



VeraCrypt

Veracrypt: Cifra y oculta tus archivos gratis

<https://www.redeszone.net/tutoriales/seguridad/veracrypt-cifra-archivos-gratis/>

VeraCrypt es un software de código abierto para **cifrar archivos, carpetas, unidades USB extraíbles, discos duros completos, e incluso el disco duro donde se encuentra el propio sistema operativo** instalado. **VeraCrypt es multiplataforma**, actualmente es compatible con sistemas operativos Microsoft Windows, cualquier sistema basado en Linux, y también es compatible con macOS. Este software está basado en el popular **TrueCrypt 7.1a**. Debemos recordar que el proyecto TrueCrypt cerró, y ya no tendremos nuevas actualizaciones de dicho software. Sin embargo, VeraCrypt ha cogido el testigo e incorpora todas las características de TrueCrypt y muchas mejoras de seguridad y rendimiento.

Principales Características de VeraCrypt

Algunas de las principales características de VeraCrypt son las siguientes:

- Creación de discos cifrados virtuales en un simple archivo, los cuales podremos montar para su lectura y escritura.
- Cifrado de dispositivos de almacenamiento extraíble como USB, tarjetas SD e incluso discos duros.
- Cifrado de cualquier partición de estos dispositivos de almacenamiento extraíble.
- Cifrado de la partición o disco completo donde Windows esté instalado
- El cifrado y el descifrado es automático y se hace en tiempo real, siendo completamente transparente al usuario.
- El cifrado y descifrado si utilizamos AES se puede acelerar si el procesador del equipo soporta AES-NI, proporcionando una mayor velocidad de lectura y escritura.
- Posibilidad de crear un volumen «oculto» para evitar que un posible atacante nos fuerce a revelar la contraseña del volumen (chantaje, extorsión etc.)

Una vez que ya conocemos sus principales características, vamos a ver cómo descargar e instalar VeraCrypt en nuestro ordenador con Windows 10 Pro.

1. Descarga e instalación de VeraCrypt

Lo primero que tenemos que hacer es descargar VeraCrypt, la descarga se realiza directamente a través de la [página web oficial](#), en la sección descargas: [Descargar VeraCrypt gratis](#). En esta web vamos a poder descargar todas las versiones de VeraCrypt, tanto para Windows, Linux, macOS, FreeBSD e incluso directamente el código fuente.



Home Source Code Downloads Documentation Donate Forums

Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

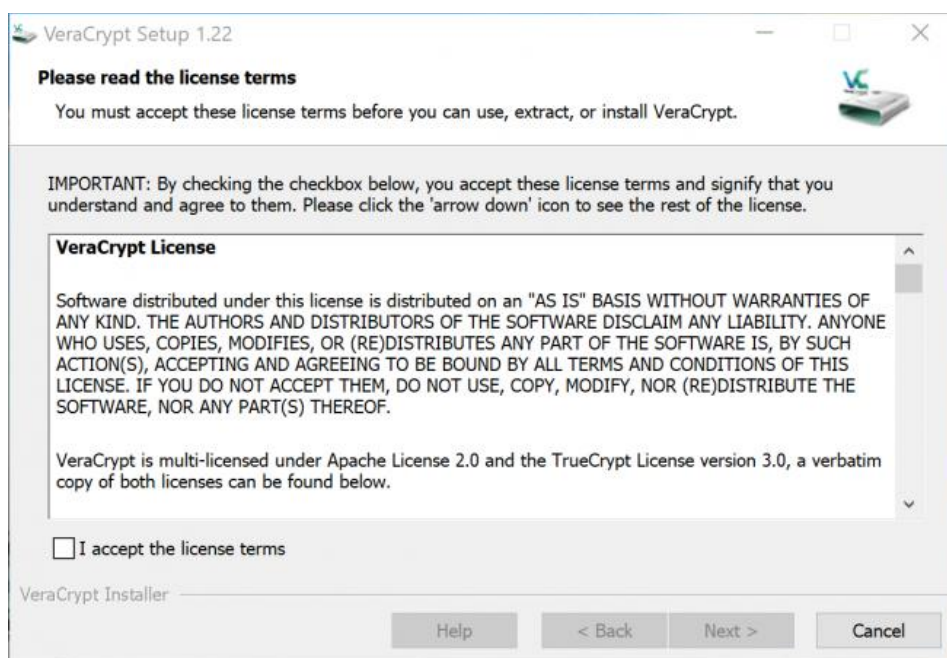
[Supported versions of operating systems](#)

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x54DDD393, Fingerprint=993B7D7E8E413809828F0F29EB559C7C54DDD393)

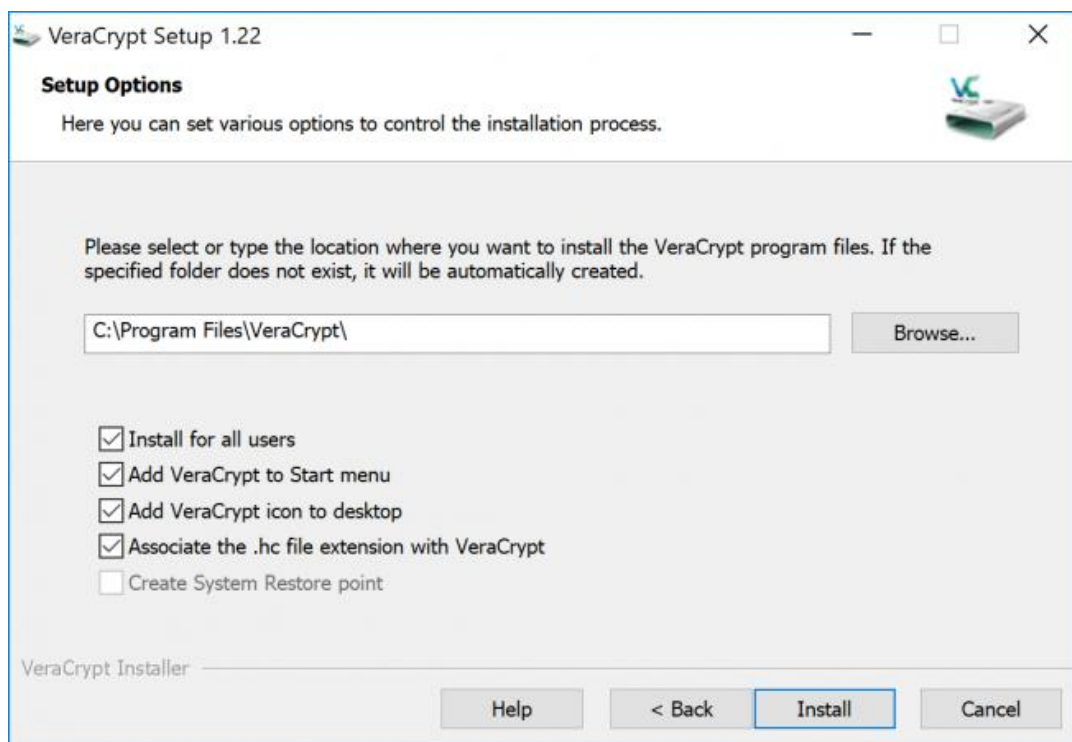
Latest Stable Release - 1.22 (Friday March 30, 2018)

-  **Windows:** [VeraCrypt Setup 1.22.exe \(29.6 MB\)](#) (PGP Signature)
 - Portable version: [VeraCrypt Portable 1.22.exe \(29.4 MB\)](#) (PGP Signature)
-  **Mac OS X:** [VeraCrypt_1.22.dmg \(11.1 MB\)](#) (PGP Signature)
 - [OSXFuse 2.5](#) or later must be installed.
-  **Linux:** [veracrypt-1.22-setup.tar.bz2 \(14.6 MB\)](#) (PGP Signature)

Una vez descargado el programa, debemos instalarlo como cualquier programa. Nos saldrá un asistente de instalación que nos dará la opción de instalarlo en el propio equipo, o extraer VeraCrypt y usarlo de manera «portable», es decir, sin instalarlo en el propio ordenador. Un detalle importante es que si vamos a cifrar el sistema completo o la partición donde está el sistema operativo, deberemos instalarlo obligatoriamente y no usarlo en modo «portable».



Una vez que hayamos pinchado en «Install», nos saldrán las típicas opciones de instalación para todos los usuarios, creación de acceso directo en escritorio y también en el menú inicio. Una vez que haya terminado de instalar, nos recomendará seguir una pequeña guía para principiantes en VeraCrypt.



