Seguridad digital integral

Materiales para mejorar tus hábitos digitales.

@cervy_0 seguridaddigitalec

Open labEc

Internews
Local voices. Global change.

USABLE

Tutorial de Veracrypt

Tomado de:

RZ redes zone

Veracrypt: Cifra y oculta tus archivos gratis

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:

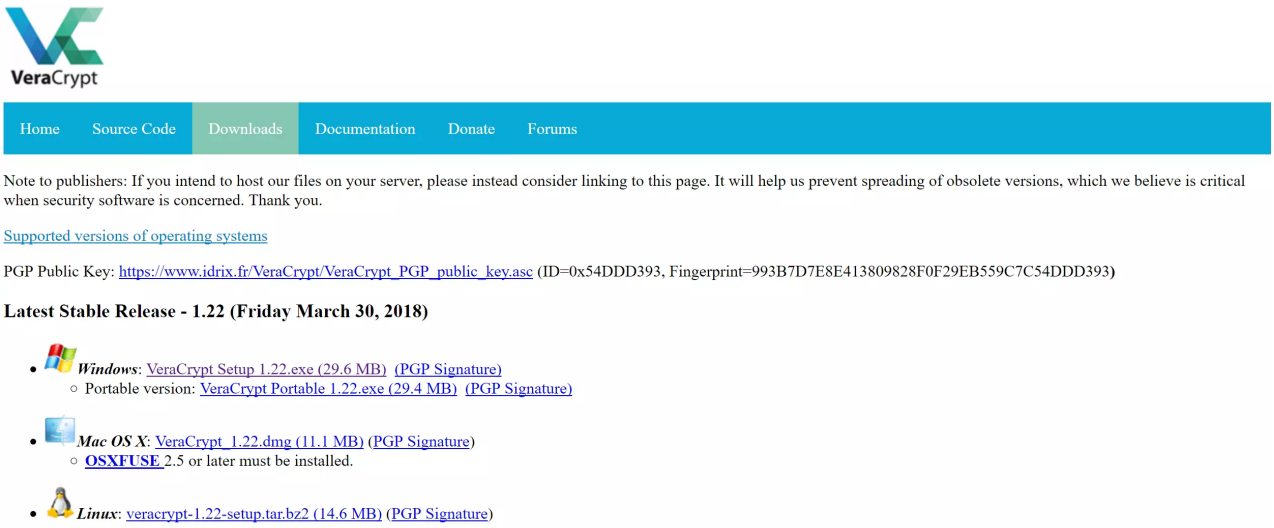
- Creación de discos cifrados virtuales en un simple archivo: podremos crear un archivo cifrado a modo de contenedor, en el cual esté toda la información importante. Este archivo lo podremos montar para su lectura y escritura con VeraCrypt, este método es ideal para moverlo a cualquier sitio e incluso para enviarlo por email, subirlo a un servidor FTP o Samba y más. Gracias a que tenemos un simple archivo que contiene toda la información confidencial, podremos guardarlo a buen recaudo grabándolo en un CD o DVD, e incluso copiarlo en un pendrive.

- Cifrado de dispositivos de almacenamiento extraíble como USB, tarjetas SD e incluso discos duros. En este caso, todo el dispositivo de almacenamiento extraíble estará complemente cifrado, Windows nos indicará que necesita formato el disco para poder leerlo, siempre debemos pinchar en cancelar y abrirlo con VeraCrypt, introduciendo la correspondiente clave de descrifrado.
- Cifrado de cualquier partición de estos dispositivos de almacenamiento extraíble.
- Cifrado de la partición o disco completo donde Windows esté instalado. Esto nos permite hacer exactamente la misma función que Bitlocker, cifrará el disco duro o SSD por completo, para que tanto el sistema operativo como todos nuestros archivos estén a salvo frente a posibles robos.
- 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.

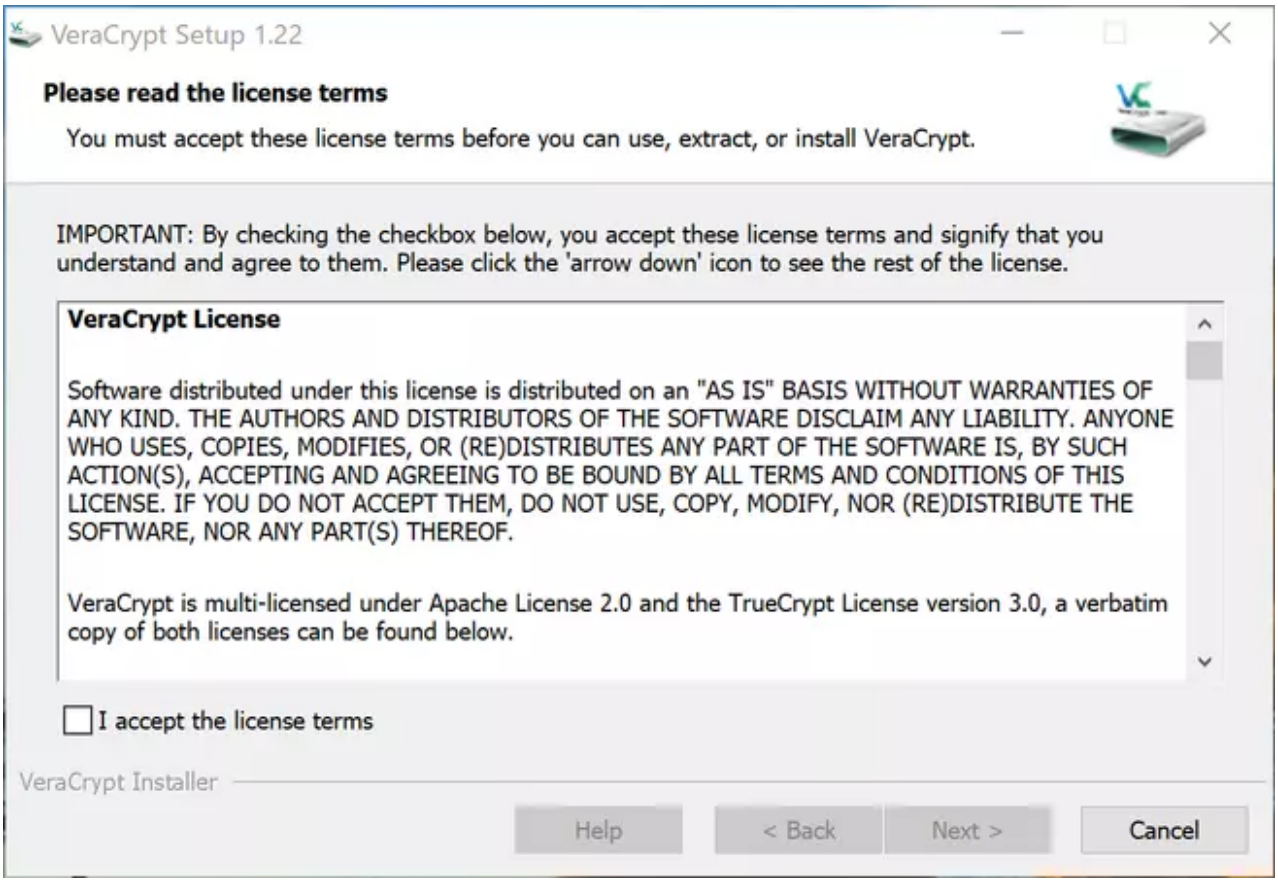
1. Descarga e instalación de VeraCrypt

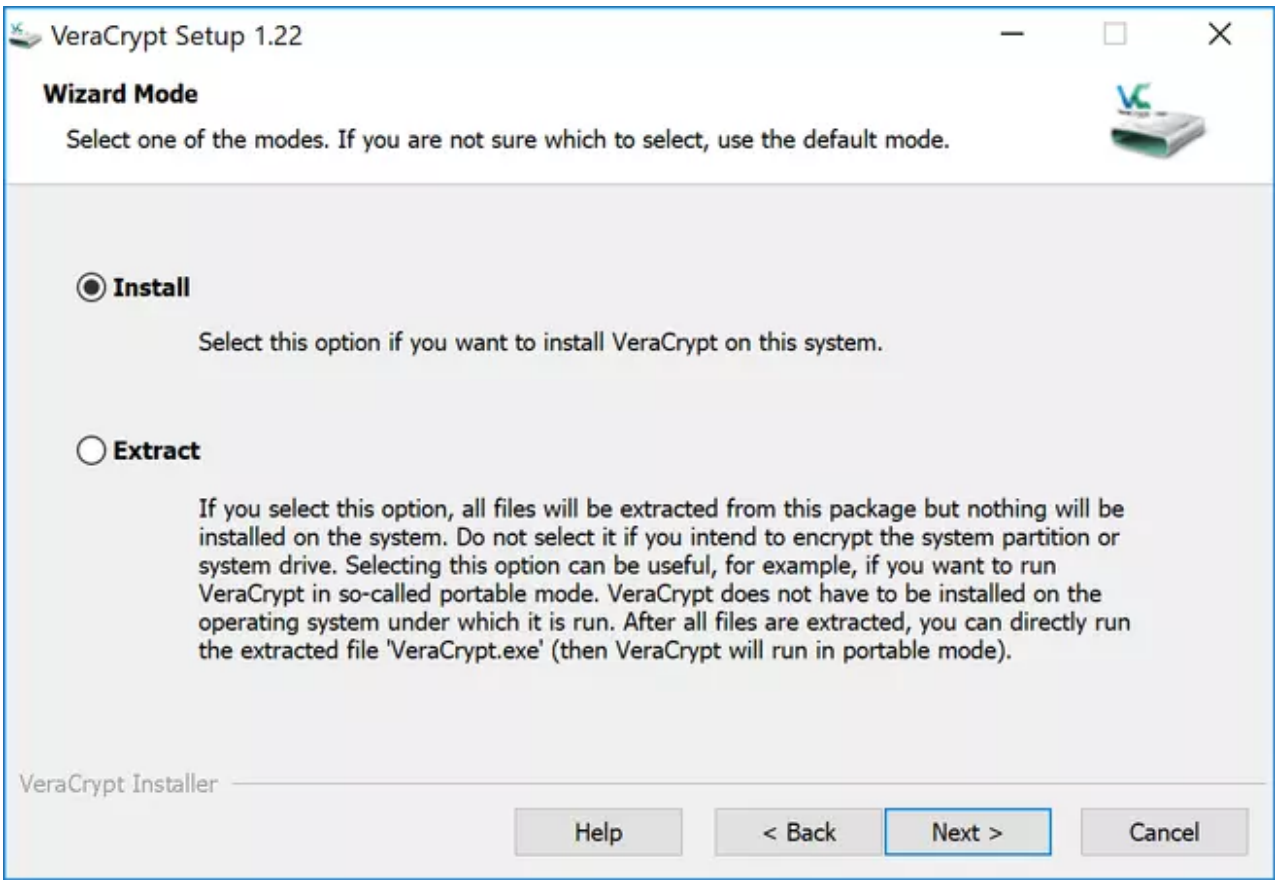
Lo primero que tenemos que hacer es descargar VeraCrypt, la descarga se realiza directamente a través de la **página web oficial**, en la sección descargas: **Descargar VeraCrypt gratis**. En esta web vamos a poder descargar todas las versiones de VeraCrypt, tanto para Windows, Linux, macOS, FreeBSD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



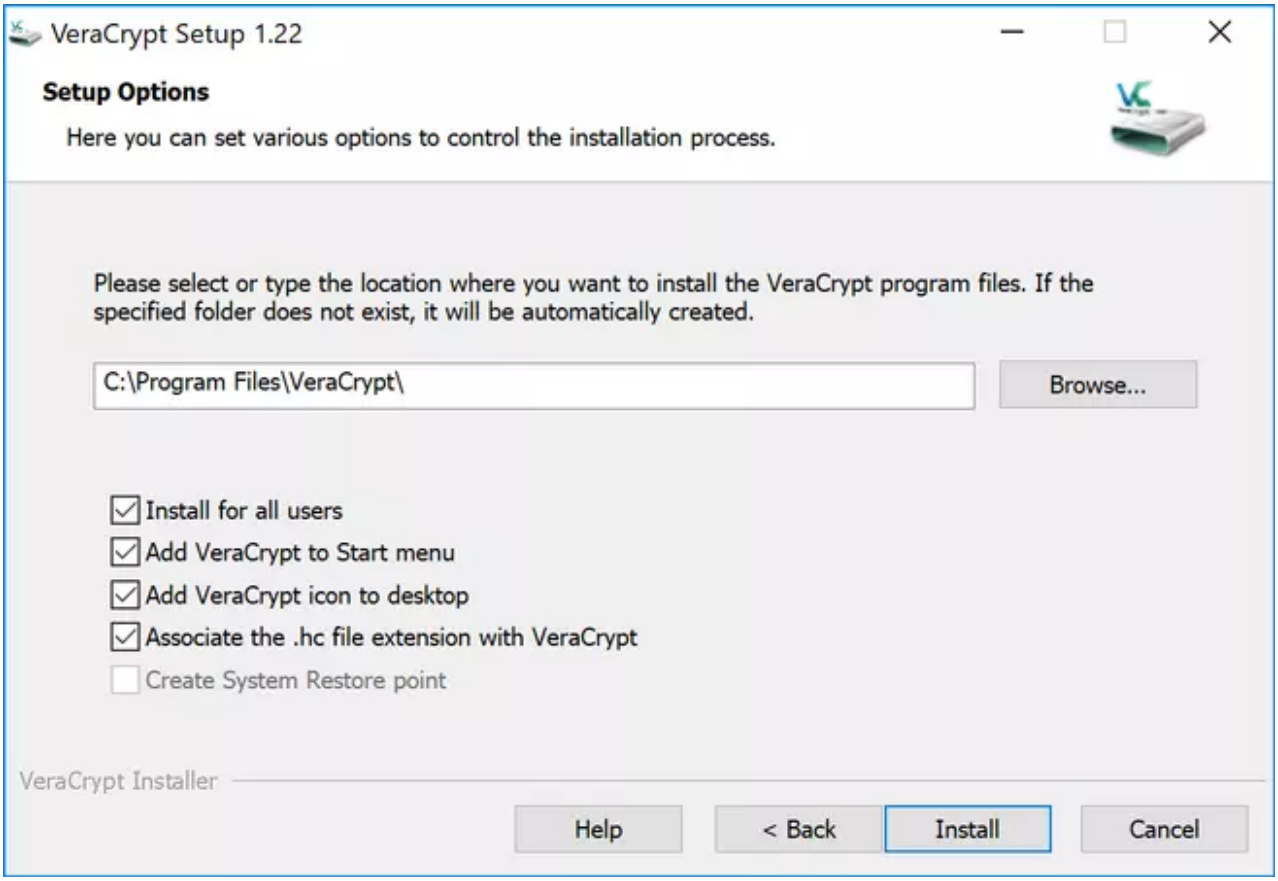
Una vez descargado el programa, debemos instalarlo como cualquier programa. Nos saldrá un asistente de instalación que nos dará la opción de instalarlo en el propio equipo, o extraer VeraCrypt y usarlo de manera «portable», es decir, sin instalarlo en el

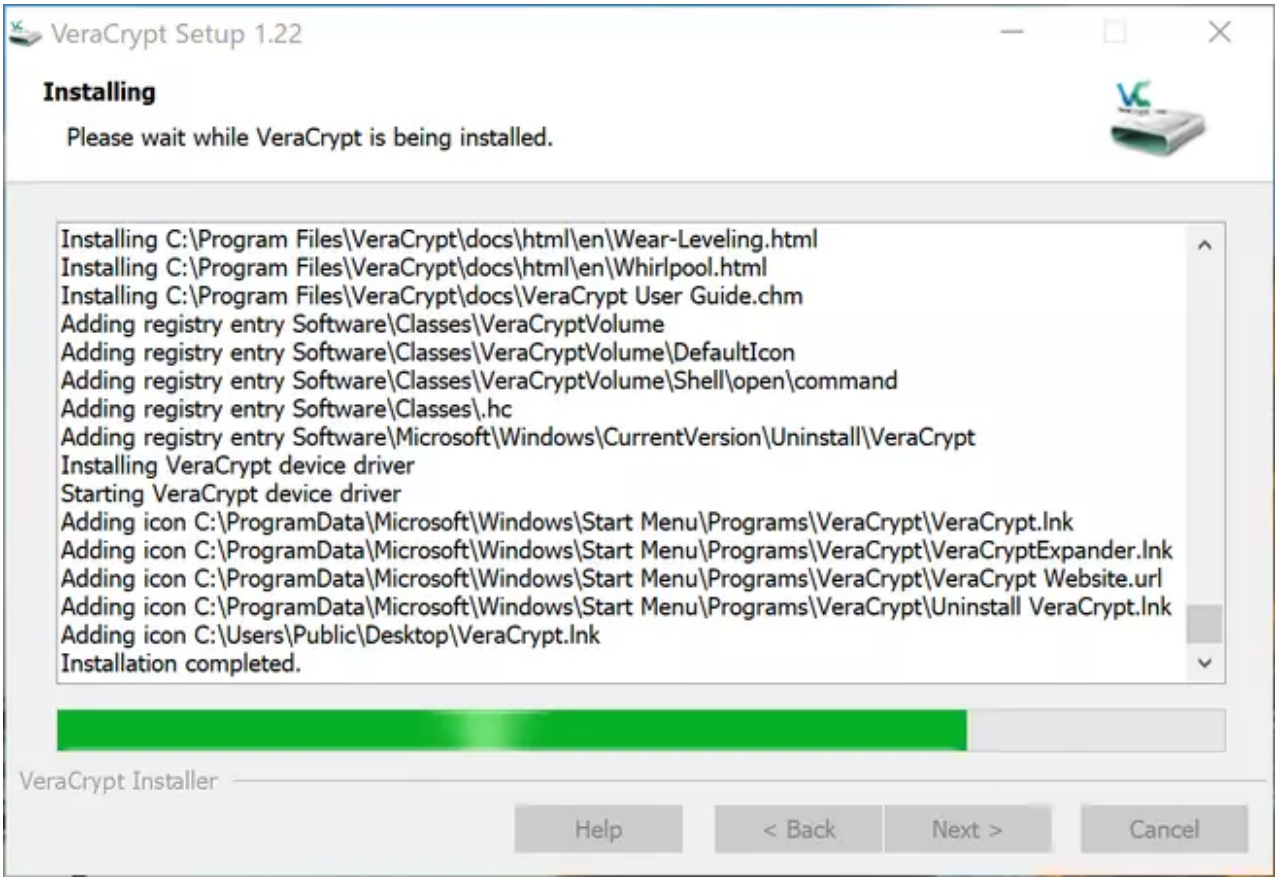
propio ordenador. Un detalle importante es que si vamos a cifrar el sistema completo o la partición donde está el sistema operativo, deberemos instalarlo obligatoriamente y no usarlo en modo «portable».

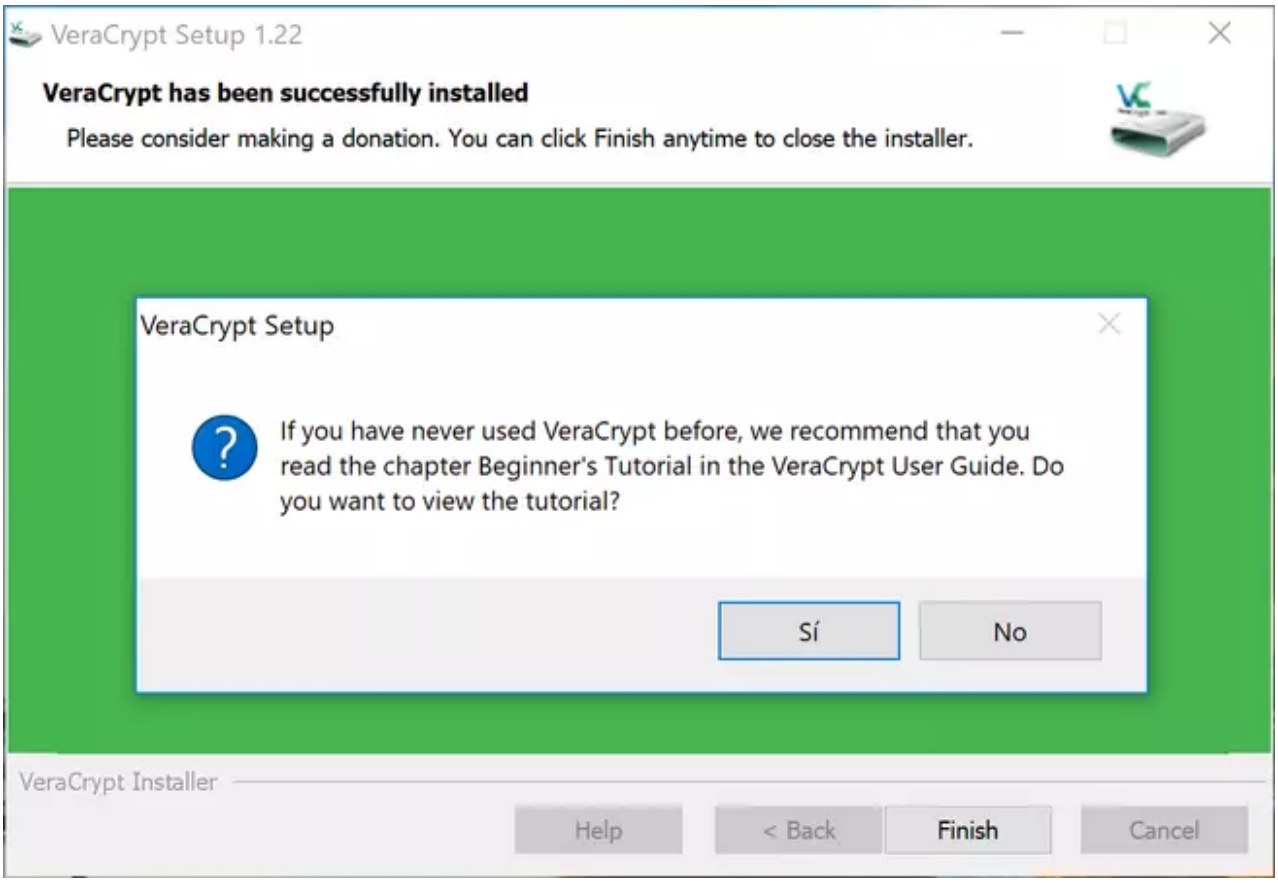




Una vez que hayamos pinchado en «Install», nos saldrán las típicas opciones de instalación para todos los usuarios, creación de acceso directo en escritorio y también en el menú inicio. Una vez que haya terminado de instalar, nos recomendará seguir una pequeña guía para principiantes en VeraCrypt.







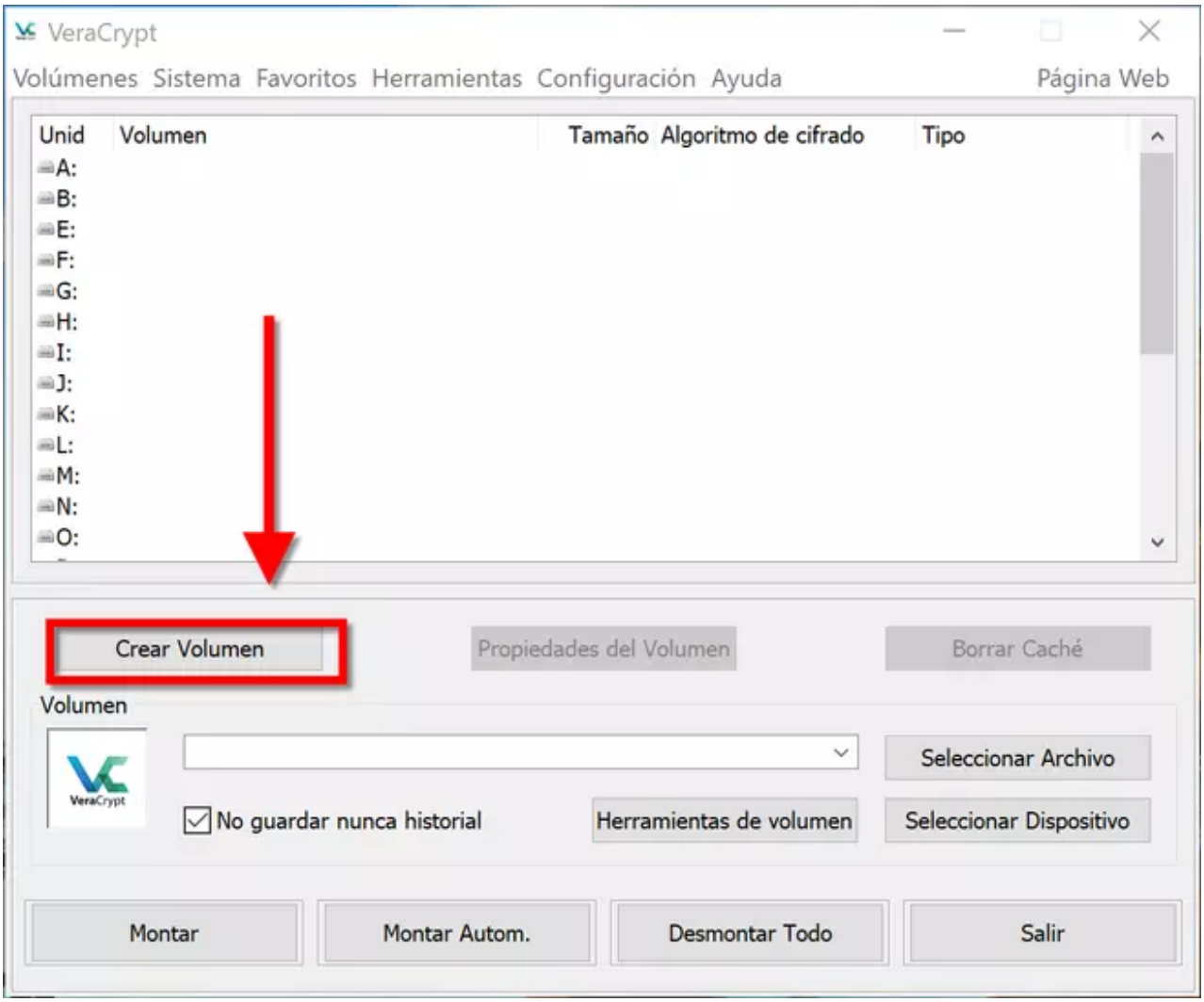
Una vez que lo tenemos instalado, vamos a proceder a crear los diferentes volúmenes, el cifrado de discos USB, y también el cifrado completo del sistema operativo.

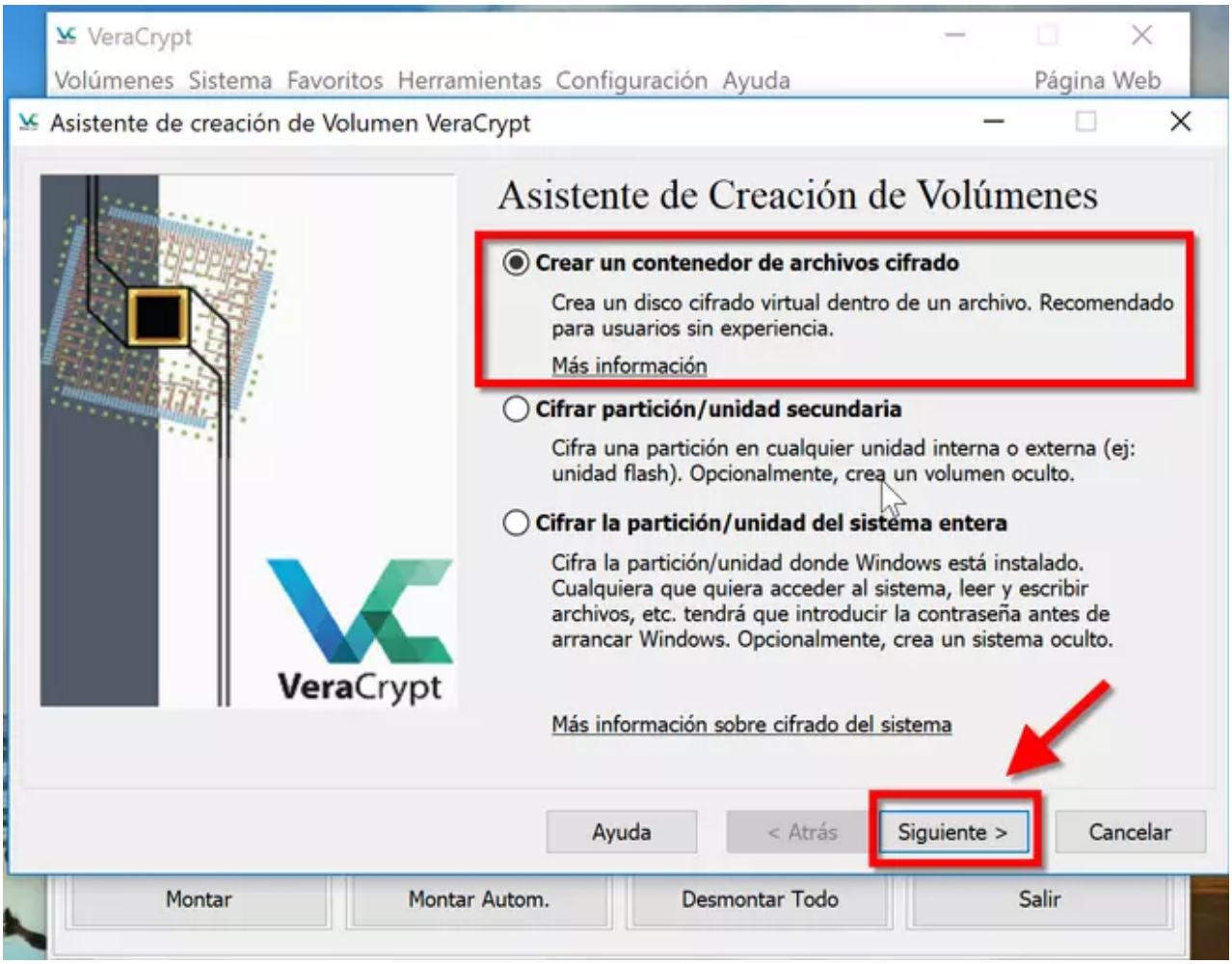
2. Creación de un volumen cifrado «normal»

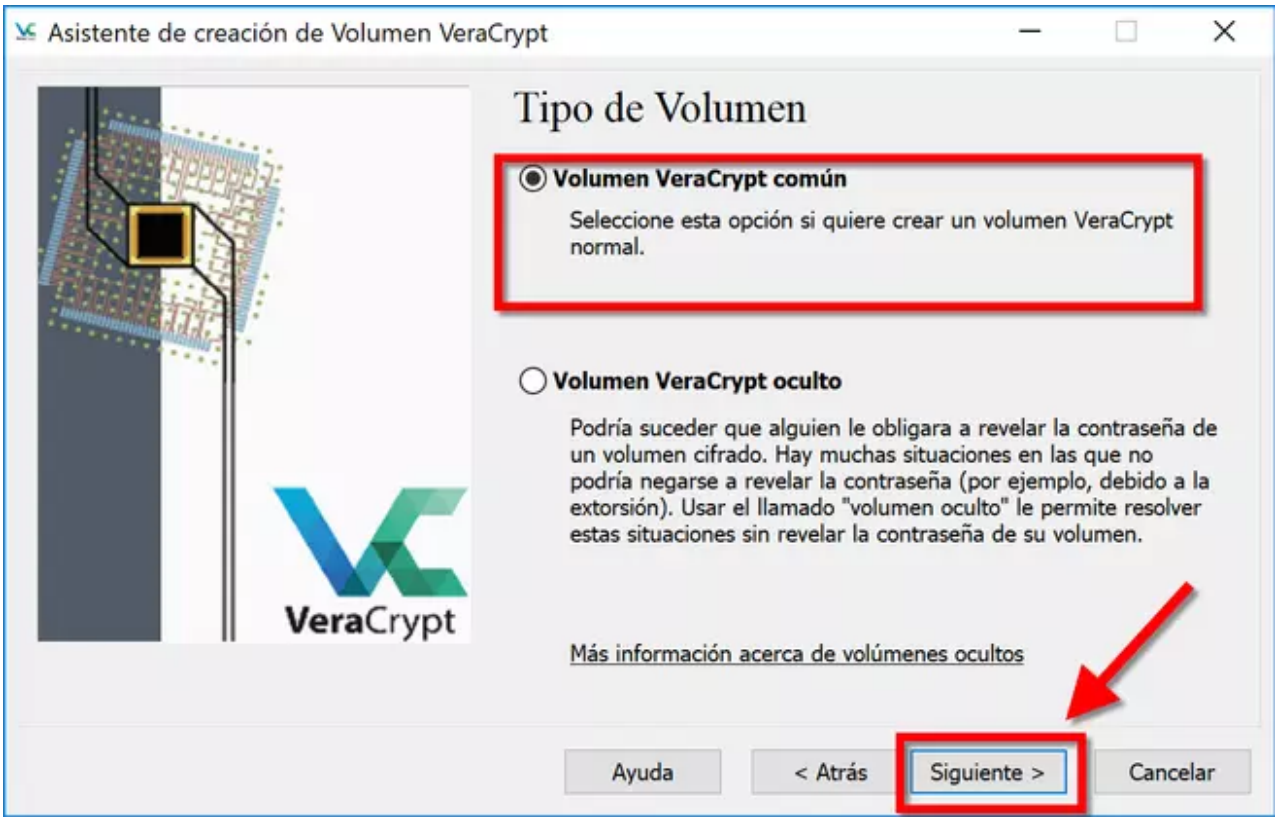
Lo primero que vamos a hacer es crear un volumen cifrado «normal», sin introducir dentro de él un volumen oculto.

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.


VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda
Página Web
Unid Volumen
Tamaño Algoritmo de cifrado
Tipo
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Crear Volumen
Propiedades del Volumen
Borrar Caché
Volumen
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir

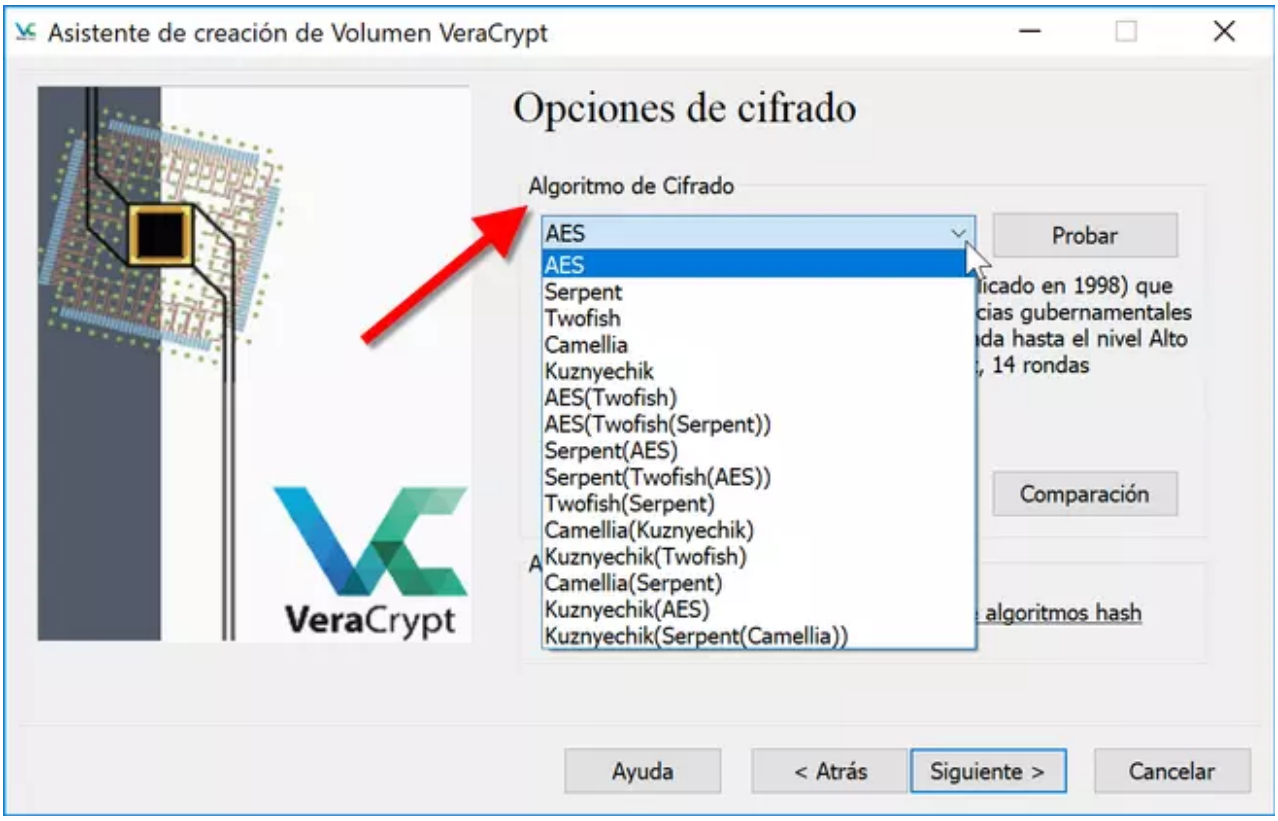

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda
Página Web
Asistente de creación de Volumen VeraCrypt
Asistente de Creación de Volúmenes
Crear un contenedor de archivos cifrado
Crea un disco cifrado virtual dentro de un archivo. Recomendado para usuarios sin experiencia.
Más información
Cifrar partición/unidad secundaria
Cifra una partición en cualquier unidad interna o externa (ej: unidad flash). Opcionalmente, crea un volumen oculto.
Cifrar la partición/unidad del sistema entera
Cifra la partición/unidad donde Windows está instalado. Cualquiera que quiera acceder al sistema, leer y escribir archivos, etc. tendrá que introducir la contraseña antes de arrancar Windows. Opcionalmente, crea un sistema oculto.
Más información sobre cifrado del sistema
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

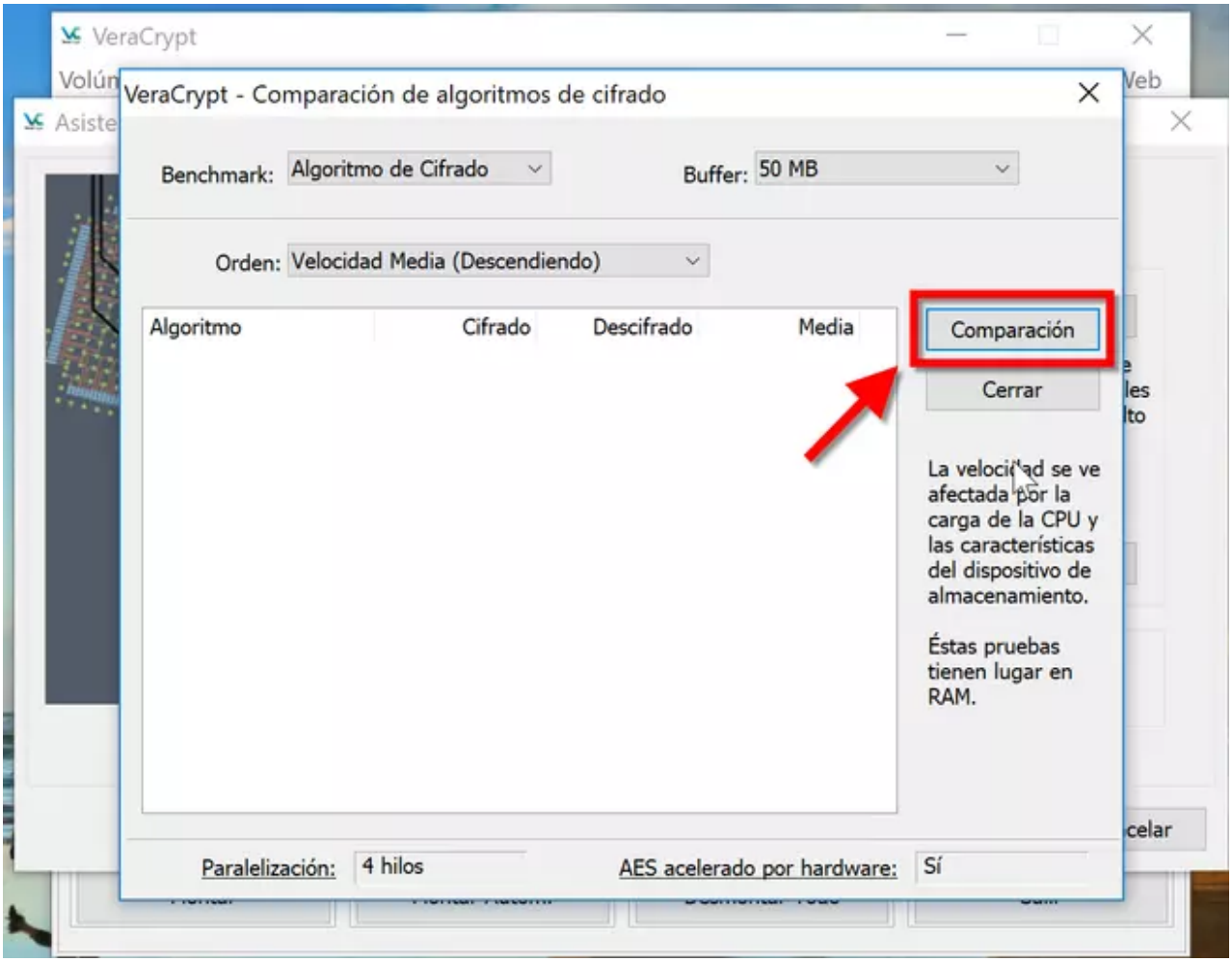

Asistente de creación de Volumen VeraCrypt
Tipo de Volumen
Volumen VeraCrypt común
Seleccione esta opción si quiere crear un volumen VeraCrypt normal.
Volumen VeraCrypt oculto
Podría suceder que alguien le obligara a revelar la contraseña de un volumen cifrado. Hay muchas situaciones en las que no podría negarse a revelar la contraseña (por ejemplo, debido a la extorsión). Usar el llamado "volumen oculto" le permite resolver estas situaciones sin revelar la contraseña de su volumen.
Más información acerca de volúmenes ocultos
Ayuda
< Atrás
Siguiente >
Cancelar

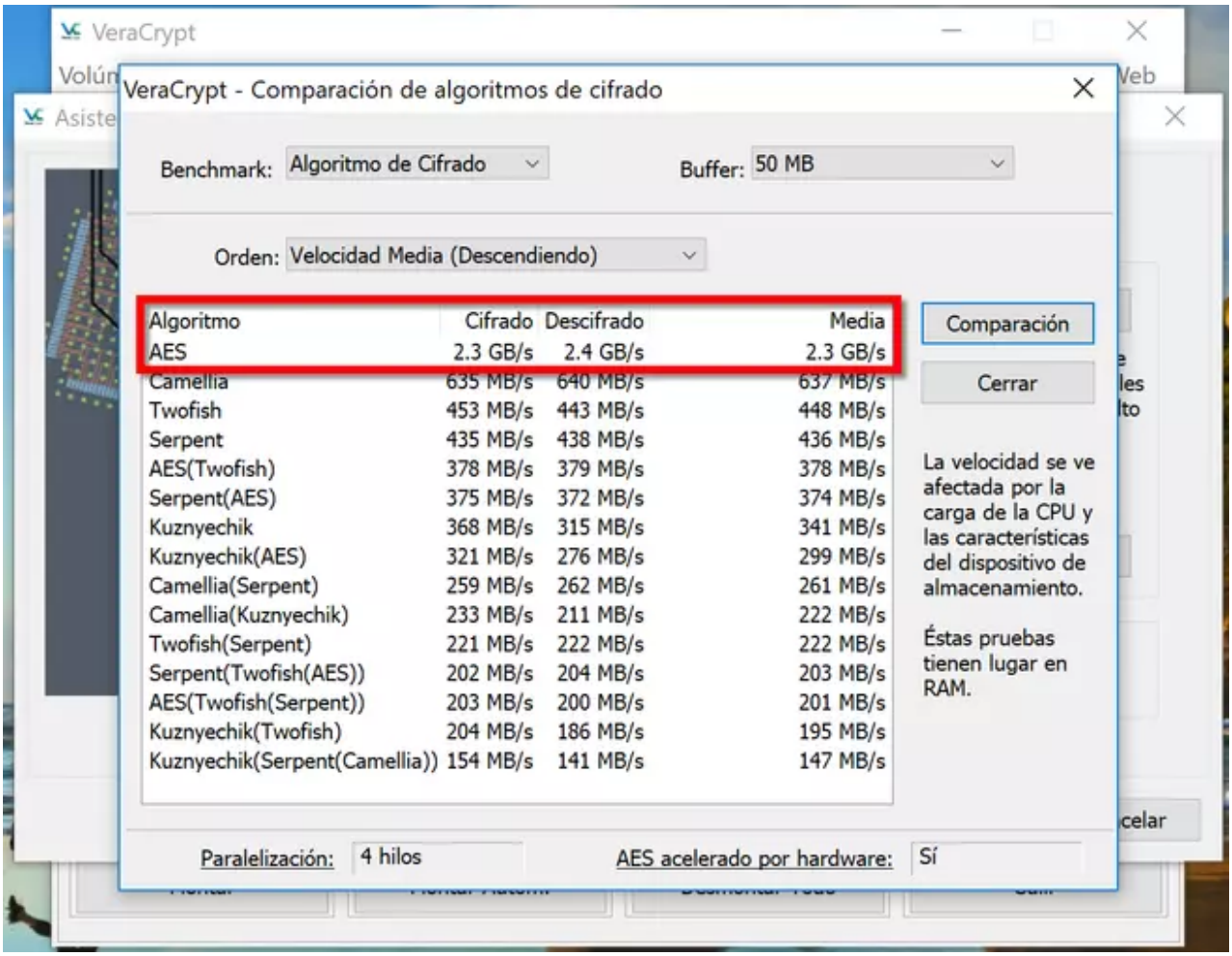
Una vez que ya tenemos configurado nuestro volumen VeraCrypt, deberemos seleccionar dos aspectos muy importantes: el cifrado simétrico para asegurar la confidencialidad, y el algoritmo de hashing para comprobar la integridad de los archivos.

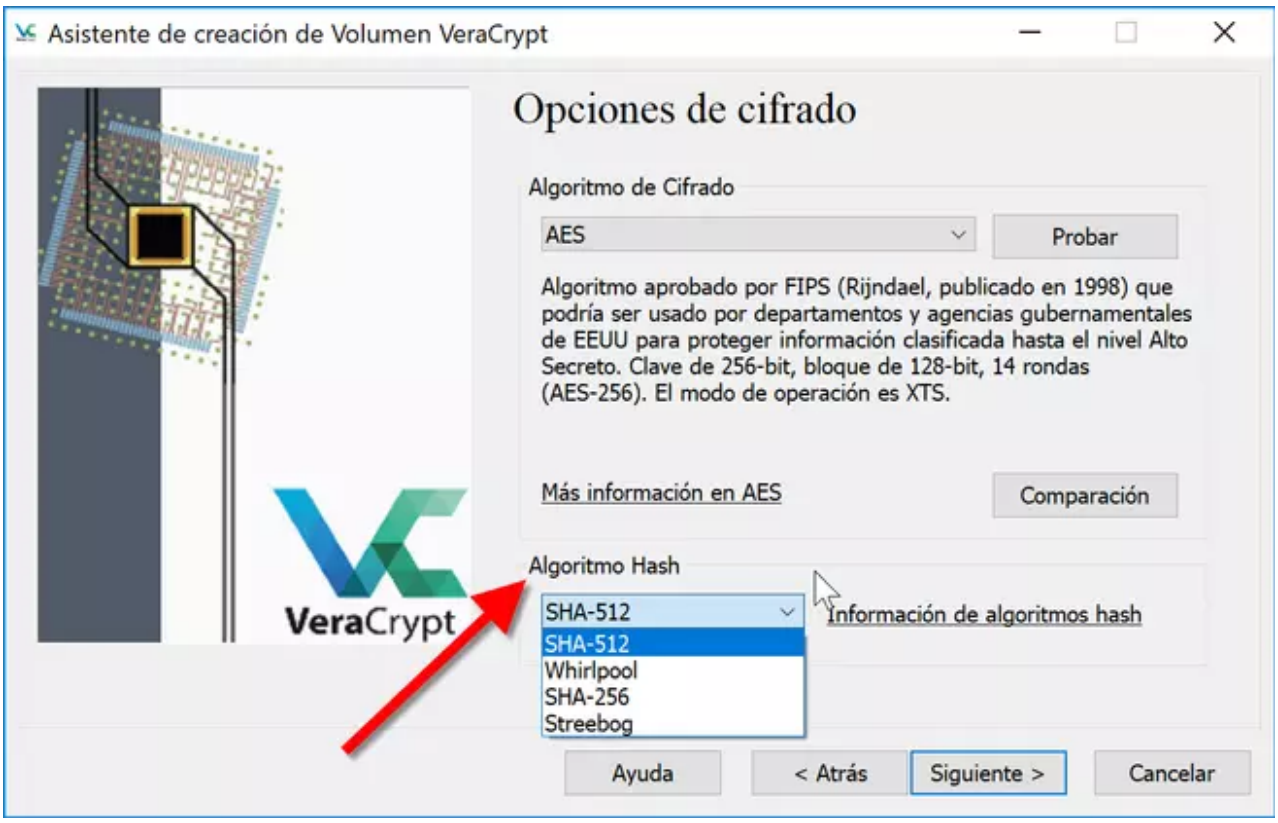
En el desplegable tendremos la posibilidad de seleccionar una gran cantidad de algoritmos de cifrado simétrico, por defecto es AES, de hecho, si nuestra CPU soporta AES-NI (AES por hardware) tendremos un grandísimo rendimiento. Si pinchamos en «Comparación» podremos ejecutar un «benchmark» para comprobar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


Asistente de creación de Volumen VeraCrypt
Opciones de cifrado
Algoritmo de Cifrado
AES
Probar
AES
Serpent
Twofish
Camellia
Kuznyechik
AES(Twofish)
AES(Twofish(Serpent))
Serpent(AES)
Serpent(Twofish(AES))
Twofish(Serpent)
Camellia(Kuznyechik)
Kuznyechik(Twofish)
Camellia(Serpent)
Kuznyechik(AES)
Kuznyechik(Serpent(Camellia))
icado en 1998) que
cias gubernamentales
da hasta el nivel Alto
, 14 rondas
Comparación
algoritmos hash
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

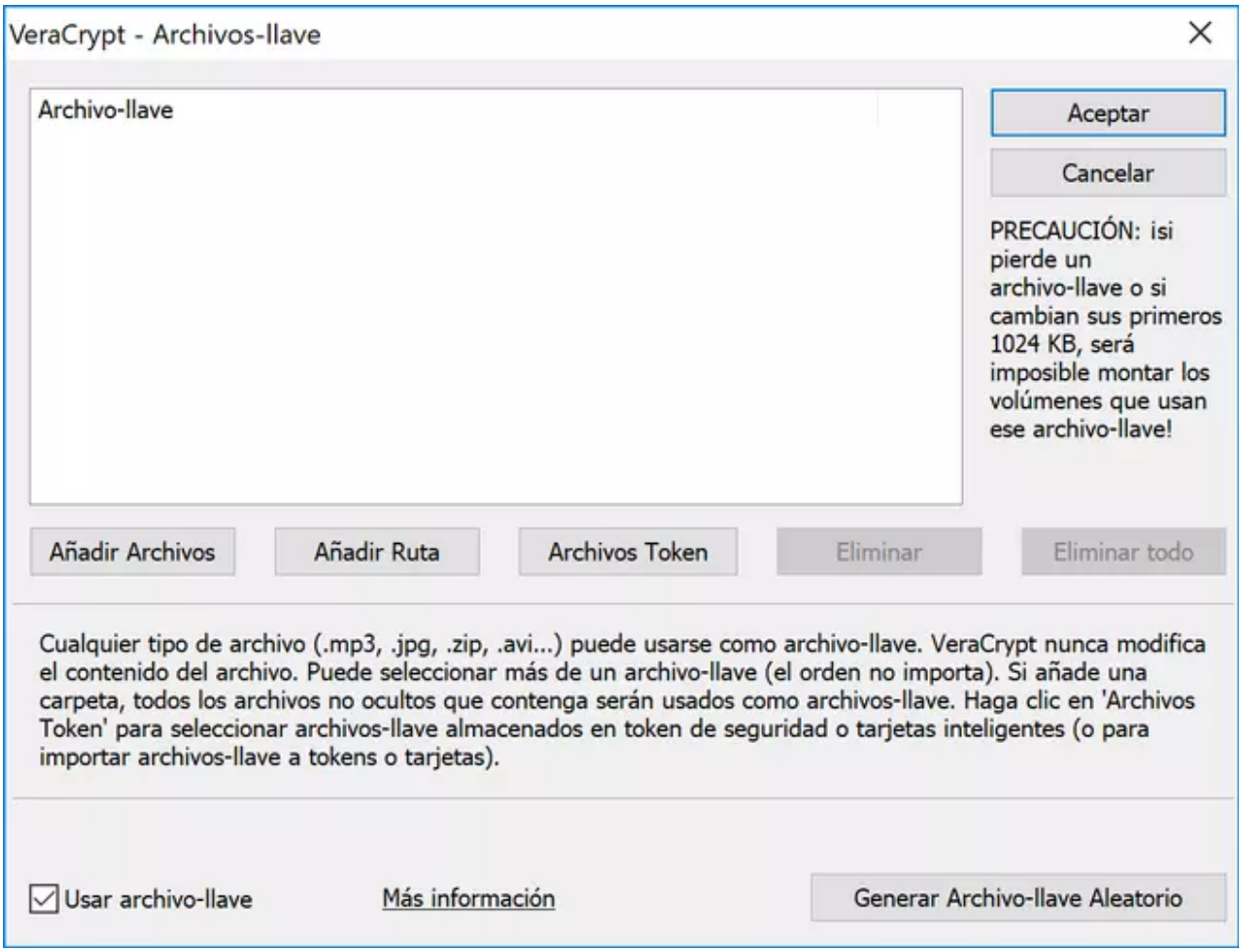

VeraCrypt
VeraCrypt - Comparación de algoritmos de cifrado
Benchmark:
Algoritmo de Cifrado
Buffer:
50 MB
Orden:
Velocidad Media (Descendiendo)
Algoritmo
Cifrado
Descifrado
Media
Comparación
Cerrar
La velocidad se ve afectada por la carga de la CPU y las características del dispositivo de almacenamiento.
Éstas pruebas tienen lugar en RAM.
Paralelización:
4 hilos
AES acelerado por hardware:
Sí

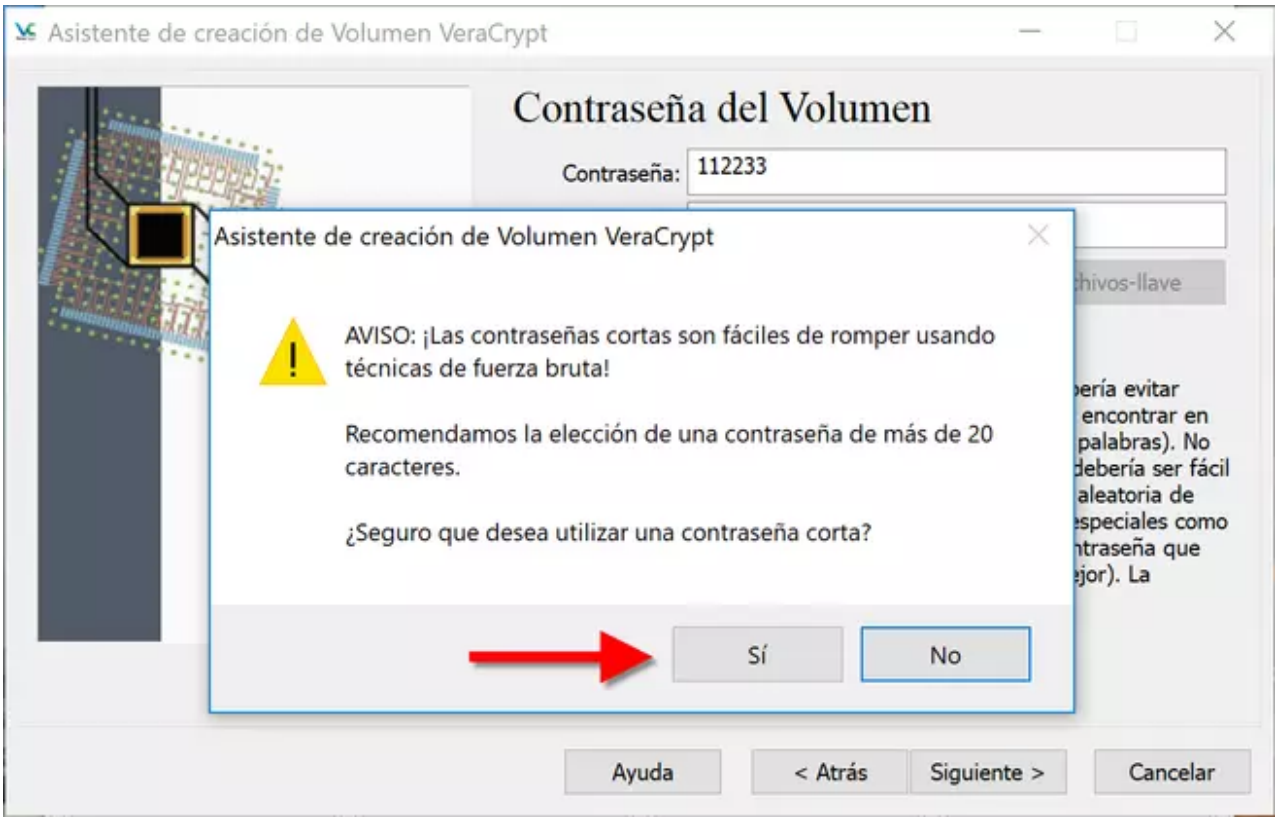




Ahora tendremos que configurar el tamaño del volumen cifrado VeraCrypt que estamos creando, y definir una contraseña (autenticación con algo que sabemos) o bien crear una clave criptográfica (autenticación con algo que tenemos). Nosotros hemos elegido la

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.

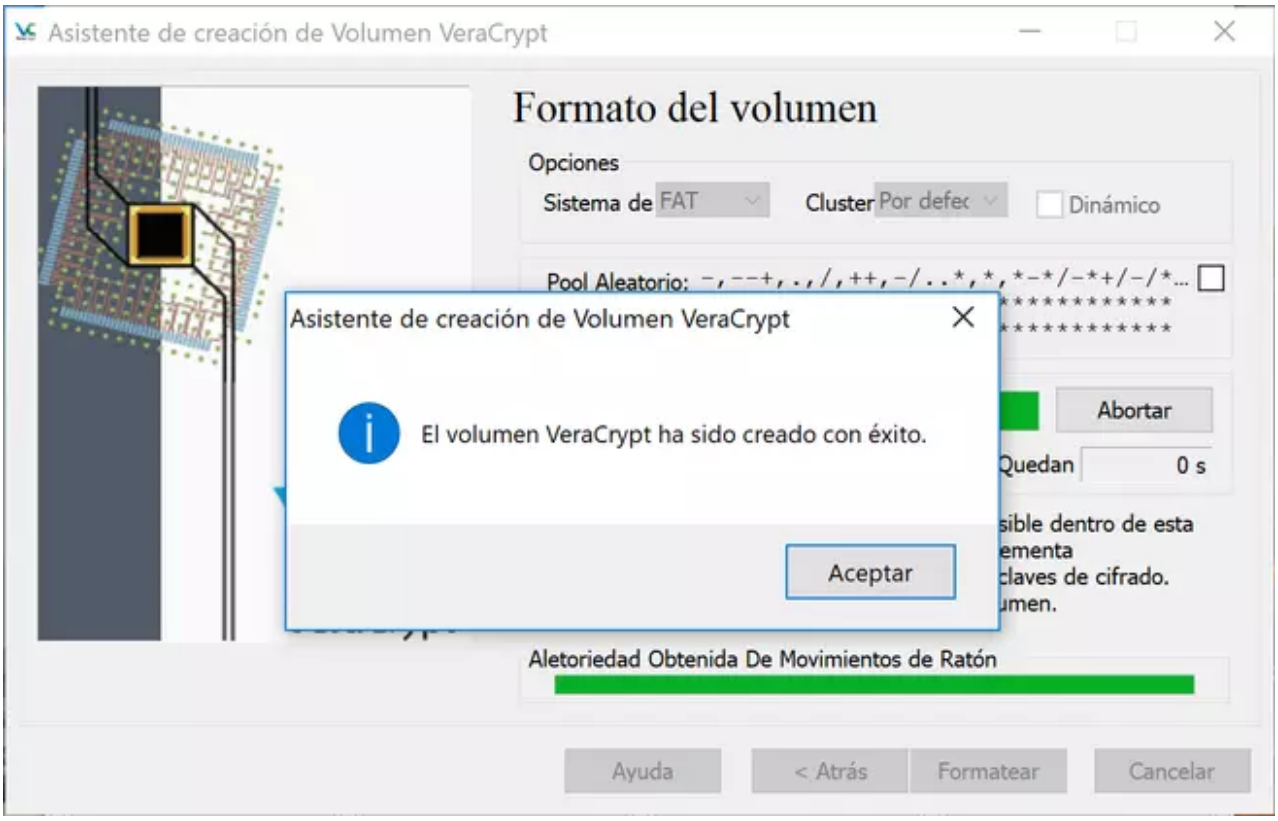


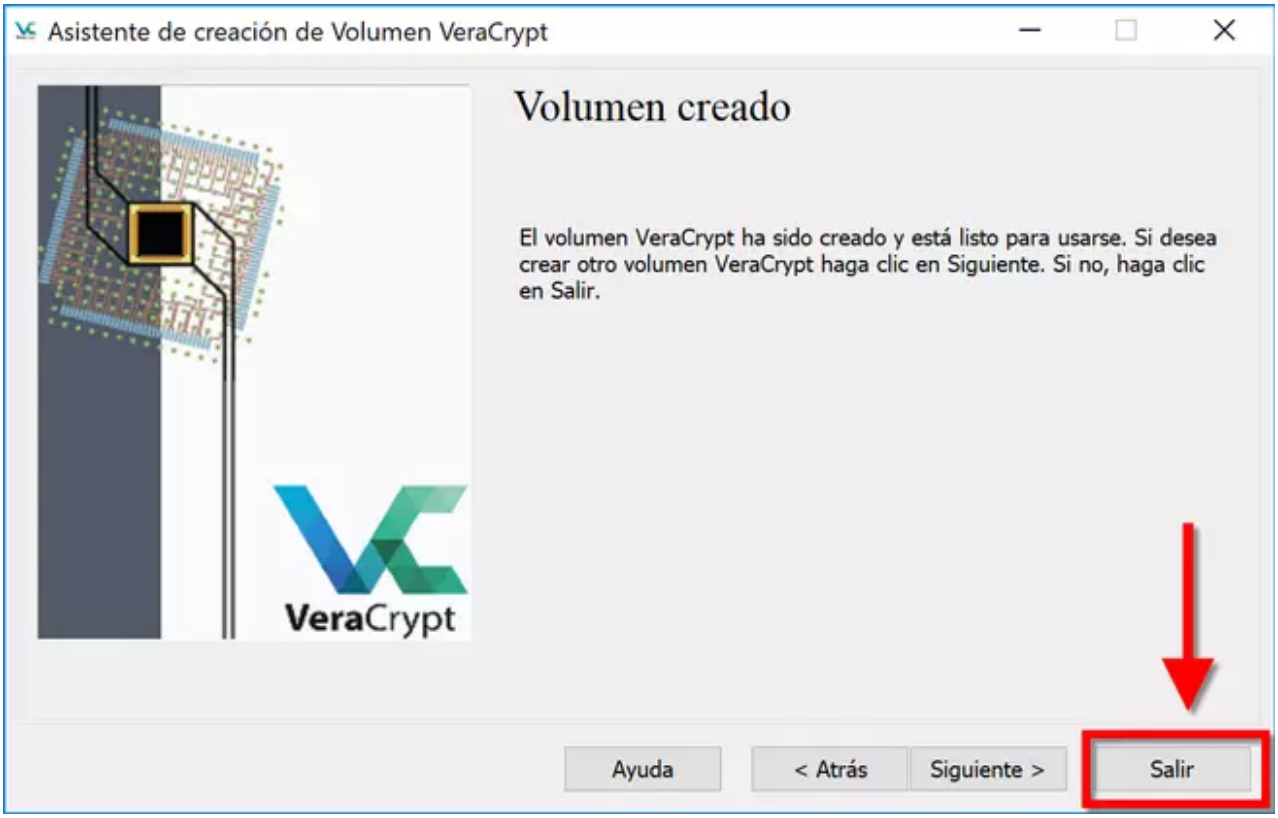


Cuando hayamos configurado la contraseña, deberemos elegir el sistema de archivos del contenedor cifrado. Si no vamos a introducir archivos mayores de 4GB, podremos seleccionar FAT, de lo contrario, podremos elegir exFAT o NTFS. Es muy importante

«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.

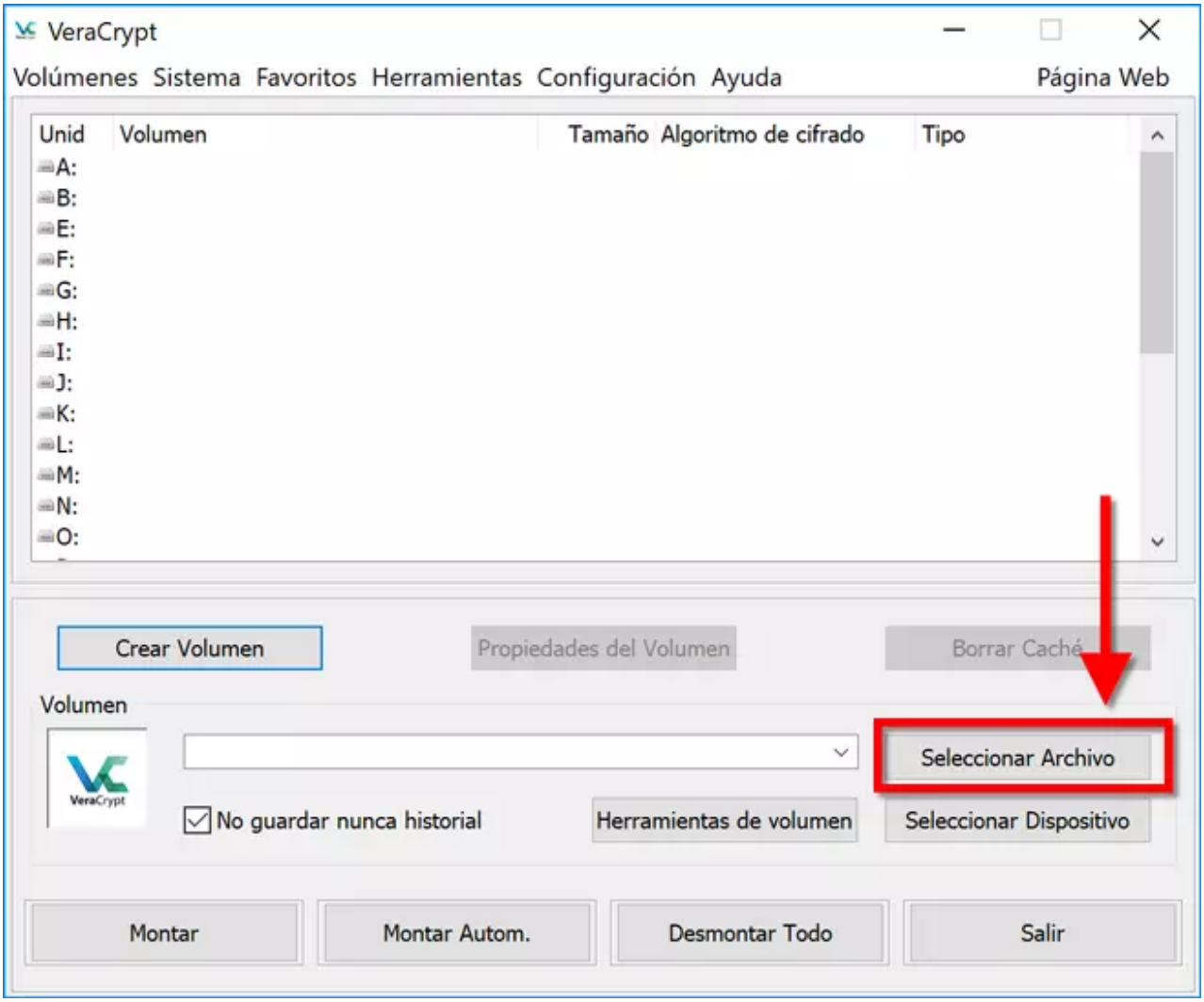


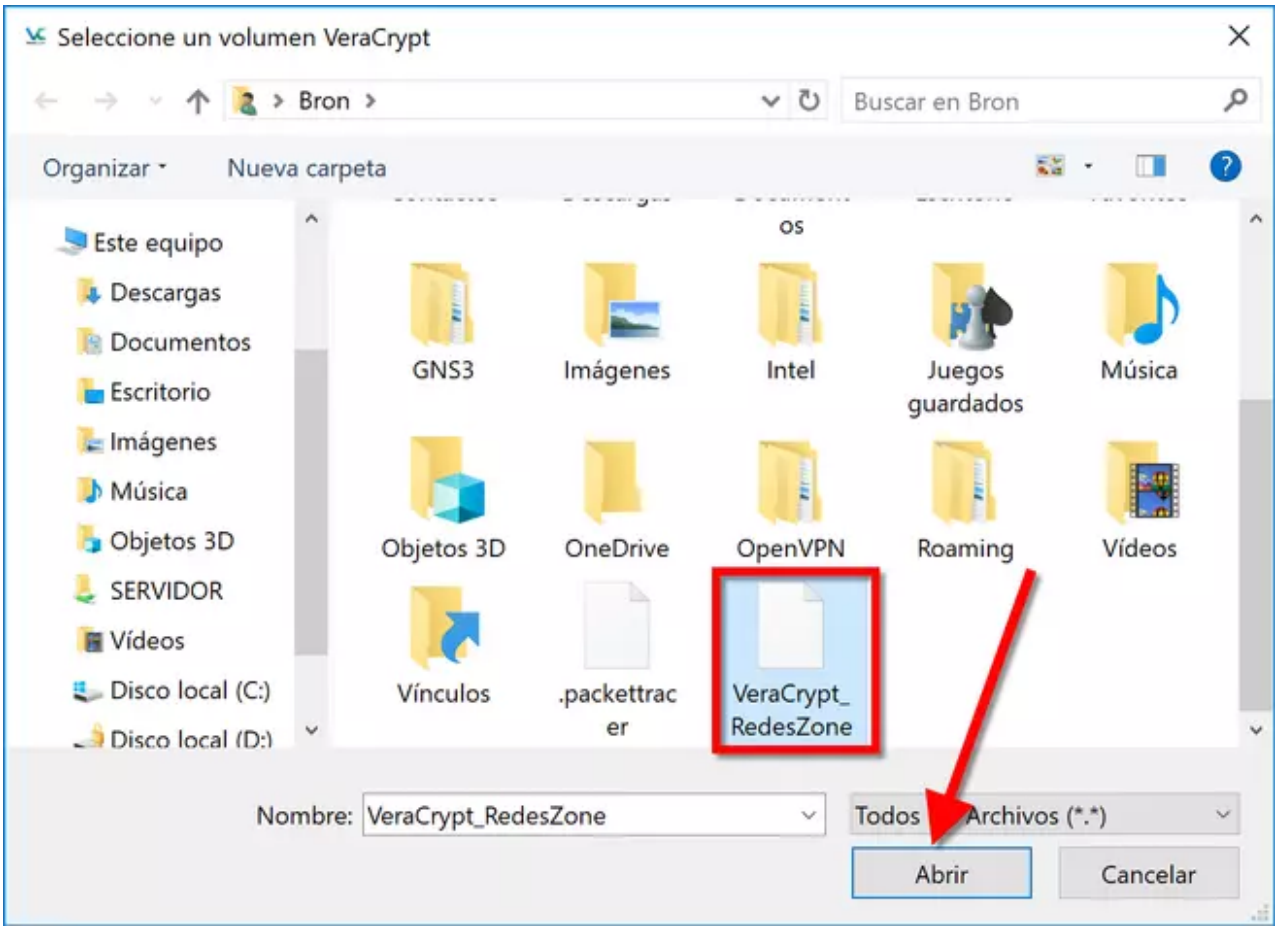


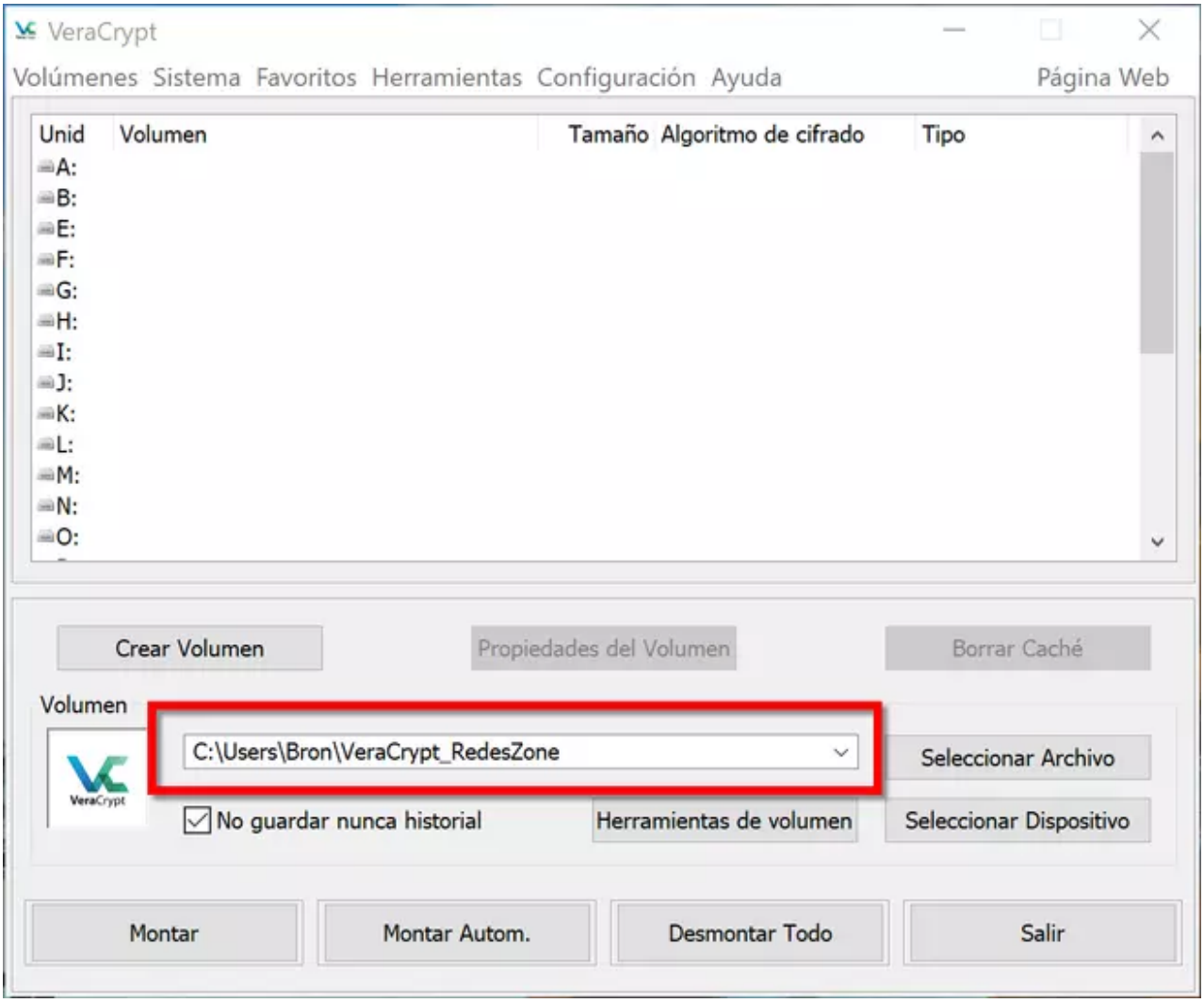
Ahora que ya hemos creado el volumen cifrado «normal», vamos a «montarlo» para poder acceder a él y empezar a cifrar nuestros archivos.

