VeraCrypt: el cifrado es tu mejor aliado

Contenido

Qué es el cifrado

El cifrado es el proceso mediante el cual se transforman datos de tal forma que estos son comprensibles únicamente para las partes (personas, computadoras, etc.) que disponen de la clave de cifrado. De este modo, datos legibles públicamente se transforman en datos confidenciales y, por ello, el cifrado es la técnica por excelencia para abordar la dimensión de la confidencialidad en la seguridad de la información.

Para conseguir esto, existen diferentes tipos de cifrado (simétrico, asimétrico) y varios algoritmos de cifrado, unos más seguros y rápidos que otros. La utilización de los tipos de cifrado es dependiente de la casuística, ya que el cifrado se utiliza en casos muy diversos y mediante el uso de diferentes algoritmos (RSA, AES, Serpent) y protocolos (un mismo protocolo puede usar varios algoritmos): cifrado de mensajes de chat (Signal, OMEMO, OTR), cifrado de correo (PGP), cifrado de comunicaciones (SSL), cifrado de archivos (VeraCrypt), etc. Muchos de los algoritmos son utilizados para diferentes casos, es decir, que alternativamente pueden utilizarse, por ejemplo, para cifrar comunicaciones y para cifrar archivos.

En esta guía nos interesa explorar un caso de uso en concreto, que es el del cifrado de archivos y soportes de información (discos duros, unidades de almacenamiento

USB, tarjetas micro SD, etc.), ya que es de gran utilidad para mantener en secreto los archivos sensibles de la militancia, como prevención ante una posible redada. Para ello, una herramienta puntera es VeraCrypt.

Casos de uso en la militancia

Los casos de uso para el cifrado en la militancia son muchos y todos altamente recomendables. Es más, es necesario que comprendamos la importancia de almacenar cifrados todos y cada uno de los archivos sensibles y no tan sensibles del ámbito militante: actas de reuniones, documentos internos, cartelería, correos, artículos, etc.

Cuando la policía llama a (o derriba) la puerta de casa de un militante político investigado, una de las primeras cosas que intentará hacer es confiscar el material informático y clonar los discos duros, para extraer de ellos toda la información que pueda asociar al militante con actividades a ser juzgadas. Cuando los discos duros y, en general, los archivos no están cifrados, la labor de la policía es trivial: extraer los archivos, consultarlos y utilizarlos para inculpar al militante. Ahora bien, si estos archivos están cifrados, la labor policial se dificulta. Porque si no hay ningún archivo relacionado con la militancia que no esté cifrado, la policía no podrá obtener ningún tipo de prueba ni ningún secreto de organización hasta que no descifre los archivos. Y descifrar no es tarea fácil, mucho menos con los algoritmos que utiliza VeraCrypt, prácticamente imposibles de descifrar sin invertir una gran potencia computacional y, sobre todo, tiempo. Como todas las herramientas informáticas, el cifrado tiene sus límites: mediante fuerza bruta (prueba-error) podría adivinarse la clave de cifrado (de ahí la importancia de utilizar buenas claves), mediante mecanismos heurísticos puede romperse el cifrado, algunos algoritmos son vulnerables y otros dependen de la longitud de la clave para medir su seguridad (por ejemplo, un algoritmo puede ser inseguro con una clave de 128 bits, pero altamente seguro con una clave de 256 bits). Lo importante es tener en cuenta, como decimos siempre, que es mejor utilizar una herramienta que aporta seguridad, en este caso el cifrado, que no usarla.

Siendo capaz VeraCrypt tanto de cifrar soportes, como de crear contenedores cifrados para archivos, a continuación listamos una serie de casos de uso para VeraCrypt:

- **En la computadora de uso habitual**, disponer de un contenedor (parecido a una carpeta, pero cifrada) en el que se depositen todos los archivos relacionados con la militancia o sensibles en general. Cuando se vayan a utilizar dichos archivos, desbloquear el contenedor y volverlo a bloquear cuando se dejen de utilizar. La cantidad de tiempo que conlleva esto es ínfima y puede marcar una diferencia muy grande en la seguridad militante.

- **Compartir archivos por Internet** de manera segura. Cuando subimos algo a Internet, ya sea en la nube, a un chat, a una red social, al correo, etc. La seguridad de los archivos depende del servidor al que se suben. Incluso si estos servidores prometen almacenar o transferir cifrados los archivos, es mejor prevenirse y tomar la responsabilidad por nuestra cuenta. Así, si queremos subir un archivo a la nube para compartirlo con el resto de militantes de nuestra organización, lo idóneo es que lo subamos dentro de un contenedor VeraCrypt con una clave conocida por el sector militante con el que lo compartimos, de tal modo que aunque la policía solicitara la información al servicio que provee la nube, se encontraría con un contenedor del que no conoce la clave.

- **Compartir archivos a mano**, dándole un soporte (USB o una tarjeta micro SD) cifrado a otra u otro militante. De este modo, la información no pasaría por la red, disminuyendo en gran parte la superficie de ataque, y en caso de que el soporte fuera incautado por la policía o incluso se perdiera, el contenido seguiría siendo secreto.