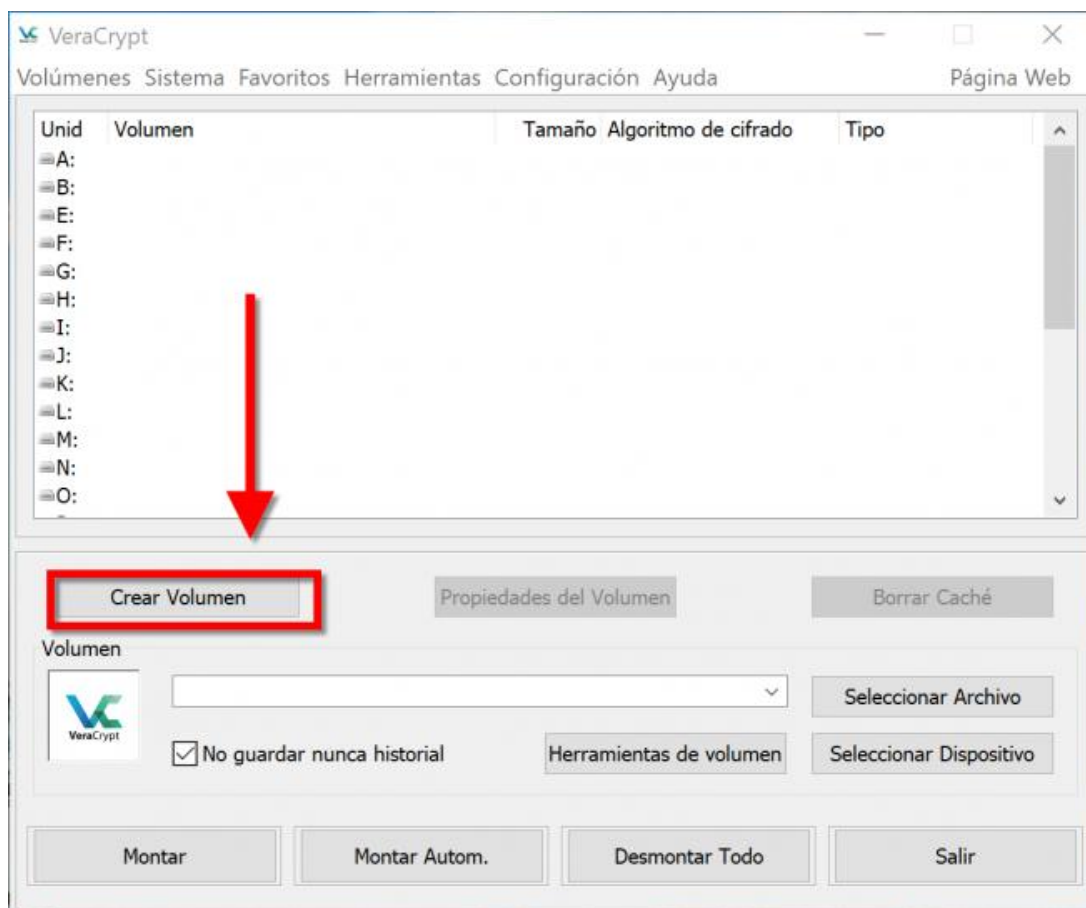
Una vez que lo tenemos instalado, vamos a proceder a crear los diferentes volúmenes, el cifrado de discos USB, y también el cifrado completo del sistema operativo.

2. Creación de un volumen cifrado «normal»

Lo primero que vamos a hacer es crear un volumen cifrado «normal», sin introducir dentro de él un volumen oculto.

En el menú principal de VeraCrypt procedemos a pinchar sobre «**Crear Volumen**», para posteriormente seleccionar la opción «**Crear un contenedor de archivos cifrado**». Una vez hecho esto, deberemos elegir si queremos crear un volumen VeraCrypt común, o un volumen VeraCrypt oculto, nosotros vamos a seleccionar la primera opción: **Crear un volumen VeraCrypt común**.

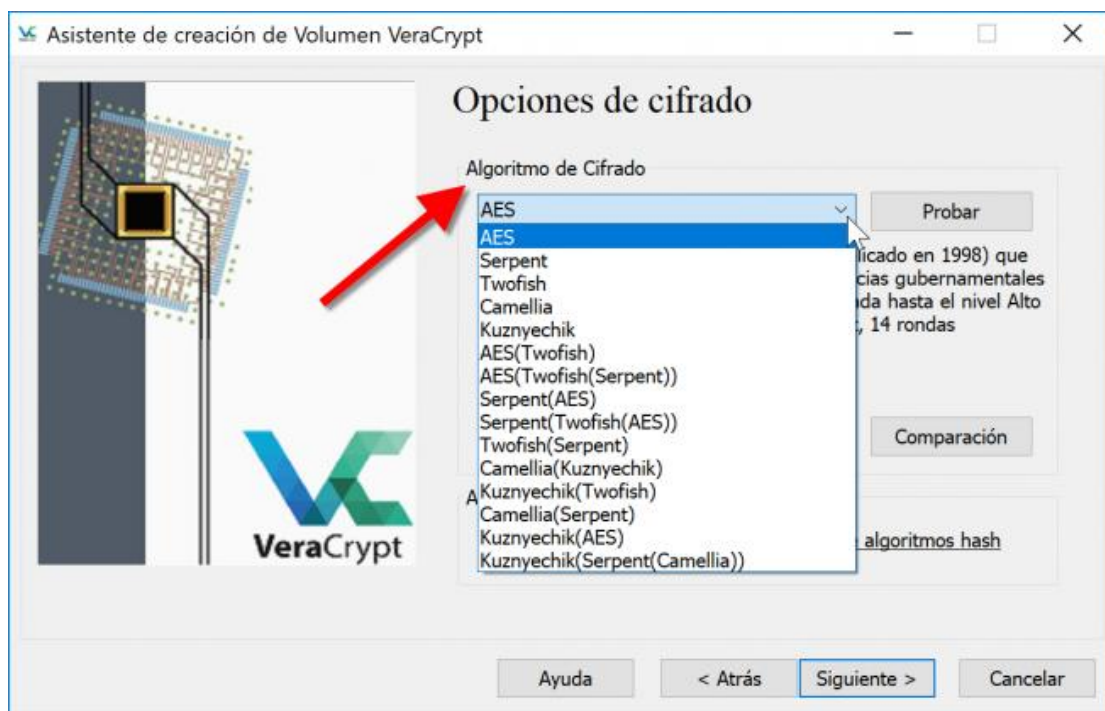
Para crear un contenedor, deberemos seleccionar una ruta y un nombre de archivo, pinchamos en «**Seleccionar archivo**» para ubicar el archivo que nosotros queramos donde nosotros queramos.



Una vez que ya tenemos configurado nuestro volumen VeraCrypt, deberemos seleccionar dos aspectos muy importantes: el cifrado simétrico para asegurar la confidencialidad, y el algoritmo de hashing para comprobar la integridad de los archivos.

En el desplegable tendremos la posibilidad de seleccionar una gran cantidad de algoritmos de cifrado simétrico, por defecto es AES, de hecho, si nuestra CPU soporta AES-NI (AES por hardware) tendremos un grandísimo rendimiento. Si pinchamos en «Comparación» podremos ejecutar un «benchmark» para comprobar cuál de todos es el más rápido.

Una vez que hayamos elegido el algoritmo de cifrado simétrico (nosotros hemos elegido **AES**), tendremos que elegir el algoritmo de hashing. Por defecto es **SHA512**, uno de los más seguros actualmente, así que elegimos este.



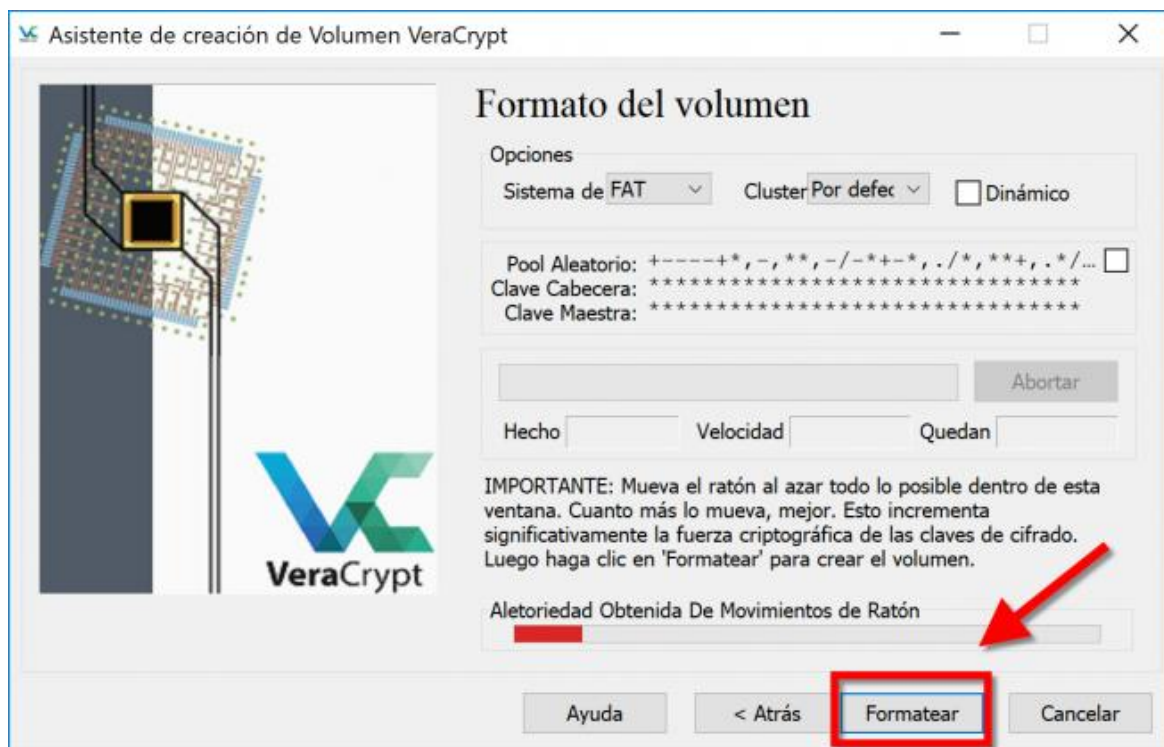
Ahora tendremos que configurar el tamaño del volumen cifrado VeraCrypt que estamos creando, y definir una contraseña (autenticación con algo que sabemos) o bien crear una clave criptográfica (autenticación con algo que tenemos). Nosotros hemos elegido la primera opción, una contraseña, y si la clave no es muy larga nos avisará que es recomendable que sea más compleja debido a que podrían atacar el contenedor por fuerza bruta o diccionario.



Cuando hayamos configurado la contraseña, deberemos elegir el sistema de archivos del contenedor cifrado. Si no vamos a introducir archivos mayores de 4GB, podremos

seleccionar FAT, de lo contrario, podremos elegir exFAT o NTFS. Es muy importante «mover el ratón» para crear la suficiente aleatoriedad en las claves, una vez que la barra esté en verde, pinchamos en «Formatear» para iniciar el proceso.

