

Protección de la información en mi ordenador. *VeraCrypt* aplicación para cifrar y proteger la información

La manera de evitar los problemas derivados de que la información privada quede expuesta a personas no autorizadas es sencilla: basta con **cifrar la información**, es decir, almacenarla codificada de tal forma que no pueda acceder a ella alguien que no conozca la **contraseña de cifrado**.

Muchas son las ocasiones en que nos interesa cifrar un archivo:

- Documentos privados almacenados en un ordenador que compartimos o son accesibles a otras personas.
- Documentos almacenados en un portátil, en una unidad usb u otro soporte externo que puede ser susceptible de robo o pérdida.
- Documentos confidenciales adjuntados en un correo electrónico. Los correos que enviamos a través de internet pueden fácilmente ser interceptados por terceras personas. Por otro lado, mientras éstos permanecen en un servidor, pueden estar accesible a terceras personas.

En situaciones como las anteriores puede ser obligado cifrar los documentos. Por supuesto es obligatorio cuando estamos trabajando con datos personales de ficheros declarados de nivel medio-alto de la Universidad de Zaragoza en la Agencia de Protección de Datos .

VeraCrypt es una herramienta sucesora de *TrueCrypt*, aplicación discontinuada por sus desarrolladores, que nos permite crear un volumen cifrado que podemos trasladar con seguridad.

Los datos almacenados en un volumen cifrado por **VeraCrypt** quedan ocultos y protegidos de tal forma que sólo se puede acceder a ellos conociendo la contraseña que permite montar un volumen de disco como una unidad/disco virtual. Por ello, es muy importante conocer y **no olvidar dicha contraseña**.

VeraCrypt es un desarrollo de software libre, que se encuentra disponible para los sistemas Windows, Linux y MacOSX