- **Almacenar todos los documentos relacionados con la militancia** en un soporte cifrado y, ante una eventual redada, romper el soporte, esconderlo, tirarlo a algún sitio de difícil acceso o dárselo a otra u otro militante. Así, el material informático quedaría limpio de trazas militantes (si obviamos otros factores que comentaremos más abajo) y sería un punto inútil para inculpar al militante o para que la policía obtuviera información sobre la organización.

En general, el uso principal es el de mantener en secreto la información relacionada con la militancia, tanto en el sentido de proteger al militante ante un juicio, como para proteger la información confidencial de la organización en su conjunto. VeraCrypt, además, nos permite crear volúmenes ocultos dentro de un volumen normal, cada uno disponiendo de su propia clave. Esto es muy útil ante una redada, porque el militante podría almacenar archivos no sensibles en la parte normal del contenedor y

los sensibles en la oculta, de tal modo que proveyera a la policía la clave de la parte no sensible y la policía no pudiera saber (ya que el diseño de VeraCrypt lo evita) que existe una parte sensible en la que están todos los documentos importantes.

Cómo usar VeraCrypt

VeraCrypt es un software que nos permite crear contenedores cifrados y cifrar soportes de información, haciendo uso de diferentes algoritmos de cifrado. Es un software muy robusto, generalmente aceptado como seguro, utilizado incluso por el CNI (Centro Nacional de Inteligencia) para cifrar sus discos duros y que ha sido auditado para comprobar su seguridad. Además, permite crear volúmenes ocultos, admitiendo la negación plausible, es decir, la capacidad de una persona de "negar el conocimiento o la responsabilidad de cualquier acción condenable", que en este caso se traduce como la capacidad de negar la existencia de un volumen cifrado.

A continuación, exploraremos cómo instalar VeraCrypt y cómo utilizarlo para crear soportes y volúmenes cifrados (normales y ocultos). No haremos un repaso por todas las capacidades de VeraCrypt, remitiéndonos en este caso a su documentación oficial, del mismo modo que recomendamos la lectura de la sección de precauciones a tomar, en la que se señalan las limitaciones de VeraCrypt, algunas de las cuales exploraremos en la sección de limitaciones de esta guía.

Instalación

La instalación la ejemplificaremos en el sistema operativo Tails, ya que queremos promover su uso para todas las actividades militantes. De todas formas, el proceso de instalación será parecido en cualquier sistema operativo GNU/Linux. En sistemas como Windows y macOS (OSX), la instalación es muy fácil y no nos detendremos mucho en su explicación.

Primero de todo, hay que ir a la página de descargas oficial de VeraCrypt:

https://www.veracrypt.fr/en/Downloads.html

Luego, según la plataforma:

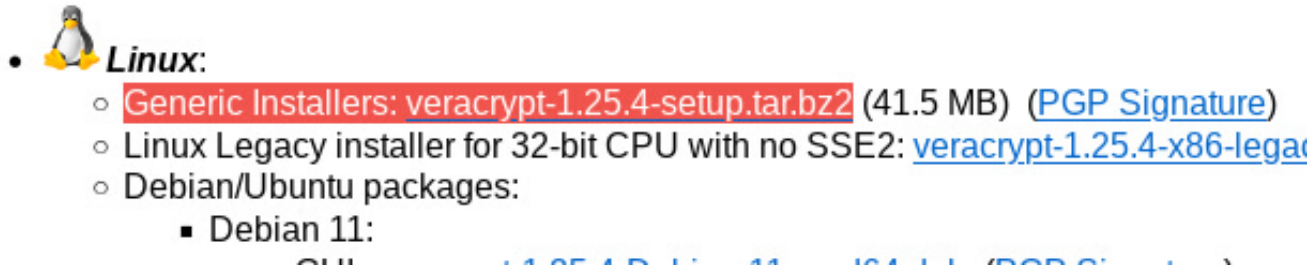
- **Windows**: en la página de descargas, ir a la sección de Windows y descargar la opción "EXE Installer", si lo que queremos es instalarlo en la computadora. Una vez descargado, ejecutar el archivo y seguir los pasos que se indican. En caso de querer la versión portable, que no es necesario instalar y es útil para llevarlo en un soporte (USB, disco duro externo, micro SD, etc.), descargar la opción "Portable version".

- **MacOS**: es necesario instalar OSXFUSE, tal y como se dice en la sección MacOS de la página de descargas de VeraCrypt, y después instalar VeraCrypt descargando el archivo DMG y ejecutándolo como se hace habitualmente en este sistema operativo.