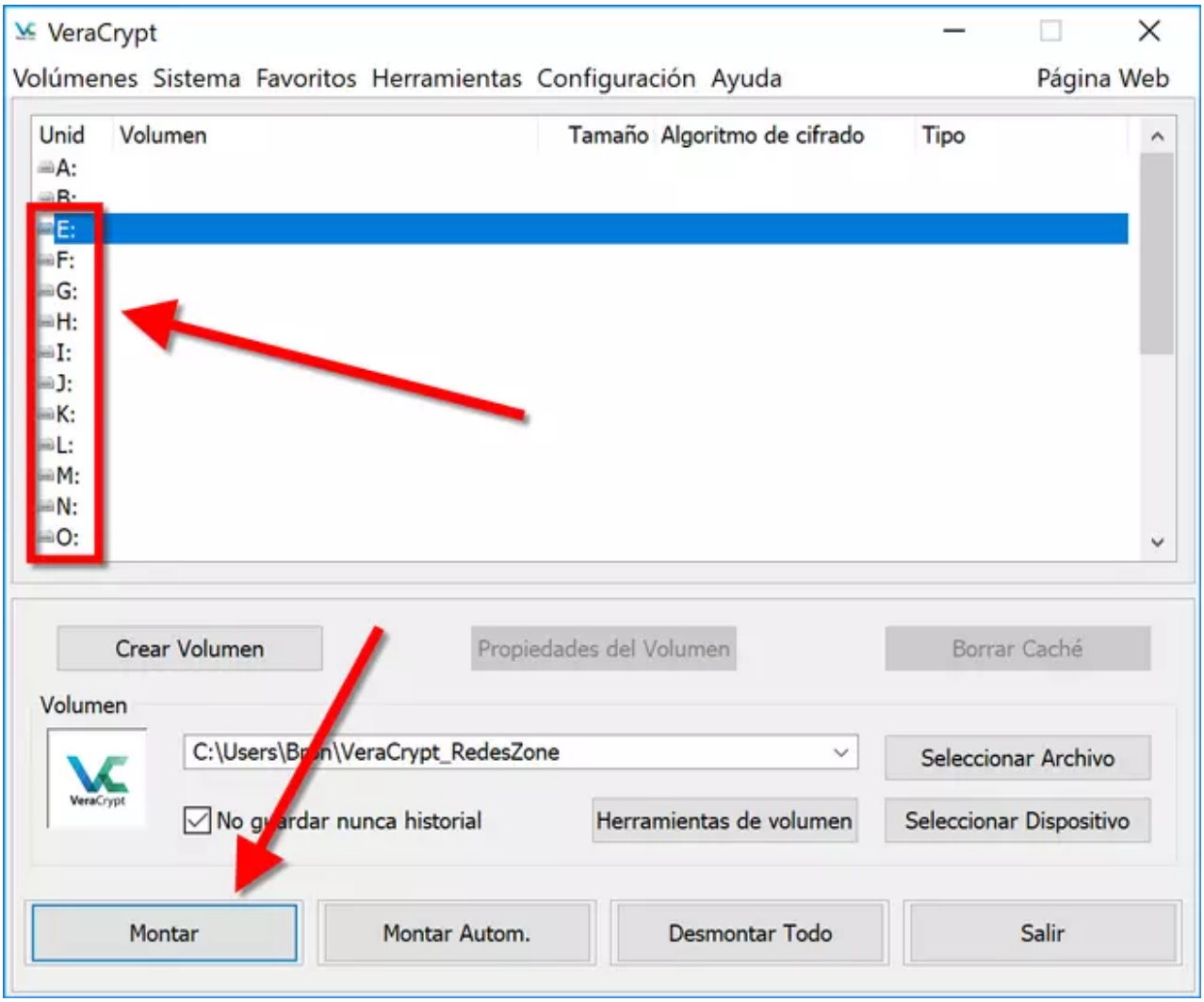
3. Montaje del volumen cifrado «normal» creado anteriormente

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».

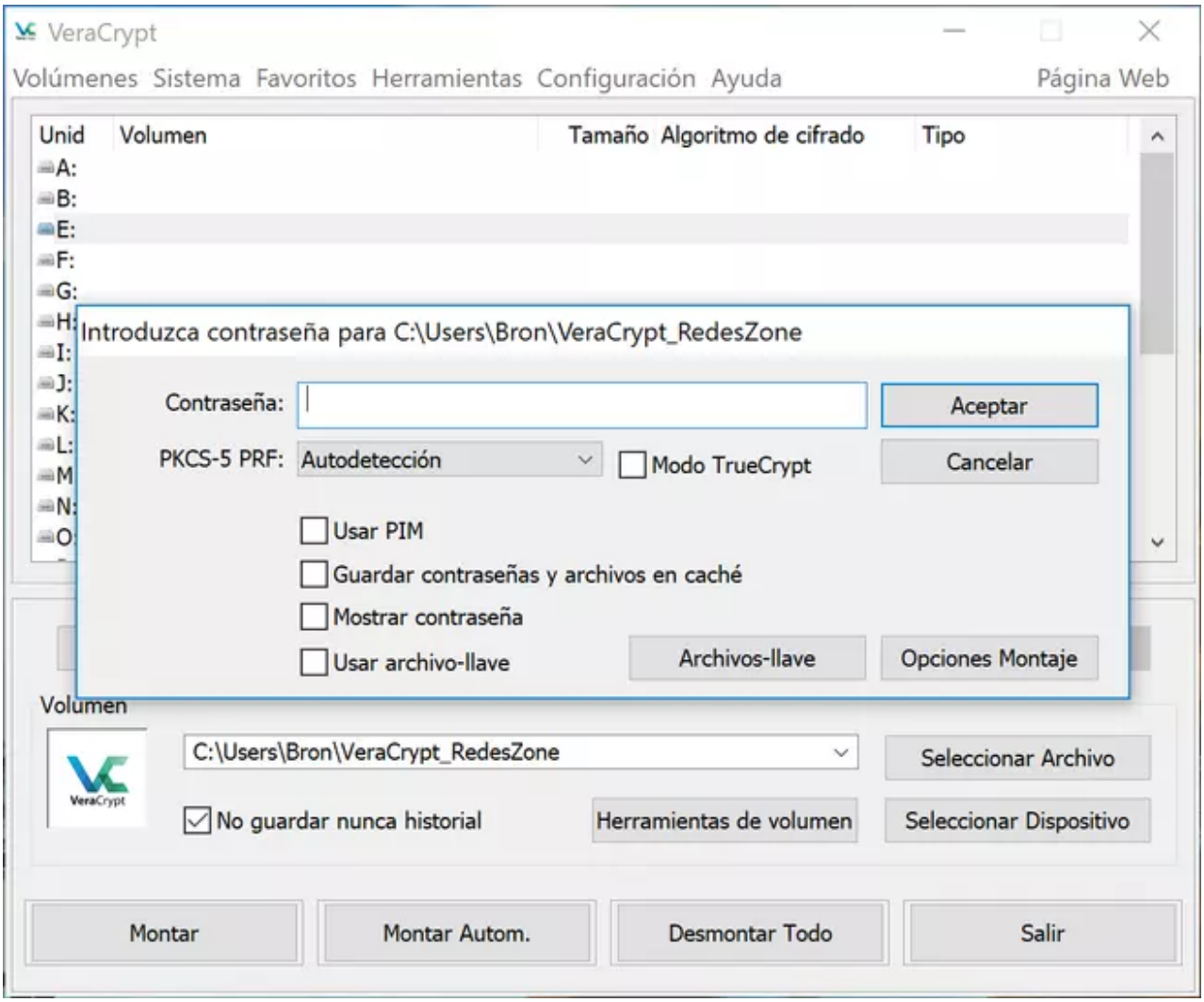


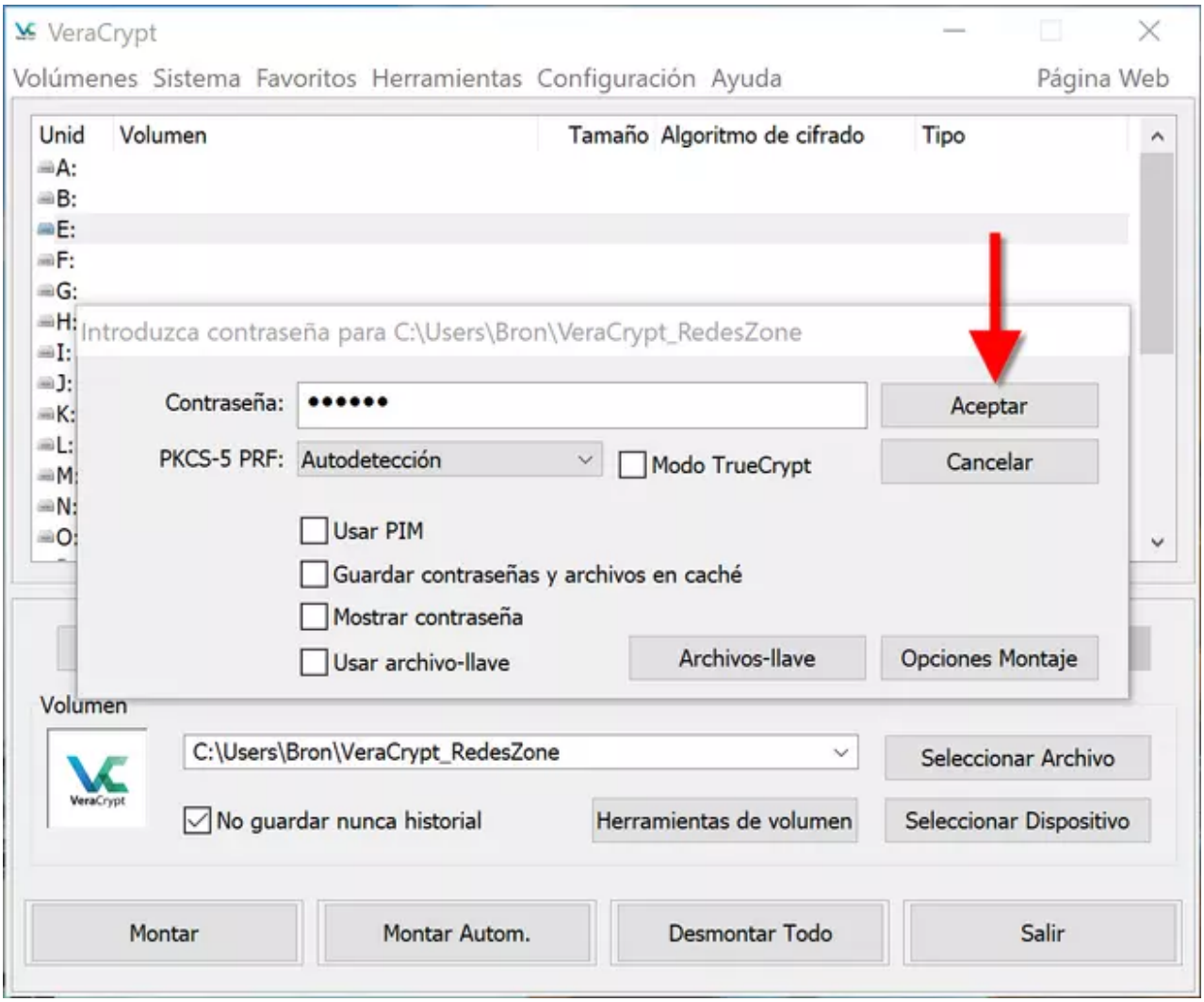

Seleccione un volumen VeraCrypt
Bron
Buscar en Bron
Organizar
Nueva carpeta
Este equipo
Descargas
Documentos
Escritorio
Imágenes
Música
Objetos 3D
SERVIDOR
Vídeos
Disco local (C:)
Disco local (D:)
GNS3
Imágenes
Intel
Juegos guardados
Música
Objetos 3D
OneDrive
OpenVPN
Roaming
Vídeos
Vínculos
.packettracer
VeraCrypt_RedesZone
Nombre:
VeraCrypt_RedesZone
Todos Archivos (*.*)
Abrir
Cancelar

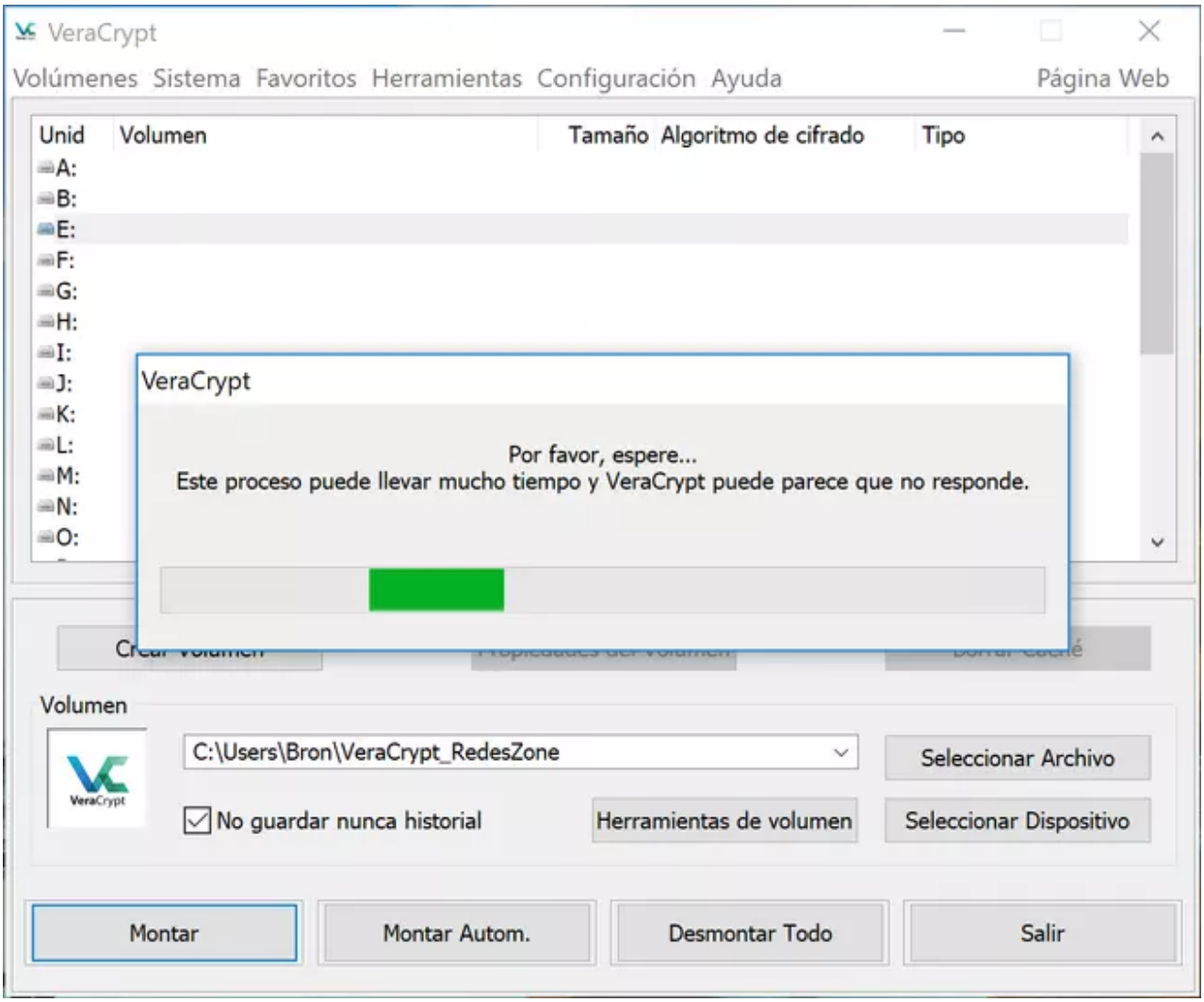

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda
Página Web
Unid
Volumen
Tamaño
Algoritmo de cifrado
Tipo
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Crear Volumen
Propiedades del Volumen
Borrar Caché
Volumen
C:\Users\Bron\VeraCrypt_RedesZone
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir

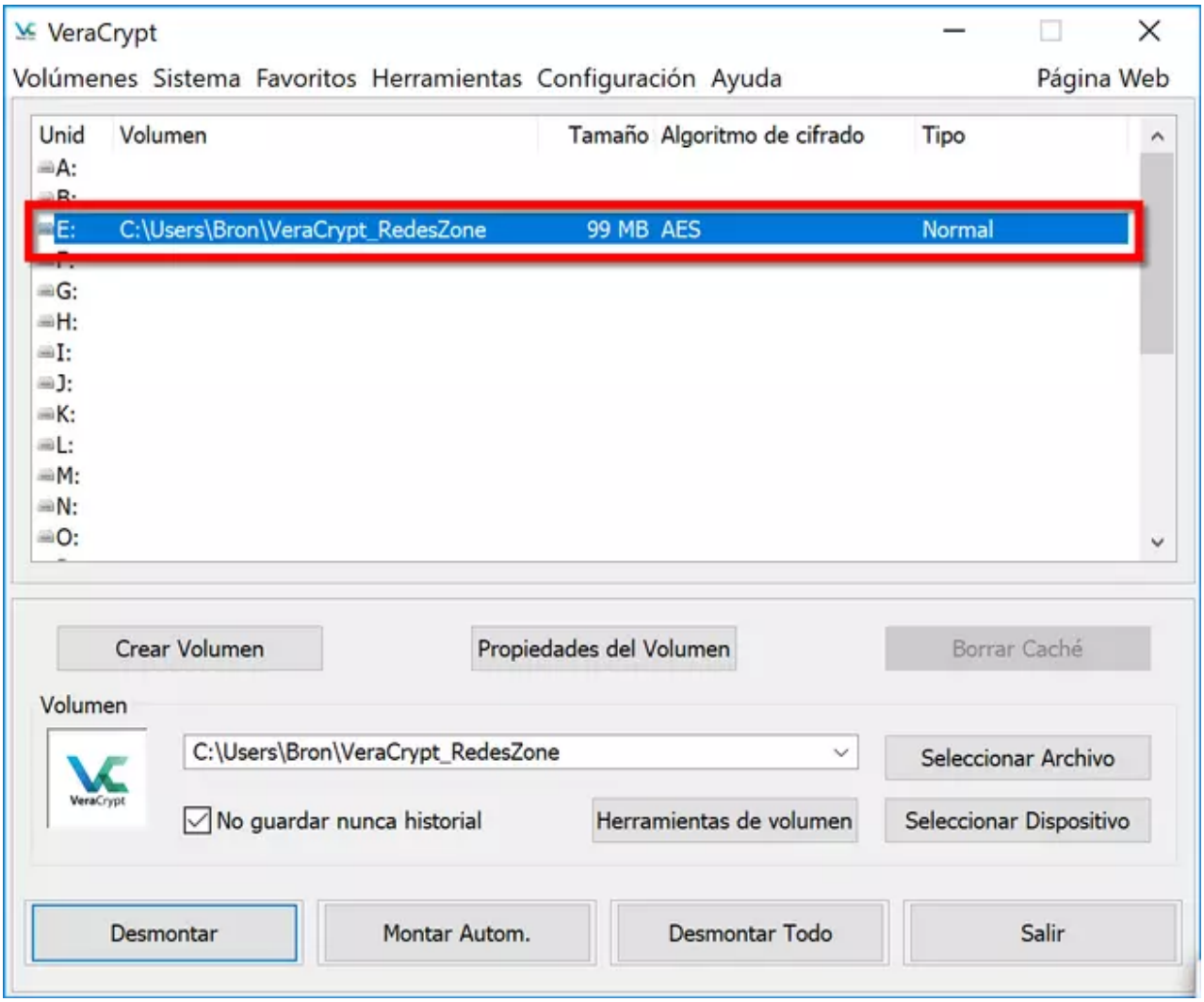


Cuando pinchemos en «Montar», nos va a pedir la contraseña de acceso o la clave criptográfica para abrirlo. Automáticamente VeraCrypt se encargará de abrir el contendor cifrado, montarlo en la unidad elegida, y hacerlo accesible.

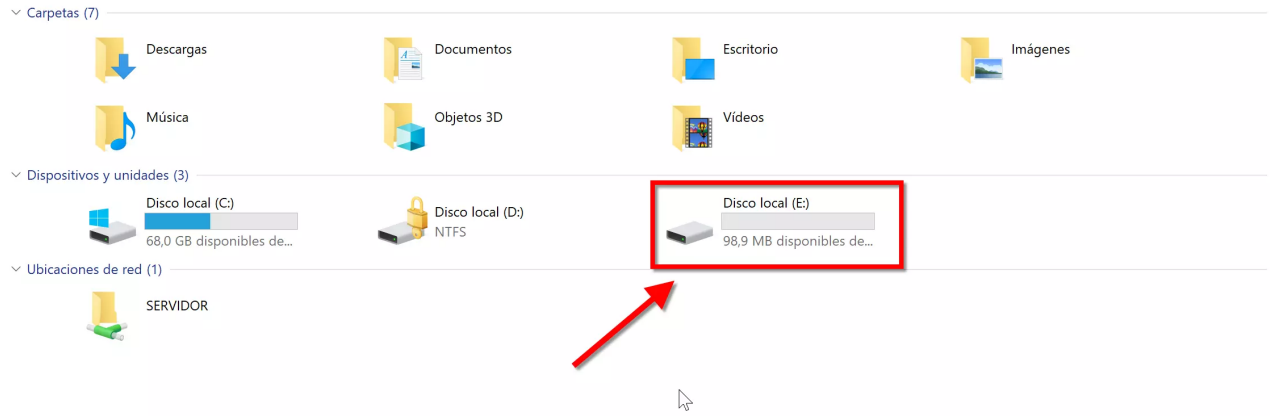

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M
N:
O
Introduzca contraseña para C:\Users\Bron\VeraCrypt_RedesZone
Contraseña:
Aceptar
PKCS-5 PRF: Autodetección
Modo TrueCrypt
Cancelar
Usar PIM
Guardar contraseñas y archivos en caché
Mostrar contraseña
Usar archivo-llave
Archivos-llave
Opciones Montaje
Volumen
C:\Users\Bron\VeraCrypt_RedesZone
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir


VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Introduzca contraseña para C:\Users\Bron\VeraCrypt_RedesZone
Contraseña: ••••••
Aceptar
PKCS-5 PRF: Autodetección
Modo TrueCrypt
Cancelar
Usar PIM
Guardar contraseñas y archivos en caché
Mostrar contraseña
Usar archivo-llave
Archivos-llave
Opciones Montaje
Volumen
C:\Users\Bron\VeraCrypt_RedesZone
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir

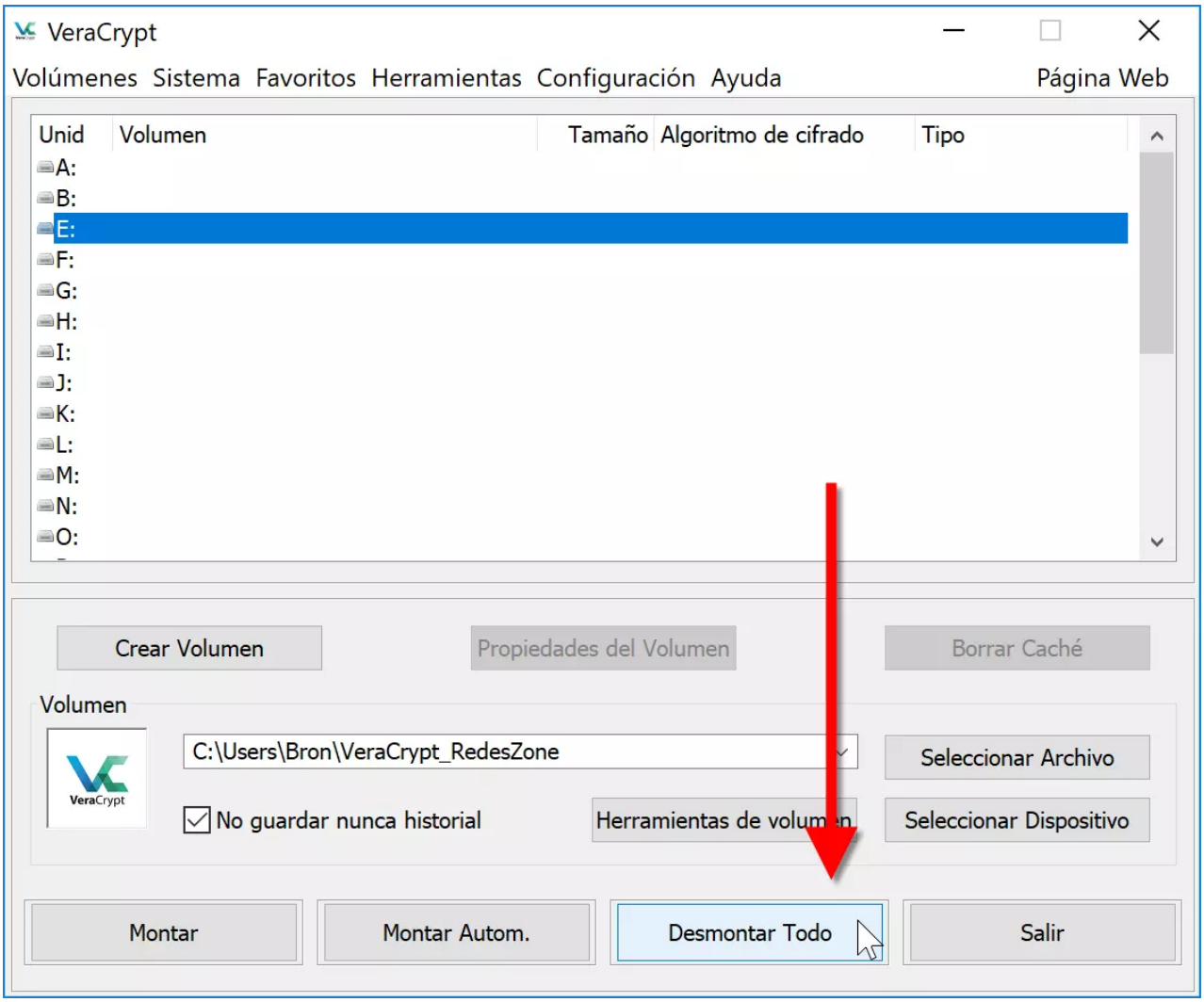

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
VeraCrypt
Por favor, espere...
Este proceso puede llevar mucho tiempo y VeraCrypt puede parece que no responde.
Volumen
C:\Users\Bron\VeraCrypt_RedesZone
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir



En «Equipo» nos aparecerá un nuevo disco local E, que es el volumen cifrado. Todo lo que copiemos 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»

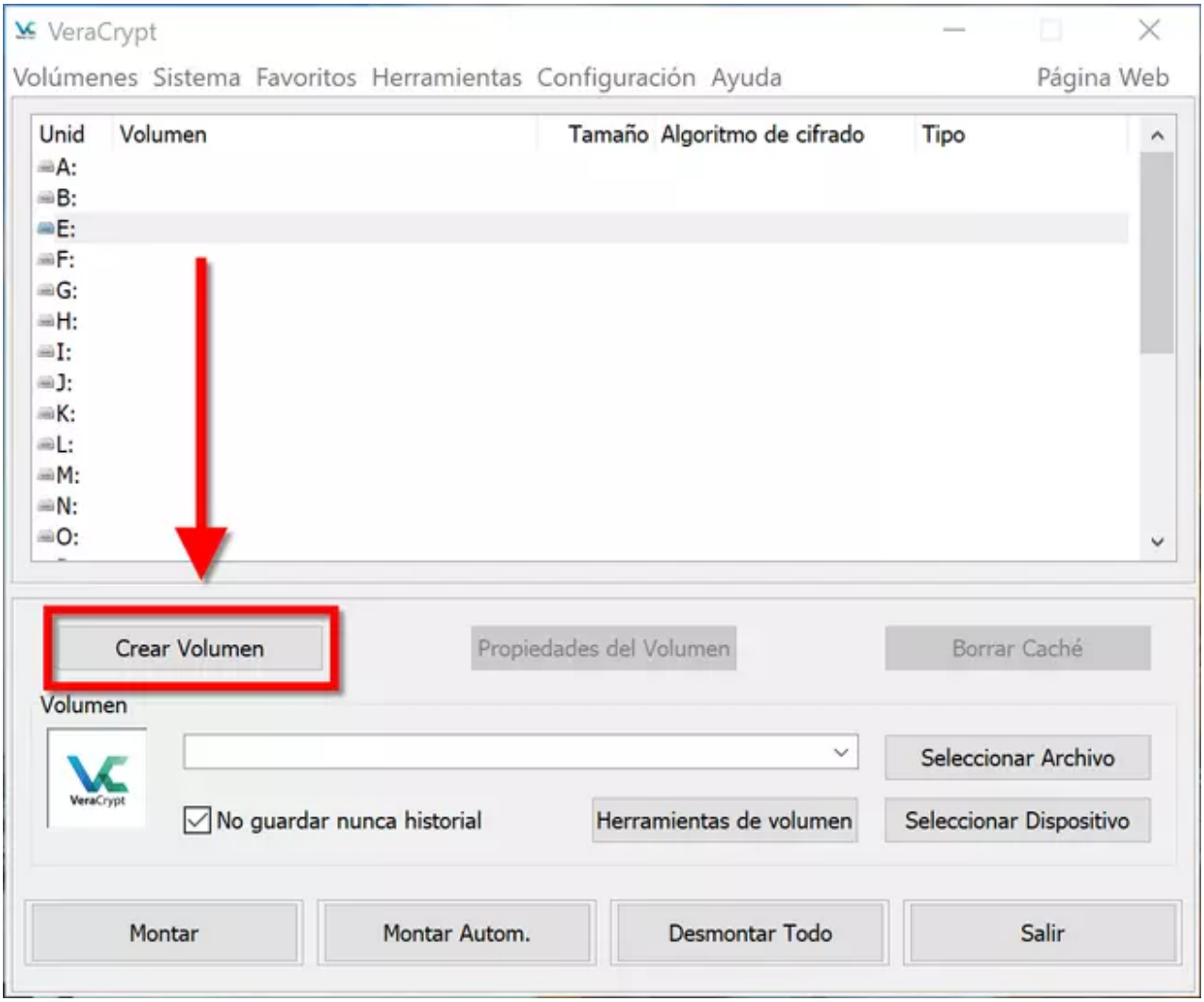
En esta sección vamos a crear un volumen cifrado, dónde meteremos nuestros datos, pero dentro de él crearemos uno OCULTO, os explico en qué consiste esto.

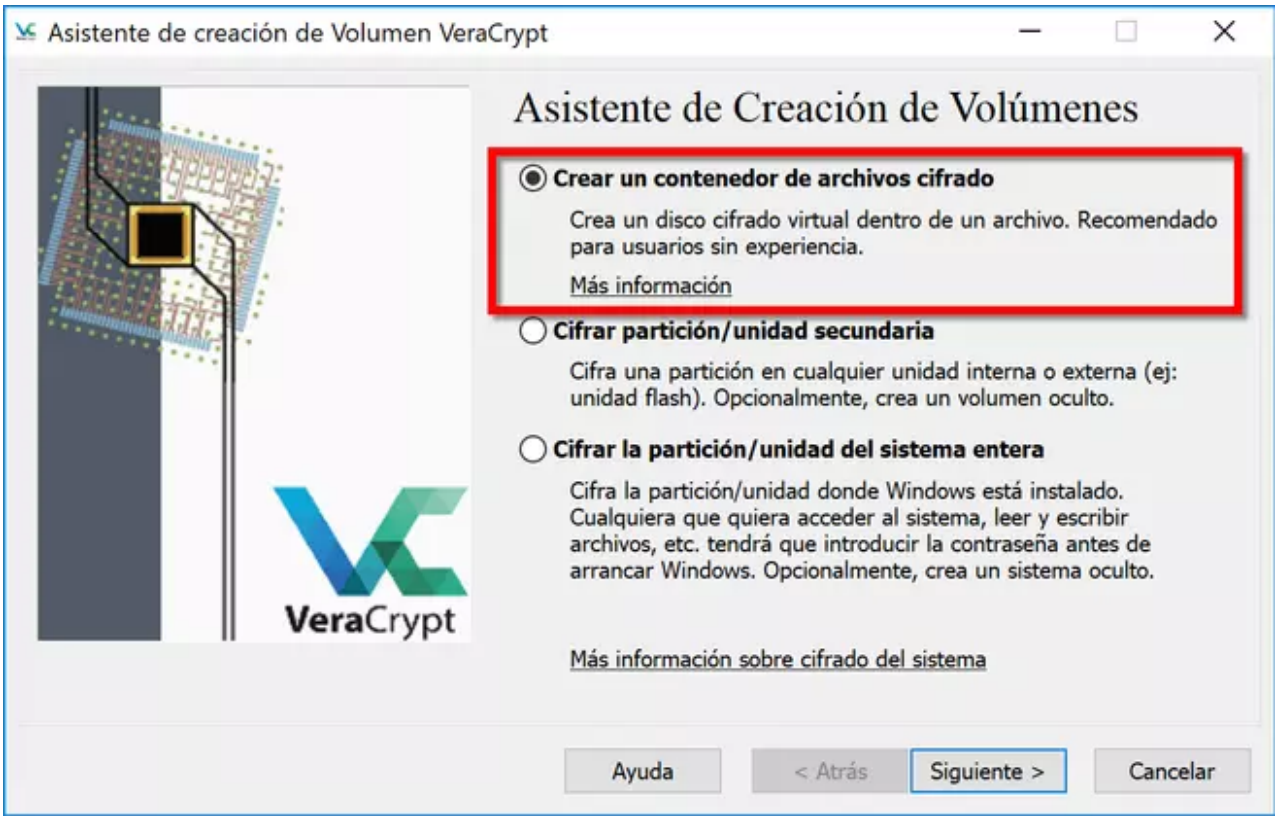
- Volumen normal: para acceder tendrás que meter la contraseña, por ejemplo 112233, entonces en Windows se montará un nuevo disco local, tal y como habéis visto anteriormente.
- Volumen oculto: para acceder tendrás que meter otra clave que hayas puesto anteriormente, por ejemplo 11223344 y se montará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

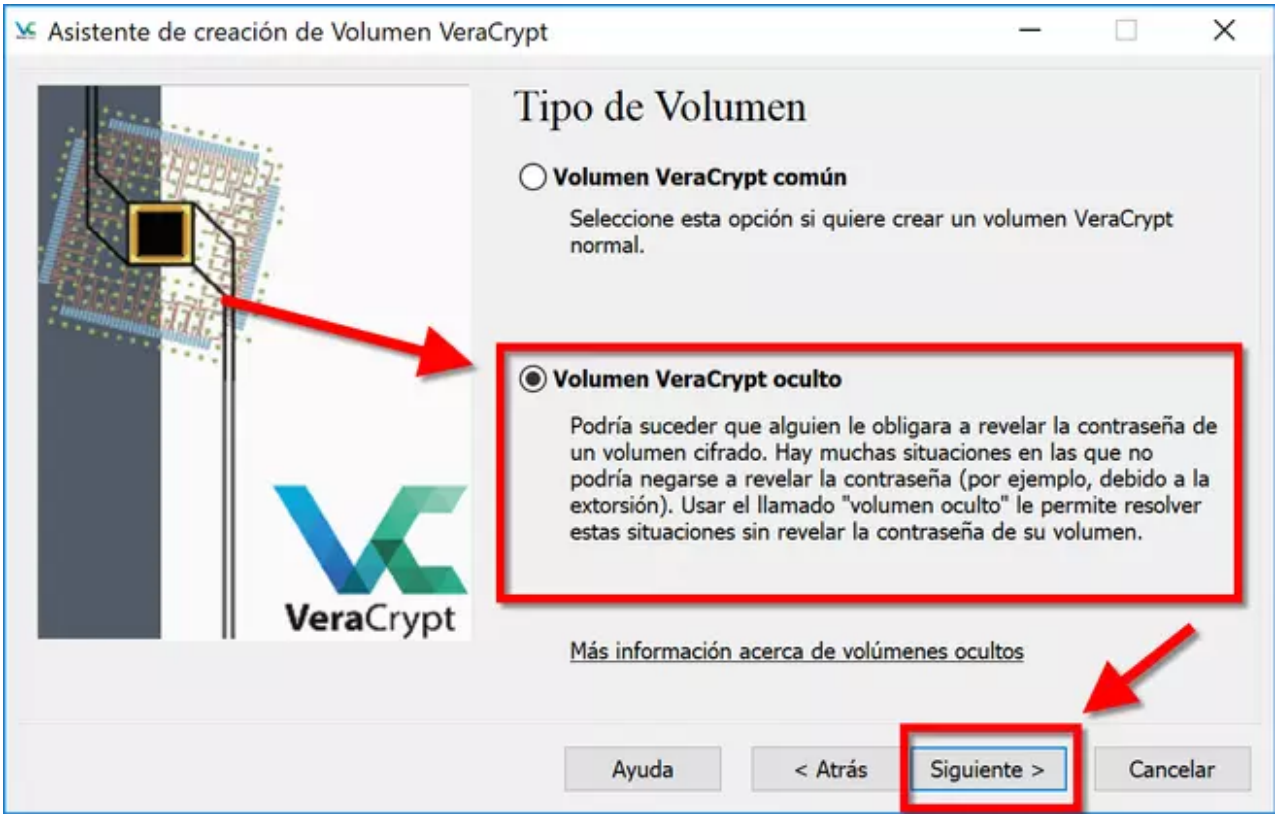
¿Para qué sirve el volumen cifrado oculto? Para guardar los archivos más importantes en su interior, como claves de bancos, emails, documentos confidenciales etc. ¿Por qué no guardar esto en el volumen normal si está cifrado? Para evitar que alguien amenace nuestra integridad física (nos haga daño), 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.