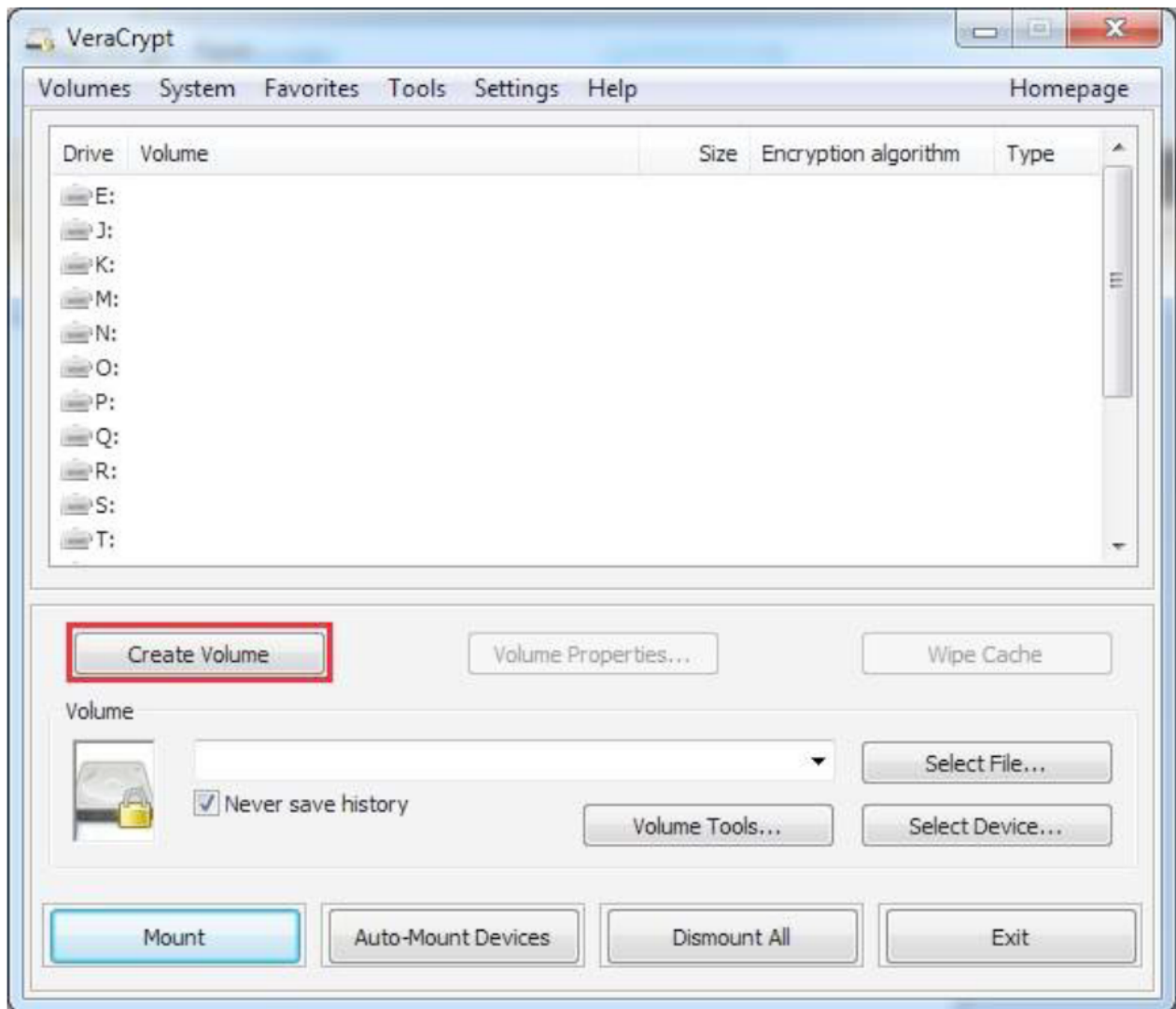
Instalación de *VeraCrypt*

Lo primero que haremos será descargarnos la aplicación de la web oficial <https://veracrypt.codeplex.com/> desde la sección *Download* y elegir la última versión estable para nuestra plataforma.

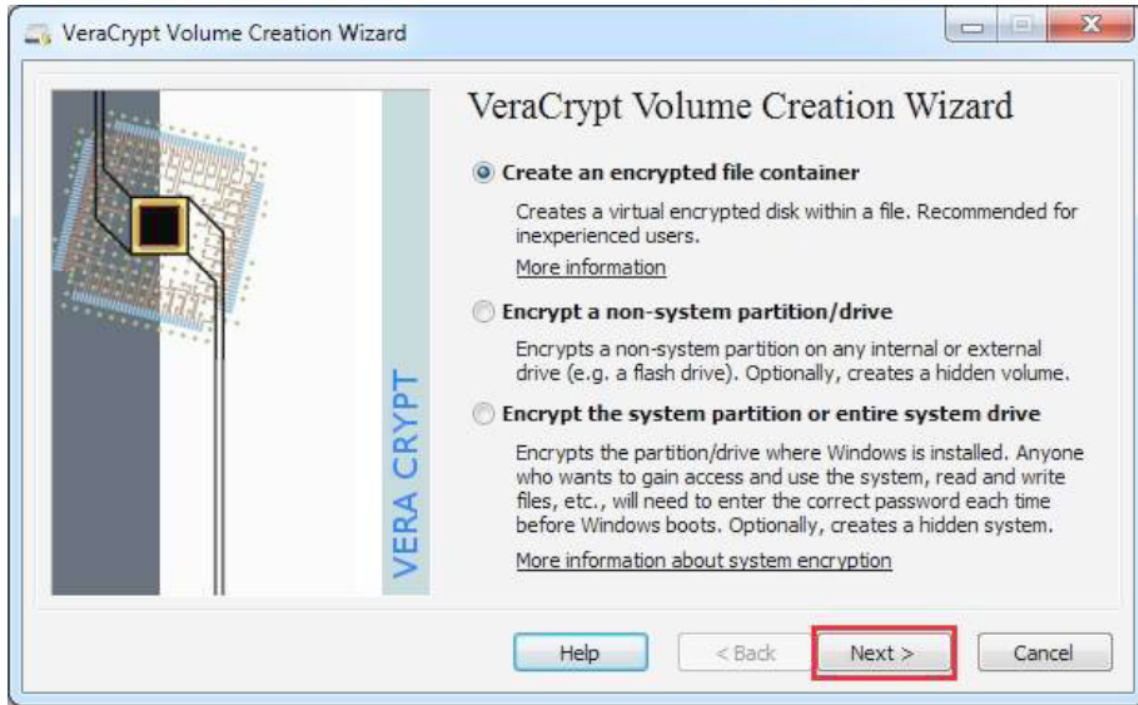
Uso de la aplicación *VeraCrypt*

Cuando lanzamos la aplicación ésta será la pantalla principal de funcionamiento. Lo que haremos es crear en un fichero de nuestro equipo un volumen/unidad de disco, o también en un dispositivo USB, Dropbox, GoogleDrive, ...puesto que se trata de usar un fichero para convertirlo en un volumen.

Seleccionaremos la opción **“Create Volume”**



Elegiremos donde queremos crear el volumen, **en un fichero cifrado**, en una partición en un "drive". En este tutorial elegiremos la primera opción, opción por defecto, y marcaremos **Next**.



Creamos un **volumen de tipo común**. En este tutorial elegiremos la primera opción, opción por defecto, y marcaremos **Next**