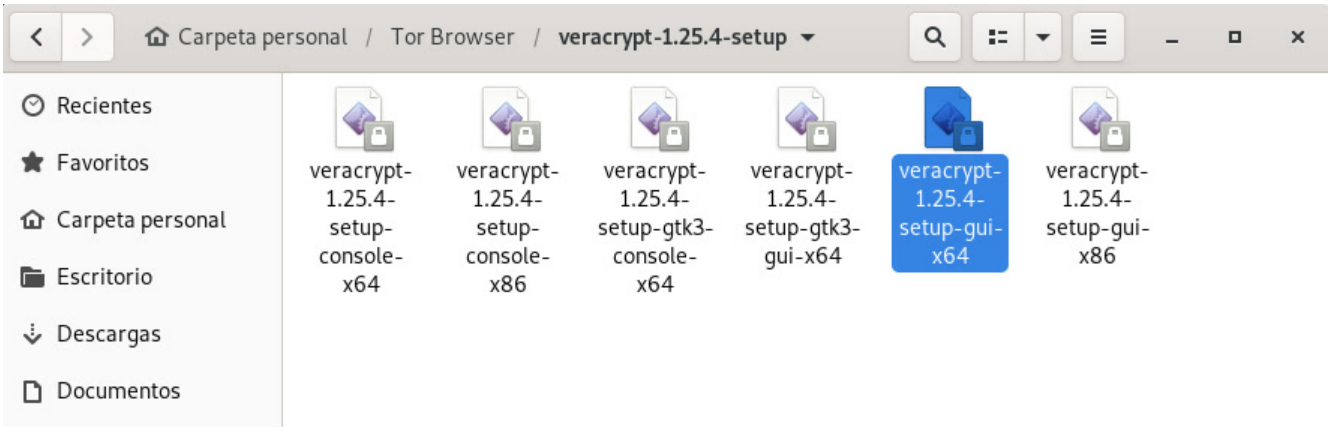
- **GNU/Linux**: en este caso hay una gran cantidad de opciones para descargar, dependientes de la distribución de GNU/Linux en la que se quiera instalar. No obstante, nosotros nos centraremos en ejemplificar la instalación en Tails:

  Aviso: para instalar paquetes, aplicaciones, etc. en Tails es necesario haber activado la contraseña de administrador en la ventana de inicio del sistema.

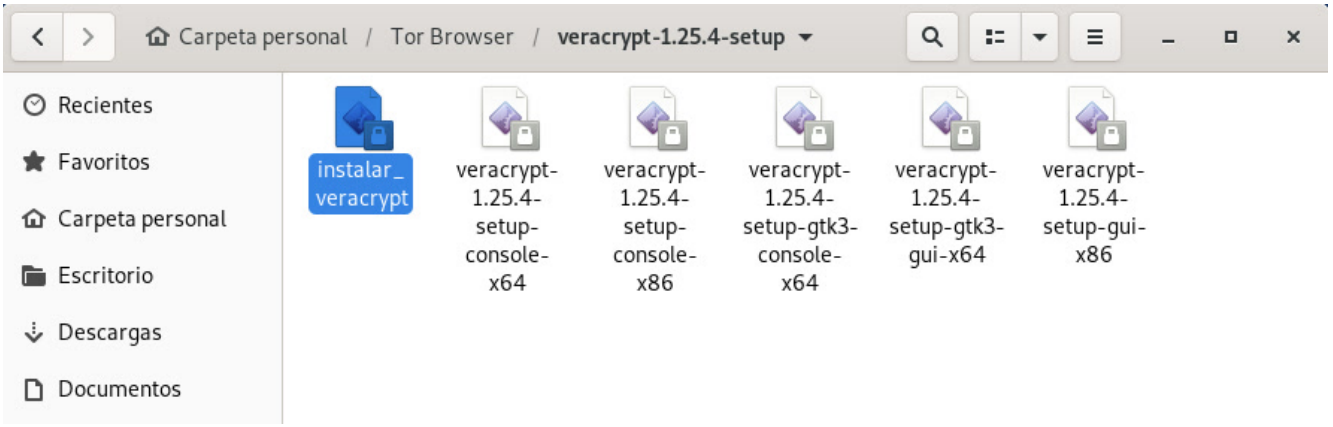
  1. Descargamos la opción "Generic Installers":