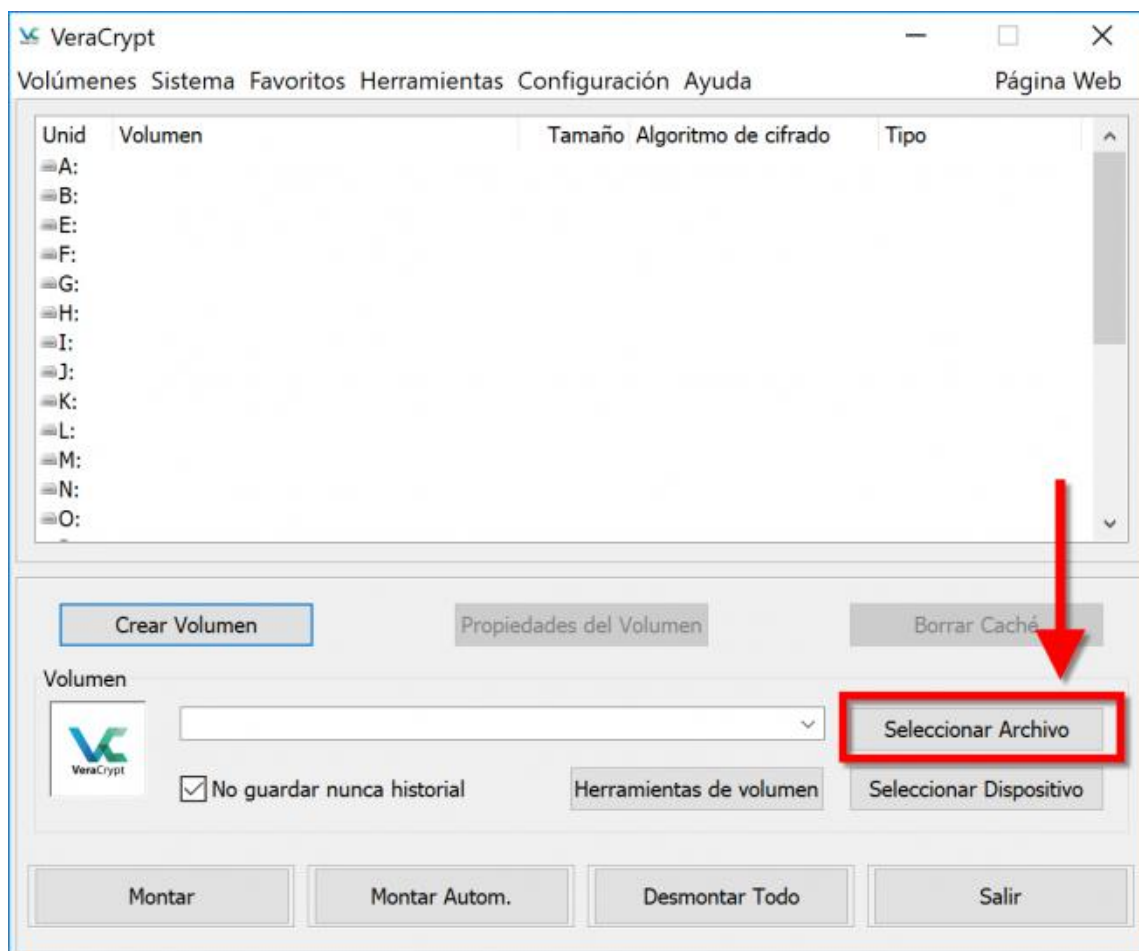
Cuando el proceso termine, pinchamos en «Salir», o en «Siguiente» si queremos crear otro volumen.



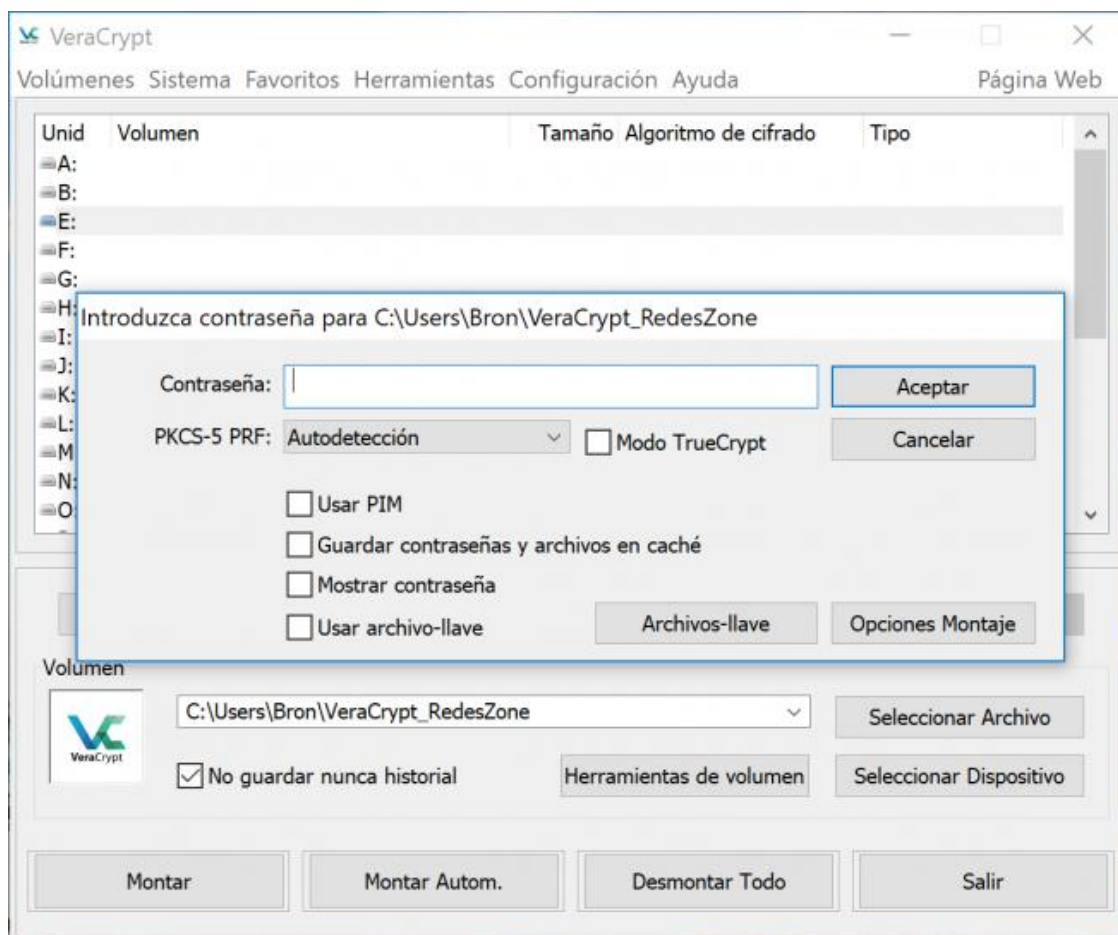
Ahora que ya hemos creado el volumen cifrado «normal», vamos a «montarlo» para poder acceder a él y empezar a cifrar nuestros archivos.

3. Montaje del volumen cifrado «normal» creado anteriormente

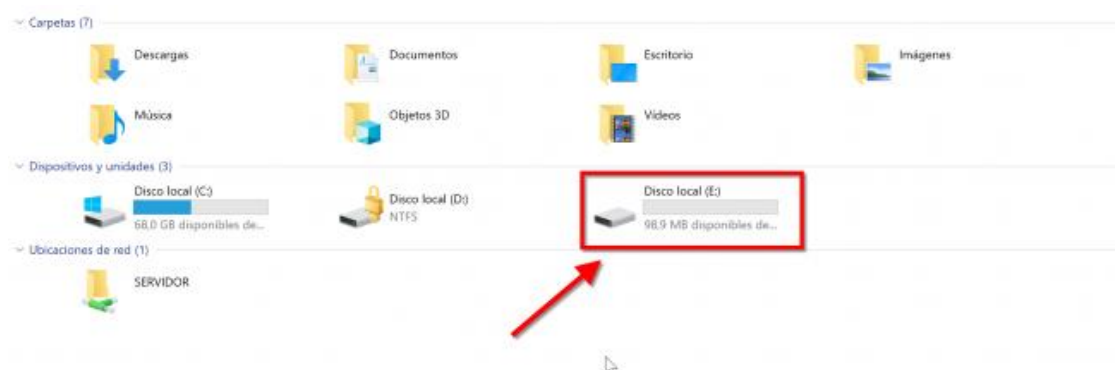
Para montar un volumen cifrado, debemos tener en cuenta que hemos debido de crearlo anteriormente. Simplemente debemos pinchar sobre «Seleccionar archivo», buscamos el volumen cifrado, elegimos una ruta en nuestro Windows para su montaje y pinchamos en «MONTAR».



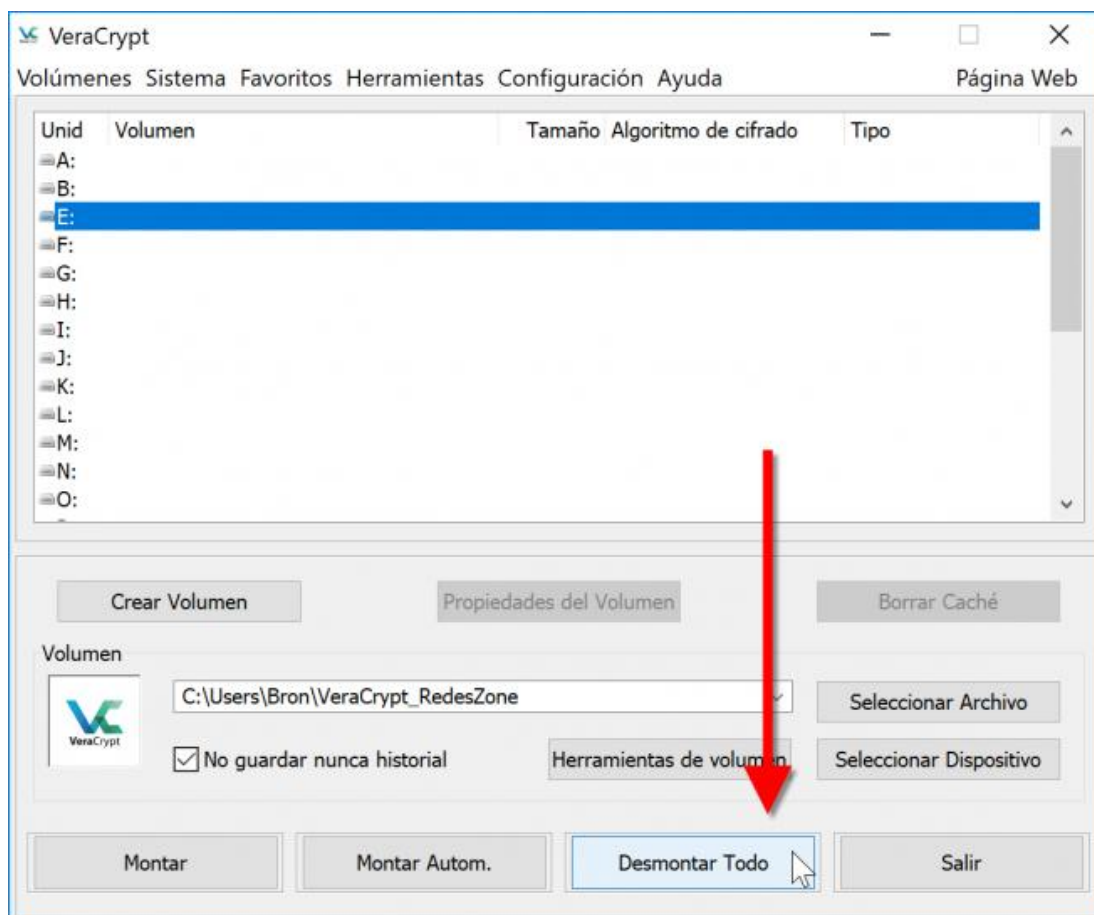
Cuando pinchemos en «Montar», nos va a pedir la contraseña de acceso o la clave criptográfica para abrirlo. Automáticamente VeraCrypt se encargará de abrir el contenedor cifrado, montarlo en la unidad elegida, y hacerlo accesible.