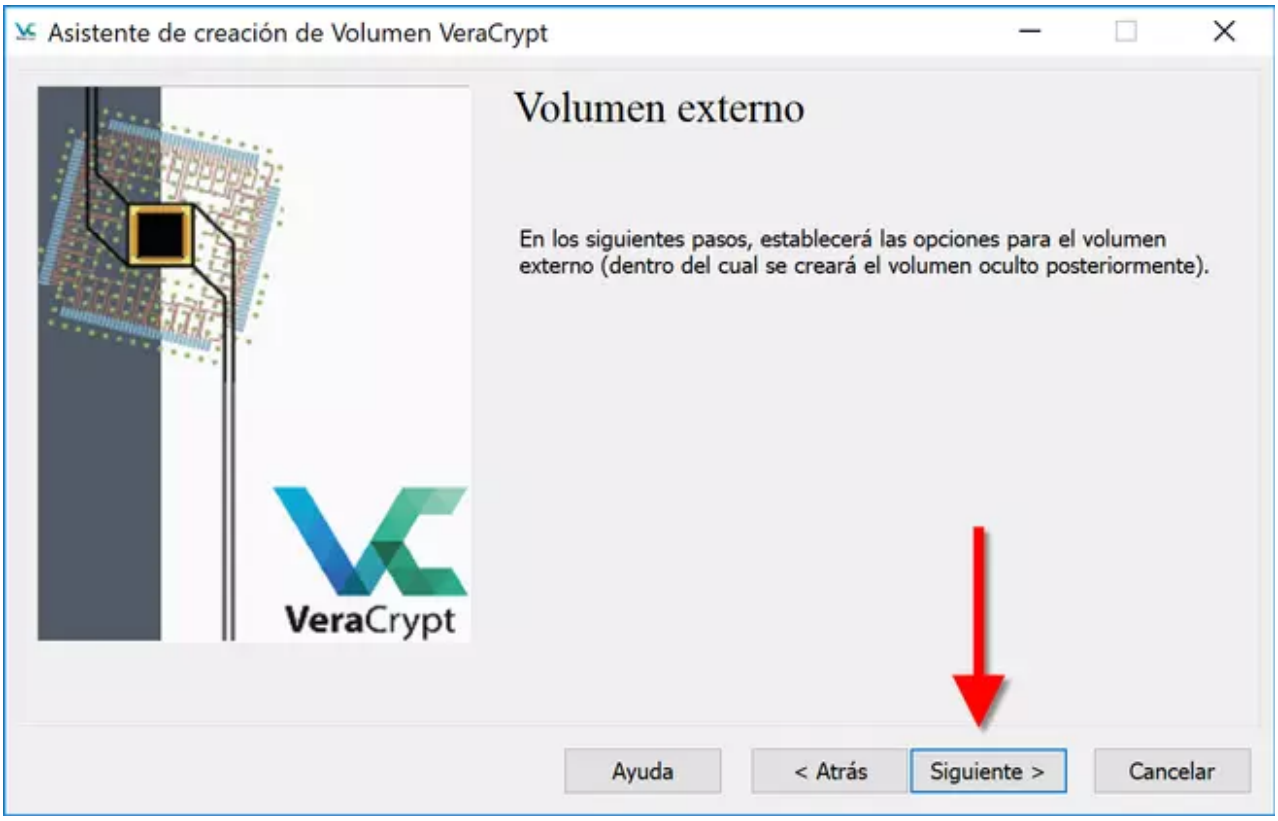
El proceso de creación del volumen cifrado oculto es muy similar al «normal». En el menú principal de VeraCrypt procedemos a pinchar sobre «**Crear Volumen**«, para posteriormente seleccionar la opción «**Crear un contenedor de archivos cifrado**«. Una vez hecho esto, deberemos elegir «**Volumen VeraCrypt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




Asistente de creación de Volumen VeraCrypt
Asistente de Creación de Volúmenes
Crear un contenedor de archivos cifrado
Crea un disco cifrado virtual dentro de un archivo. Recomendado para usuarios sin experiencia.
Más información
Cifrar partición/unidad secundaria
Cifra una partición en cualquier unidad interna o externa (ej: unidad flash). Opcionalmente, crea un volumen oculto.
Cifrar la partición/unidad del sistema entera
Cifra la partición/unidad donde Windows está instalado. Cualquiera que quiera acceder al sistema, leer y escribir archivos, etc. tendrá que introducir la contraseña antes de arrancar Windows. Opcionalmente, crea un sistema oculto.
Más información sobre cifrado del sistema
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

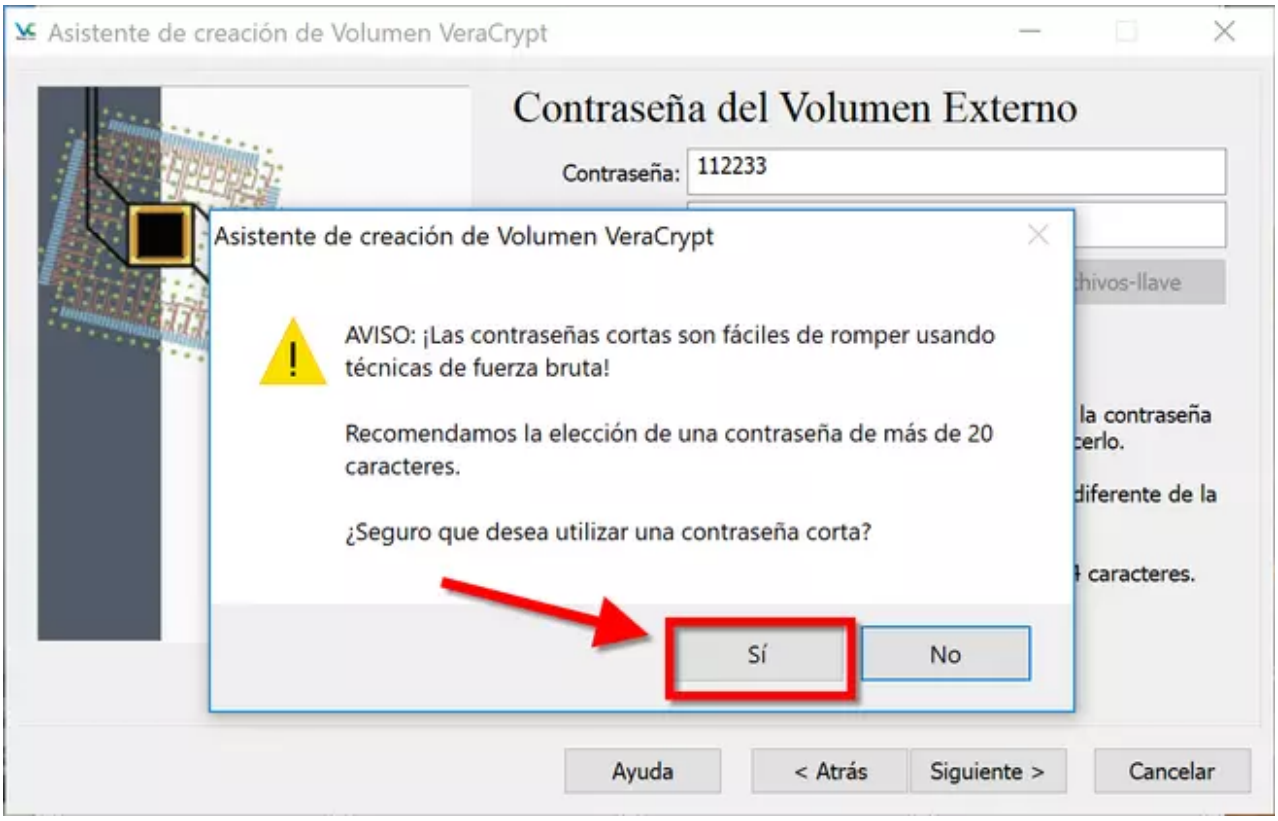

Asistente de creación de Volumen VeraCrypt
Tipo de Volumen
Volumen VeraCrypt común
Seleccione esta opción si quiere crear un volumen VeraCrypt normal.
Volumen VeraCrypt oculto
Podría suceder que alguien le obligara a revelar la contraseña de un volumen cifrado. Hay muchas situaciones en las que no podría negarse a revelar la contraseña (por ejemplo, debido a la extorsión). Usar el llamado "volumen oculto" le permite resolver estas situaciones sin revelar la contraseña de su volumen.
Más información acerca de volúmenes ocultos
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

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.


Asistente de creación de Volumen VeraCrypt
Volumen externo
En los siguientes pasos, establecerá las opciones para el volumen externo (dentro del cual se creará el volumen oculto posteriormente).
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

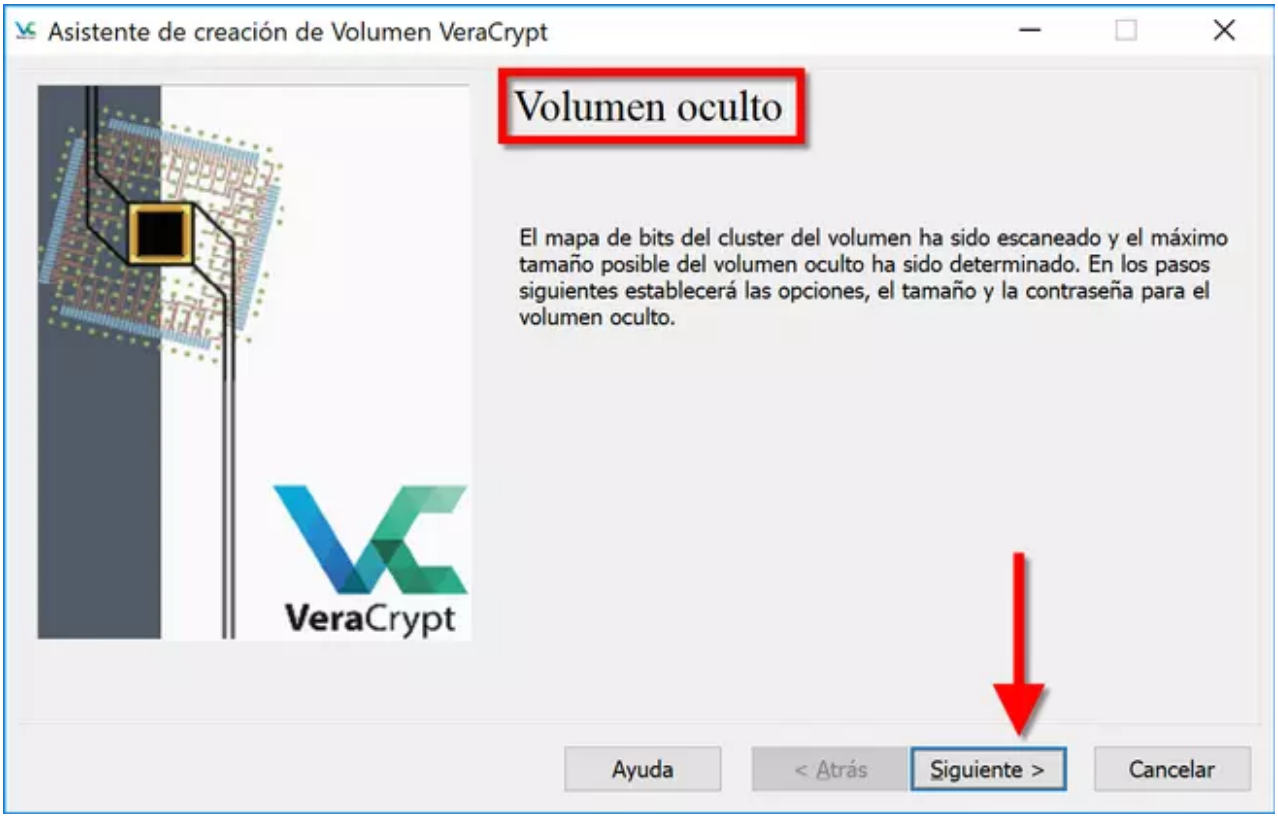

Asistente de creación de Volumen VeraCrypt
Opciones de cifrado del volumen externo
Algoritmo de Cifrado
AES
Probar
Algoritmo aprobado por FIPS (Rijndael, publicado en 1998) que podría ser usado por departamentos y agencias gubernamentales de EEUU para proteger información clasificada hasta el nivel Alto Secreto. Clave de 256-bit, bloque de 128-bit, 14 rondas (AES-256). El modo de operación es XTS.
Más información en AES
Comparación
Algoritmo Hash
SHA-512
Información de algoritmos hash
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

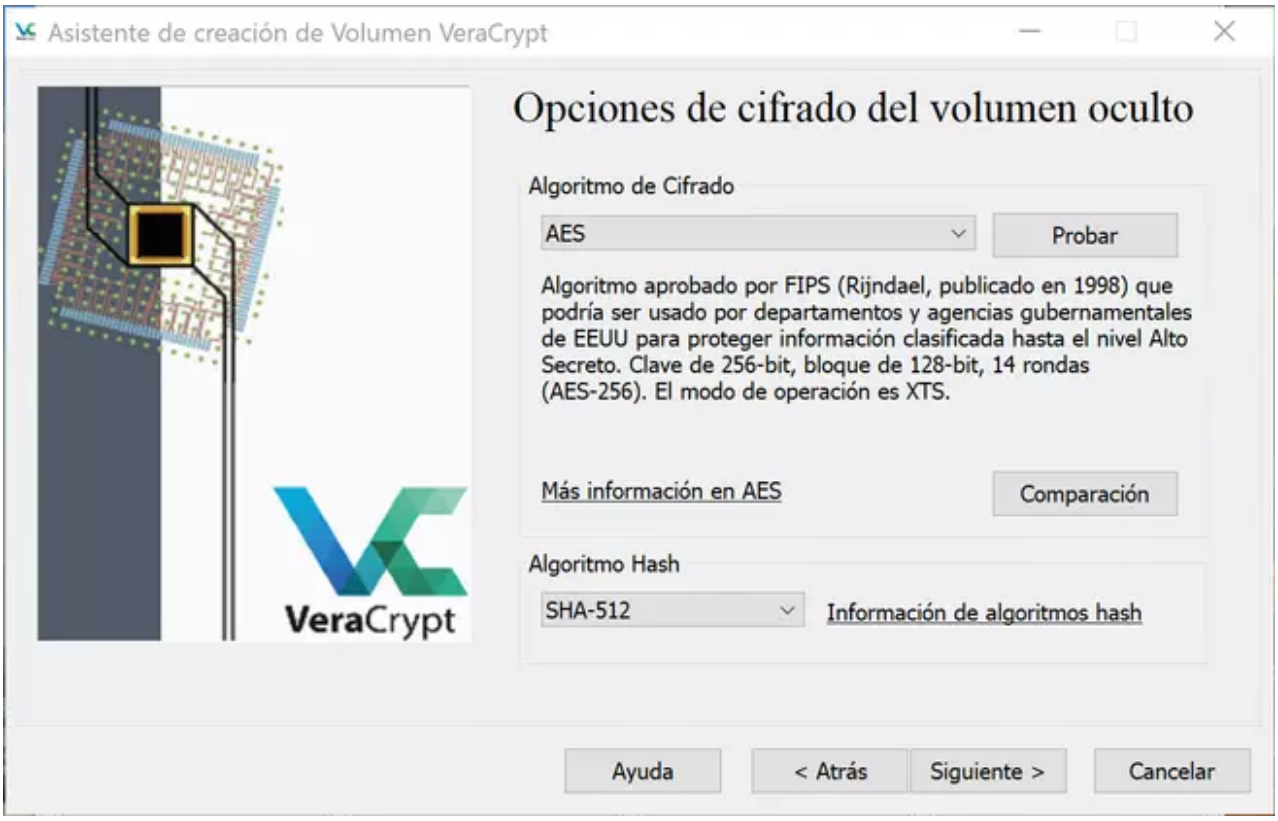
Pondremos una contraseña o una clave criptográfica como antes os hemos explicado, también elegimos el sistema de archivos, y pinchamos en «Formatear».



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).

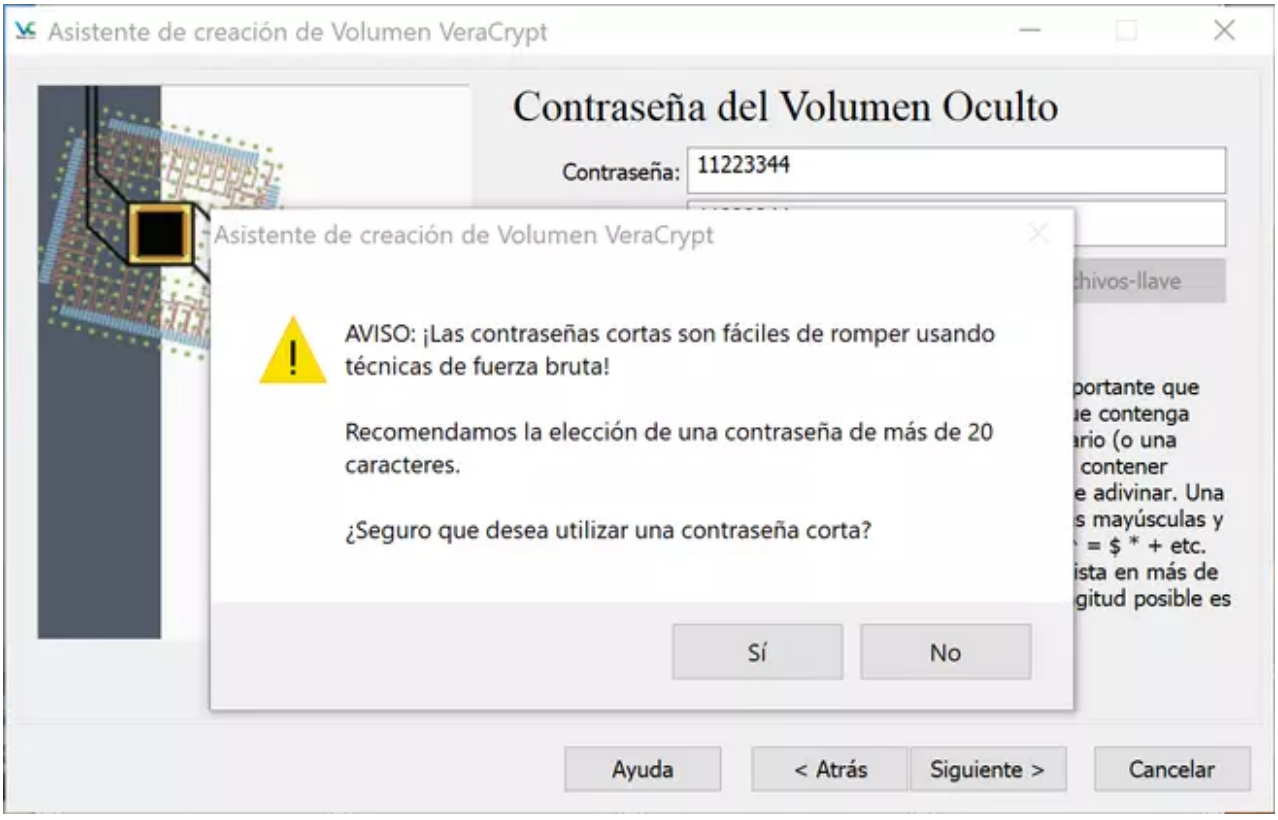
VeraCrypt nos permite crear un volumen externo e interno con diferente cifrado y hash, no hay problema porque el volumen externo esté con AES, y el interno esté con una combinación de AES con otros algoritmos de cifrado simétrico.



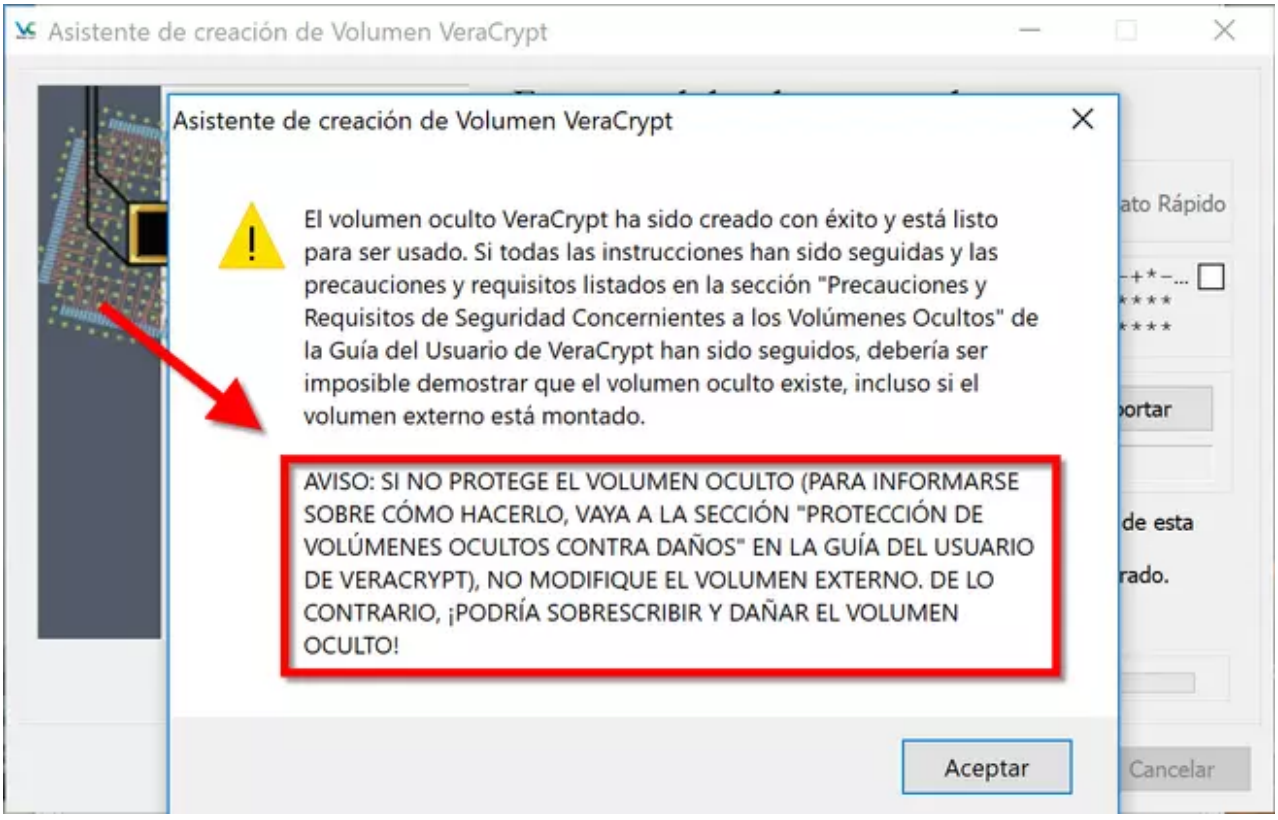

Asistente de creación de Volumen VeraCrypt
Opciones de cifrado del volumen oculto
Algoritmo de Cifrado
AES
Probar
Algoritmo aprobado por FIPS (Rijndael, publicado en 1998) que podría ser usado por departamentos y agencias gubernamentales de EEUU para proteger información clasificada hasta el nivel Alto Secreto. Clave de 256-bit, bloque de 128-bit, 14 rondas (AES-256). El modo de operación es XTS.
Más información en AES
Comparación
Algoritmo Hash
SHA-512
Información de algoritmos hash
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar


Asistente de creación de Volumen VeraCrypt
Tamaño del volumen oculto
100
KB
MB
GB
TB
El tamaño máximo posible de volumen oculto para este volumen es 197.16 MB.
Especifique el tamaño del volumen oculto. El mínimo tamaño posible de un volumen oculto es 40 KB (o 3664 KB si se formatea como NTFS). El máximo tamaño posible que puede especificar para el volumen oculto se muestra más arriba.
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar


Asistente de creación de Volumen VeraCrypt
Contraseña del Volumen Oculto
Contraseña: 11223344
Confirmar: 11223344
Usar archivo-llave
Archivos-llave
Mostrar contraseña
Usar PIM
Elija una contraseña para el volumen oculto. Es muy importante que elija una buena contraseña. Debería evitar elegir una que contenga sólo una palabra que se pueda encontrar en un diccionario (o una combinación de 2, 3, o 4 de estas palabras). No debería contener nombres ni fechas de nacimiento. No debería ser fácil de adivinar. Una buena contraseña es una combinación aleatoria de letras mayúsculas y minúsculas, números, y caracteres especiales como @ ^ = $ * + etc. Recomendamos la elección de una contraseña que consista en más de 20 caracteres (cuanto más larga, mejor). La máxima longitud posible es 64 caracteres.
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar


Asistente de creación de Volumen VeraCrypt
Contraseña del Volumen Oculto
Contraseña: 11223344
Asistente de creación de Volumen VeraCrypt
AVISO: ¡Las contraseñas cortas son fáciles de romper usando técnicas de fuerza bruta!
Recomendamos la elección de una contraseña de más de 20 caracteres.
¿Seguro que desea utilizar una contraseña corta?
Sí
No
Ayuda
< Atrás
Siguiente >
Cancelar

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».

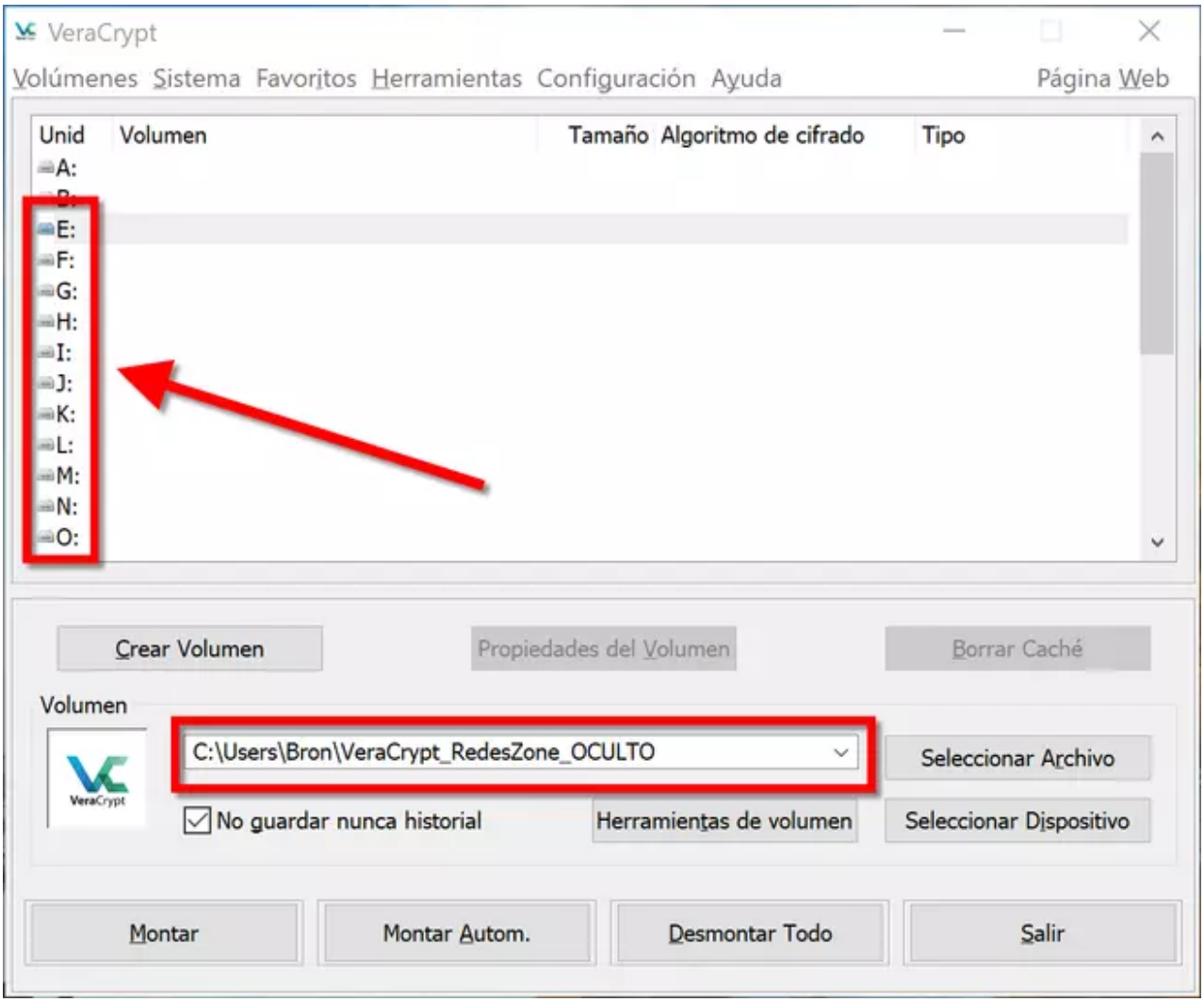


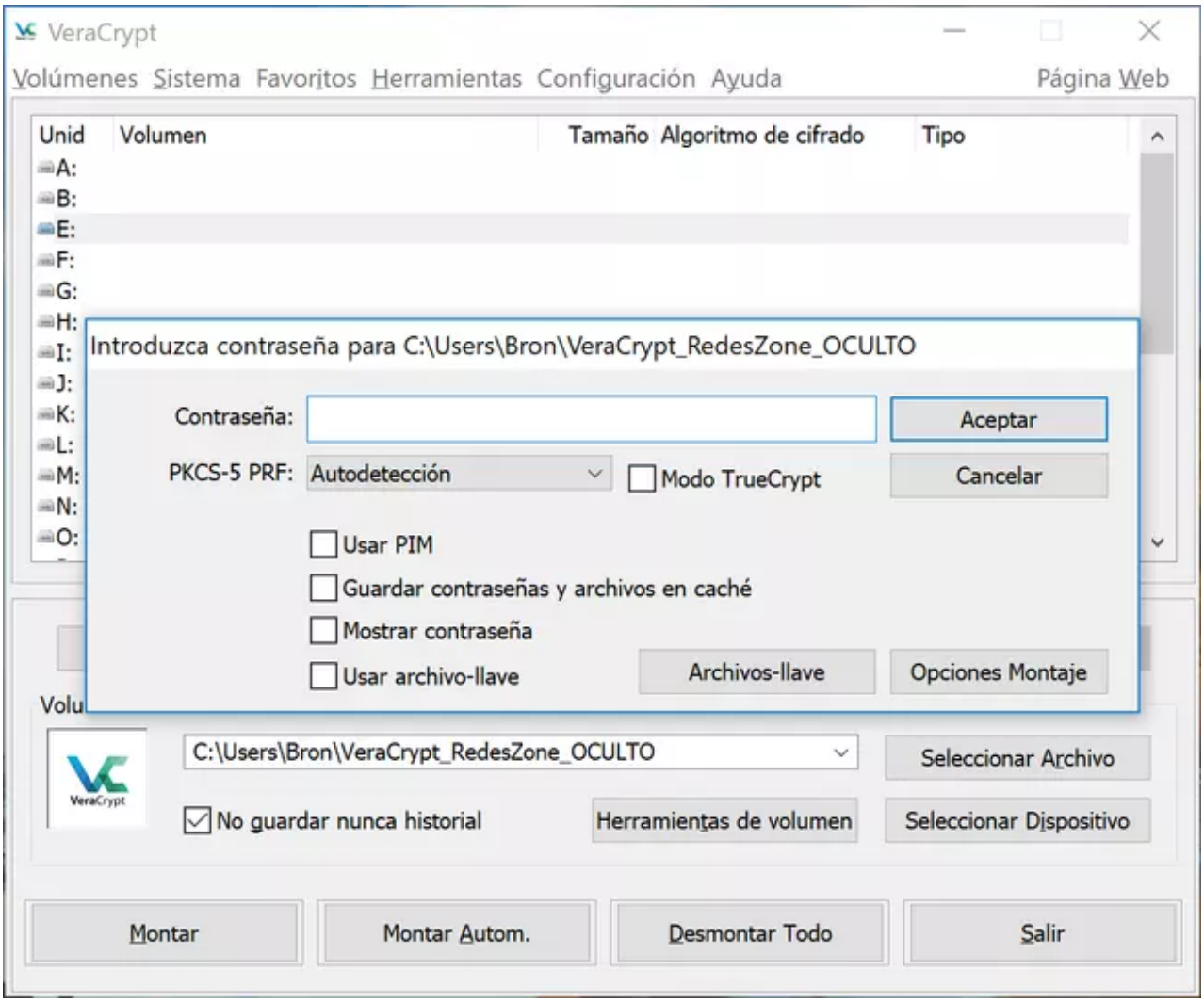
Ahora vamos a montar este volumen cifrado oculto, y vais a ver cómo diferenciarlos.