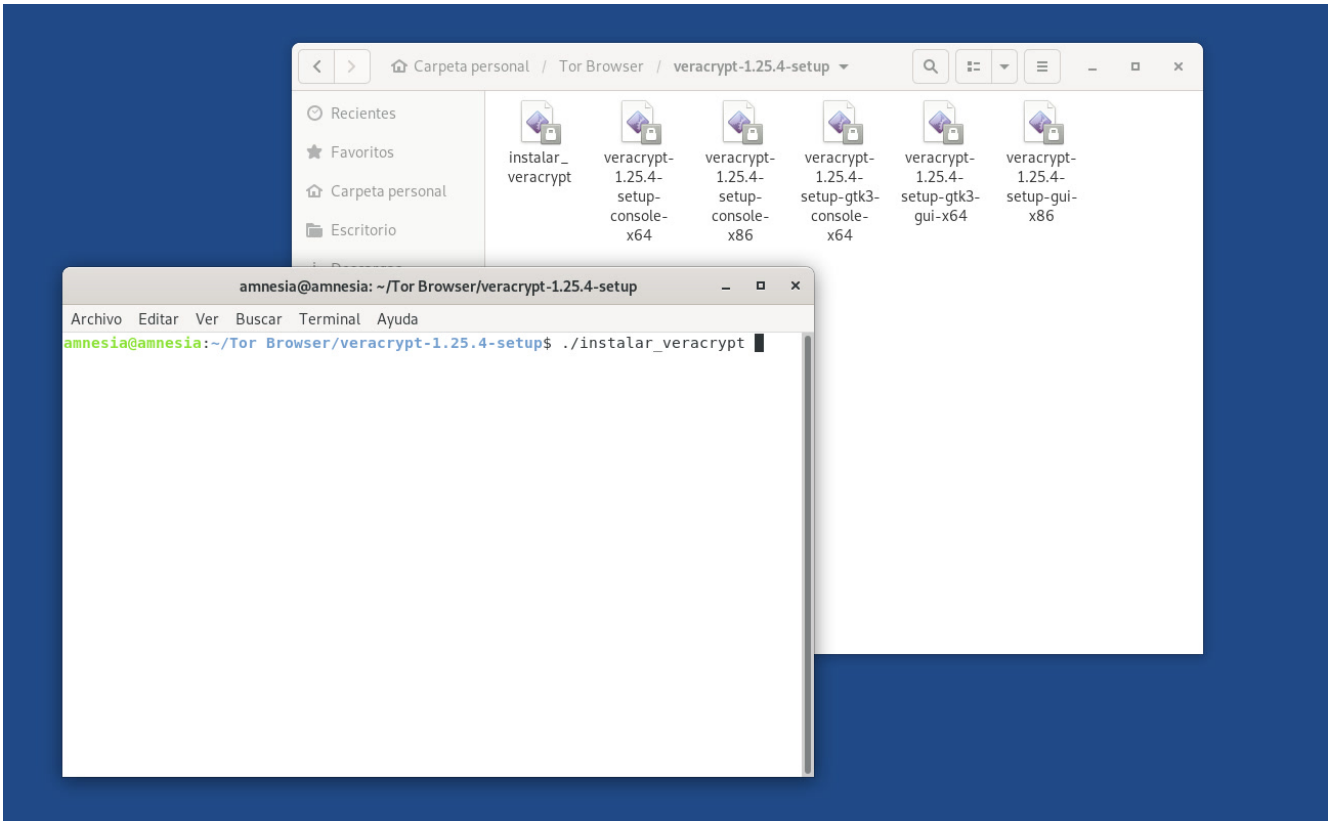
  2. Descomprimimos el archivo descargado, haciendo click derecho y pulsando en "Extraer aquí". Entramos en la carpeta descomprimida y buscamos el archivo cuyo nombre termina en "setup-gui-x64". Es el más habitual, pero puede variar según si la computadora es de 64 bits (habrá que optar por el archivo terminado en x64) o si es de 32 bits (suelen ser máquinas más antiguas, y habrá que optar por el archivo terminado en x86):



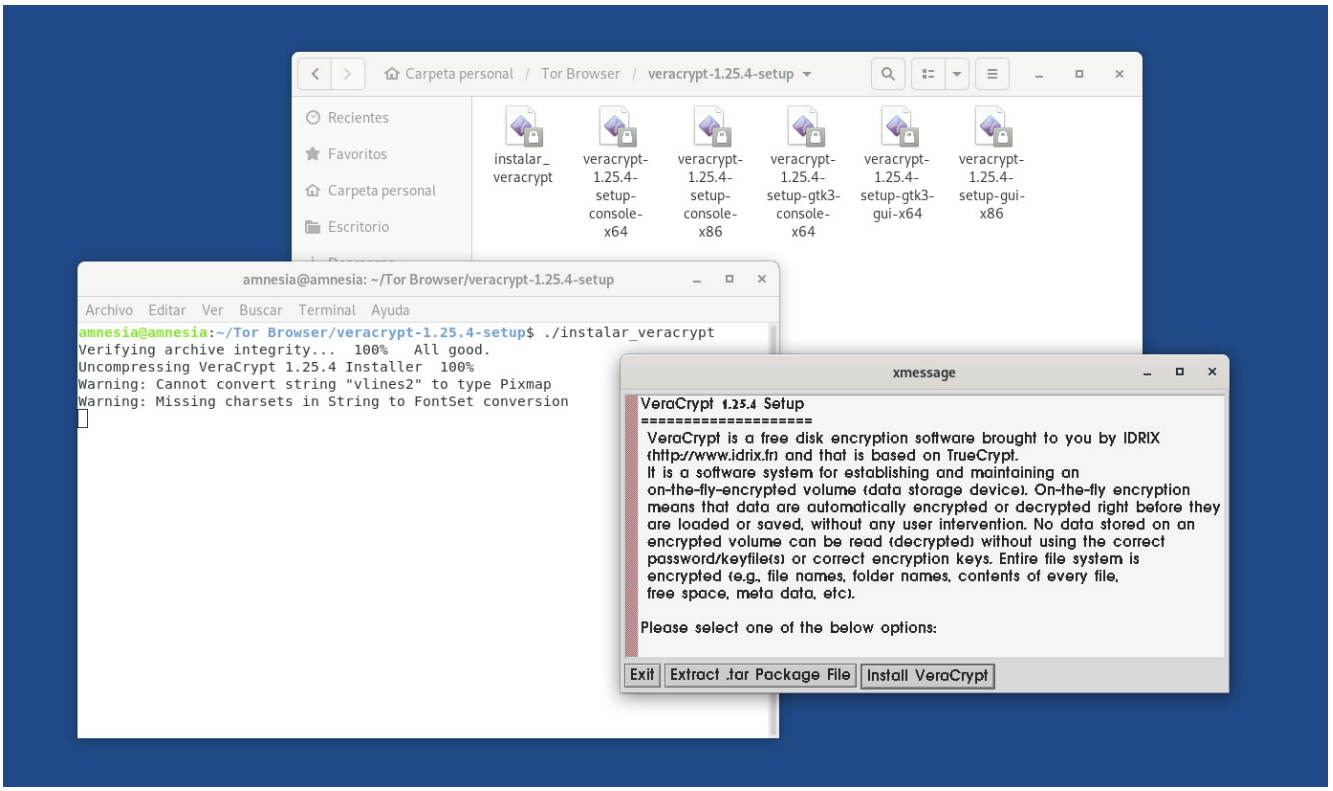
3. Por facilidad, renombramos ese archivo (en este ejemplo lo nombramos como "instalar_veracrypt"):