En «Equipo» nos aparecerá un nuevo disco local E, que es el volumen cifrado. Todo lo que copiamos en este «Disco local E» estará cifrado con AES, el cifrado y descifrado se realiza en tiempo real y «al vuelo».



Si queremos desmontar la unidad, simplemente pinchamos en «**Desmontar todo**», o con click derecho sobre la unidad y pinchar en «Desmontar».



Una vez que ya sabemos cómo crear y montar un volumen cifrado VeraCrypt normal, vamos a explicar el volumen cifrado oculto.

4. Creación de un volumen cifrado «oculto»

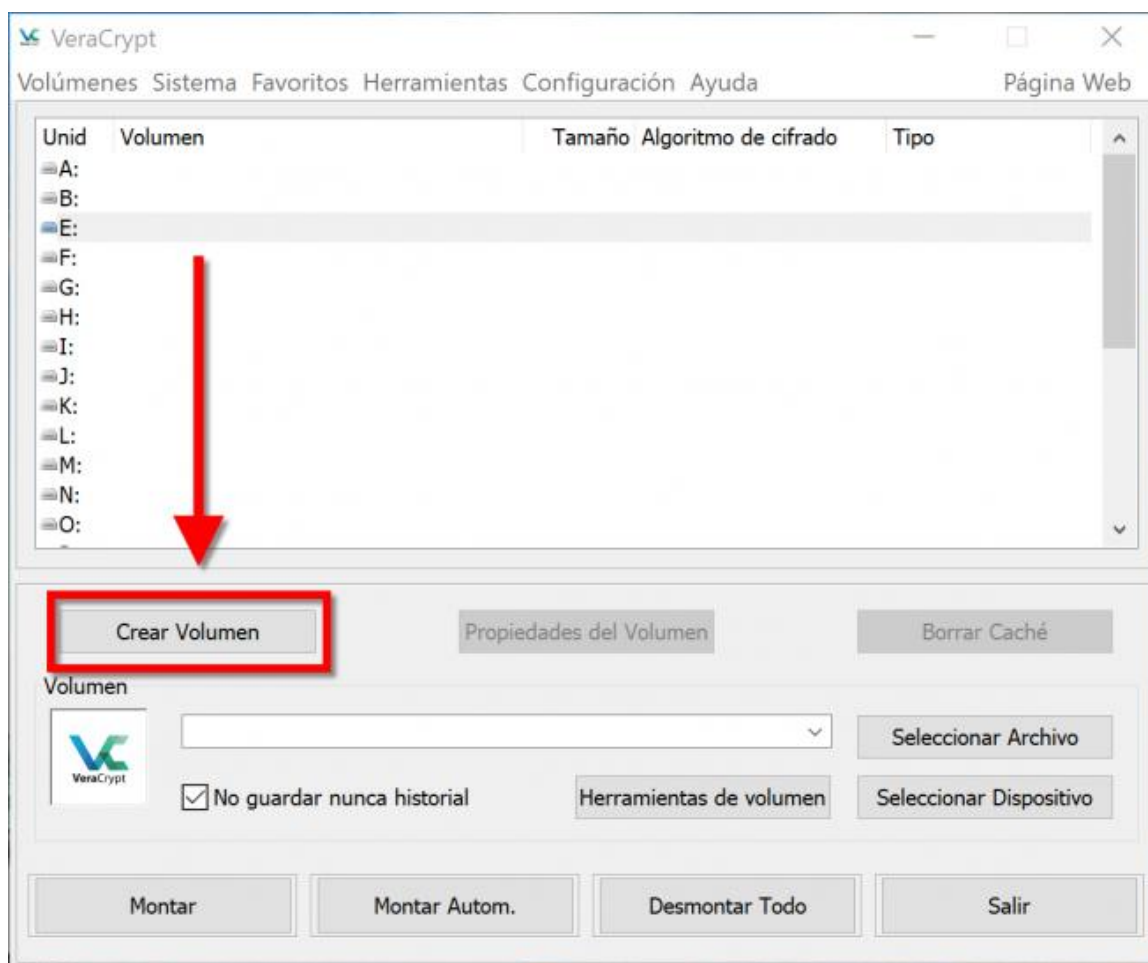
En esta sección vamos a crear un volumen cifrado, dónde meteremos nuestros datos, pero dentro de él crearemos uno OCULTO, os explico en qué consiste esto.

- Volumen normal: para acceder tendrás que meter la contraseña, por ejemplo 112233, entonces en Windows se montará un nuevo disco local, tal y como habéis visto anteriormente.
- Volumen oculto: para acceder tendrás que meter otra clave que hayas puesto anteriormente, por ejemplo 11223344 y se montará SÓLO el volumen oculto

¿Para qué sirve el volumen cifrado oculto? Para guardar los archivos más importantes en su interior, como claves de bancos, emails, documentos confidenciales etc. ¿Por qué no guardar esto en el volumen normal si está cifrado? Para evitar que alguien amenace nuestra integridad física (nos haga daño), nos chantajee o extorsione, ya que, de esta forma, podremos darle la clave del volumen cifrado «normal», pero no la del volumen oculto, y ellos no pueden saber de ninguna manera si hay un volumen oculto o no.

Un detalle muy importante que debemos tener en cuenta es lo siguiente: imaginemos que el volumen normal es de 50Mb, y el oculto de 25Mb, si tú llenas 26Mb de datos o más en el volumen normal, estás sobrescribiendo los datos del volumen oculto (ya sean archivos o espacio en blanco si no lo has llenado por completo), así que cuidado, dejad margen.

El proceso de creación del volumen cifrado oculto es muy similar al «normal». En el menú principal de VeraCrypt procedemos a pinchar sobre «**Crear Volumen**», para posteriormente seleccionar la opción «**Crear un contenedor de archivos cifrado**». Una vez hecho esto, deberemos elegir «**Volumen VeraCrypt oculto**», y si estás creando un volumen nuevo, pinchamos en «Modo normal» para que todo funcione más rápido.



Para crear un contenedor, deberemos seleccionar una ruta y un nombre de archivo, pinchamos en «**Seleccionar archivo**» para ubicar el archivo que nosotros queramos donde nosotros queramos. Una vez elegido, vamos a «configurar» el volumen externo, es decir, el volumen «normal», seleccionando el cifrado simétrico, hash y también el tamaño.



Pondremos una contraseña o una clave criptográfica como antes os hemos explicado, también elegimos el sistema de archivos, y pinchamos en «Formatear».

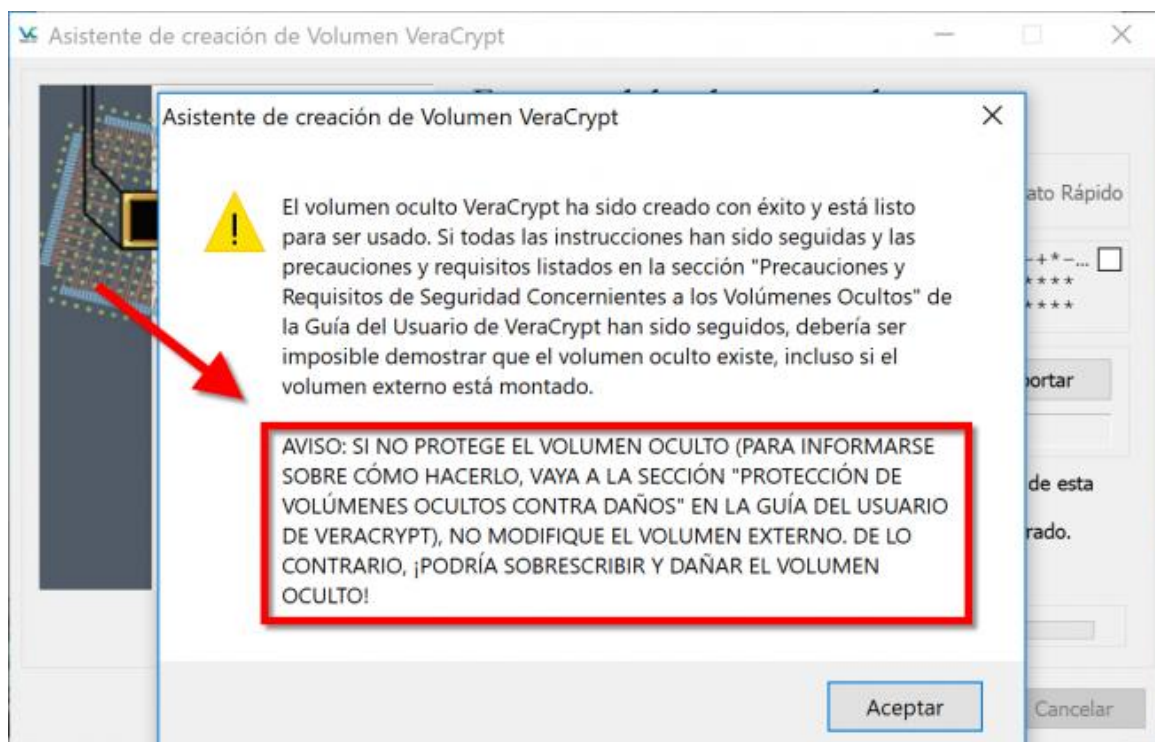


Una vez que hayamos creado el volumen externo, procedemos a crear el volumen oculto, y es que el asistente de configuración es exactamente igual que para el volumen externo, tendremos que configurar el cifrado, hash y también el tamaño (aunque en este caso tenemos un límite que depende del volumen normal creado anteriormente).