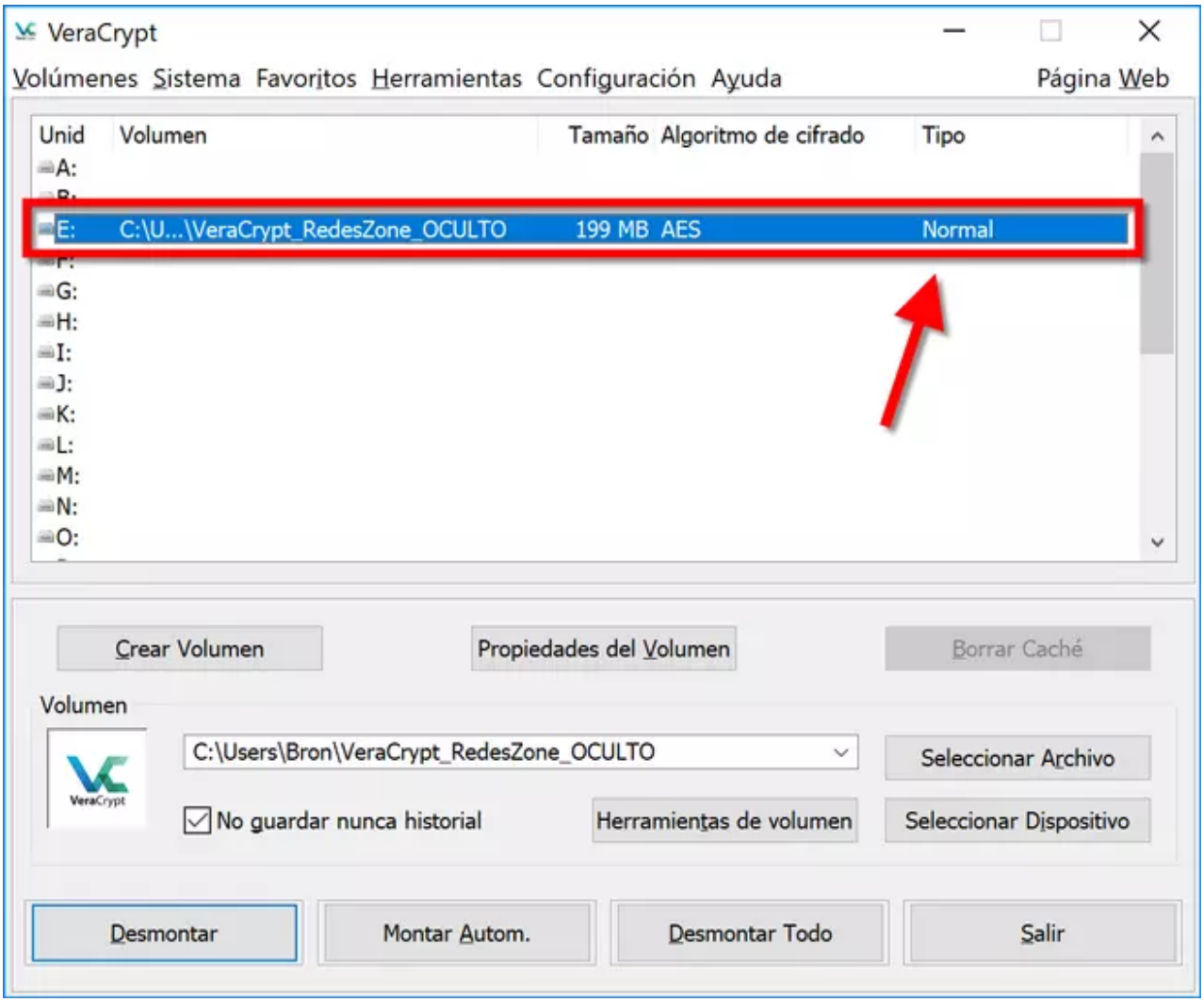
5. Montaje del volumen cifrado «oculto» creado anteriormente

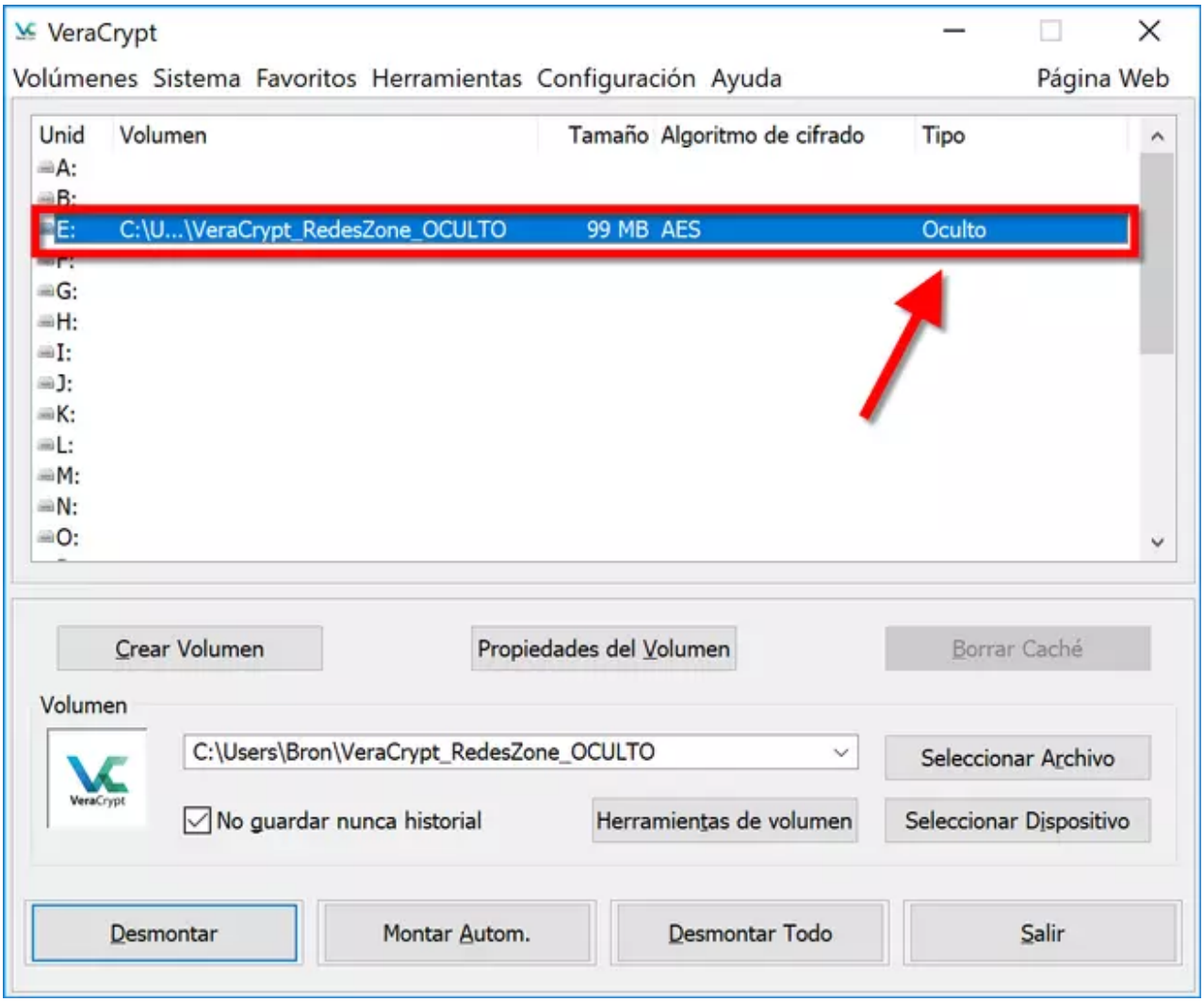
El montaje del volumen oculto se realiza como antes, seleccionamos el volumen cifrado, seleccionamos una unidad para su montaje e introducimos la contraseña.

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.


VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda
Página Web
Unid
Volumen
Tamaño
Algoritmo de cifrado
Tipo
A:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Crear Volumen
Propiedades del Volumen
Borrar Caché
Volumen
C:\Users\Bron\VeraCrypt_RedesZone_OCULTO
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir


VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Introduzca contraseña para C:\Users\Bron\VeraCrypt_RedesZone_OCULTO
Contraseña:
Aceptar
PKCS-5 PRF: Autodetección
Modo TrueCrypt
Cancelar
Usar PIM
Guardar contraseñas y archivos en caché
Mostrar contraseña
Usar archivo-llave
Archivos-llave
Opciones Montaje
C:\Users\Bron\VeraCrypt_RedesZone_OCULTO
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir

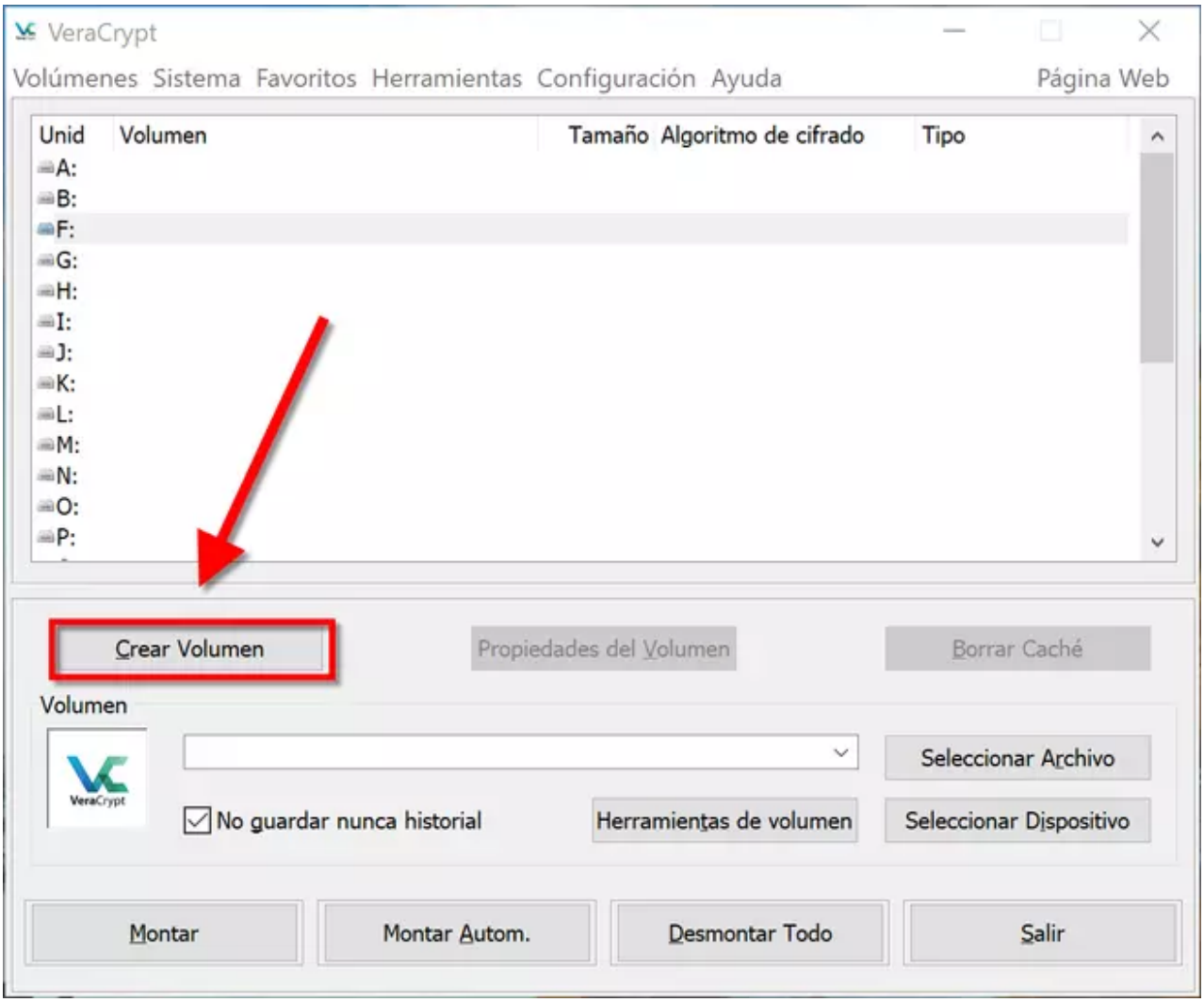

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda
Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
E: C:\U...\VeraCrypt_RedesZone_OCULTO 199 MB AES Normal
G:
H:
I:
J:
K:
L:
M:
N:
O:
Crear Volumen
Propiedades del Volumen
Borrar Caché
Volumen
C:\Users\Bron\VeraCrypt_RedesZone_OCULTO
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Desmontar
Montar Autom.
Desmontar Todo
Salir



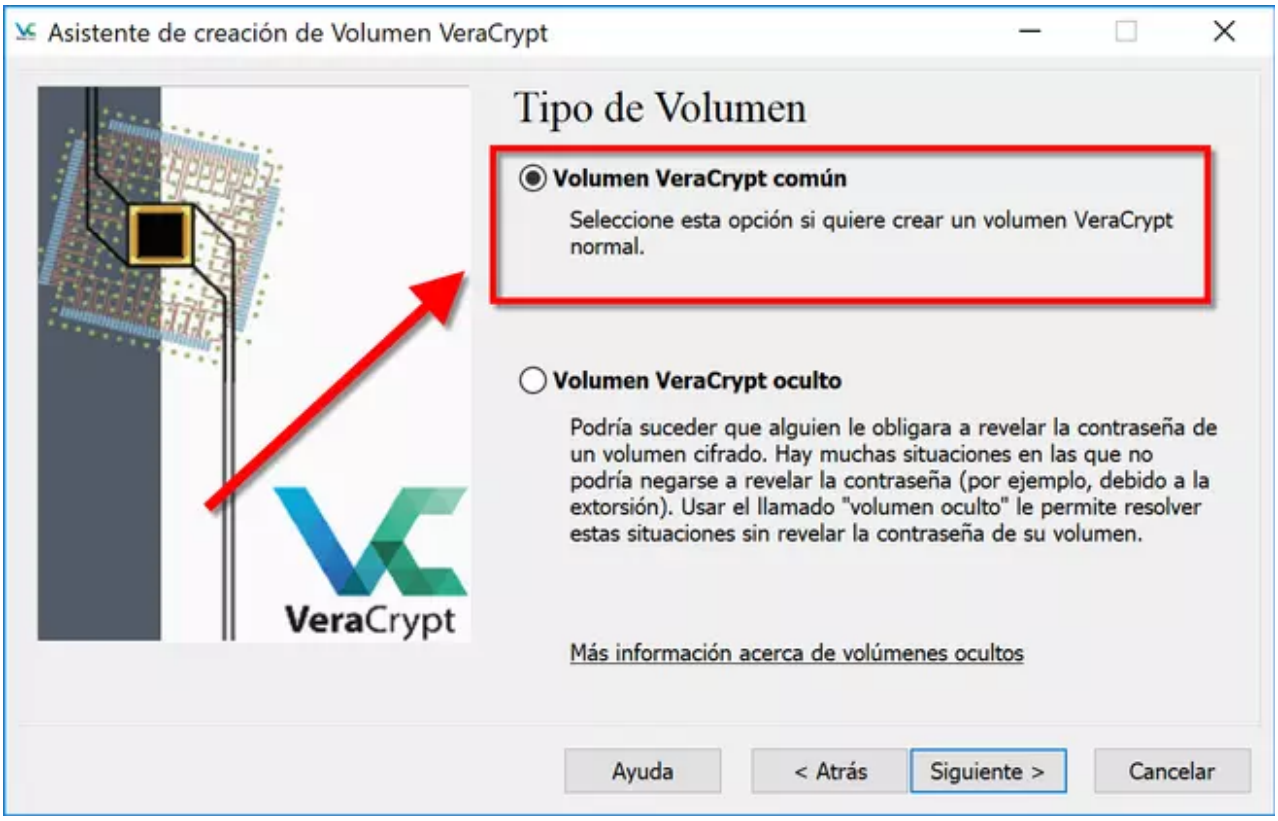
Una vez que ya sabemos cómo crear volúmenes cifrados ocultos y cómo montarlos en una unidad, vamos a ver cómo podemos cifrar una unidad de almacenamiento extraíble entera.

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

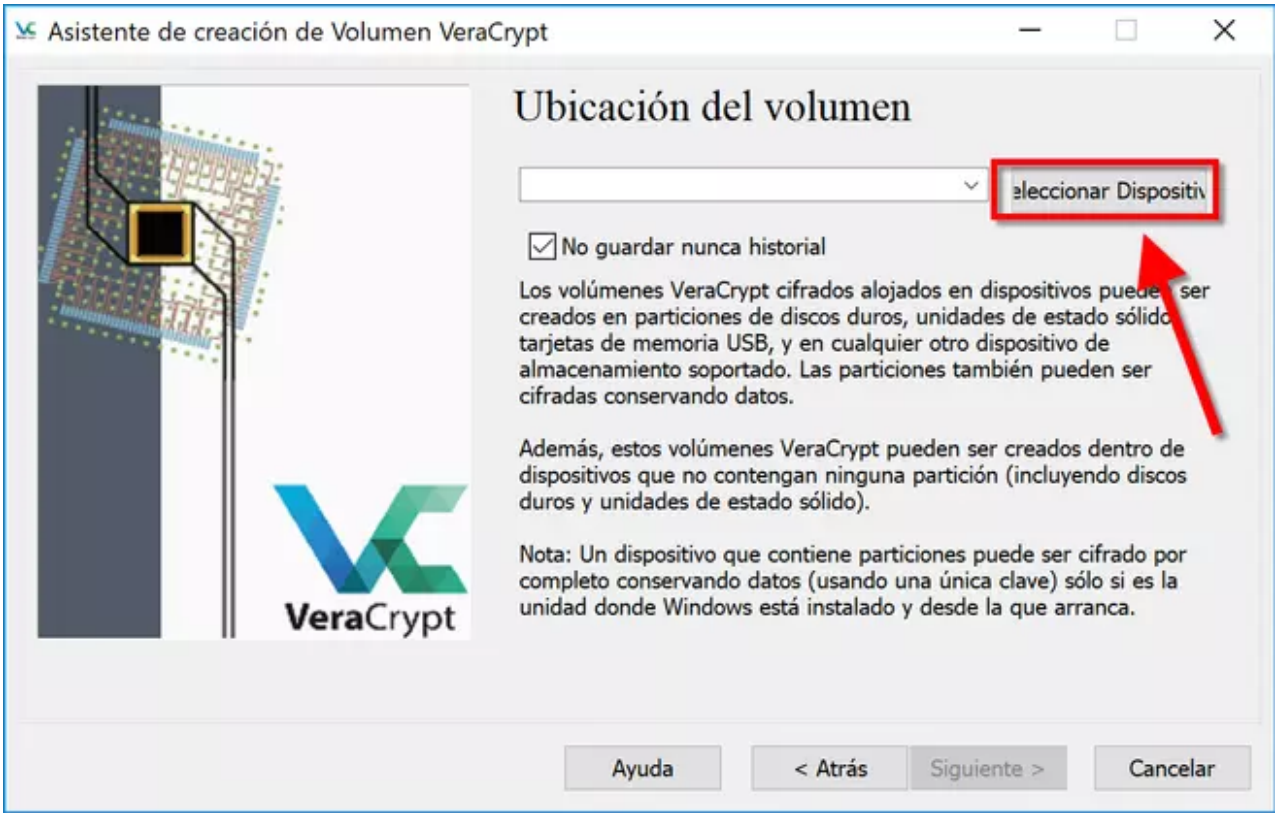
Lo primero que tenemos que hacer es introducir el dispositivo de almacenamiento extraíble en nuestro ordenador. Una vez introducido, pinchamos en «**Crear Volumen**«, y seleccionamos «**Cifrar partición/unidad secundaria**» ya que vamos a cifrar una partición que no tiene el sistema operativo. Una vez 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.

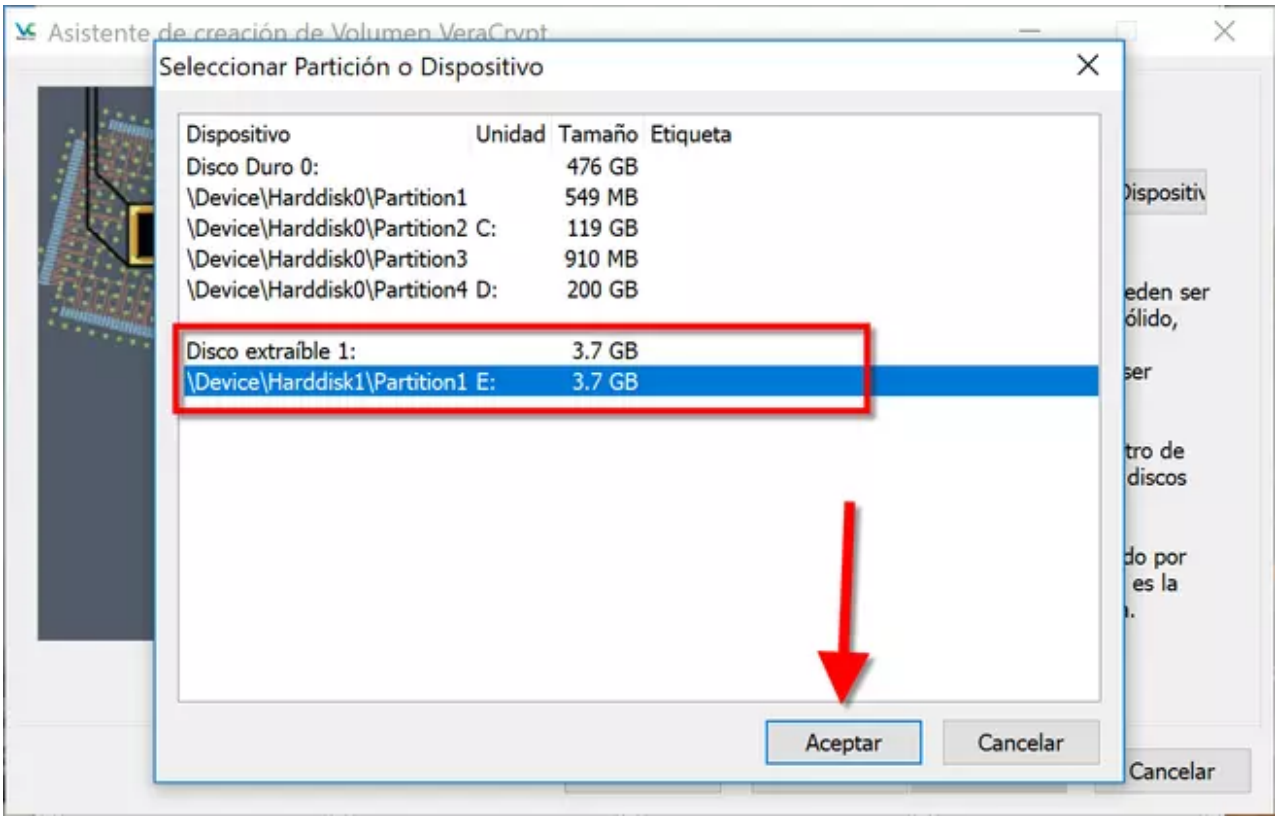

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Crear Volumen
Propiedades del Volumen
Borrar Caché
Volumen
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir


Asistente de creación de Volumen VeraCrypt
Asistente de Creación de Volúmenes
Crear un contenedor de archivos cifrado
Crea un disco cifrado virtual dentro de un archivo. Recomendado para usuarios sin experiencia.
Más información
Cifrar partición/unidad secundaria
Cifra una partición en cualquier unidad interna o externa (ej: unidad flash). Opcionalmente, crea un volumen oculto.
Cifrar la partición/unidad del sistema entera
Cifra la partición/unidad donde Windows está instalado. Cualquiera que quiera acceder al sistema, leer y escribir archivos, etc. tendrá que introducir la contraseña antes de arrancar Windows. Opcionalmente, crea un sistema oculto.
Más información sobre cifrado del sistema
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar



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.

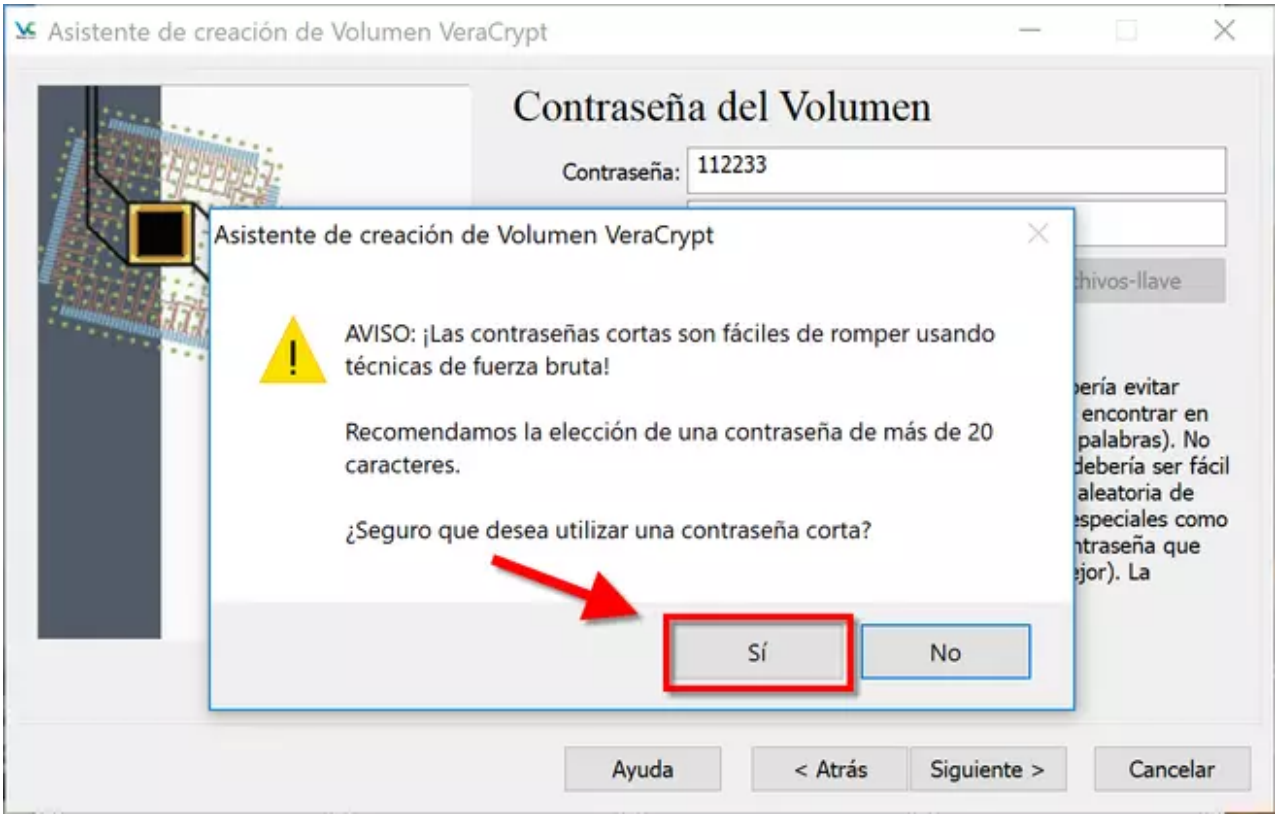

Asistente de creación de Volumen VeraCrypt
Modo de Creación de Volumen
Crear volumen cifrado y formatearlo
Esta es la forma más rápida de crear un volumen VeraCrypt alojado en partición o dispositivo (cifrar conservando datos, que es la otra opción, es más lenta ya que el contenido de cada sector debe ser leído primero, cifrado y después escrito). Cualquier dato almacenado en la partición/dispositivo seleccionado se perderá (los datos NO serán cifrados; serán sobrescritos con datos aleatorios). Si desea cifrar los datos existentes en una partición, elija la otra opción.
Cifrar partición conservando datos
La partición seleccionada entera y todos los datos que almacena serán cifrados conservando datos. Si la partición está vacía, debería elegir la otra opción (el volumen será creado mucho más rápido).
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

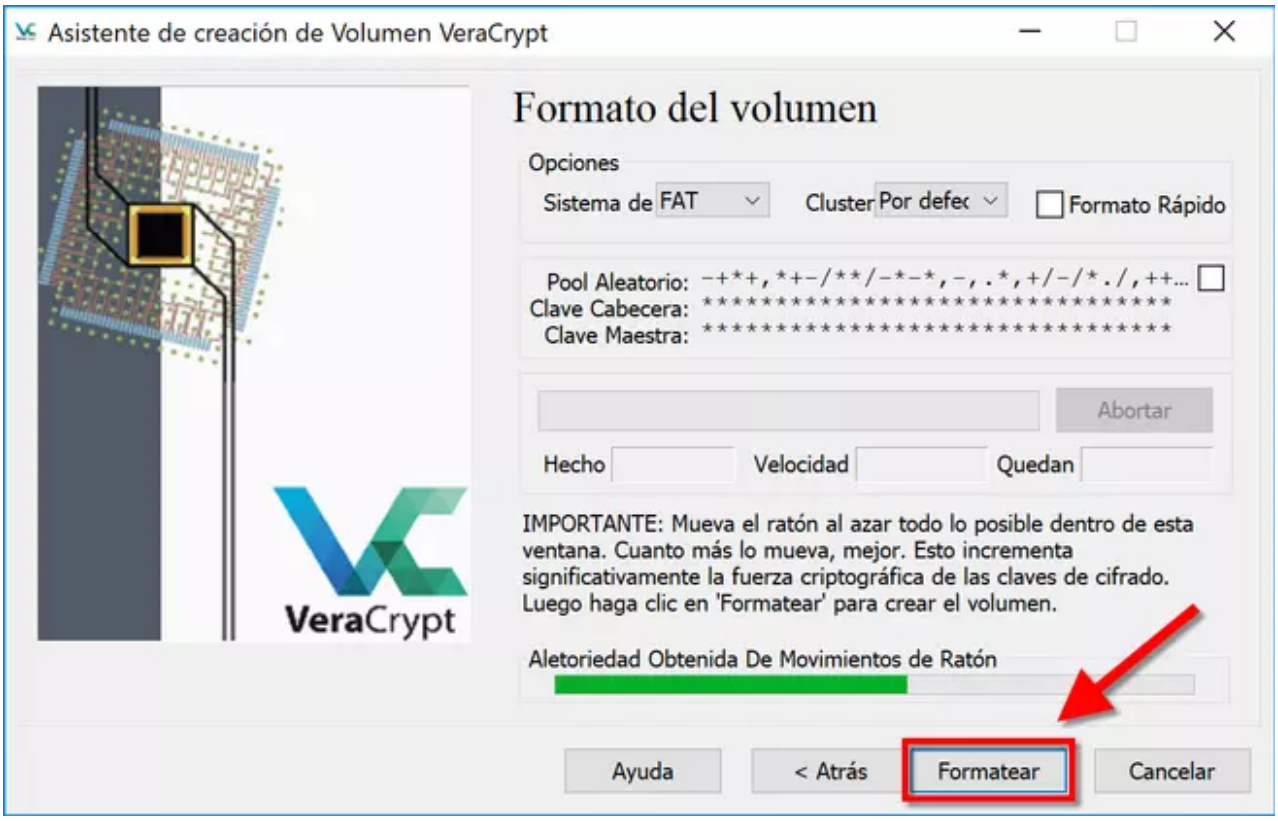

Asistente de creación de Volumen VeraCrypt
Opciones de cifrado
Algoritmo de Cifrado
AES
Probar
Algoritmo aprobado por FIPS (Rijndael, publicado en 1998) que podría ser usado por departamentos y agencias gubernamentales de EEUU para proteger información clasificada hasta el nivel Alto Secreto. Clave de 256-bit, bloque de 128-bit, 14 rondas (AES-256). El modo de operación es XTS.
Más información en AES
Comparación
Algoritmo Hash
SHA-512
Información de algoritmos hash
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

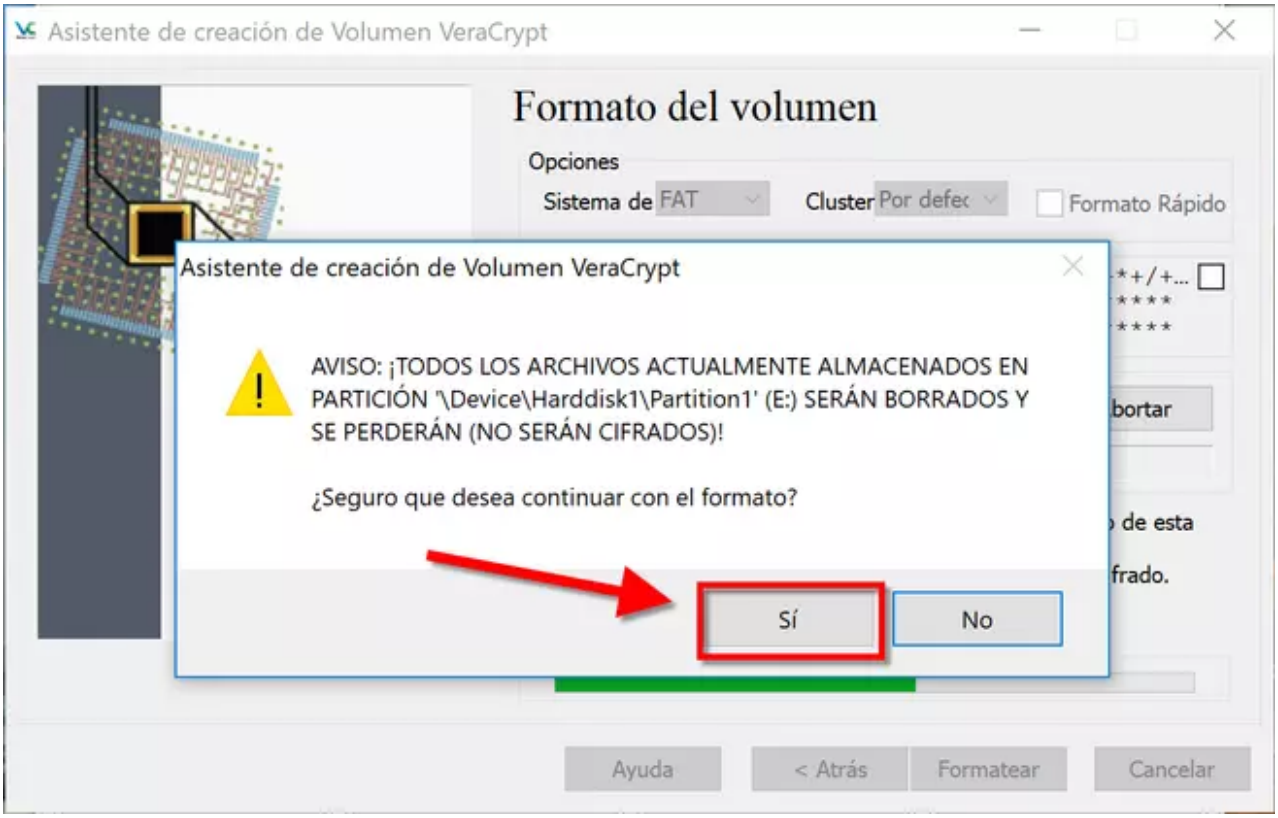
De cara a la autenticación para acceder a los datos, podremos introducir la típica contraseña de paso, o también elegir una clave criptográfica para acceder al propio dispositivo cifrado. Si seleccionamos una contraseña que sea muy corta, nos avisará que no es recomendable de cara a la seguridad.

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.