4. Hacemos clic derecho en la carpeta en la que estamos y elegimos "Abrir una terminal aquí". Se nos abrirá una terminal, en la que tendremos que escribir "./" seguido del nombre que hemos puesto al archivo anterior:



5. Nos aparecerá una ventana, en la que tendremos que pulsar en "Install VeraCrypt" y aceptar los términos de uso:

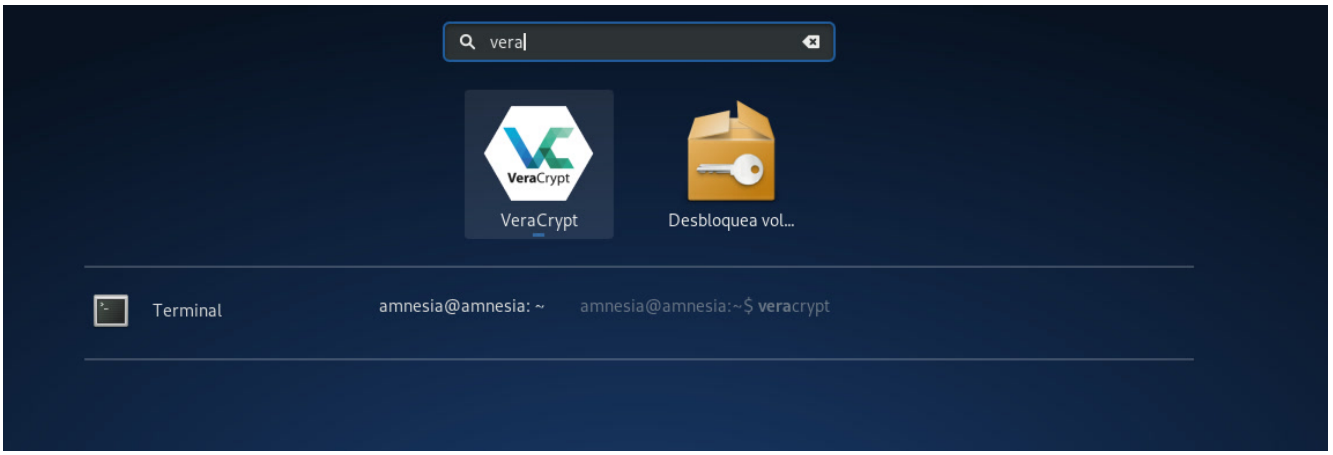


6. Nos pedirá la contraseña de administrador que hemos puesto antes de iniciar Tails. La introducimos y pulsamos Intro (Enter).

Una vez terminado el proceso de instalación, en la pantalla de una terminal nos

pedirá que pulsemos Enter (Intro) y después de pulsarlo se cerrará. Ya podemos cerrar la terminal que habíamos usado antes.