VeraCrypt nos permite crear un volumen externo e interno con diferente cifrado y hash, no hay problema porque el volumen externo esté con AES, y el interno esté con una combinación de AES con otros algoritmos de cifrado simétrico.



Al finalizar la configuración del volumen oculto, nos va a informar que debemos tener mucho cuidado con sobrescribir los datos, tal y como os hemos explicado anteriormente. Una vez que hayamos creado el volumen oculto, pinchamos en «Finalizar».

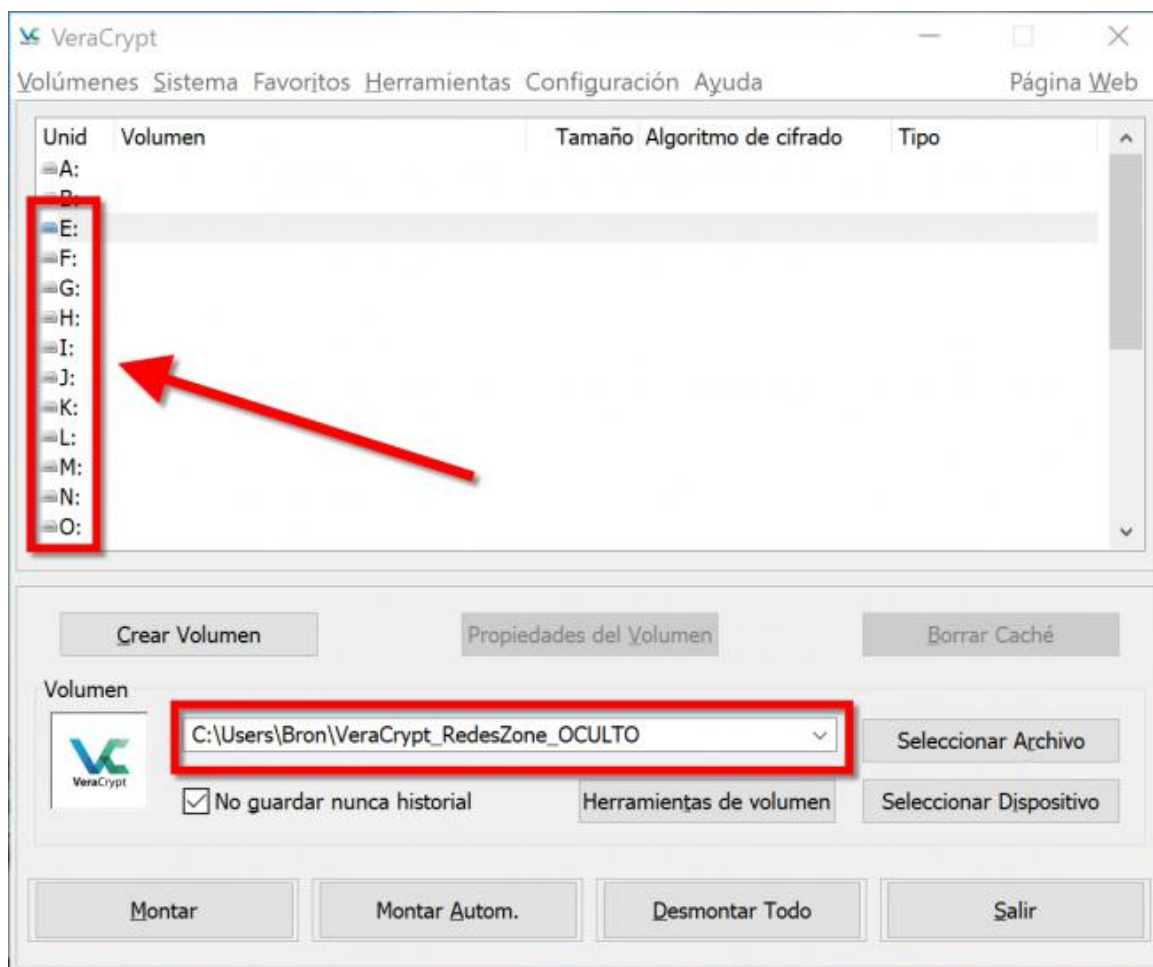


Ahora vamos a montar este volumen cifrado oculto, y vais a ver cómo diferenciarlos.

5. Montaje del volumen cifrado «oculto» creado anteriormente

El montaje del volumen oculto se realiza como antes, seleccionamos el volumen cifrado, seleccionamos una unidad para su montaje e introducimos la contraseña.

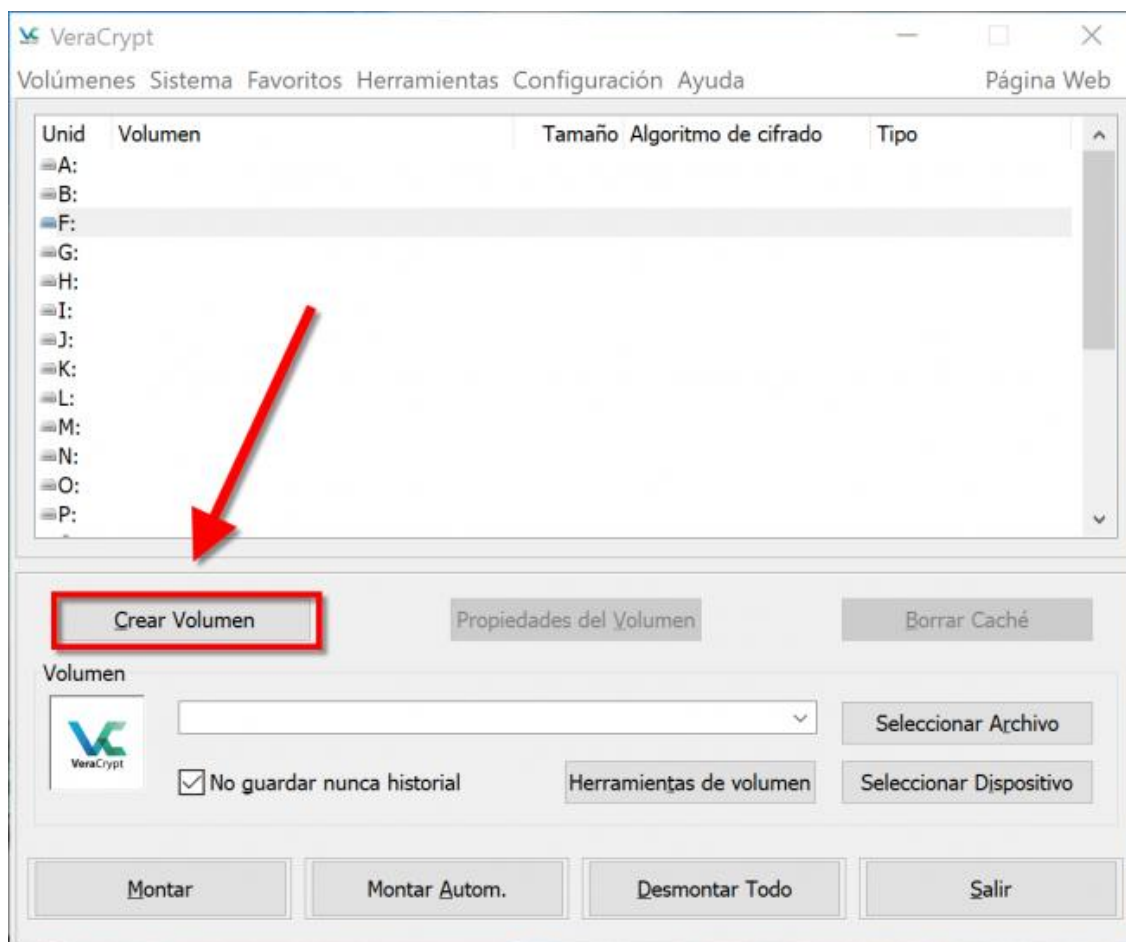
1. Si introducimos la contraseña del volumen «normal», se montará ese volumen.
2. Si introducimos la contraseña del volumen «oculto», se montará el volumen oculto.



Una vez que ya sabemos cómo crear volúmenes cifrados ocultos y cómo montarlos en una unidad, vamos a ver cómo podemos cifrar una unidad de almacenamiento extraíble entera.

6. Cifrado de un dispositivo de almacenamiento extraíble (USB, tarjeta SD, disco duro externo)

Lo primero que tenemos que hacer es introducir el dispositivo de almacenamiento extraíble en nuestro ordenador. Una vez introducido, pinchamos en «**Crear Volumen**», y seleccionamos «**Cifrar partición/unidad secundaria**» ya que vamos a cifrar una partición que no tiene el sistema operativo. Una vez seleccionada esta opción, elegimos entre «**Volumen VeraCrypt común**» o «**Volumen VeraCrypt oculto**», nosotros hemos seleccionado la primera opción para simplificar, pero podéis seleccionar la segunda opción con las mismas características que justo antes os hemos explicado.