Asistente de creación de Volumen VeraCrypt
Contraseña del Volumen
Contraseña: 112233
Confirmar: 112233
Usar archivo-llave
Archivos-llave
Mostrar contraseña
Usar PIM
Es muy importante que elija una buena contraseña. Debería evitar elegir una que contenga sólo una palabra que se pueda encontrar en un diccionario (o una combinación de 2, 3, o 4 de estas palabras). No debería contener nombres ni fechas de nacimiento. No debería ser fácil de adivinar. Una buena contraseña es una combinación aleatoria de letras mayúsculas y minúsculas, números, y caracteres especiales como @ ^ = $ * + etc. Recomendamos la elección de una contraseña que consista en más de 20 caracteres (cuanto más larga, mejor). La máxima longitud posible es 64 caracteres.
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar

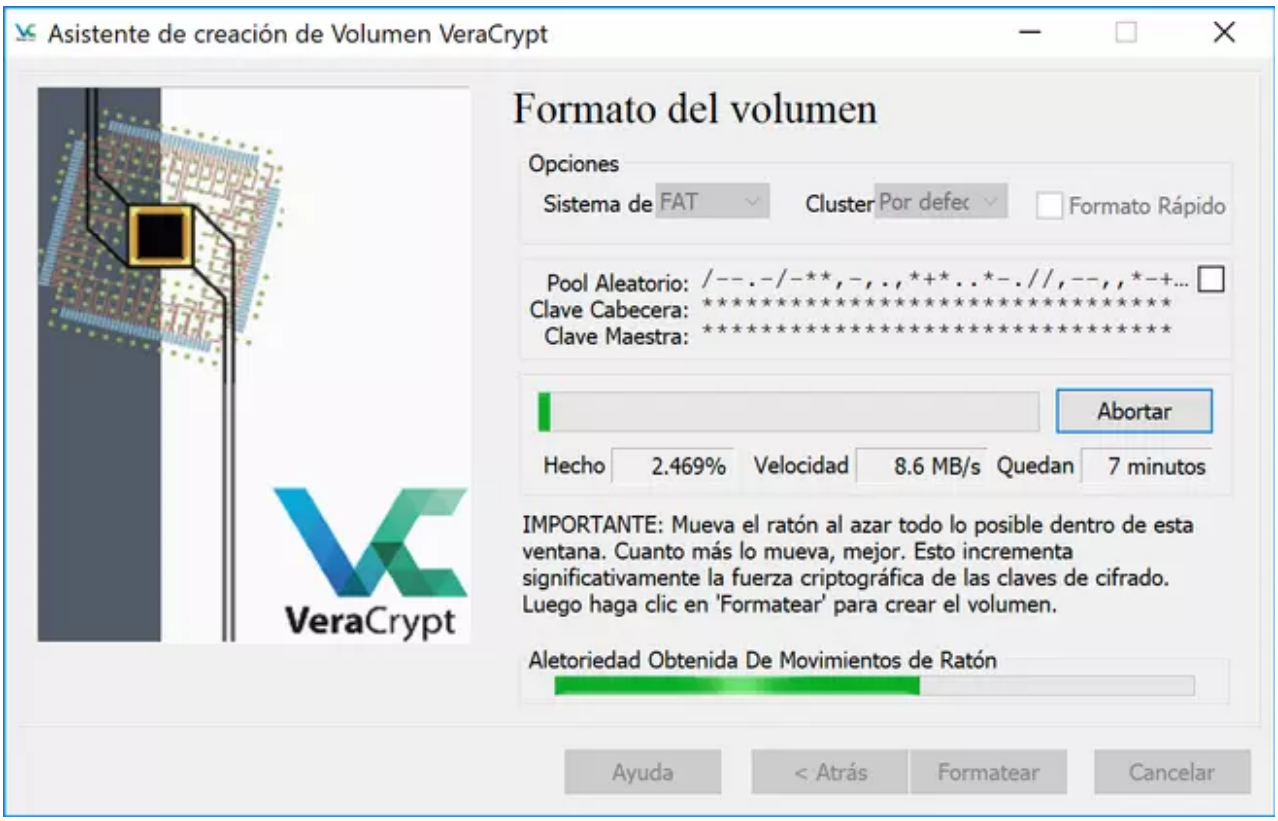

Asistente de creación de Volumen VeraCrypt
Contraseña del Volumen
Contraseña: 112233
Asistente de creación de Volumen VeraCrypt
AVISO: ¡Las contraseñas cortas son fáciles de romper usando técnicas de fuerza bruta!
Recomendamos la elección de una contraseña de más de 20 caracteres.
¿Seguro que desea utilizar una contraseña corta?
Sí
No
Ayuda
< Atrás
Siguiente >
Cancelar

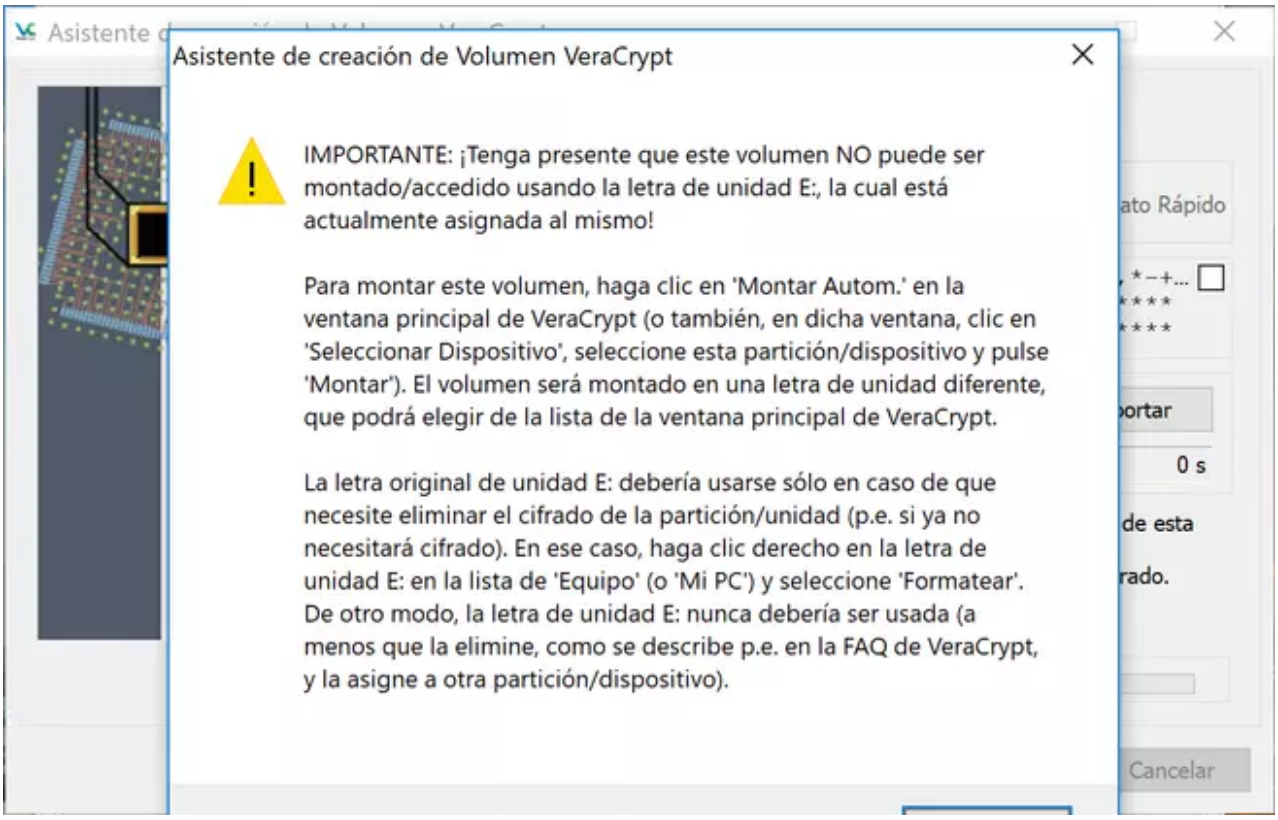


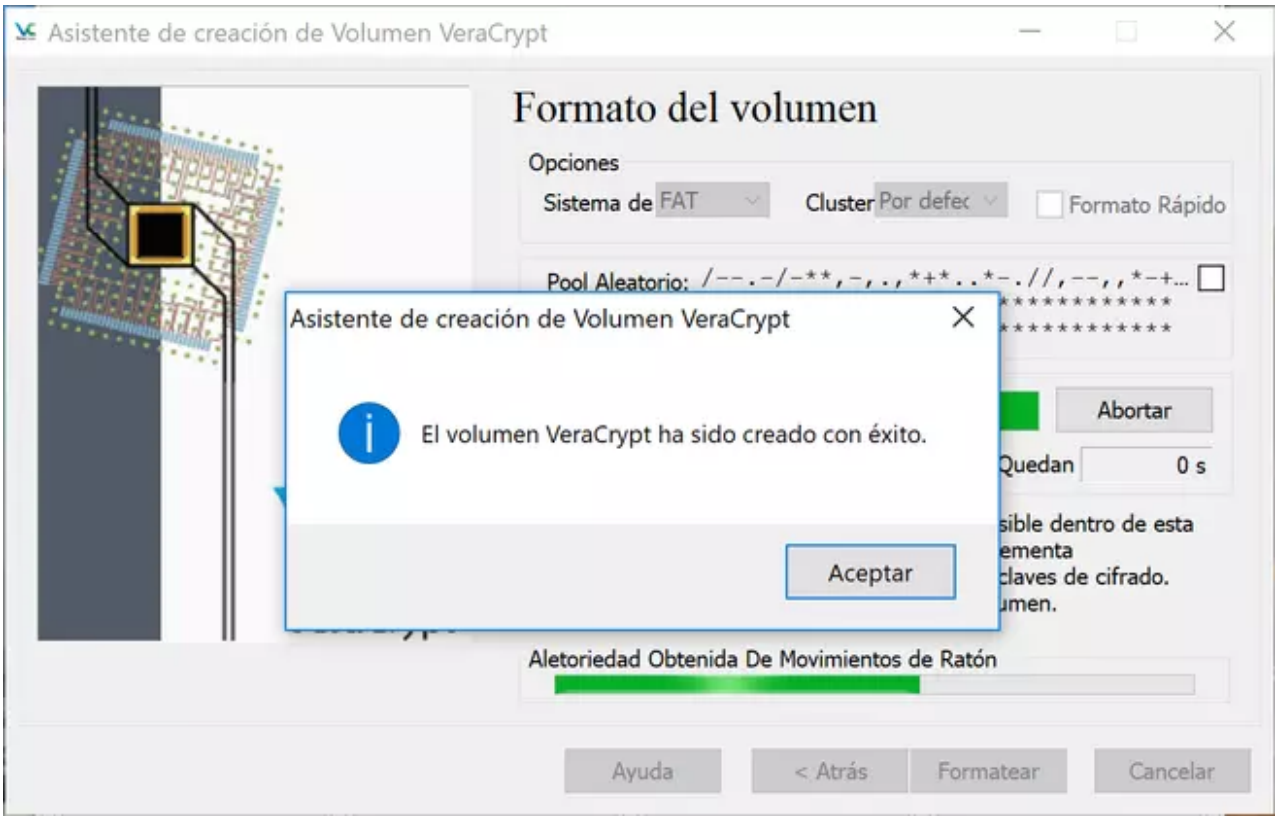


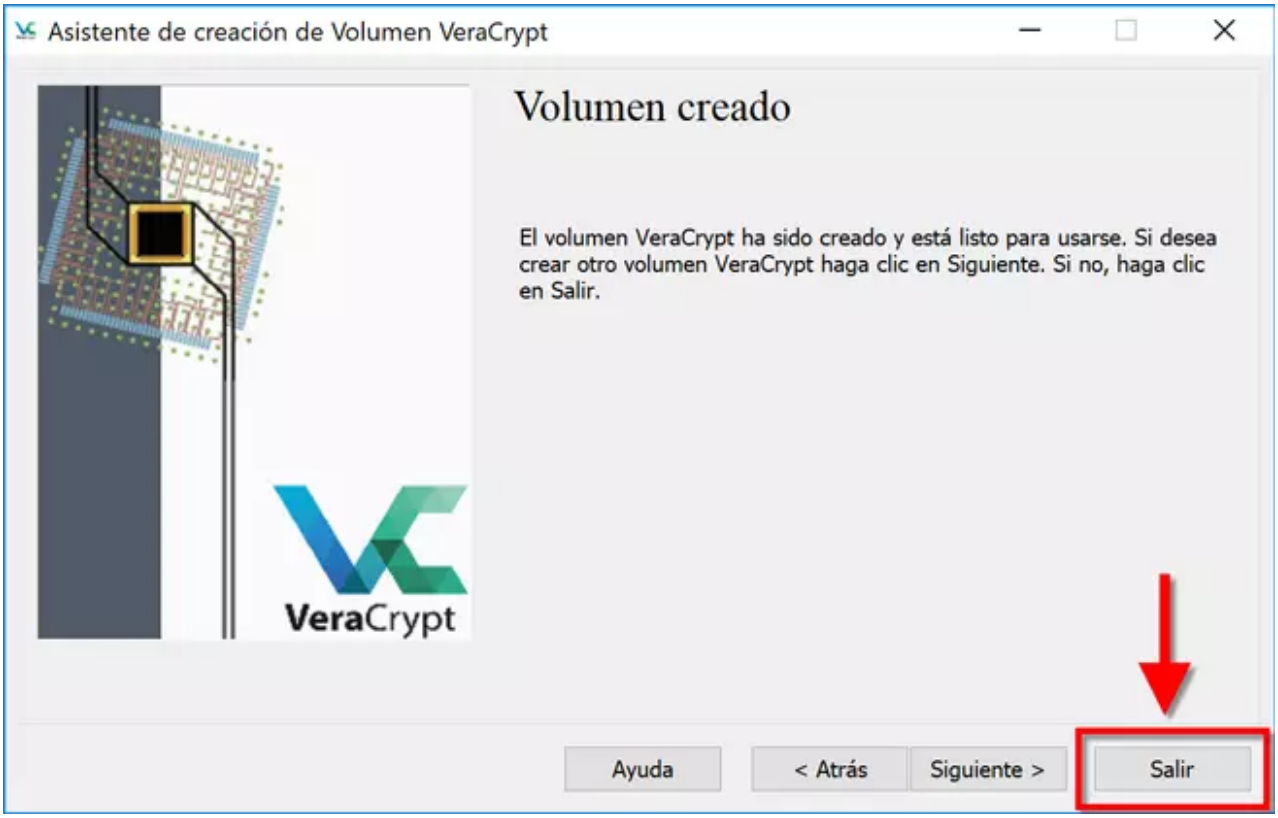
Cuando el proceso termine, **nos avisará que la unidad E no va a ser accesible**, ya que en esta unidad es el propio sistema operativo donde «coloca» el dispositivo de almacenamiento extraíble. Una vez que nosotros montemos este dispositivo en VeraCrypt, e introduzcamos la contraseña de acceso, sí vamos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





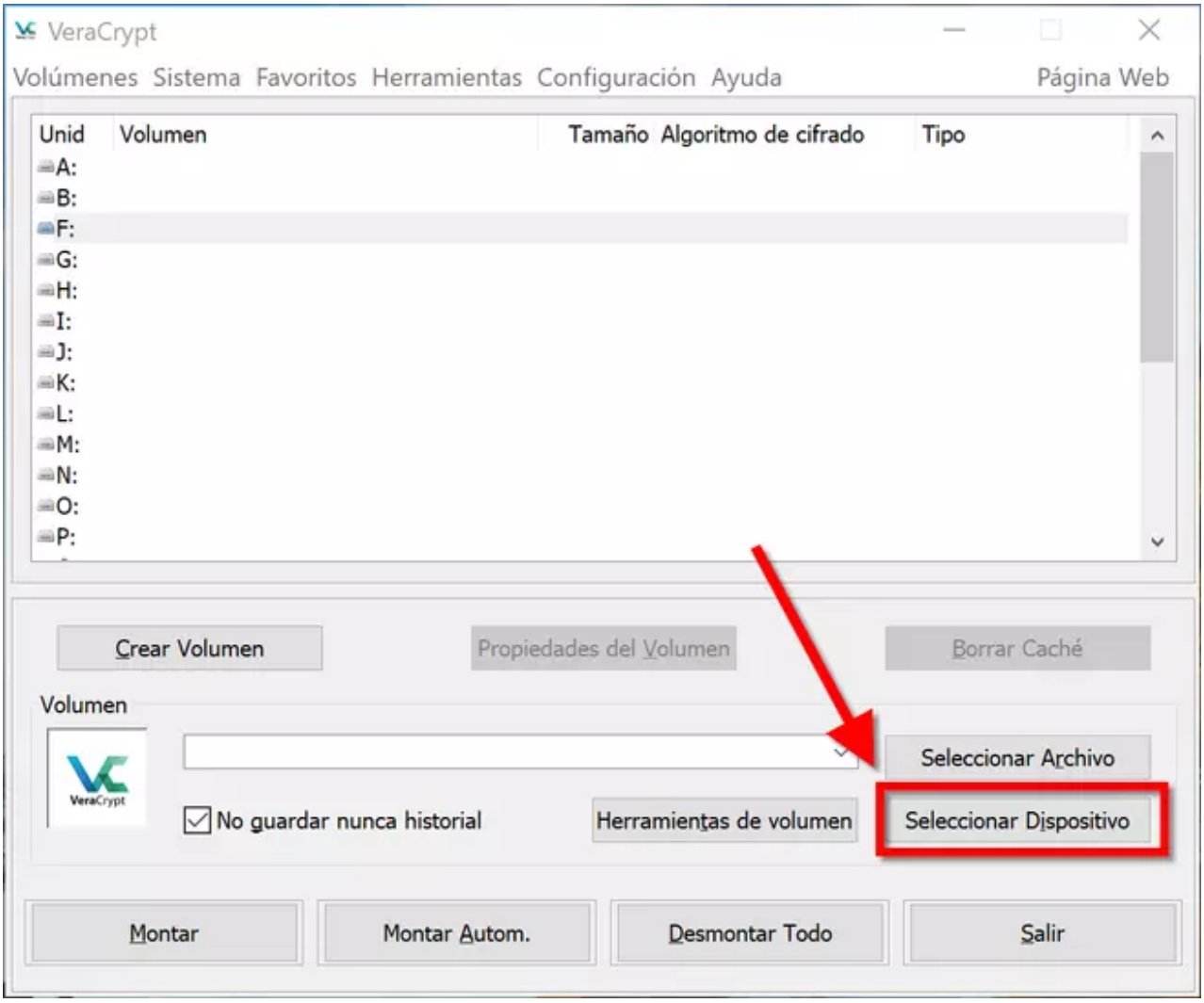


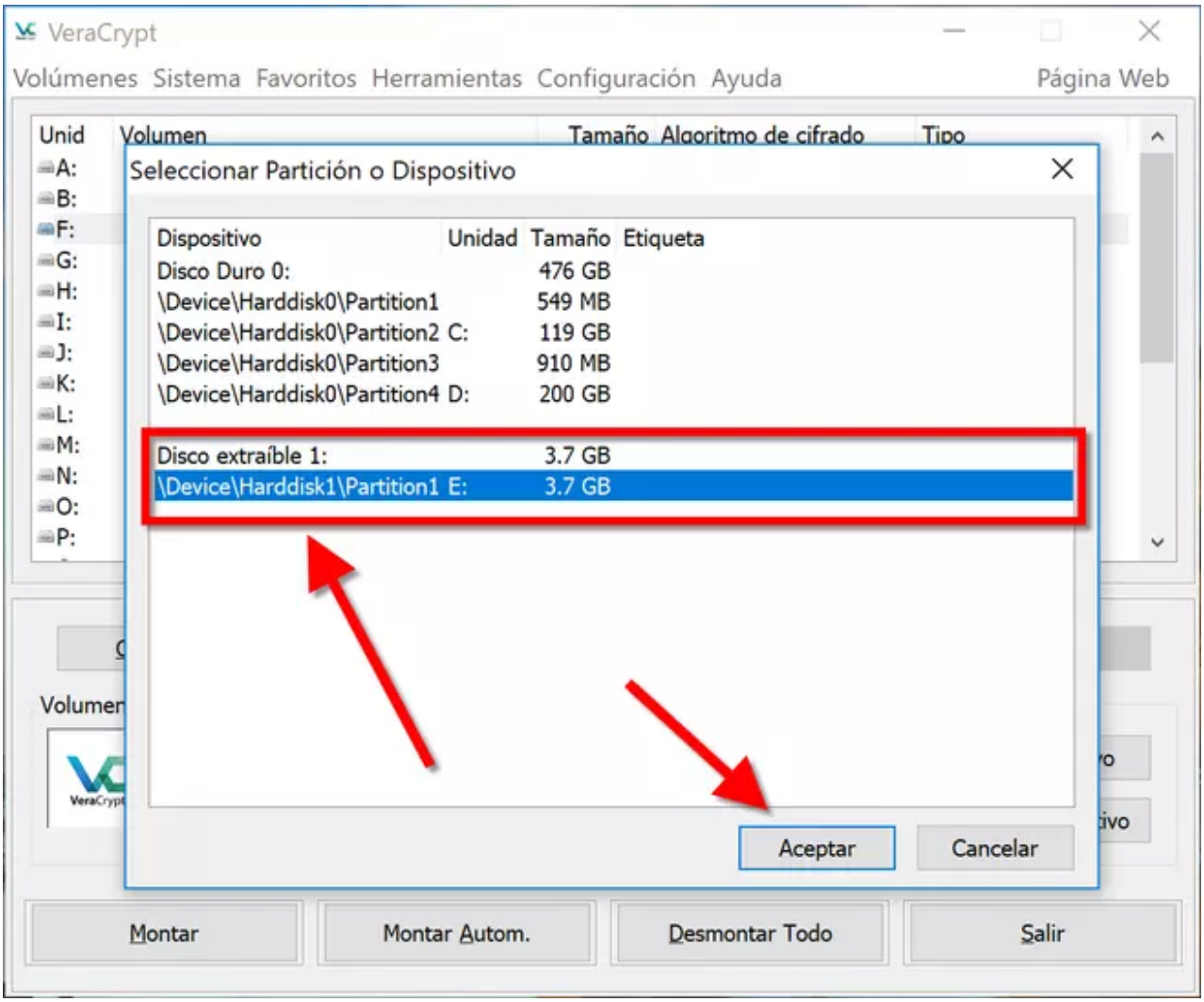


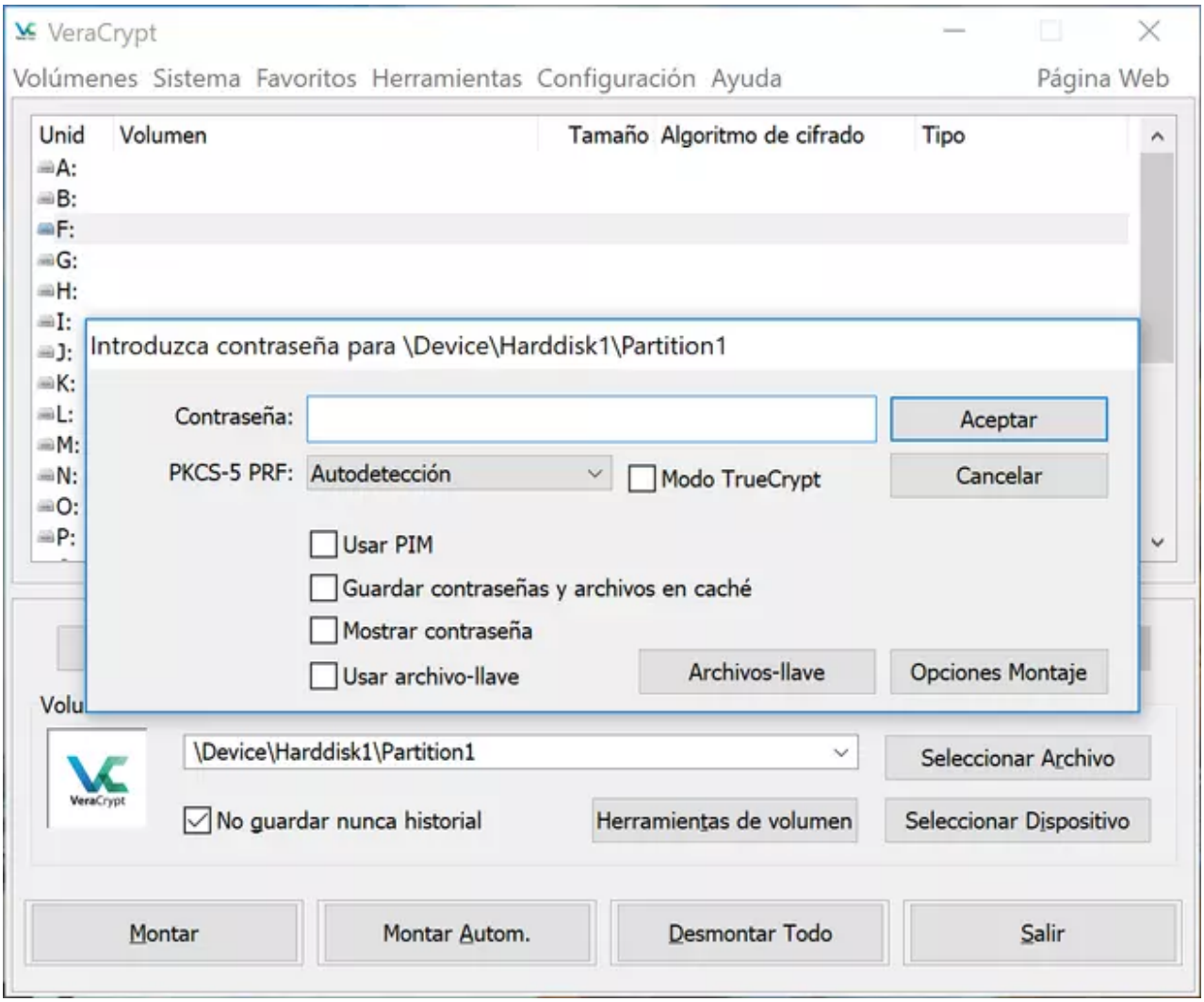
Ahora ya tendremos nuestra unidad de almacenamiento perfectamente cifrada, y para usarla, deberemos «montarla» en el propio «VeraCrypt».

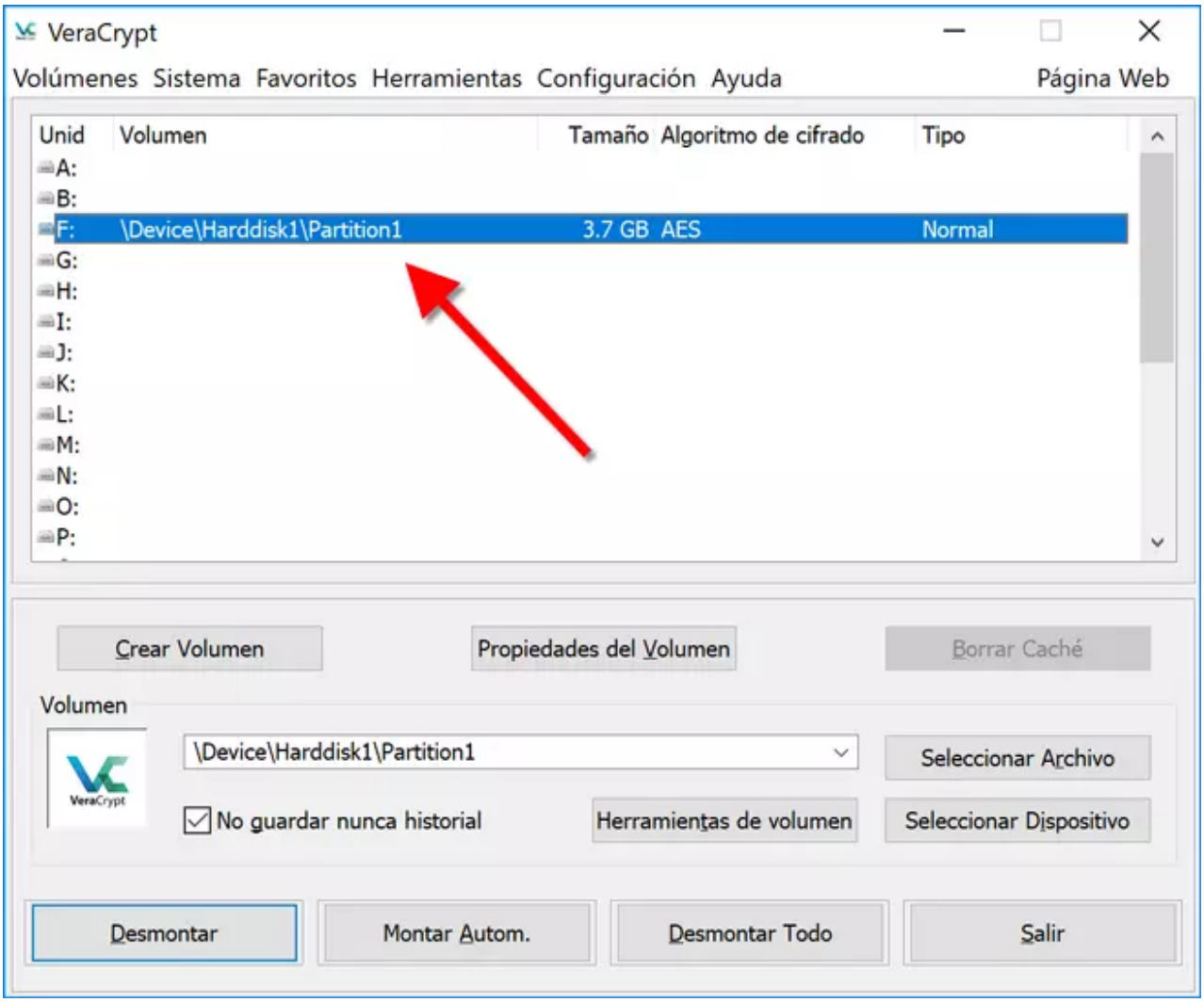
7. Montaje del dispositivo de almacenamiento extraíble cifrado

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.




VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Seleccionar Partición o Dispositivo
Dispositivo Unidad Tamaño Etiqueta
Disco Duro 0: 476 GB
\Device\Harddisk0\Partition1 549 MB
\Device\Harddisk0\Partition2 C: 119 GB
\Device\Harddisk0\Partition3 910 MB
\Device\Harddisk0\Partition4 D: 200 GB
Disco extraíble 1: 3.7 GB
\Device\Harddisk1\Partition1 E: 3.7 GB
Aceptar
Cancelar
Volumen
Montar
Montar Autom.
Desmontar Todo
Salir

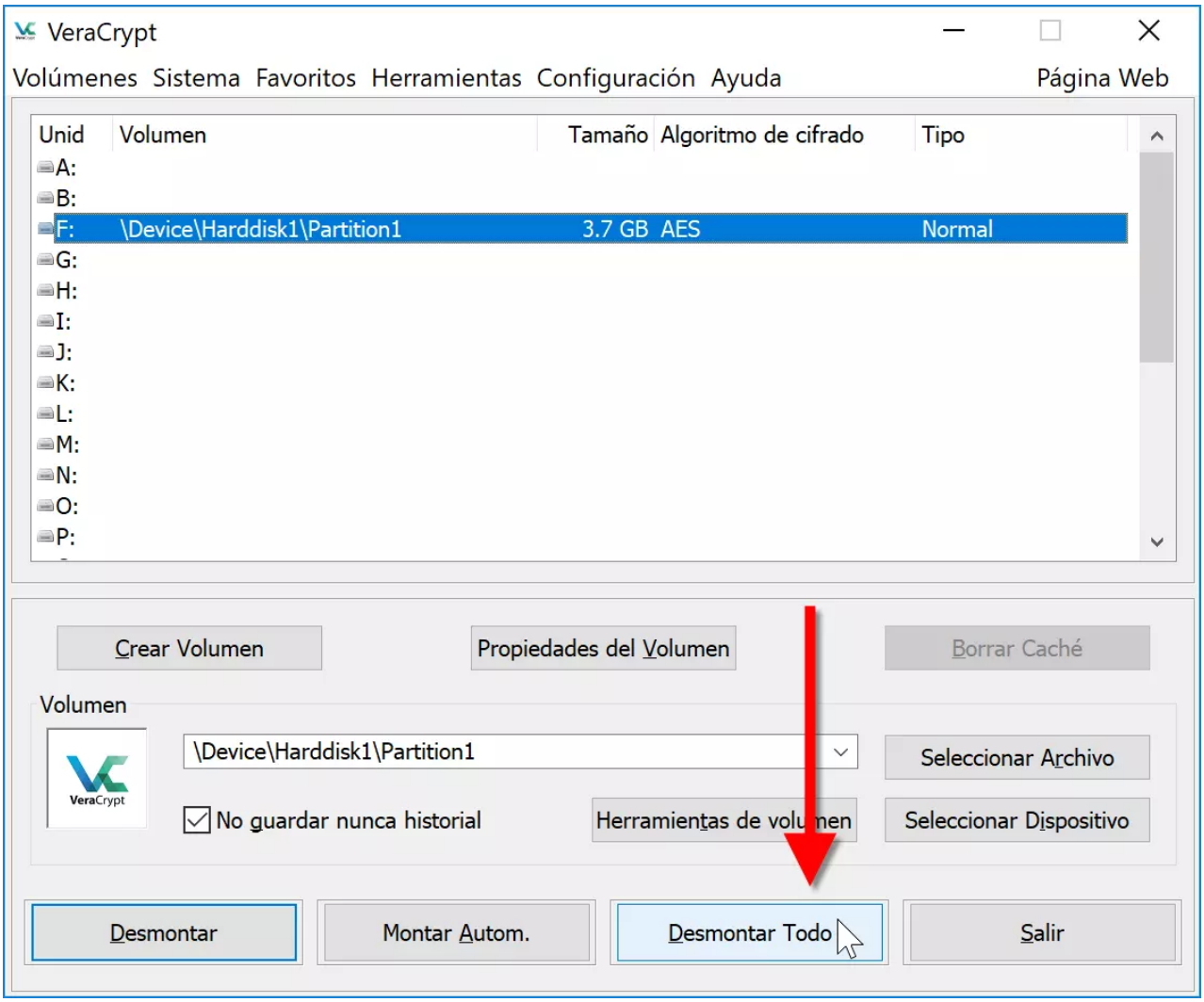

VeraCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Unid Volumen Tamaño Algoritmo de cifrado Tipo
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Introduzca contraseña para \Device\Harddisk1\Partition1
Contraseña:
Aceptar
PKCS-5 PRF: Autodetección
Modo TrueCrypt
Cancelar
Usar PIM
Guardar contraseñas y archivos en caché
Mostrar contraseña
Usar archivo-llave
Archivos-llave
Opciones Montaje
Volu
\Device\Harddisk1\Partition1
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir



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.

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.

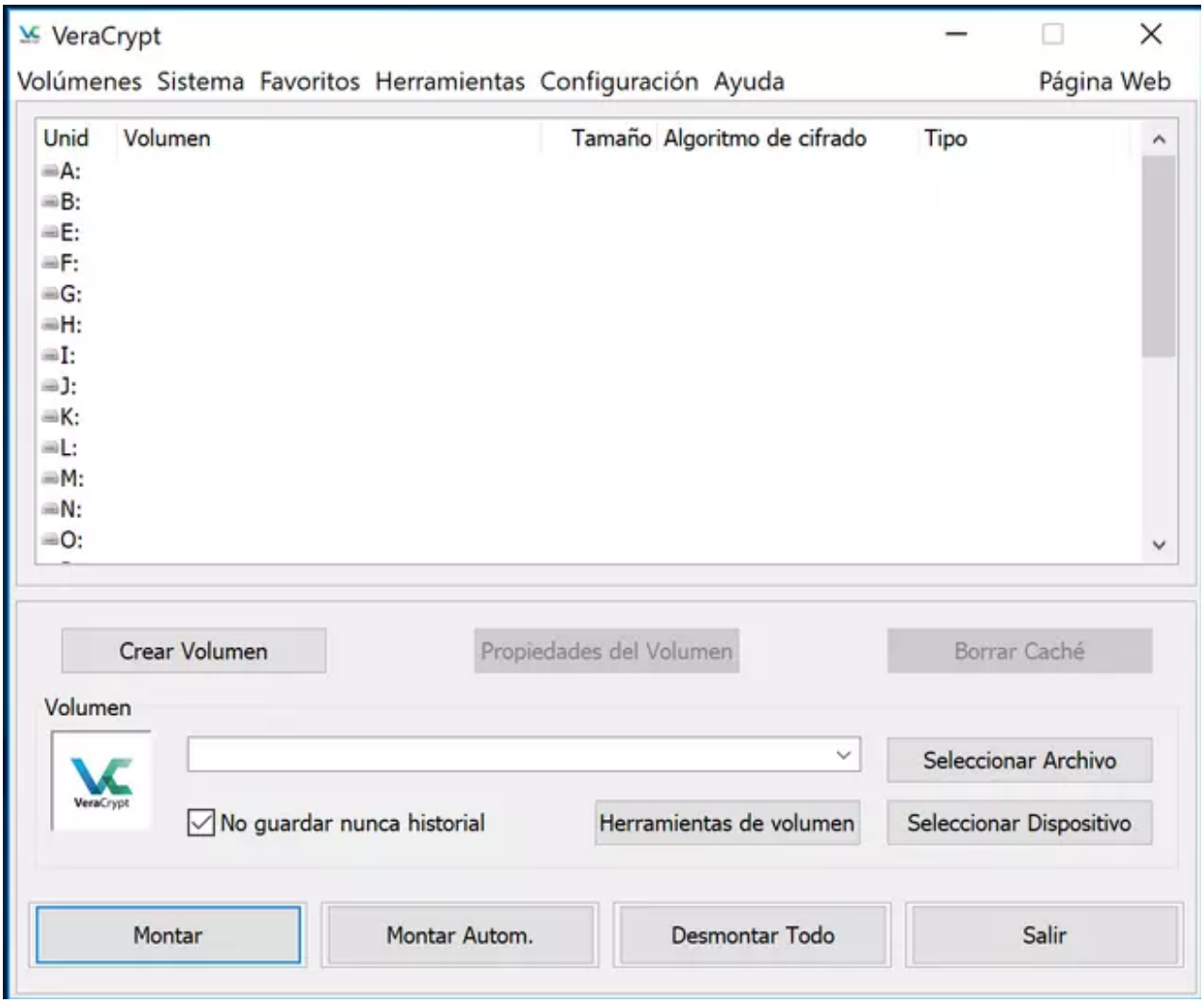
8. Cifrado de todo el sistema operativo (cifrar la partición/unidad del sistema entera) en VeraCrypt

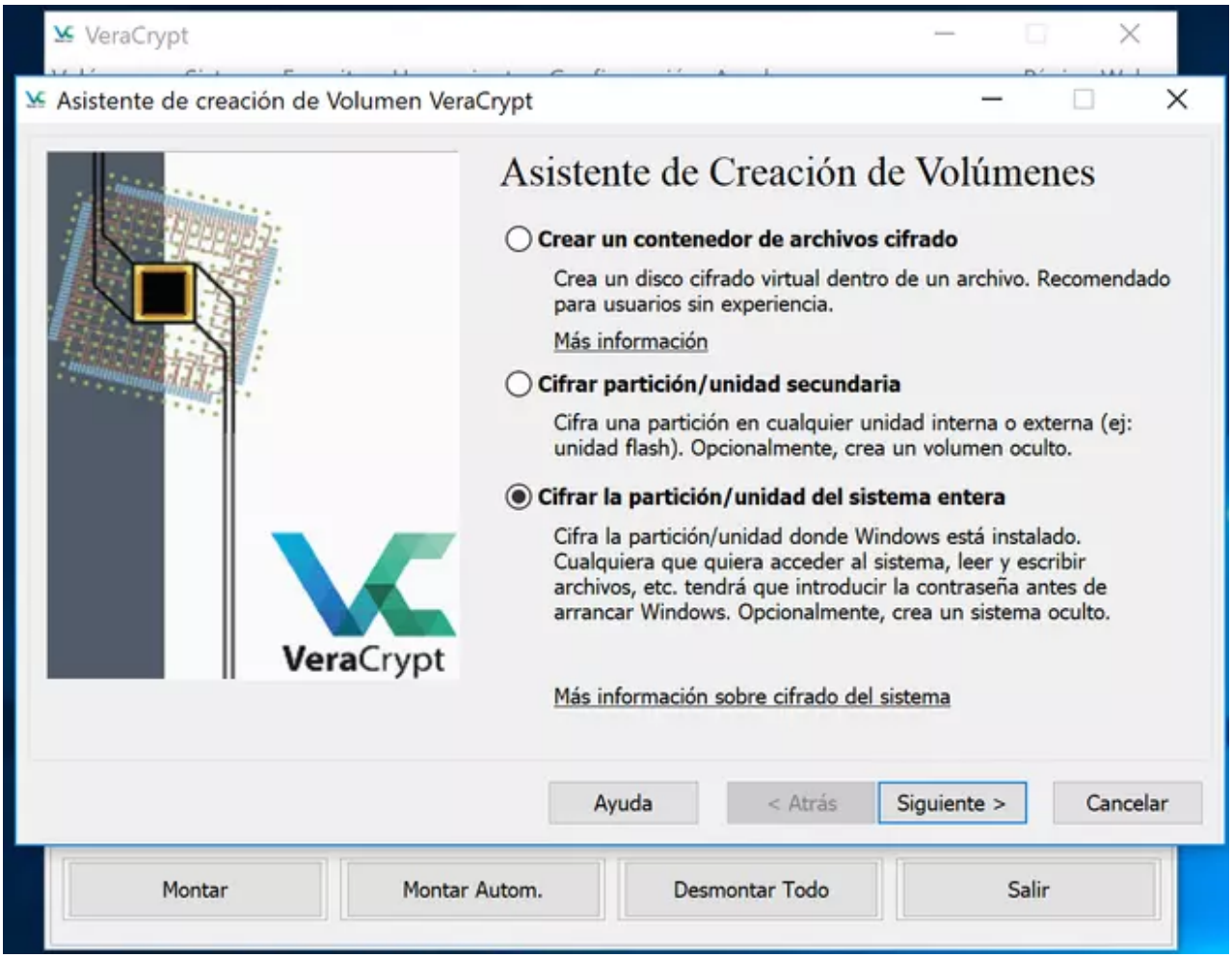
Este proceso lo debemos realizar con mucho cuidado, ya que de lo contrario podríamos perder toda la información. Es recomendable realizar una copia de seguridad completa de nuestro PC con programas como Acronis True Image o similares, y sobre todo, no olvidar la clave de acceso al sistema que pongamos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