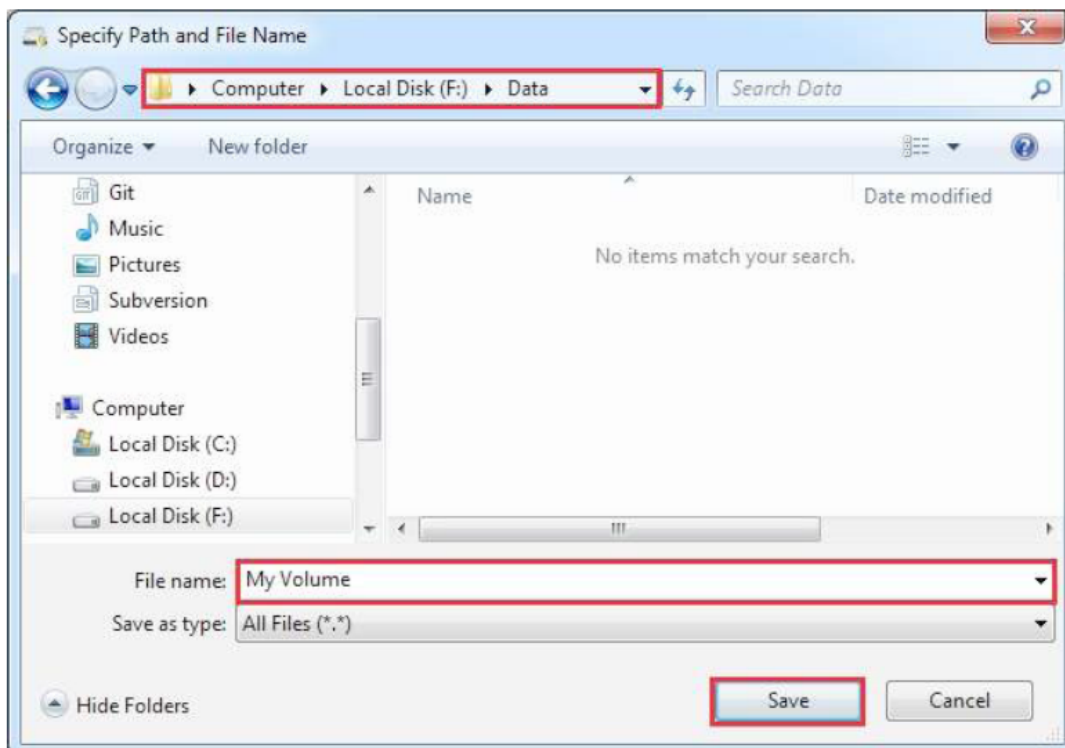


Seguimos el asistente para la creación de volúmenes y decidimos en que unidad y que nombre de fichero le vamos a dar para contener nuestro volumen/unidad de disco .
Seleccionaremos el fichero:



En este tutorial el fichero sobre el que se creara el “volumen” VeraCrypt lo llamamos

F:\Data\ y el nombre del “volumen” será My Volume.



Seleccionaremos **el tipo de cifrado**

Encryption Options

Encryption Algorithm

AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

[More information on AES](#)

Hash Algorithm

SHA-512 [Information on hash algorithms](#)

A continuación elegimos el **tamaño** para nuestro **volumen/** unidad virtual. Será el adecuado a nuestras necesidades.

Volume Size

KB MB GB


Free space on drive F:\ is 27.87 GB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KB.
The minimum possible size of an NTFS volume is 3792 KB.

Se nos pide una **contraseña**. Hay que tener presente que dicha contraseña será la que en el futuro usaremos para montar y usar el volumen que estamos creando.



Volume Password

Password: [Redacted]

Confirm: [Redacted]

Use keyfiles Keyfiles...