Ahora debemos elegir el dispositivo a cifrar, si estamos introduciendo una unidad de almacenamiento extraíble, vamos a poder seleccionar su propia partición. En nuestro caso hemos introducido un pendrive que ha sido montado en la unidad E: por el sistema operativo, con un tamaño de 3,7GB. Cuando hayamos elegido la partición del dispositivo a cifrar, pinchamos en «**Aceptar**».



Cuando hayamos elegido el dispositivo, tenemos dos opciones para elegir:

- **Crear volumen cifrado y formatearlo:** esta opción es recomendable seleccionarla siempre y cuando lo que haya en el pendrive esté vacío, o que no nos importe que se formatee el dispositivo. Esta opción es muy rápida, y formatea todo el dispositivo.
- **Cifrar partición conservando datos:** este proceso es mucho más largo, ya que se encarga de cifrar el propio contenido sin pérdida de datos.

Una vez elegido el modo de creación de volumen, deberemos **elegir las diferentes opciones de cifrado simétrico, y también hashing**. Por supuesto, en esta ocasión **no podremos elegir el tamaño del volumen** ya que el tamaño viene dado por el propio tamaño del dispositivo de almacenamiento extraíble.



De cara a la autenticación para acceder a los datos, podremos introducir la típica contraseña de paso, o también elegir una clave criptográfica para acceder al propio dispositivo cifrado. Si seleccionamos una contraseña que sea muy corta, nos avisará que no es recomendable de cara a la seguridad.

Una vez elegida la autenticación, procedemos a «mover» el ratón para aumentar la aleatoriedad del volumen y pinchamos en «Formatear». Por último, nos avisará que todos los datos almacenados se perderán.



Cuando el proceso termine, **nos avisará que la unidad E no va a ser accesible**, ya que en esta unidad es el propio sistema operativo donde «coloca» el dispositivo de almacenamiento extraíble. Una vez que nosotros montemos este dispositivo en VeraCrypt, e introduzcamos la contraseña de acceso, sí vamos a poder acceder sin ningún tipo de problema.

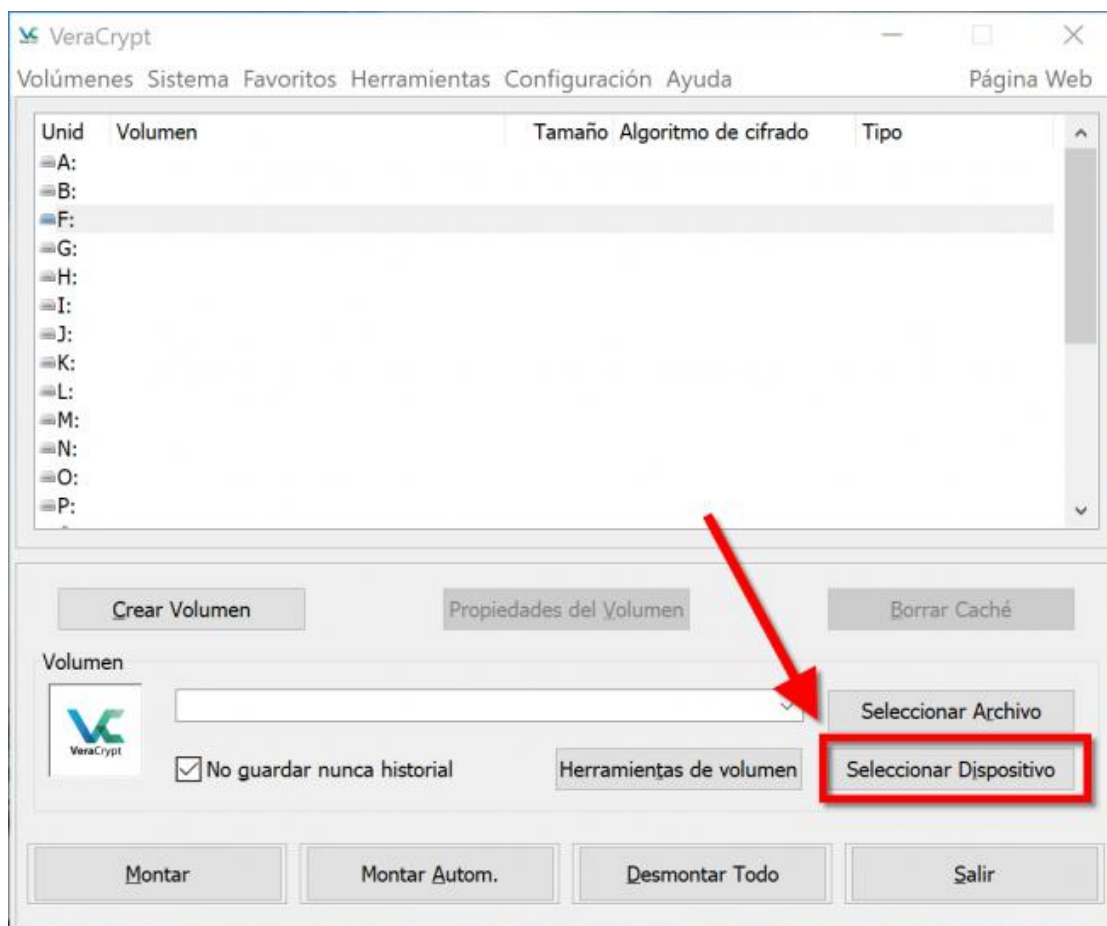
Cuando el proceso termine (la duración depende sobre todo del tamaño y velocidad de la unidad USB), nos avisará que todo está correcto, y pinchamos en «Salir».



Ahora ya tendremos nuestra unidad de almacenamiento perfectamente cifrada, y para usarla, deberemos «montarla» en el propio «VeraCrypt».

7. Montaje del dispositivo de almacenamiento extraíble cifrado

El montaje del dispositivo de almacenamiento extraíble cifrado es realmente fácil y sencillo, ahora pinchamos en «**Seleccionar Dispositivos**», elegimos la partición que antes hemos elegido, introducimos la contraseña de acceso y automáticamente se nos montará en otra unidad para poder acceder a los datos.



Al montar la unidad, veremos algo como lo siguiente:

- Unidad de USB E: es el propio dispositivo hardware (pendrive)
- Disco local F: es el dispositivo cifrado que hemos «montado» con VeraCrypt.

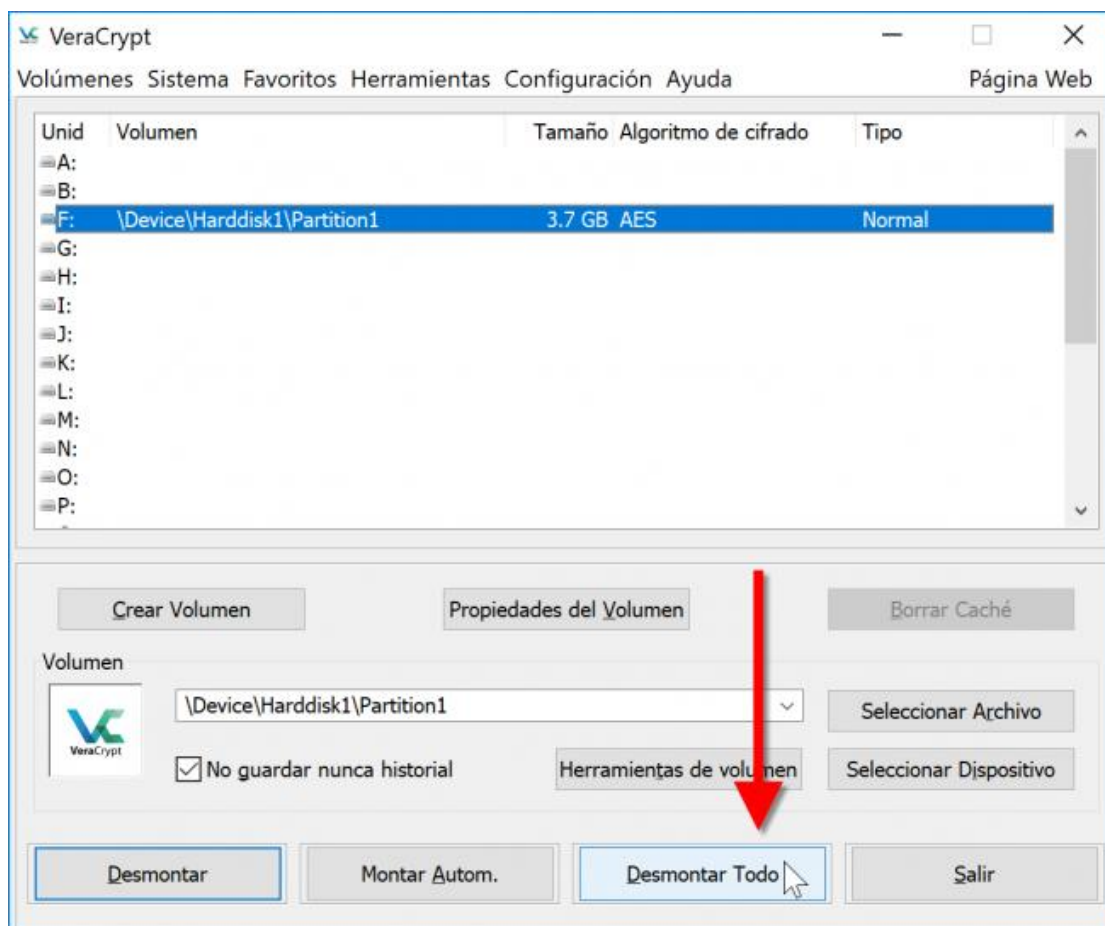


Unidad de USB (E:)
FAT32



Disco local (F:)
3,73 GB disponibles de...

Una vez que terminemos de leer o escribir en dicho disco cifrado, procedemos a desmontarlo pinchando en «Desmontar» sobre la unidad que nosotros queramos, o bien en «**Desmontar todo**» si es que solo tenemos uno o queremos desmontar todas las unidades que tengamos en ese instante.