Para iniciar VeraCrypt en Tails, basta con abrir una terminal, teclear "veracrypt" y pulsar Enter. También puede abrirse pulsando la tecla Windows (o cmd en macOS), buscando "veracrypt" y pulsando en el icono:

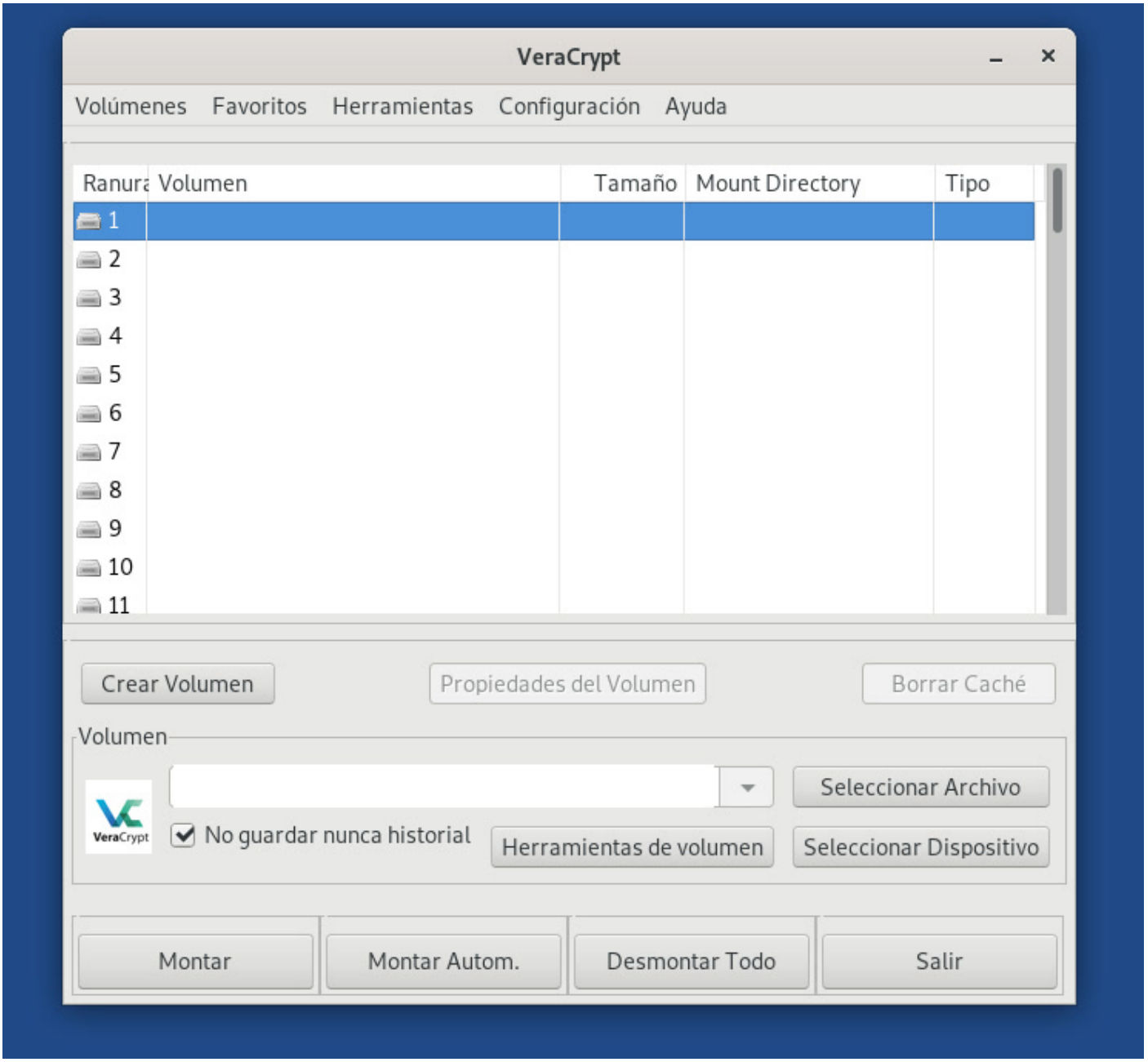


A partir de aquí, la interfaz gráfica es igual en todos los sistemas operativos y, por tanto, los pasos son los mismos.