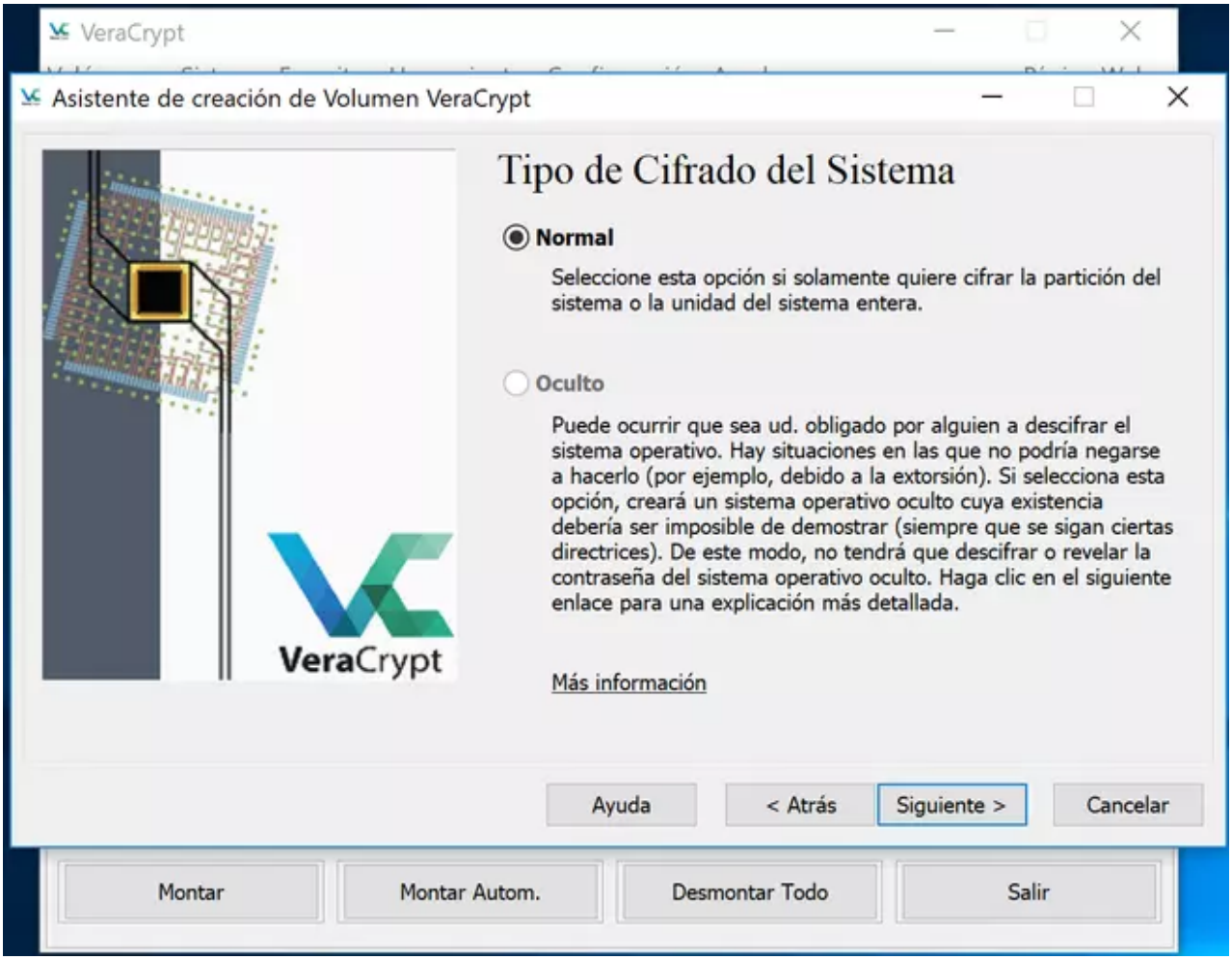
Lo primero que debemos hacer es pinchar en «**Crear Volumen**«, y posteriormente elegir «**Cifrar la particion/unidad del sistema entera**«. Una vez dentro, tenemos dos opciones principales:

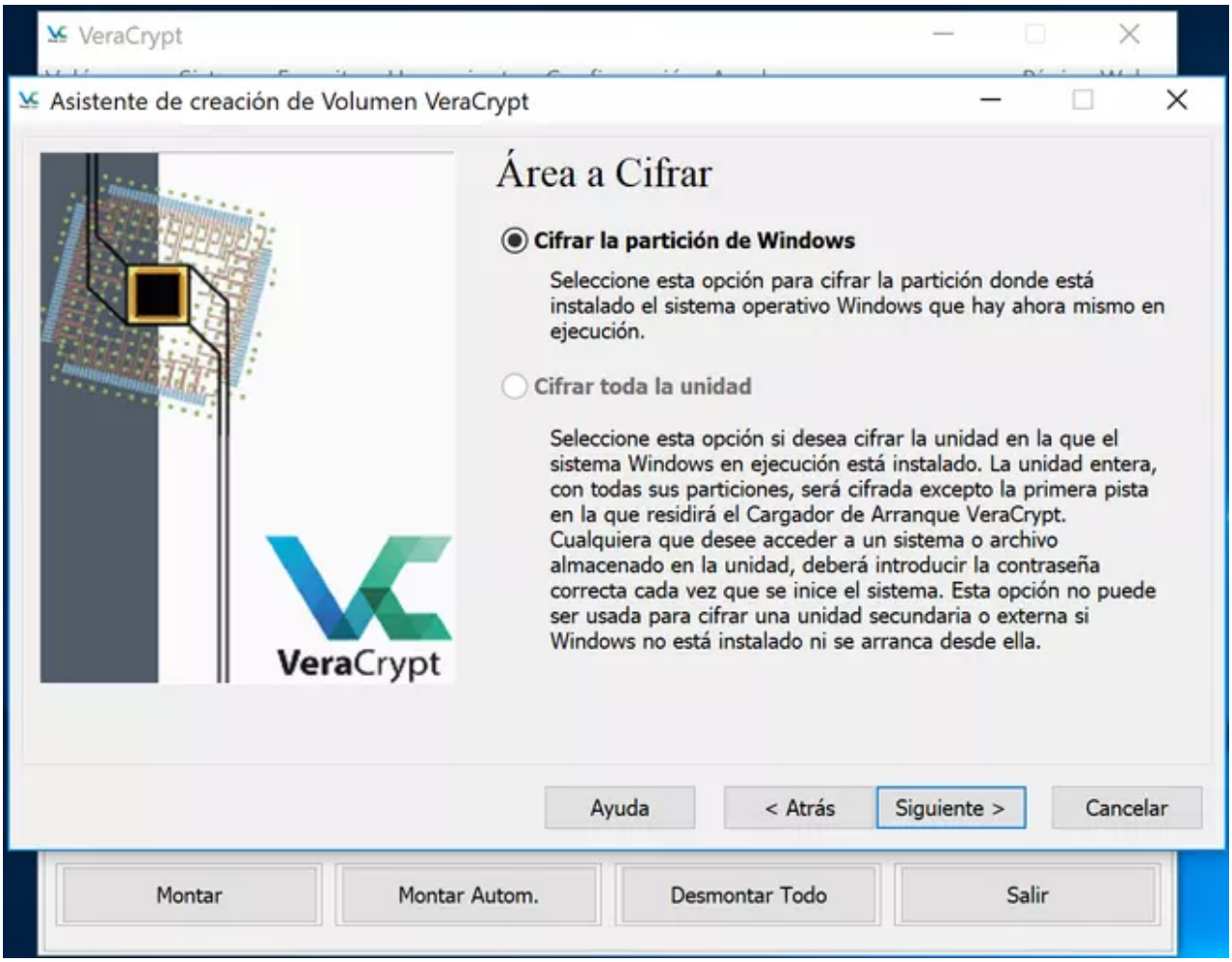
- Normal: se cifra con una clave de paso o una clave criptográfica en un volumen con el sistema operativo nuestro.
- Oculto: se cifra el sistema operativo dentro de un volumen oculto para evitar una extorsión, de esta forma, podremos poner una clave y acceder a un sistema operativo que no sea el «bueno».

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.



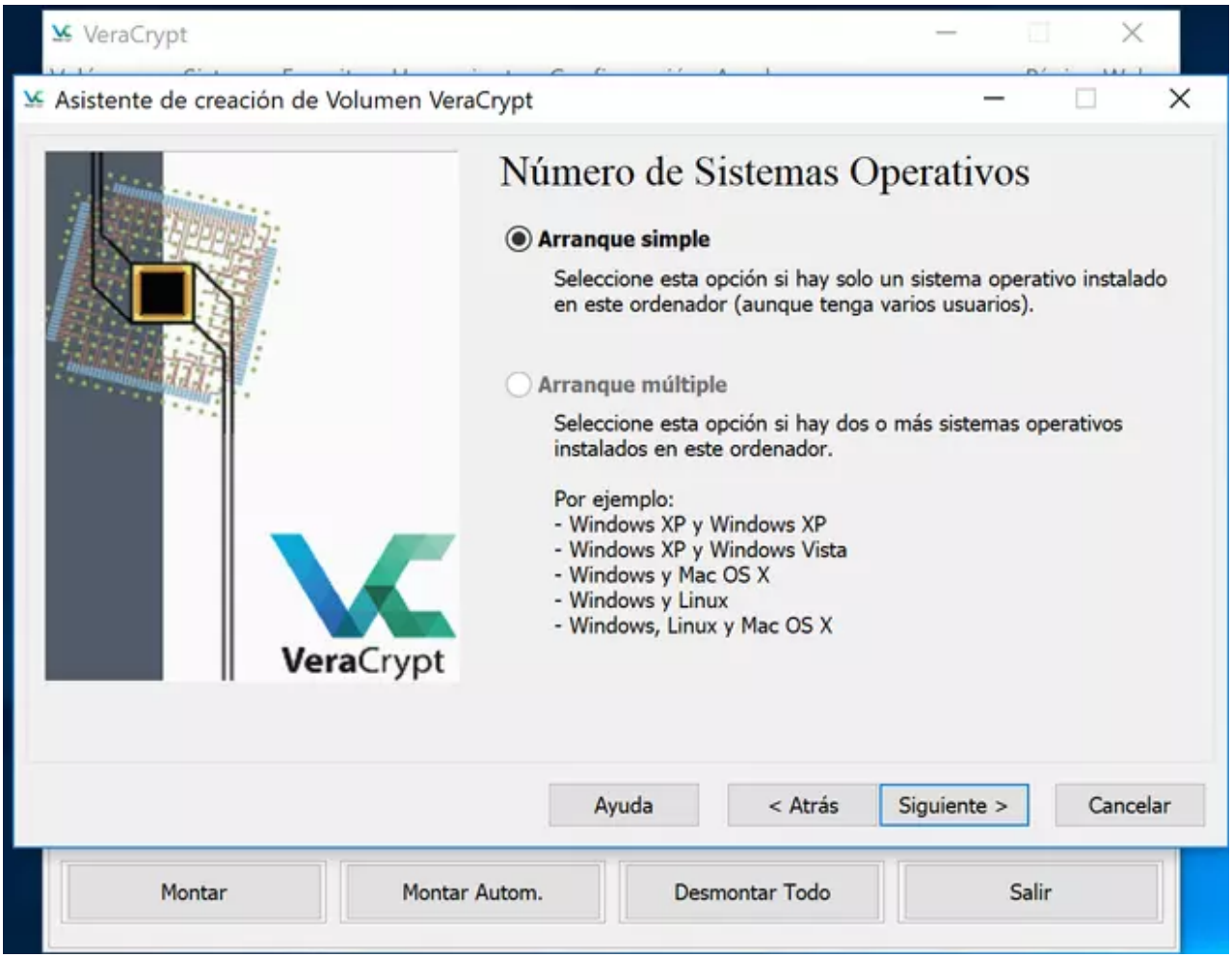

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Asistente de Creación de Volúmenes
Crear un contenedor de archivos cifrado
Crea un disco cifrado virtual dentro de un archivo. Recomendado para usuarios sin experiencia.
Más información
Cifrar partición/unidad secundaria
Cifra una partición en cualquier unidad interna o externa (ej: unidad flash). Opcionalmente, crea un volumen oculto.
Cifrar la partición/unidad del sistema entera
Cifra la partición/unidad donde Windows está instalado. Cualquiera que quiera acceder al sistema, leer y escribir archivos, etc. tendrá que introducir la contraseña antes de arrancar Windows. Opcionalmente, crea un sistema oculto.
Más información sobre cifrado del sistema
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

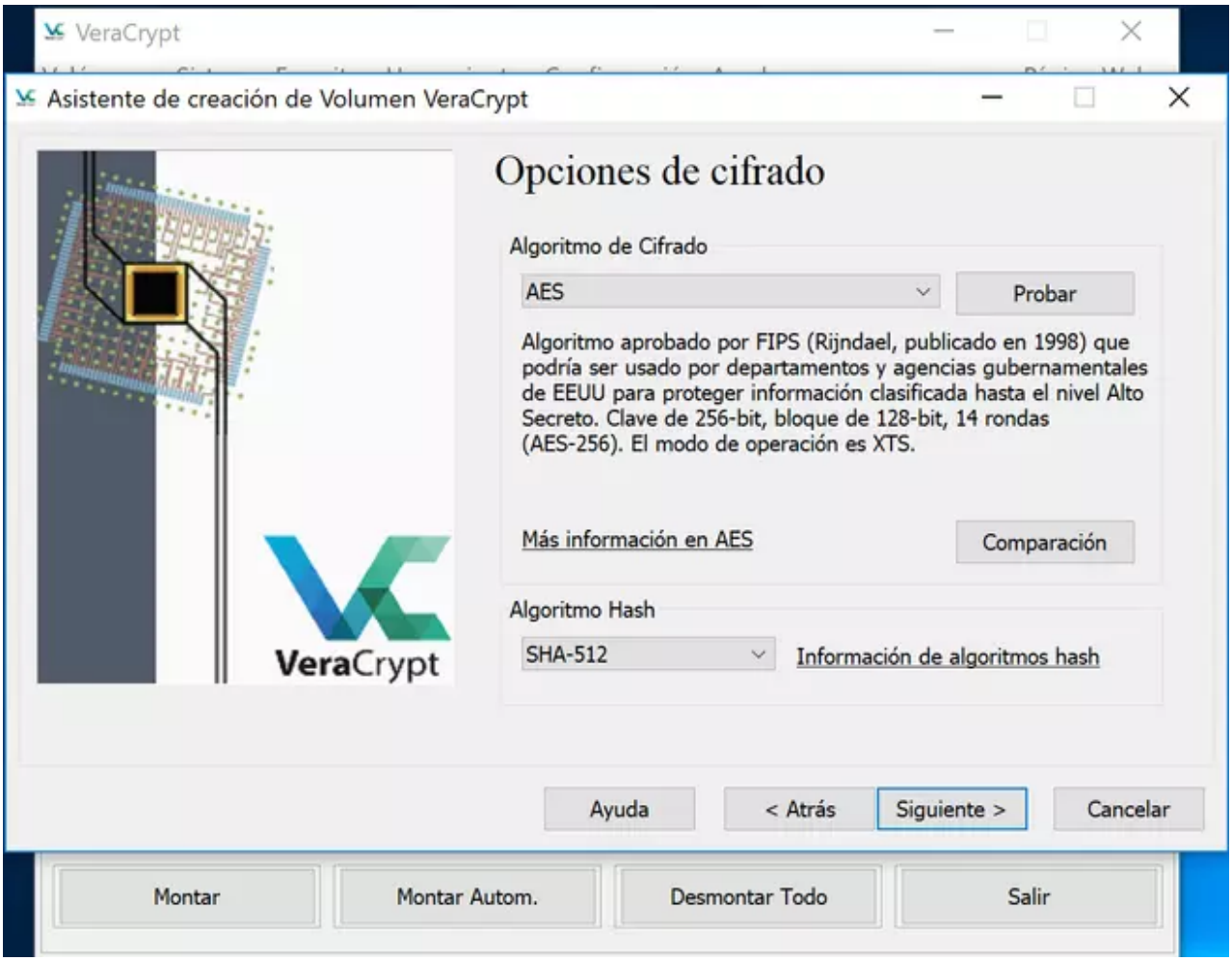

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Tipo de Cifrado del Sistema
Normal
Seleccione esta opción si solamente quiere cifrar la partición del sistema o la unidad del sistema entera.
Oculto
Puede ocurrir que sea ud. obligado por alguien a descifrar el sistema operativo. Hay situaciones en las que no podría negarse a hacerlo (por ejemplo, debido a la extorsión). Si selecciona esta opción, creará un sistema operativo oculto cuya existencia debería ser imposible de demostrar (siempre que se sigan ciertas directrices). De este modo, no tendrá que descifrar o revelar la contraseña del sistema operativo oculto. Haga clic en el siguiente enlace para una explicación más detallada.
Más información
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

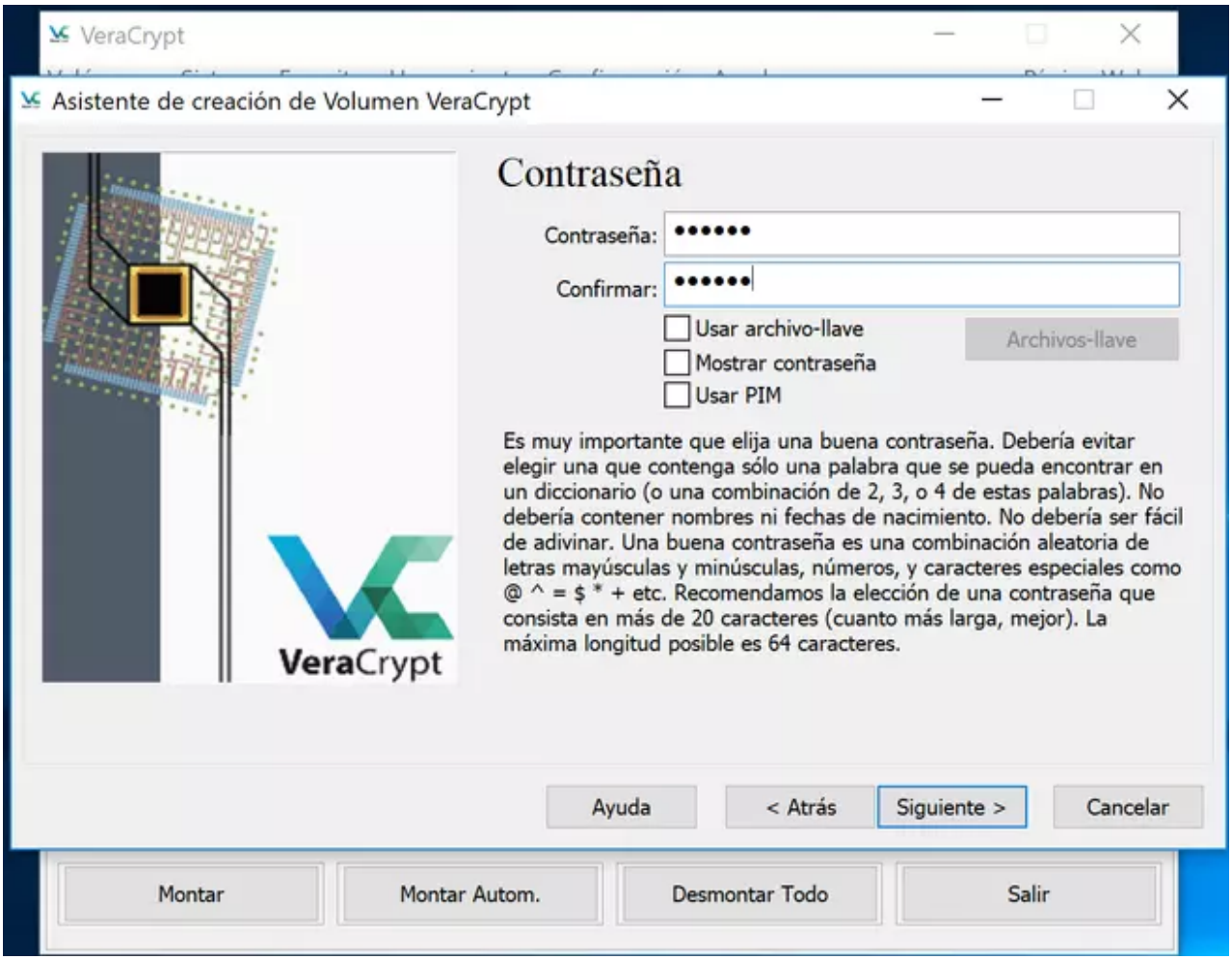


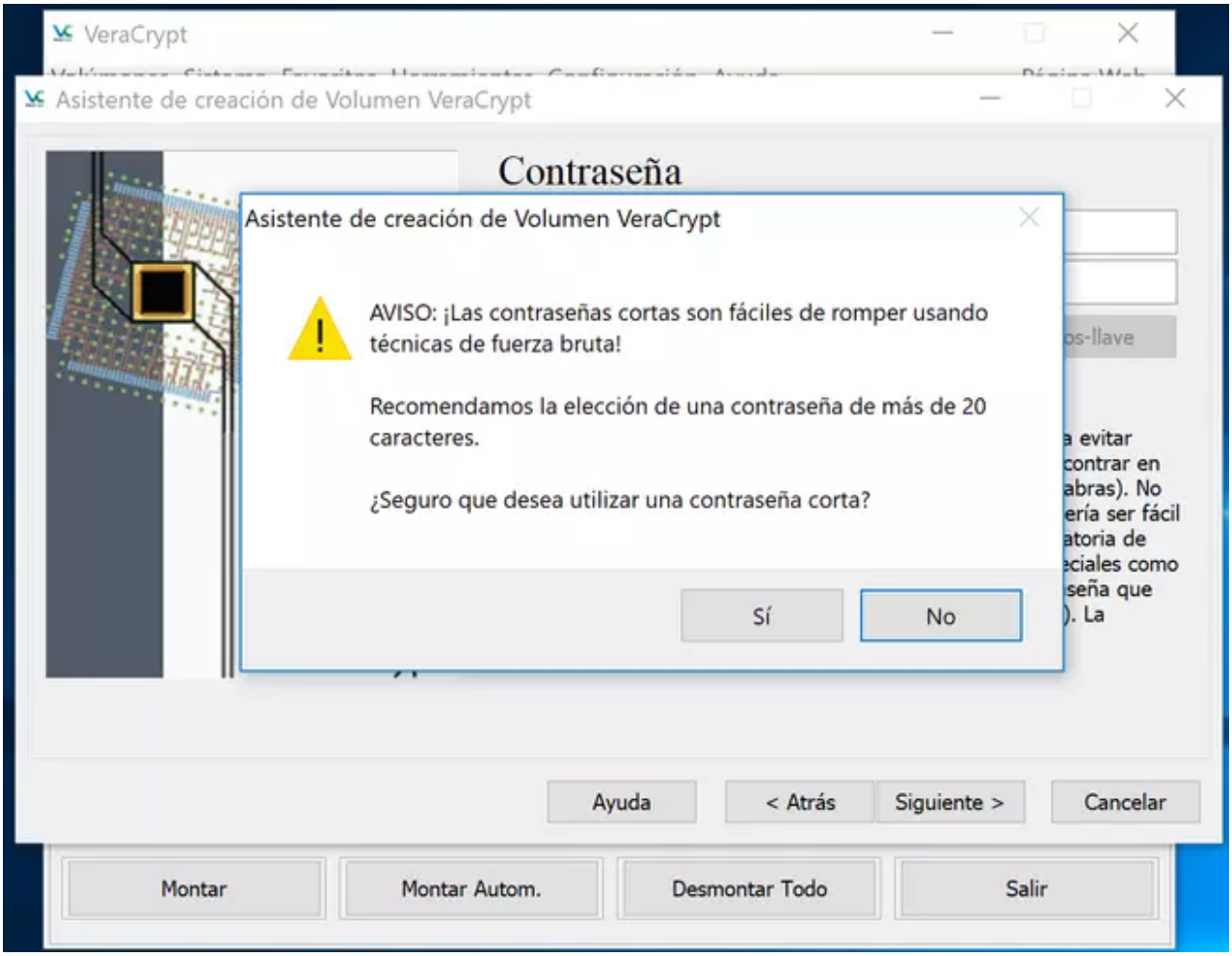
Si nuestro equipo incorpora varios sistemas operativos con multi arranque, tendremos que elegir la opción correspondiente. De lo contrario, elegimos la opción de «**Arranque simple**» tal y como hemos hecho nosotros.

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.

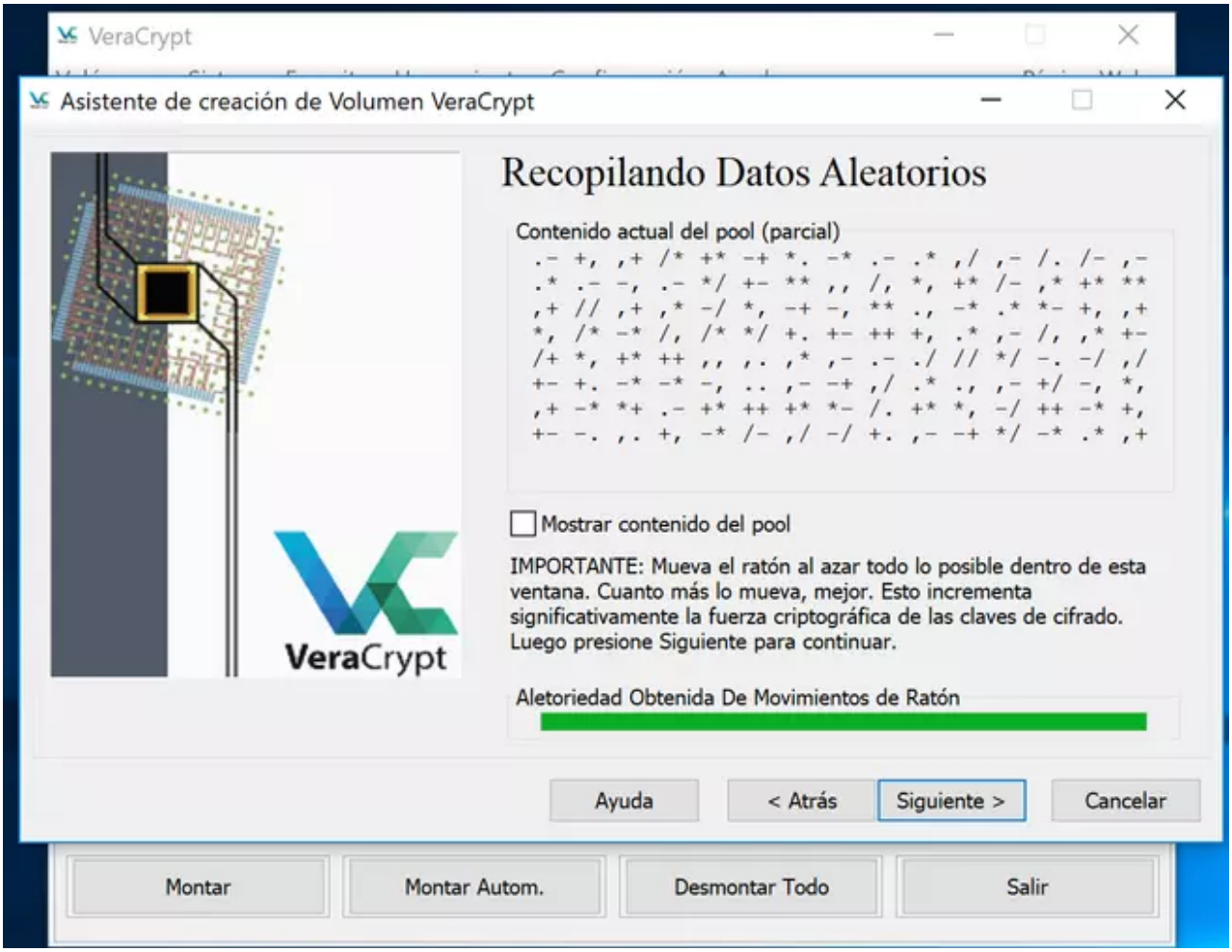

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Número de Sistemas Operativos
Arranque simple
Seleccione esta opción si hay solo un sistema operativo instalado en este ordenador (aunque tenga varios usuarios).
Arranque múltiple
Seleccione esta opción si hay dos o más sistemas operativos instalados en este ordenador.
Por ejemplo:
- Windows XP y Windows XP
- Windows XP y Windows Vista
- Windows y Mac OS X
- Windows y Linux
- Windows, Linux y Mac OS X
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

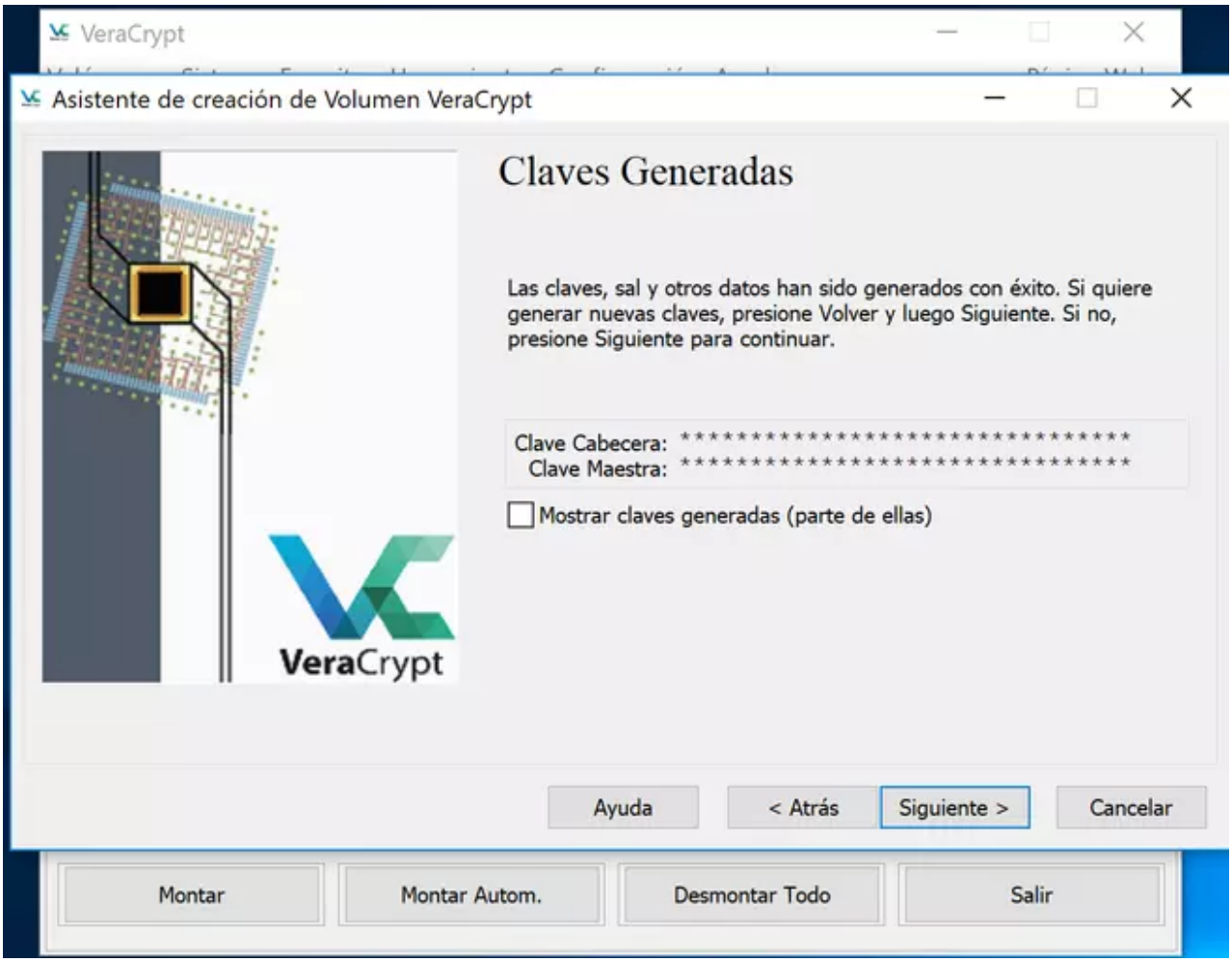

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Opciones de cifrado
Algoritmo de Cifrado
AES
Probar
Algoritmo aprobado por FIPS (Rijndael, publicado en 1998) que podría ser usado por departamentos y agencias gubernamentales de EEUU para proteger información clasificada hasta el nivel Alto Secreto. Clave de 256-bit, bloque de 128-bit, 14 rondas (AES-256). El modo de operación es XTS.
Más información en AES
Comparación
Algoritmo Hash
SHA-512
Información de algoritmos hash
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

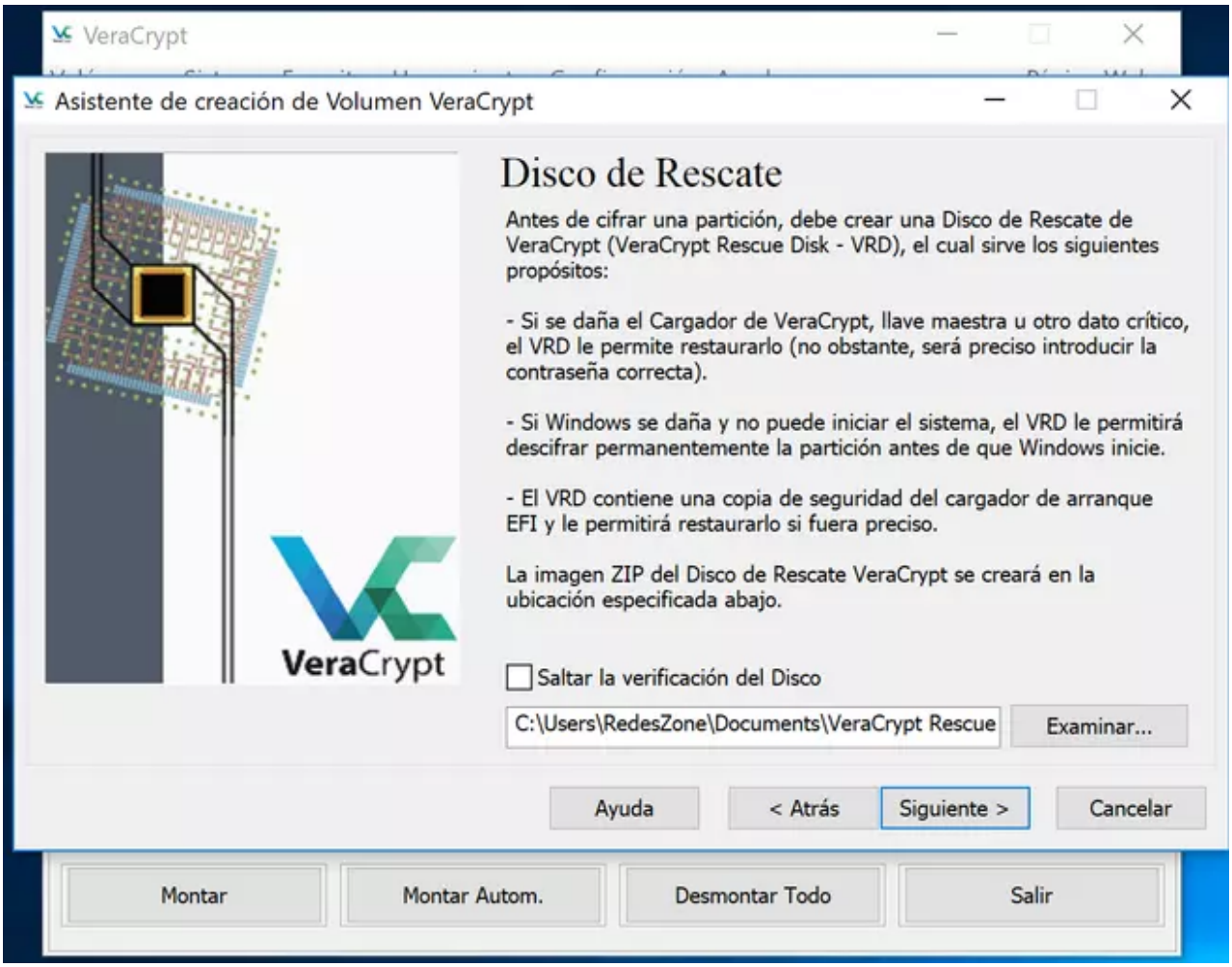

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Contraseña
Contraseña:
Confirmar:
Usar archivo-llave
Archivos-llave
Mostrar contraseña
Usar PIM
Es muy importante que elija una buena contraseña. Debería evitar elegir una que contenga sólo una palabra que se pueda encontrar en un diccionario (o una combinación de 2, 3, o 4 de estas palabras). No debería contener nombres ni fechas de nacimiento. No debería ser fácil de adivinar. Una buena contraseña es una combinación aleatoria de letras mayúsculas y minúsculas, números, y caracteres especiales como @ ^ = $ * + etc. Recomendamos la elección de una contraseña que consista en más de 20 caracteres (cuanto más larga, mejor). La máxima longitud posible es 64 caracteres.
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir


VeraCrypt
Asistente de creación de Volumen VeraCrypt
Contraseña
Asistente de creación de Volumen VeraCrypt
AVISO: ¡Las contraseñas cortas son fáciles de romper usando técnicas de fuerza bruta!
Recomendamos la elección de una contraseña de más de 20 caracteres.
¿Seguro que desea utilizar una contraseña corta?
Sí
No
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

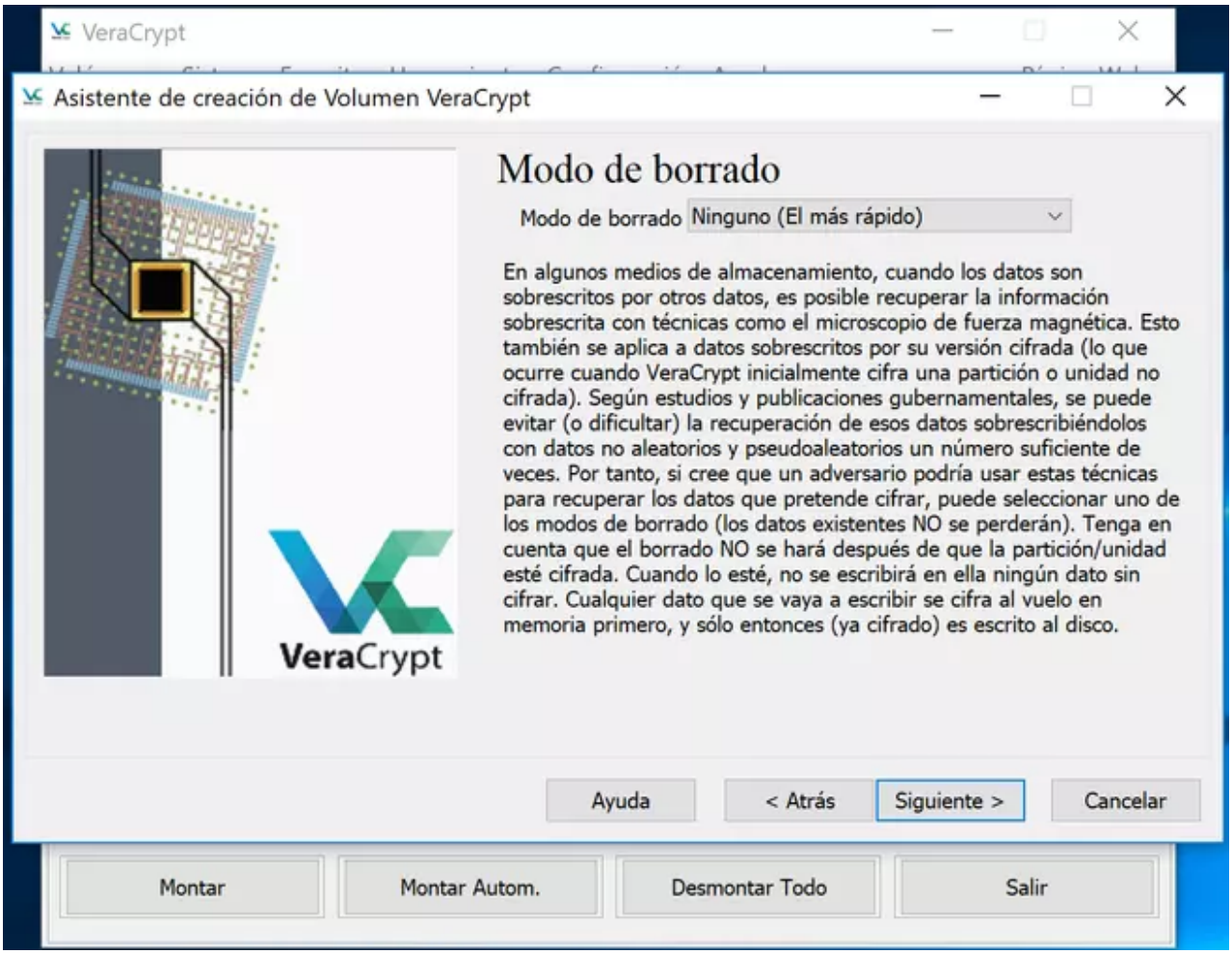
Una vez configurado por completo el volumen, se crearán las claves internas, y nos recomendará crear un disco de rescate por si ocurre algún tipo de problema, poder recuperar toda la información, aunque siempre vamos a tener que introducir la contraseña de acceso.