Ahora que ya sabemos cómo crear una unidad de almacenamiento extraíble cifrada, y que sabemos cómo montarla, vamos a cifrar el sistema operativo entero.

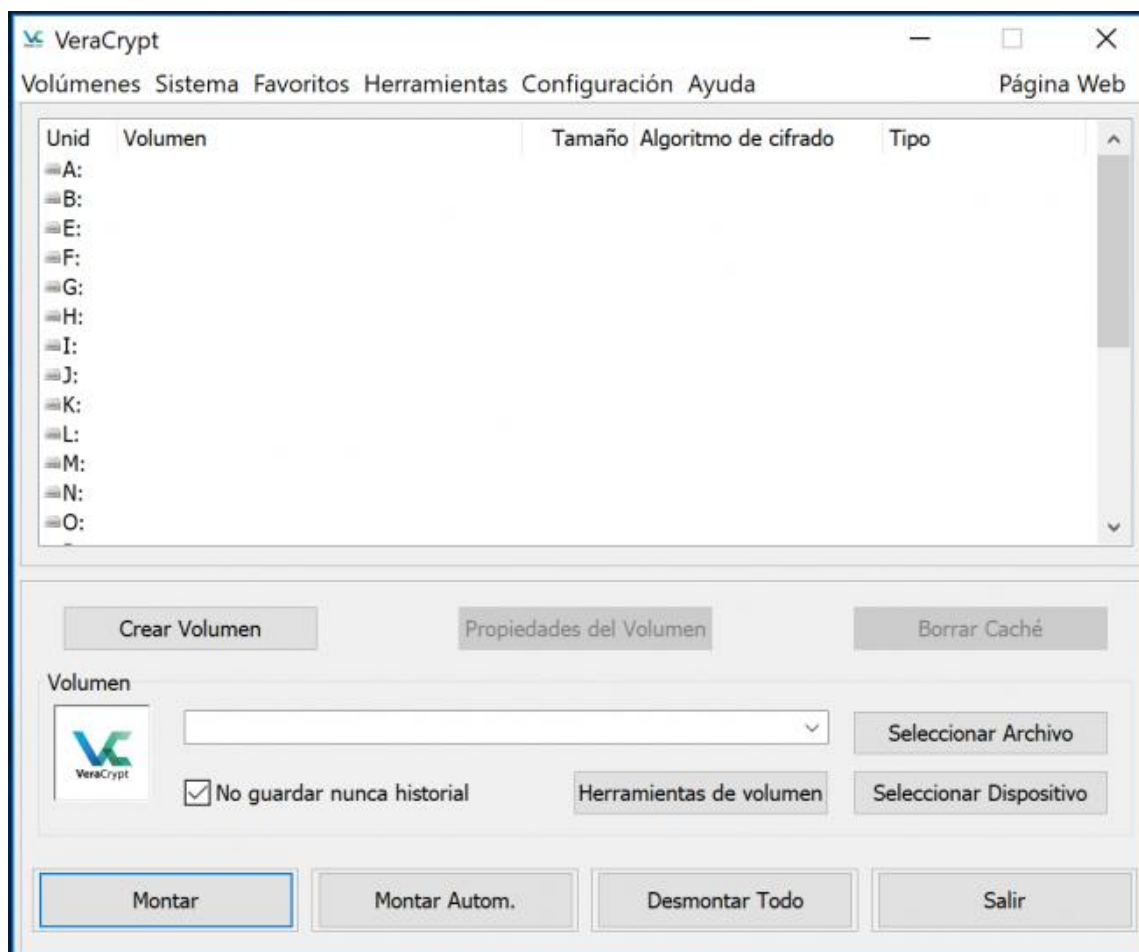
8. Cifrado de todo el sistema operativo (cifrar la partición/unidad del sistema entera) en VeraCrypt

Este proceso lo debemos realizar con mucho cuidado, ya que de lo contrario podríamos perder toda la información. Es recomendable realizar una copia de seguridad completa de nuestro PC con programas como Acronis True Image o similares, y sobre todo, no olvidar la clave de acceso al sistema que pongamos en VeraCrypt.

Lo primero que debemos hacer es pinchar en «**Crear Volumen**», y posteriormente elegir «**Cifrar la partición/unidad del sistema entera**». Una vez dentro, tenemos dos opciones principales:

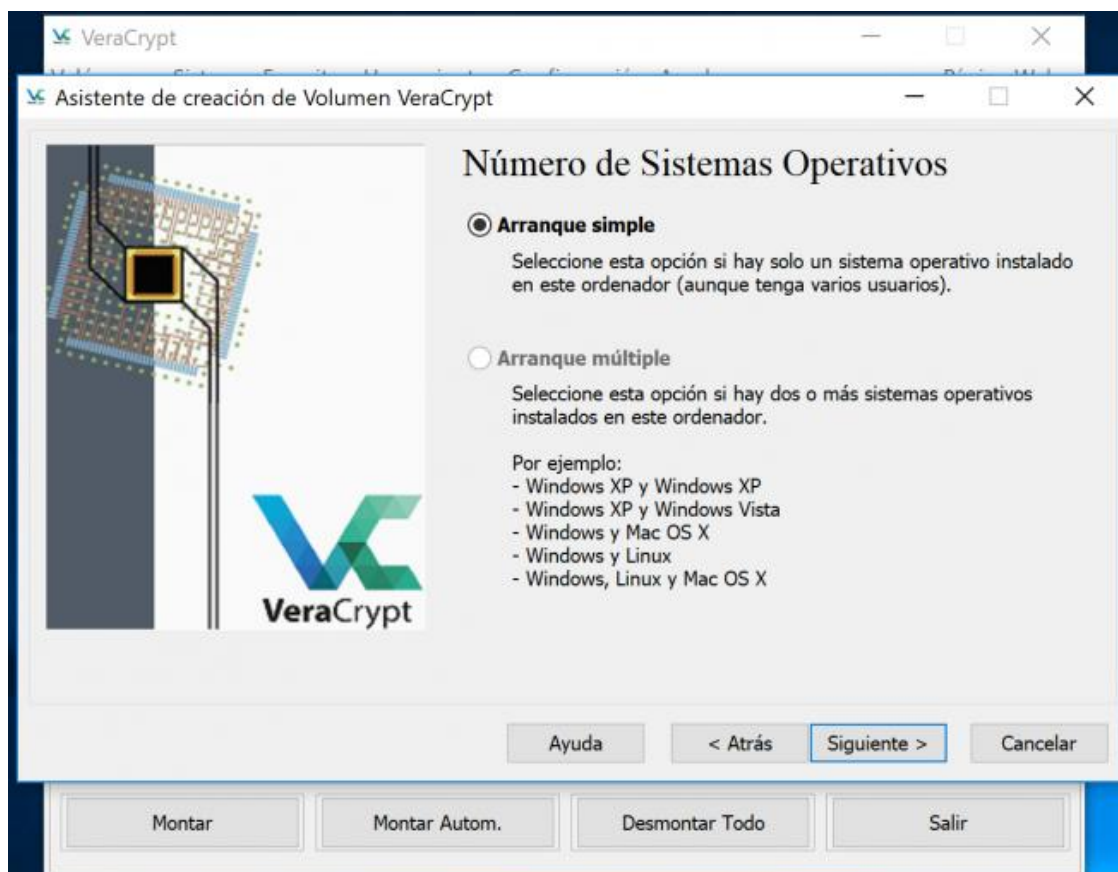
- Normal: se cifra con una clave de paso o una clave criptográfica en un volumen con el sistema operativo nuestro.
- Oculto: se cifra el sistema operativo dentro de un volumen oculto para evitar una extorsión, de esta forma, podremos poner una clave y acceder a un sistema operativo que no sea el «bueno».

Nosotros hemos elegido el modo «normal». A continuación, también nos da la opción de «**Cifrar la partición de Windows**», o bien pinchar en «**Cifrar toda la unidad**» si queremos realizar justo esto.

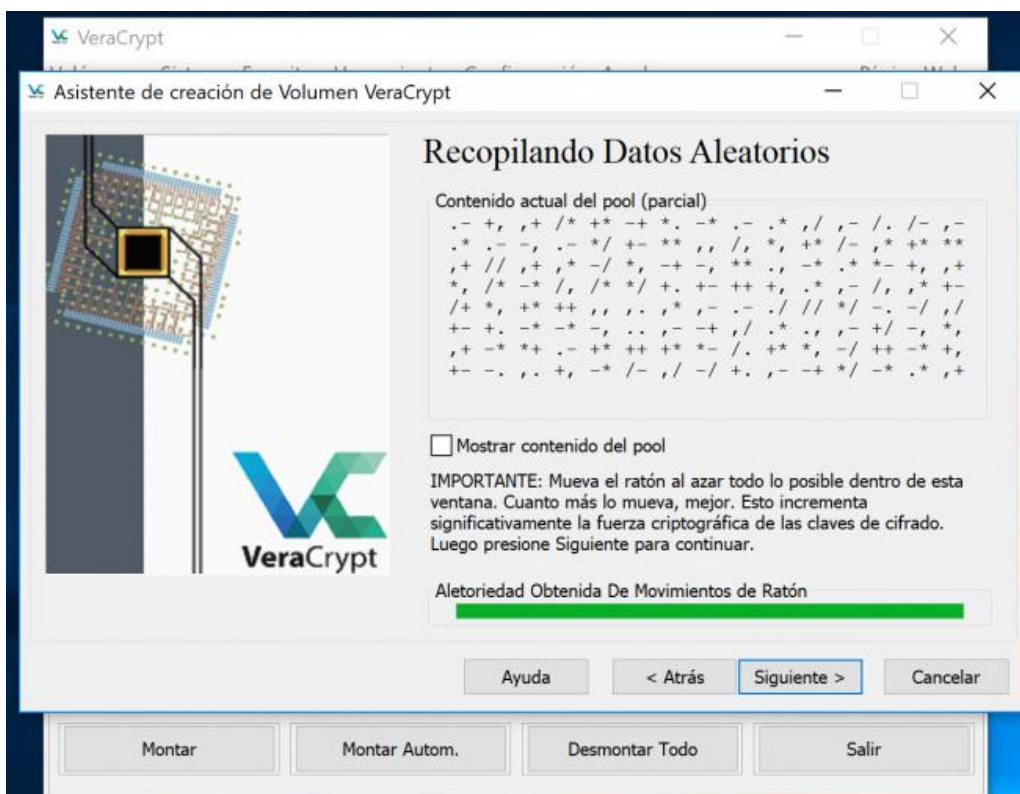


Si nuestro equipo incorpora varios sistemas operativos con multi arranque, tendremos que elegir la opción correspondiente. De lo contrario, elegimos la opción de «**Arranque simple**» tal y como hemos hecho nosotros.

