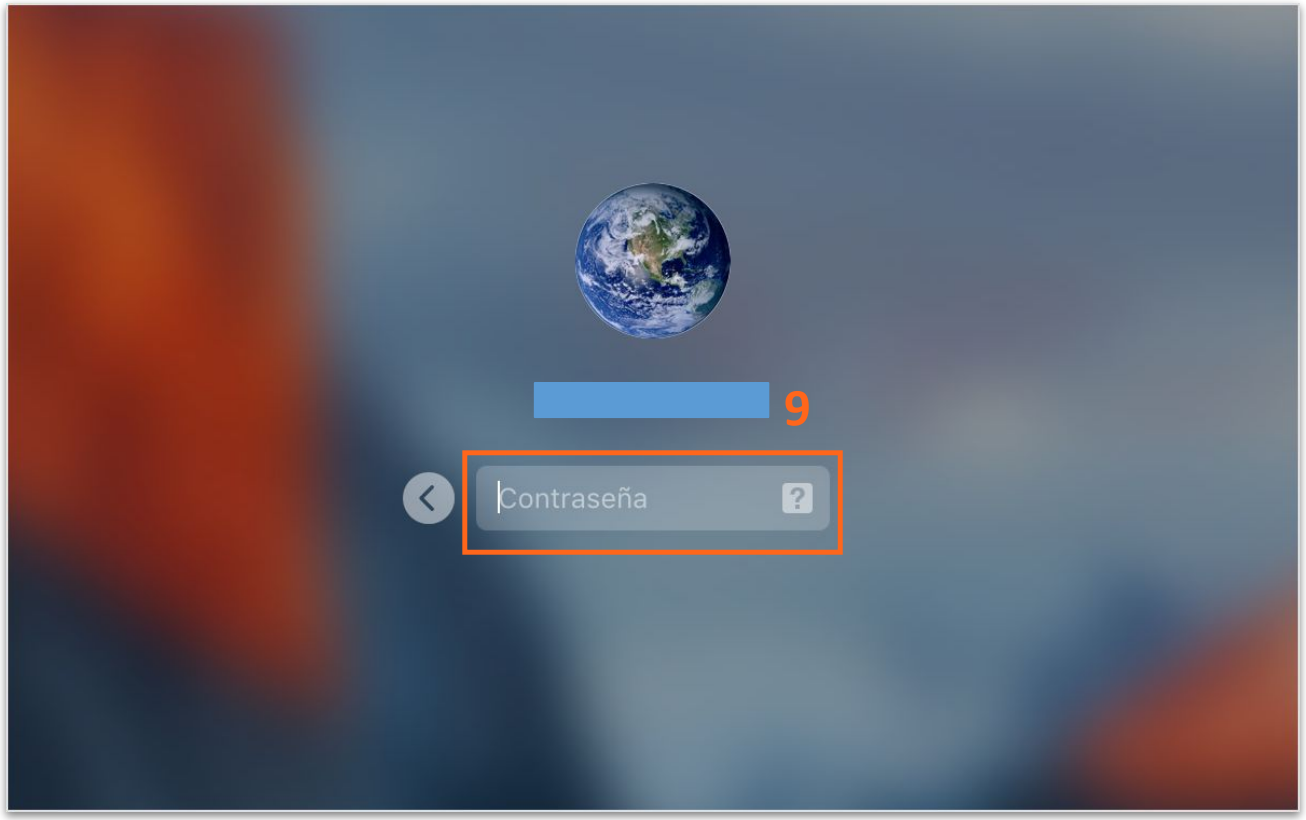
- ➔ Selecciona cómo quieres desbloquear el disco y restablecer tu contraseña en caso de que alguna vez la olvides. Se recomienda **seleccionar la vía de la clave de recuperación y guardarla en un lugar seguro.**
- ➔ Haz clic en "**Continuar**" para seguir las instrucciones de acuerdo a la opción que elijas.
- ➔ Se iniciará el proceso de encriptado del disco, mientras esto sucede puedes utilizar la computadora como usualmente.

Nota: Si pierdes tanto la contraseña de tu cuenta como la clave de recuperación de FileVault, no podrás iniciar sesión en tu Mac o tener acceso a los datos en tu disco de arranque.



CIFRADO EN DISCO

8. Filevault (para usuarios de MacOS)



Cuando se completa la configuración de FileVault y reinicias la Mac, deberás usar la contraseña de tu cuenta para desbloquear el disco y permitirle a la Mac que complete el inicio.
Al usar FileVault, es necesario que introduzcas la contraseña cada vez que la Mac se inicia.

REFERENCIAS

- Security in a box (2016). VeraCrypt para Windows - Almacenamiento Seguro de Archivos. Recuperado de: https://securityinabox.org/es/tools/veracrypt/.