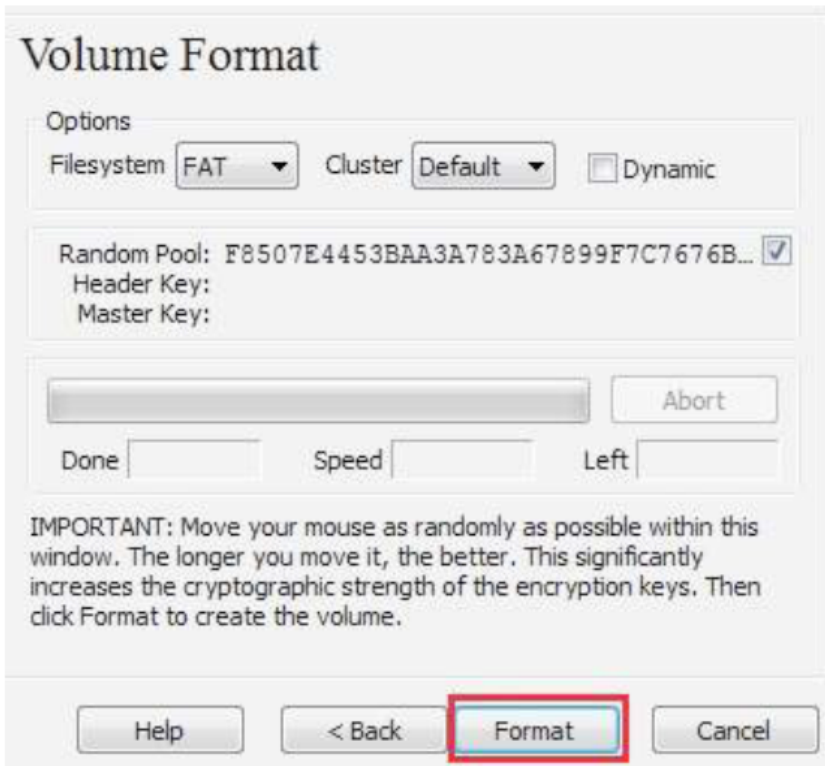
Display password

Use PIM

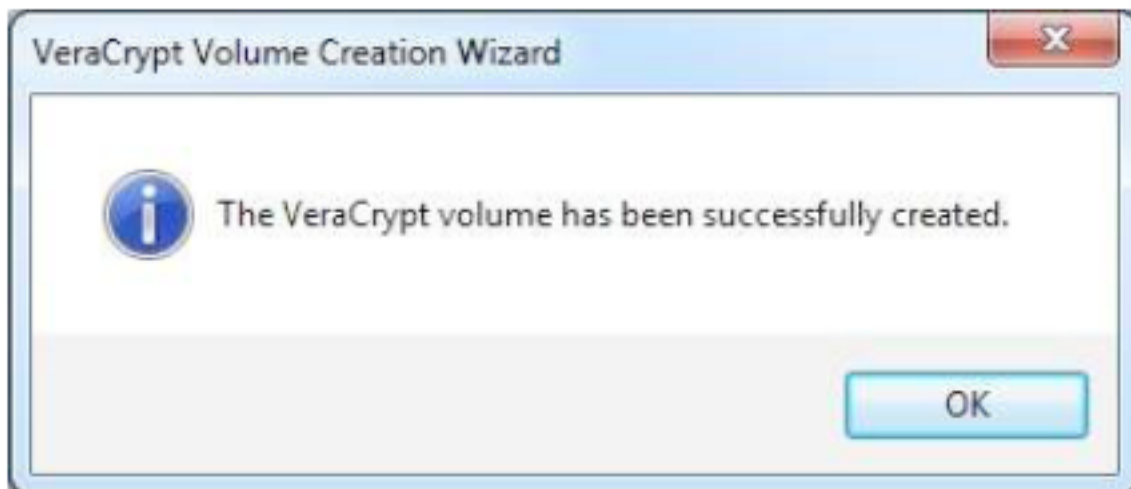
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

Help < Back **Next >** Cancel

Procedemos a dar **formato al volumen** creado:



Al finalizar el formato que puede llevar más de 30 segundos, aparecerá el siguiente diálogo que cerraremos marcando OK