Contenedor cifrado

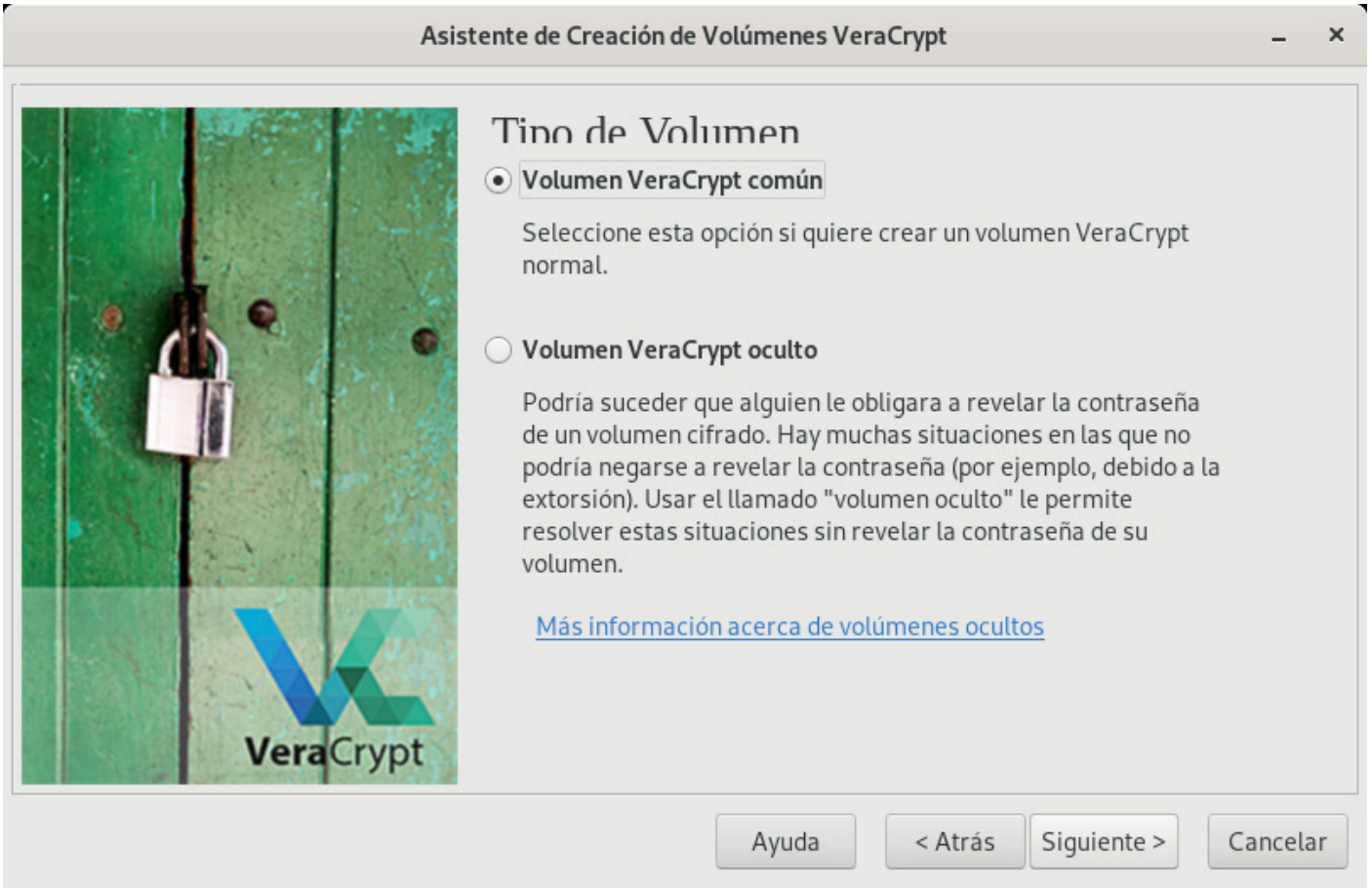
Un contenedor cifrado es como una carpeta cifrada en la que se meten archivos, como si fuera un cajón con llave: se desbloquea con la clave, se meten, sacan o utilizan archivos y, finalmente, cuando se ha dejado de utilizar, se cierra, quedando en secreto su contenido.

Para crear un contenedor cifrado, debemos pulsar en el botón "Crear Volumen":



Después seleccionar la opción "Crear un contenedor de archivos cifrado" y pulsar en "Siguiente":

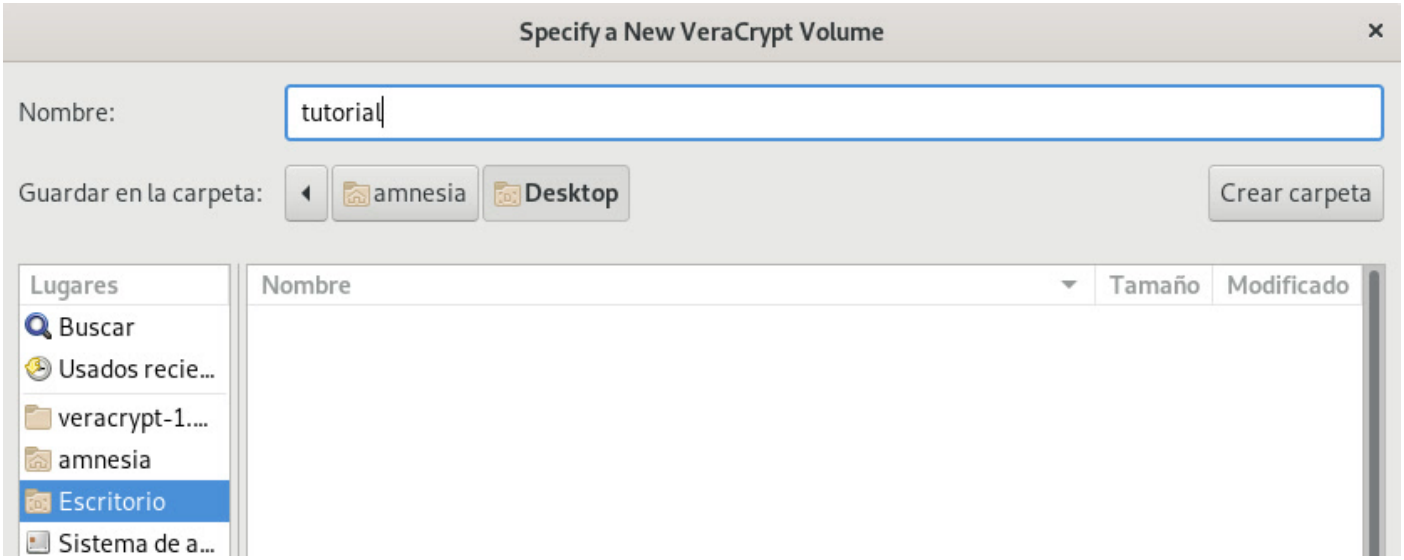
De momento, utilizaremos la opción "Volumen VeraCrypt común", que es la versión normal de un volumen VeraCrypt y más tarde exploraremos la opción de crear volúmenes ocultos. Pulsamos en "Siguiente":