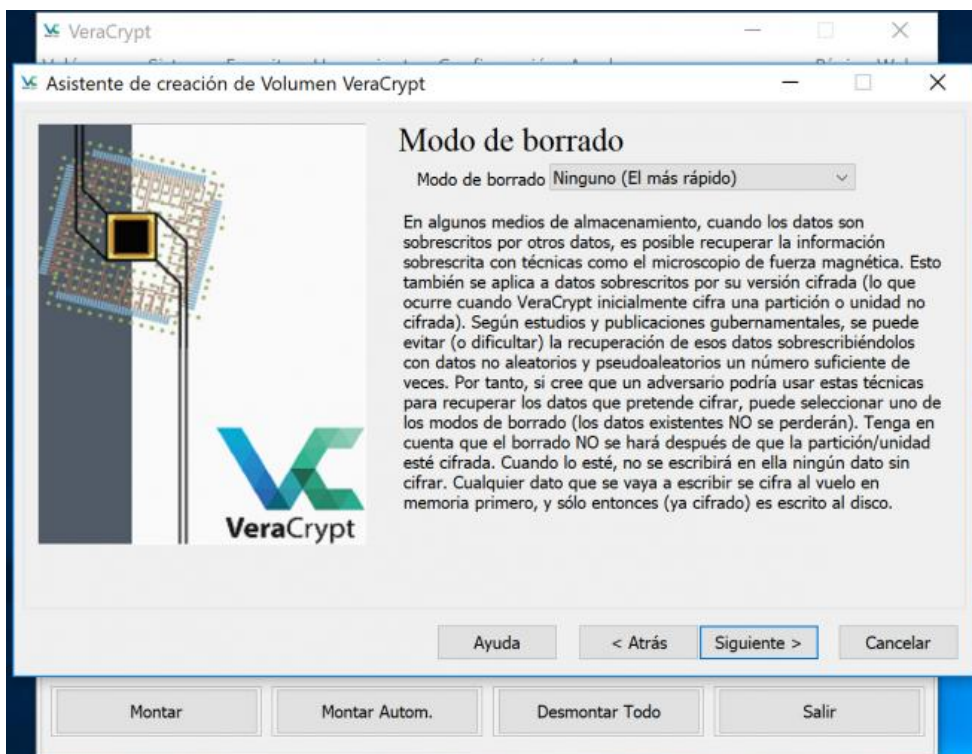
Cuando hayamos terminado de configurar el volumen para el sistema operativo, nos queda seleccionar el algoritmo de cifrado simétrico, el algoritmos de hashing y la clave de autenticación o clave criptográfica.



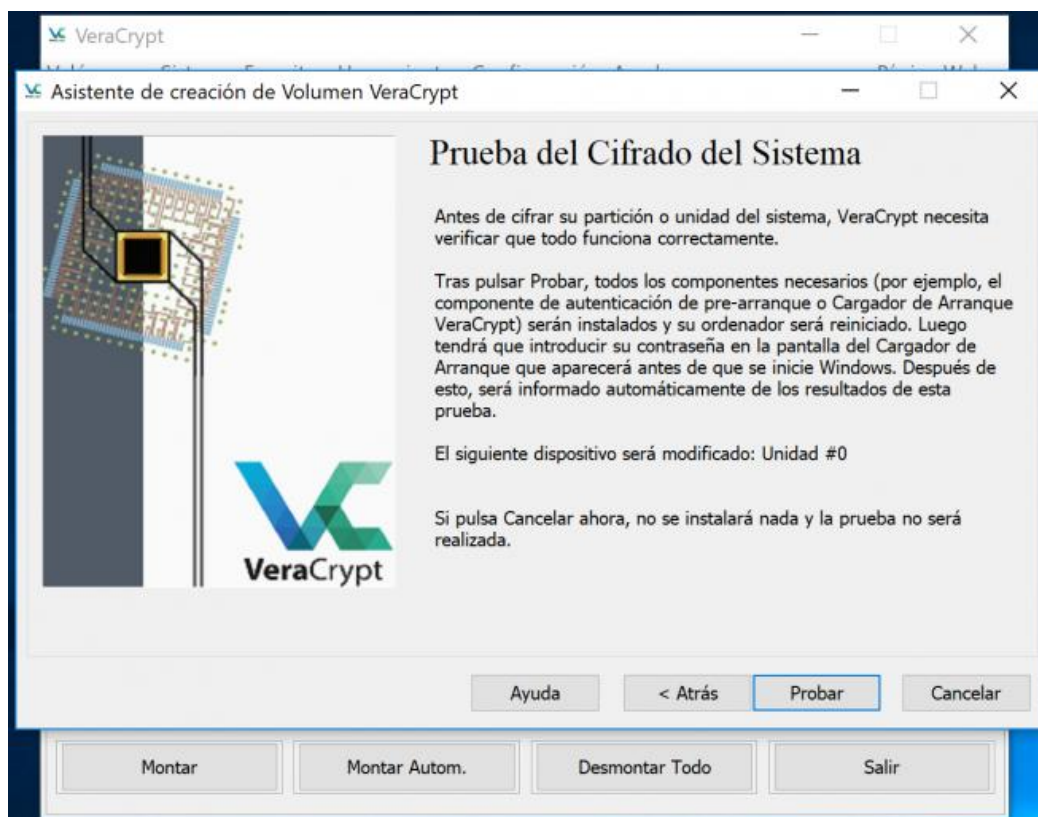
Una vez configurado por completo el volumen, se crearán las claves internas, y nos recomendará crear un disco de rescate por si ocurre algún tipo de problema, poder recuperar toda la información, aunque siempre vamos a tener que introducir la contraseña de acceso.



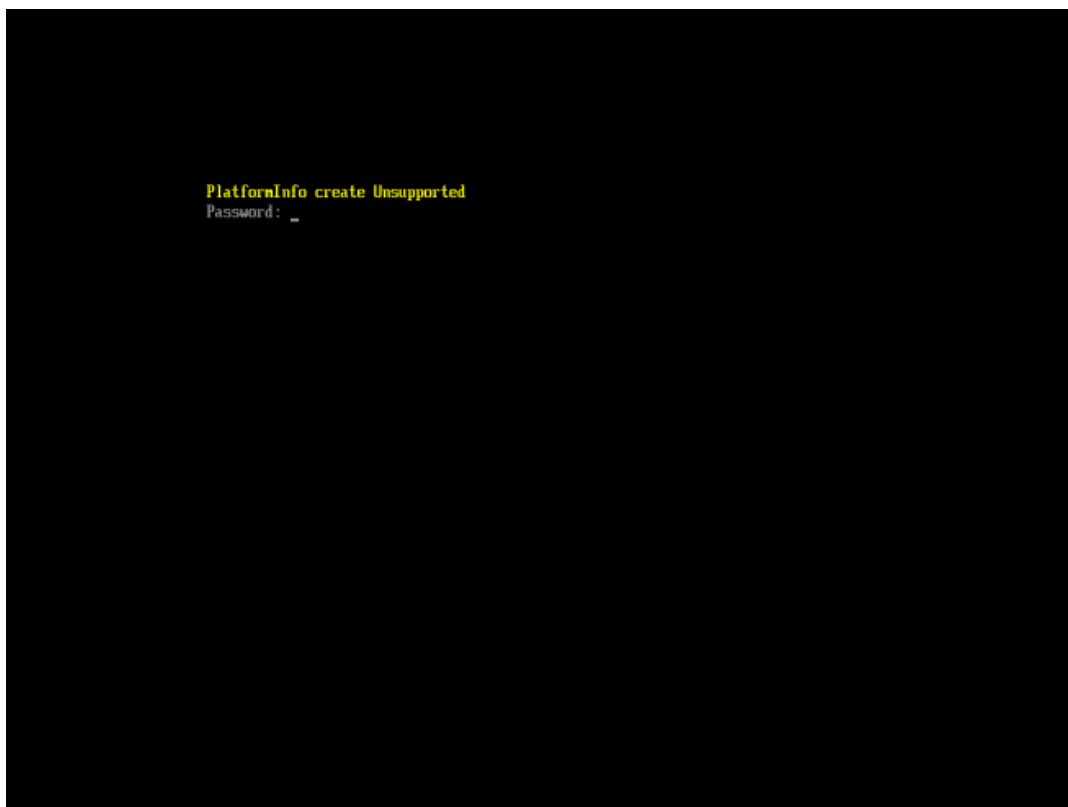
También tenemos la posibilidad de seleccionar la política si borramos algún archivo dentro del propio sistema operativo, y es que nos va a permitir utilizar diferentes métodos de borrado seguro, ideal para mantener nuestra privacidad.



Una vez configurado el modo de borrado, pinchamos en «probar», pinchamos en «sí» y posteriormente en «aceptar». De manera automática VeraCrypt se encargará de cifrar todo nuestro disco duro, y nos pedirá reiniciar el sistema operativo.



Al reiniciar el sistema operativo, tendremos que introducir nuestra contraseña de acceso, y dejar en blanco la segunda opción (por defecto), y automáticamente entraremos en el sistema operativo nuestro como siempre.



Hasta aquí hemos llegado con nuestro manual de instalación, configuración y creación de volúmenes de VeraCrypt para almacenar de manera segura nuestros datos. Esperamos que os haya gustado y os recomendamos [visitar la documentación oficial del software VeraCrypt](#) donde encontraréis toda la información sobre esta fantástica herramienta.