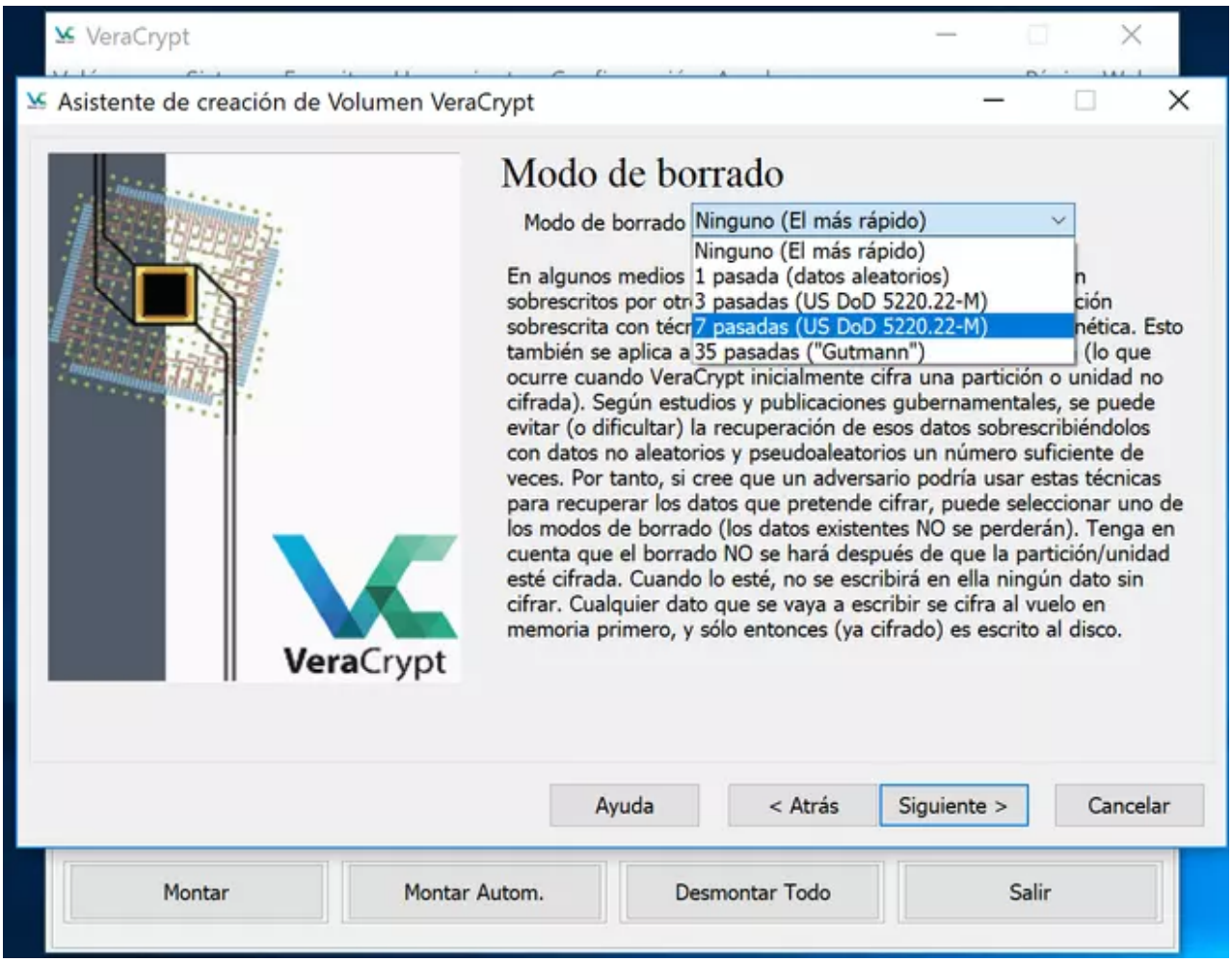


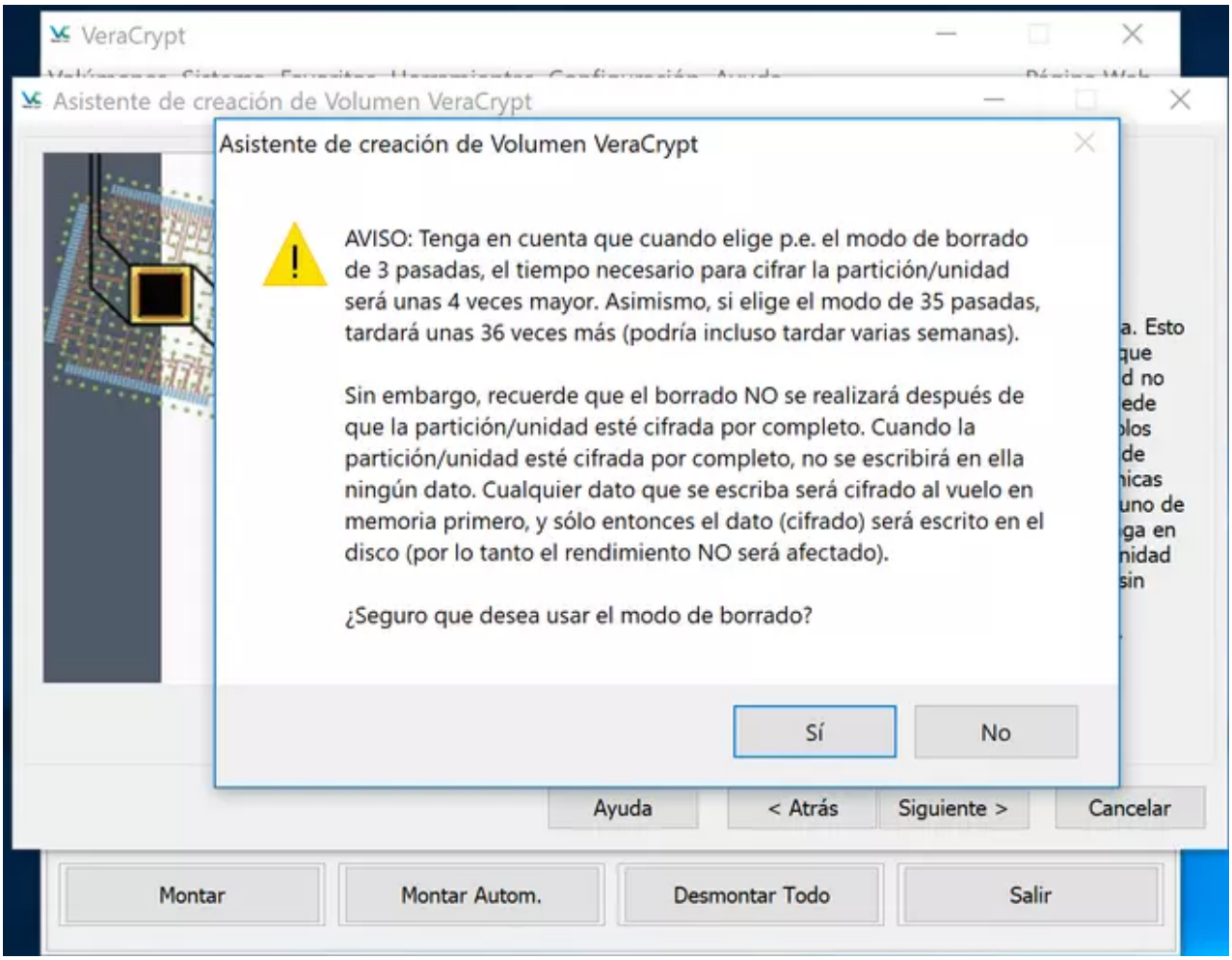

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Claves Generadas
Las claves, sal y otros datos han sido generados con éxito. Si quiere generar nuevas claves, presione Volver y luego Siguiente. Si no, presione Siguiente para continuar.
Clave Cabecera: **********
Clave Maestra: **********
Mostrar claves generadas (parte de ellas)
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir


VeraCrypt
Asistente de creación de Volumen VeraCrypt
Disco de Rescate
Antes de cifrar una partición, debe crear una Disco de Rescate de VeraCrypt (VeraCrypt Rescue Disk - VRD), el cual sirve los siguientes propósitos:
- Si se daña el Cargador de VeraCrypt, llave maestra u otro dato crítico, el VRD le permite restaurarlo (no obstante, será preciso introducir la contraseña correcta).
- Si Windows se daña y no puede iniciar el sistema, el VRD le permitirá descifrar permanentemente la partición antes de que Windows inicie.
- El VRD contiene una copia de seguridad del cargador de arranque EFI y le permitirá restaurarlo si fuera preciso.
La imagen ZIP del Disco de Rescate VeraCrypt se creará en la ubicación especificada abajo.
Saltar la verificación del Disco
C:\Users\RedesZone\Documents\VeraCrypt Rescue
Examinar...
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

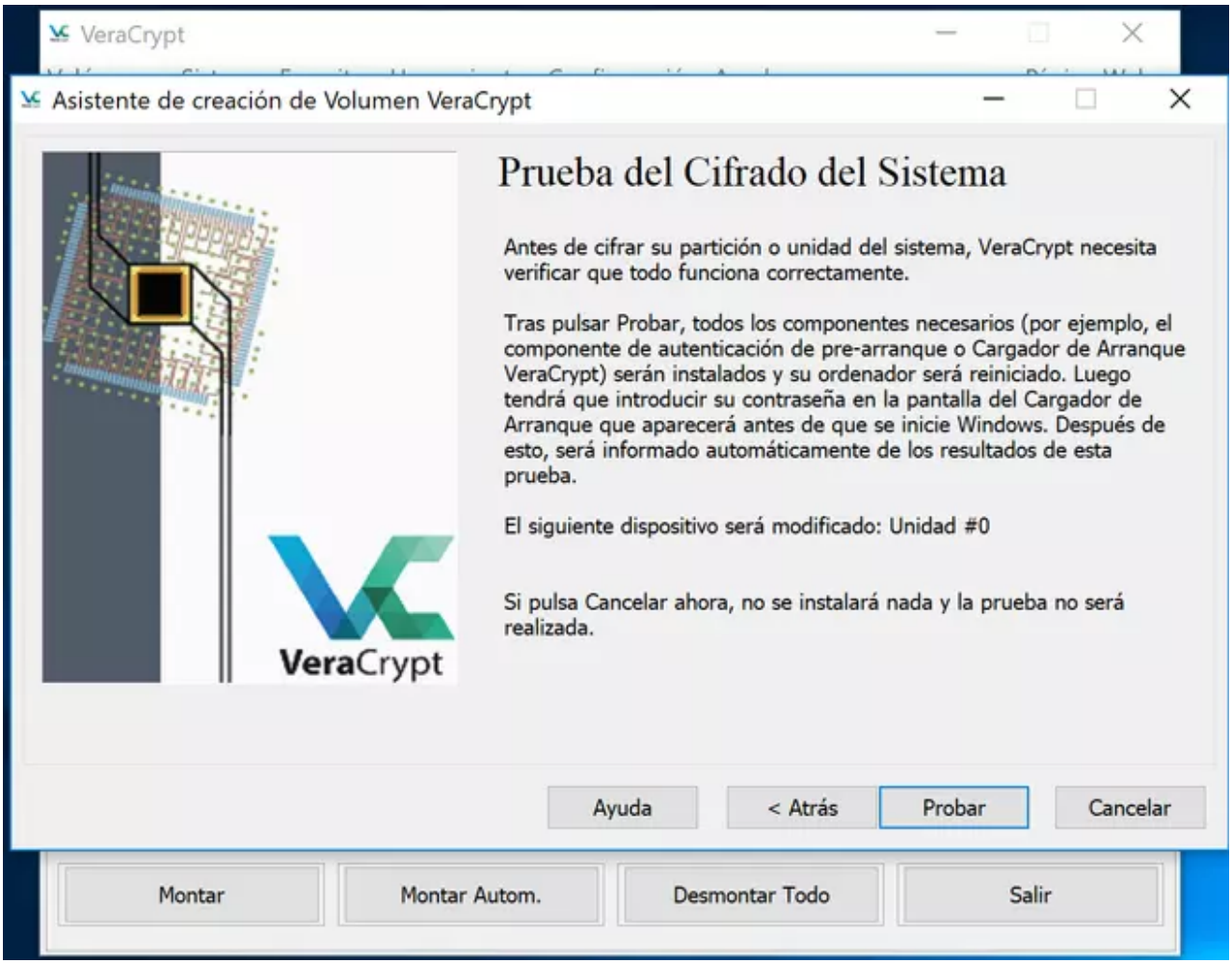
También tenemos la posibilidad de seleccionar la política si borramos algún archivo dentro del propio sistema operativo, y es que nos va a permitir utilizar diferentes métodos de borrado seguro, ideal para mantener nuestra privacidad.

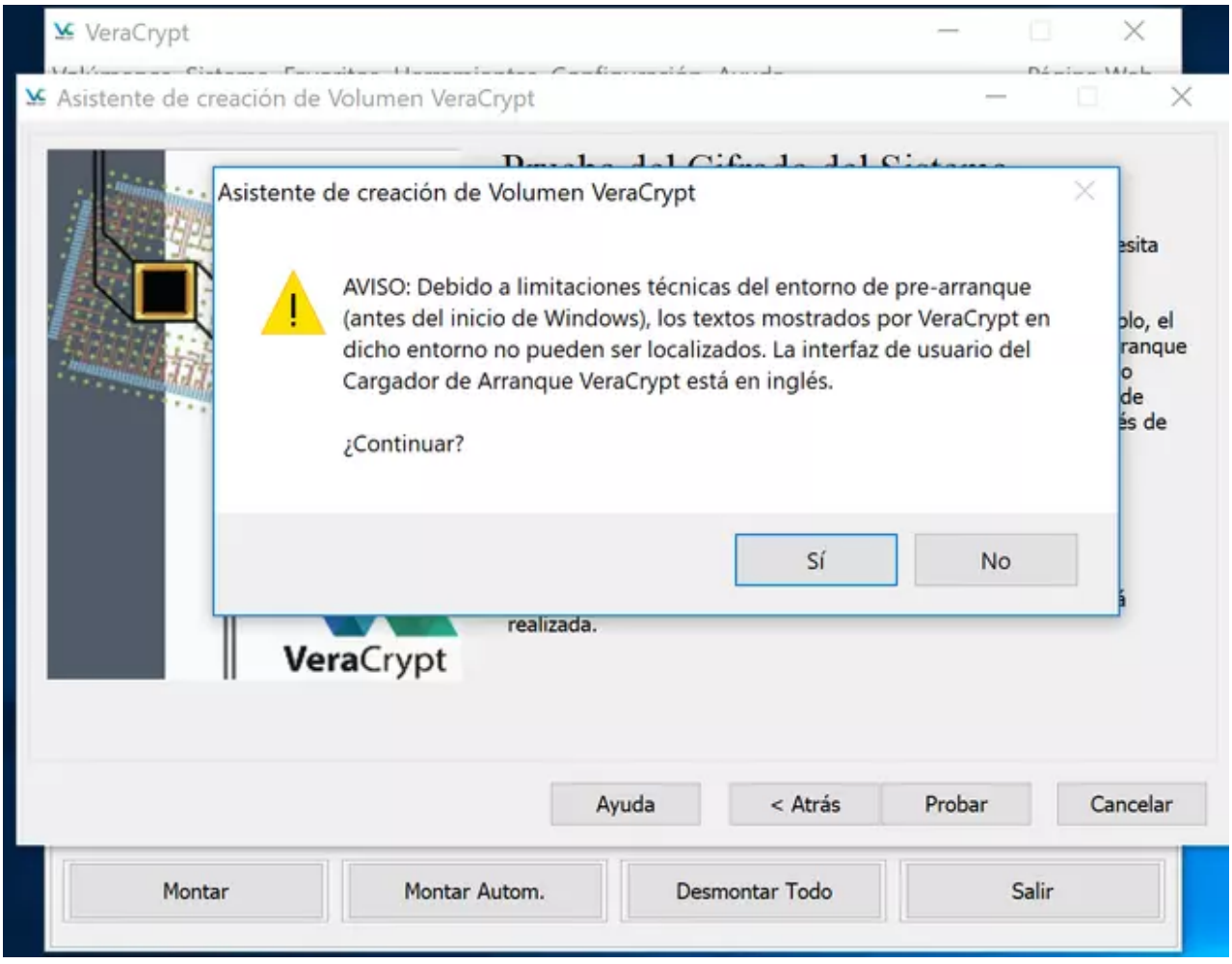

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Modo de borrado
Modo de borrado
Ninguno (El más rápido)
En algunos medios de almacenamiento, cuando los datos son sobrescritos por otros datos, es posible recuperar la información sobrescrita con técnicas como el microscopio de fuerza magnética. Esto también se aplica a datos sobrescritos por su versión cifrada (lo que ocurre cuando VeraCrypt inicialmente cifra una partición o unidad no cifrada). Según estudios y publicaciones gubernamentales, se puede evitar (o dificultar) la recuperación de esos datos sobrescribiéndolos con datos no aleatorios y pseudoaleatorios un número suficiente de veces. Por tanto, si cree que un adversario podría usar estas técnicas para recuperar los datos que pretende cifrar, puede seleccionar uno de los modos de borrado (los datos existentes NO se perderán). Tenga en cuenta que el borrado NO se hará después de que la partición/unidad esté cifrada. Cuando lo esté, no se escribirá en ella ningún dato sin cifrar. Cualquier dato que se vaya a escribir se cifra al vuelo en memoria primero, y sólo entonces (ya cifrado) es escrito al disco.
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir

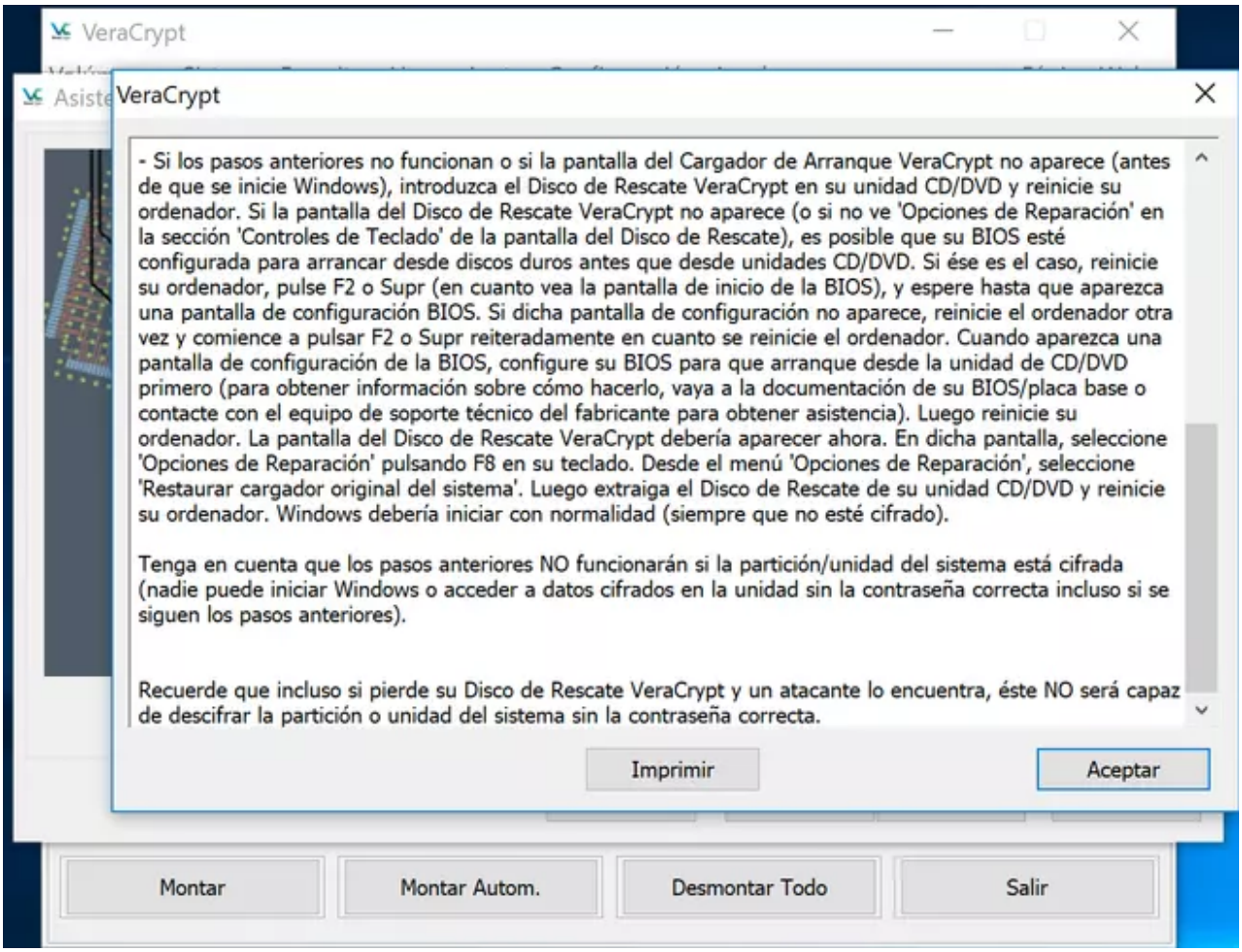

VeraCrypt
Asistente de creación de Volumen VeraCrypt
Modo de borrado
Modo de borrado
Ninguno (El más rápido)
Ninguno (El más rápido)
1 pasada (datos aleatorios)
3 pasadas (US DoD 5220.22-M)
7 pasadas (US DoD 5220.22-M)
35 pasadas ("Gutmann")
En algunos medios
sobrescritos por otr
sobrescrita con técr
también se aplica a
(lo que
ocurre cuando VeraCrypt inicialmente cifra una partición o unidad no cifrada). Según estudios y publicaciones gubernamentales, se puede evitar (o dificultar) la recuperación de esos datos sobrescribiéndolos con datos no aleatorios y pseudoaleatorios un número suficiente de veces. Por tanto, si cree que un adversario podría usar estas técnicas para recuperar los datos que pretende cifrar, puede seleccionar uno de los modos de borrado (los datos existentes NO se perderán). Tenga en cuenta que el borrado NO se hará después de que la partición/unidad esté cifrada. Cuando lo esté, no se escribirá en ella ningún dato sin cifrar. Cualquier dato que se vaya a escribir se cifra al vuelo en memoria primero, y sólo entonces (ya cifrado) es escrito al disco.
VeraCrypt
Ayuda
< Atrás
Siguiente >
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir



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.


VeraCrypt
Asistente de creación de Volumen VeraCrypt
Prueba del Cifrado del Sistema
Antes de cifrar su partición o unidad del sistema, VeraCrypt necesita verificar que todo funciona correctamente.
Tras pulsar Probar, todos los componentes necesarios (por ejemplo, el componente de autenticación de pre-arranque o Cargador de Arranque VeraCrypt) serán instalados y su ordenador será reiniciado. Luego tendrá que introducir su contraseña en la pantalla del Cargador de Arranque que aparecerá antes de que se inicie Windows. Después de esto, será informado automáticamente de los resultados de esta prueba.
El siguiente dispositivo será modificado: Unidad #0
Si pulsa Cancelar ahora, no se instalará nada y la prueba no será realizada.
VeraCrypt
Ayuda
< Atrás
Probar
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir


VeraCrypt
Asistente de creación de Volumen VeraCrypt
Asistente de creación de Volumen VeraCrypt
AVISO: Debido a limitaciones técnicas del entorno de pre-arranque (antes del inicio de Windows), los textos mostrados por VeraCrypt en dicho entorno no pueden ser localizados. La interfaz de usuario del Cargador de Arranque VeraCrypt está en inglés.
¿Continuar?
Sí
No
realizada.
VeraCrypt
Ayuda
< Atrás
Probar
Cancelar
Montar
Montar Autom.
Desmontar Todo
Salir



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.


PlatformInfo create Unsupported
Password: _

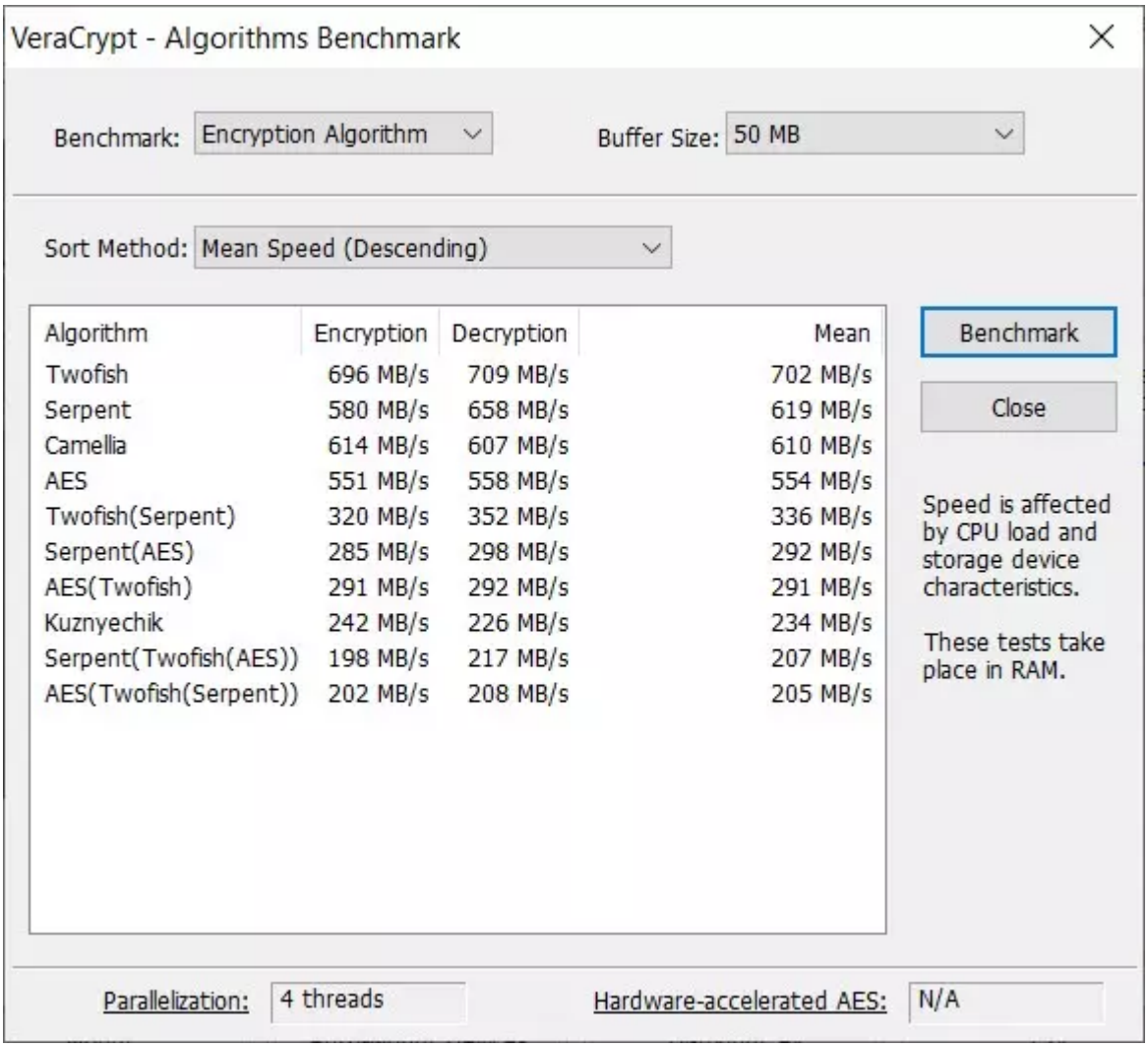

PlatformInfo create Unsupported
Password: *
PIM (Leave empty for default): _


PlatformInfo create Unsupported
Password: *
PIM (Leave empty for default):
Authorizing...
Success
Start 0 644874240 len 0

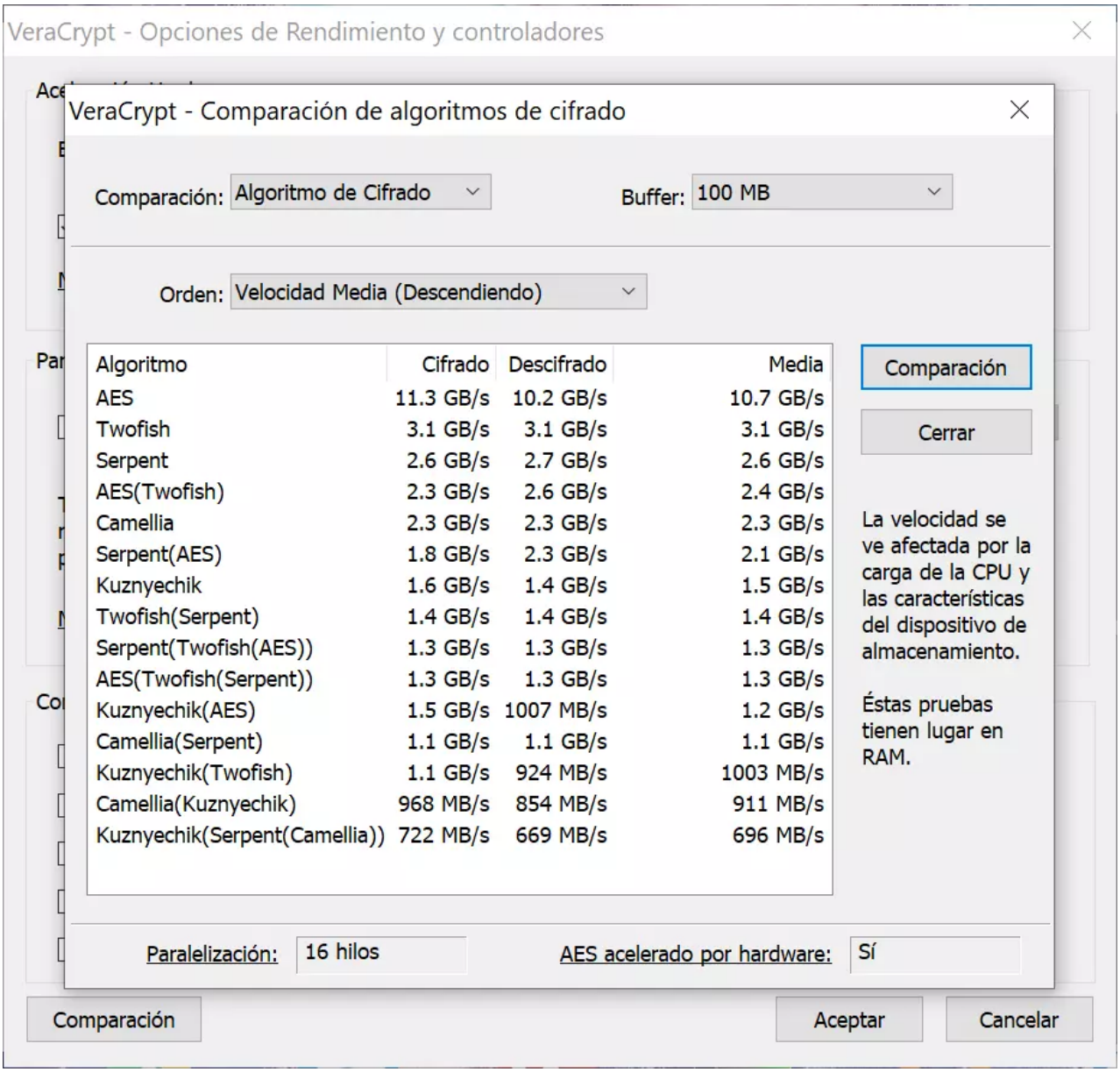
Tal y como habéis visto en este completo tutorial, VeraCrypt es una de las formas más fácil y rápidas para crear contenedores cifrados, cifrar dispositivos USB o discos duros enteros, e incluso cifrar la partición donde almacenamos nuestro sistema operativo. Un aspecto muy importante cuando vayamos a usar VeraCrypt, es elegir correctamente el algoritmo de cifrado simétrico, nuestra recomendación es AES por varios motivos:

- Es actualmente el estándar, y no se conocen vulnerabilidades
- Los procesadores nuevos incorporan el juego de instrucciones AES-NI, esto significa que tendremos aceleración de cifrado por hardware, de tal forma que tengamos una gran velocidad de lectura/escritura.

Para que veáis la gran diferencia de rendimiento entre un procesador SIN AES-NI, y un procesador con AES-NI, en la siguiente imagen podéis ver el rendimiento que obtenemos con un procesador Intel i5 760 del año 2010, el cual no tiene esta tecnología, y, por tanto, obtendremos una velocidad de lectura/escritura muy baja:



Si utilizamos nuestro nuevo procesador AMD Ryzen 7 3800X que sí tiene la tecnología AES-NI, podremos ver que llegamos fácilmente a más de 10GB/s de velocidad, por supuesto, actualmente no hay disco duro o SSD capaz de gestionar tan altas velocidades:



Aunque este último procesador es mucho más potente, la diferencia sustancial la encontramos en el «AES acelerado por hardware», ya que es cuando realmente notamos una grandísima diferencia entre ambos procesadores.

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.