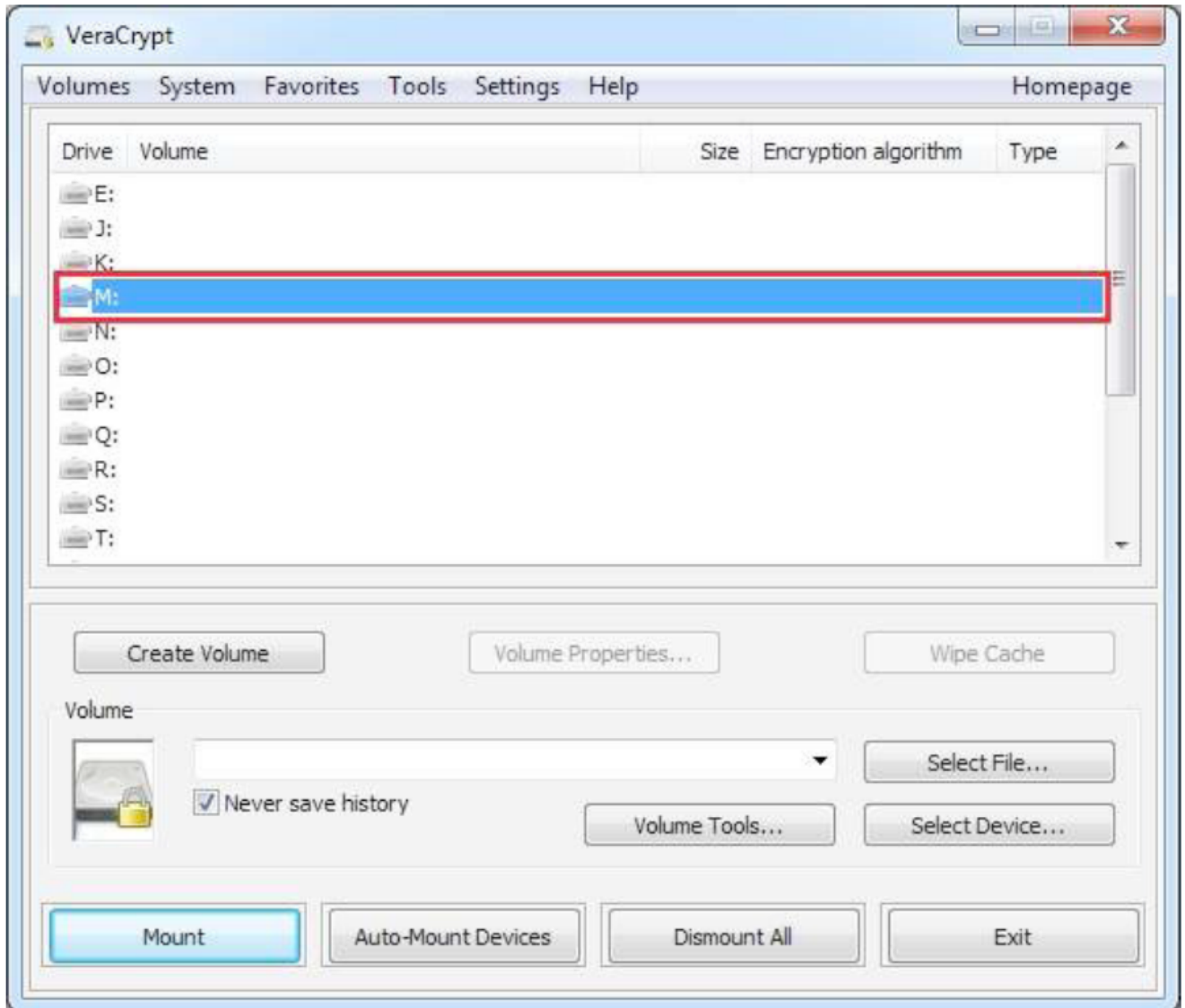


La aplicación nos permite crear otro volumen si seleccionamos Next. Si no lo deseamos saldremos de la misma marcando **Exit**

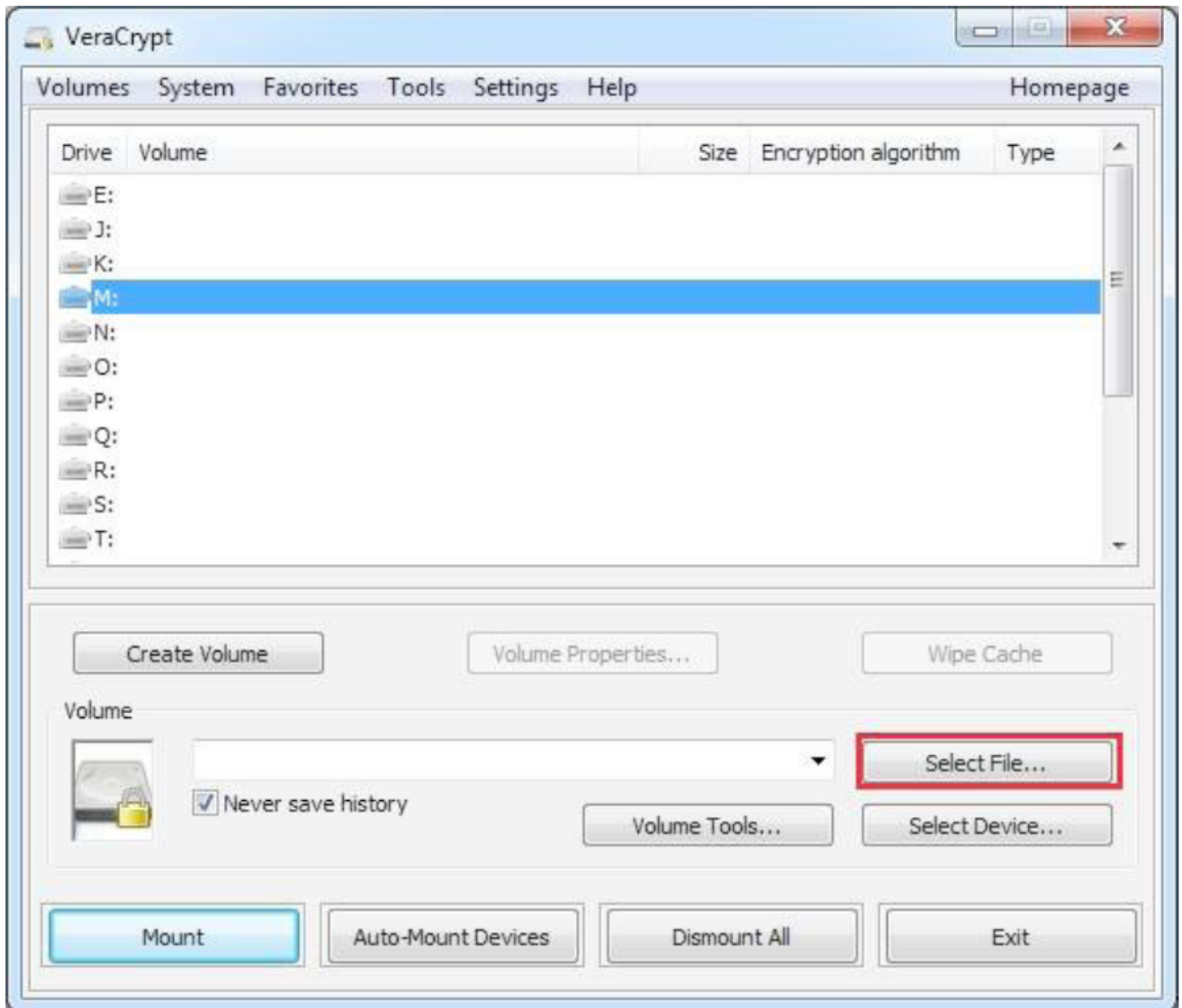


Y ya podemos proceder a usar la unidad creada:

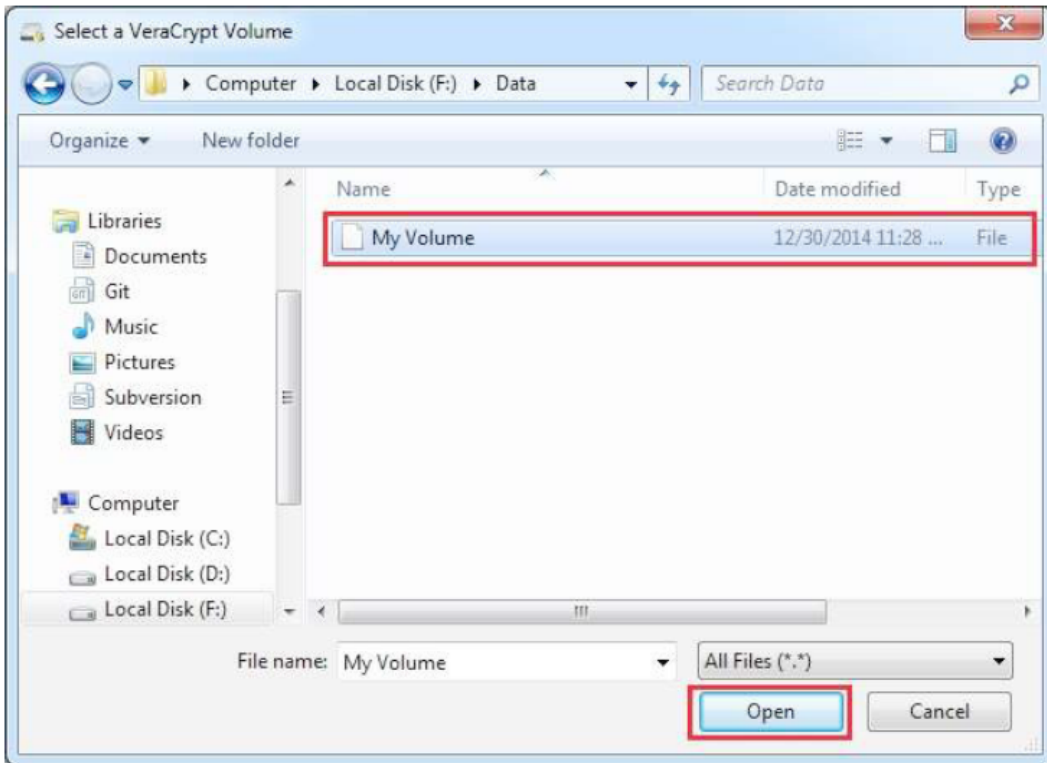
Desde la aplicación VeraCrypt, elegimos una letra para asignar a la unidad



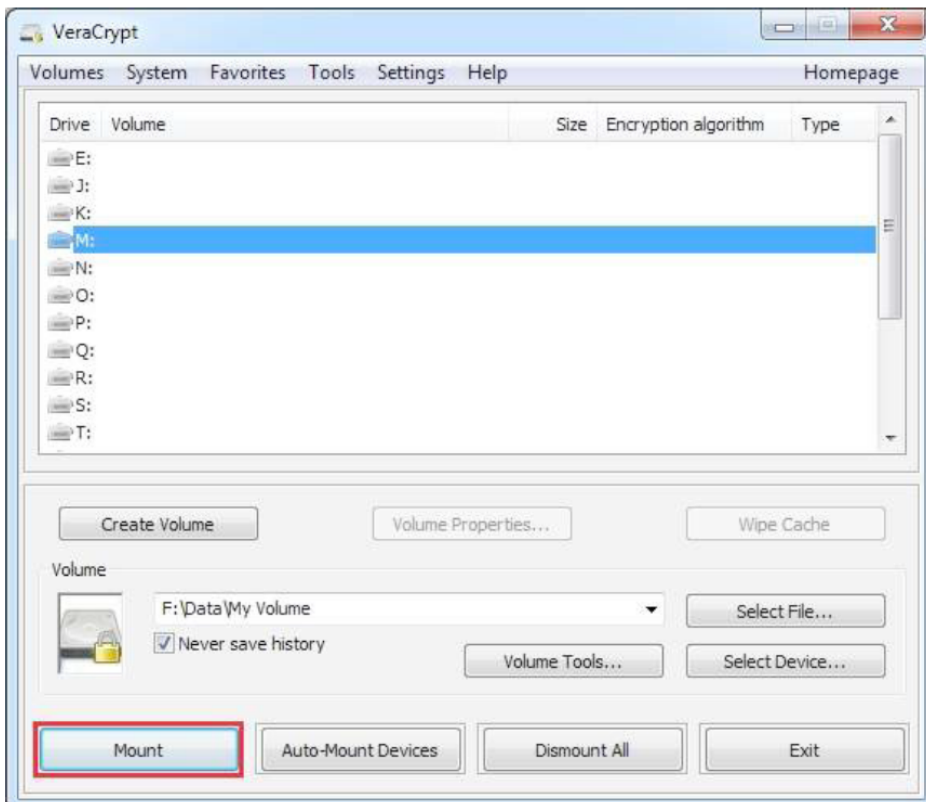
Seleccionamos el volumen creado.



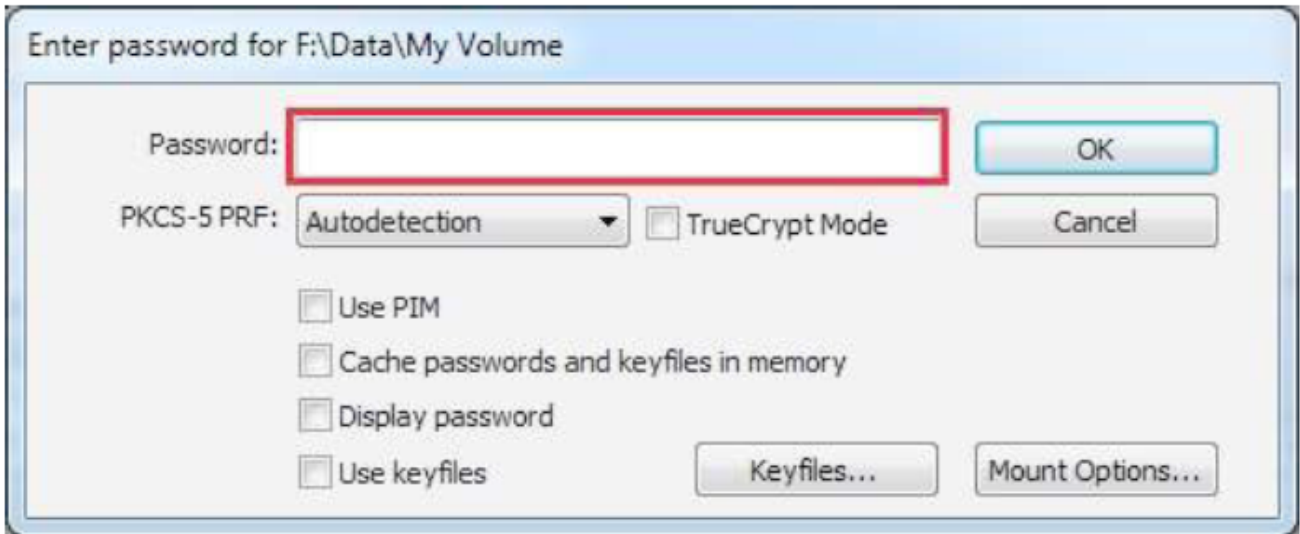
Una vez localizado marcaremos **Open**



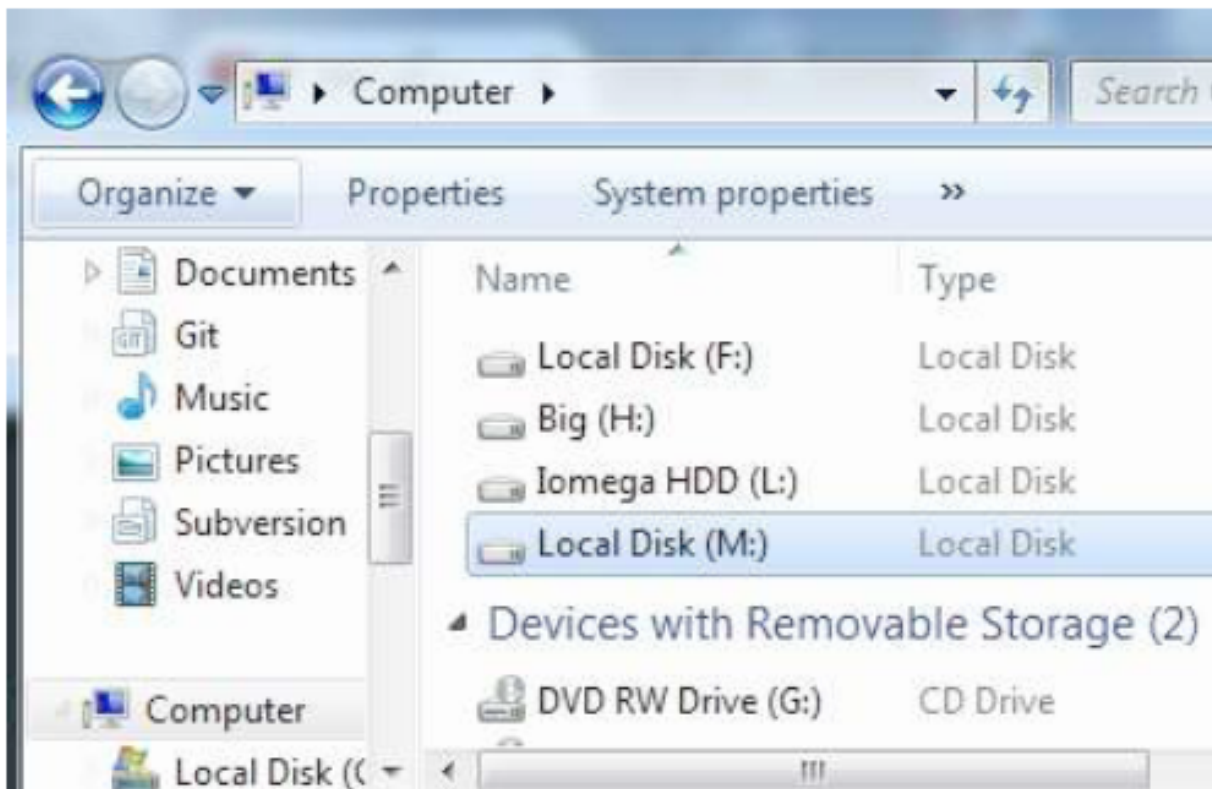
Y montaremos el volumen marcando **Mount**:



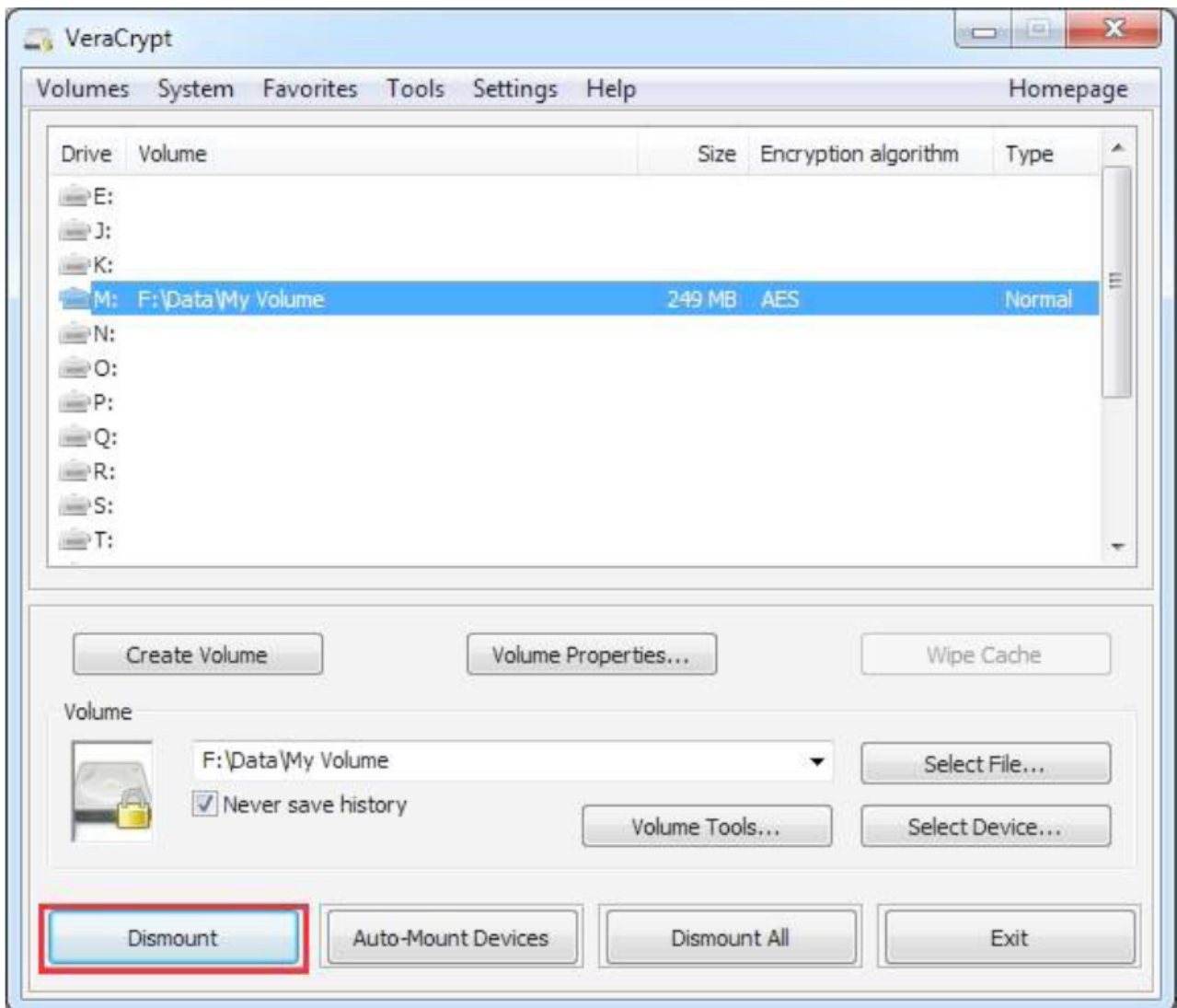
Al seleccionar Mount se nos pedirá la contraseña de protección y con ello ya tendremos nuestra **unidad montada y lista para usar**.



Si miramos en nuestro equipo veremos el volumen creado como cualquier otra unidad de nuestro equipo.



Para dejar de usarla basta con seleccionar **Dismount**



REFERENCIAS

- VERACRYPT (FREE OPEN-SOURCE ON -THE-FLY ENCRYPTION).- USER´S GUIDE, versión 1.16.- Released by IDRIX on October 7, 2015 (veracrypt.codeplex.com)
- CIFRADO_TrueCrypt.pdf. Tutorial SICUZ