Ahora, pulsamos en "Seleccionar archivo":

Navegamos hasta la ruta en la que queremos crear el archivo, escribimos un nombre

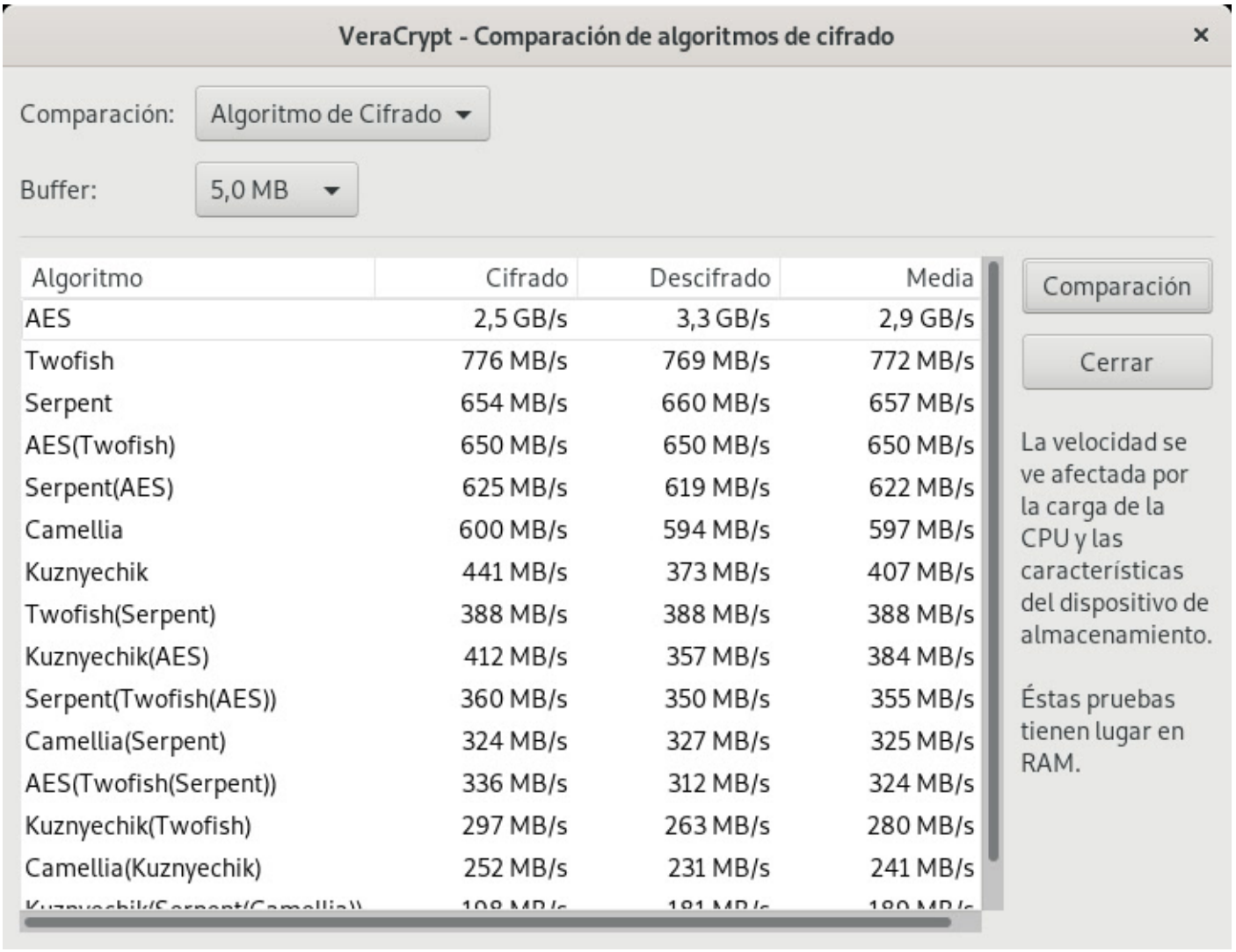
de archivo y aceptamos (no hay que seleccionar un archivo existente, ya que lo vamos a crear):



Pulsamos en "Siguiente" y nos llevará a la pantalla de selección de algoritmo:

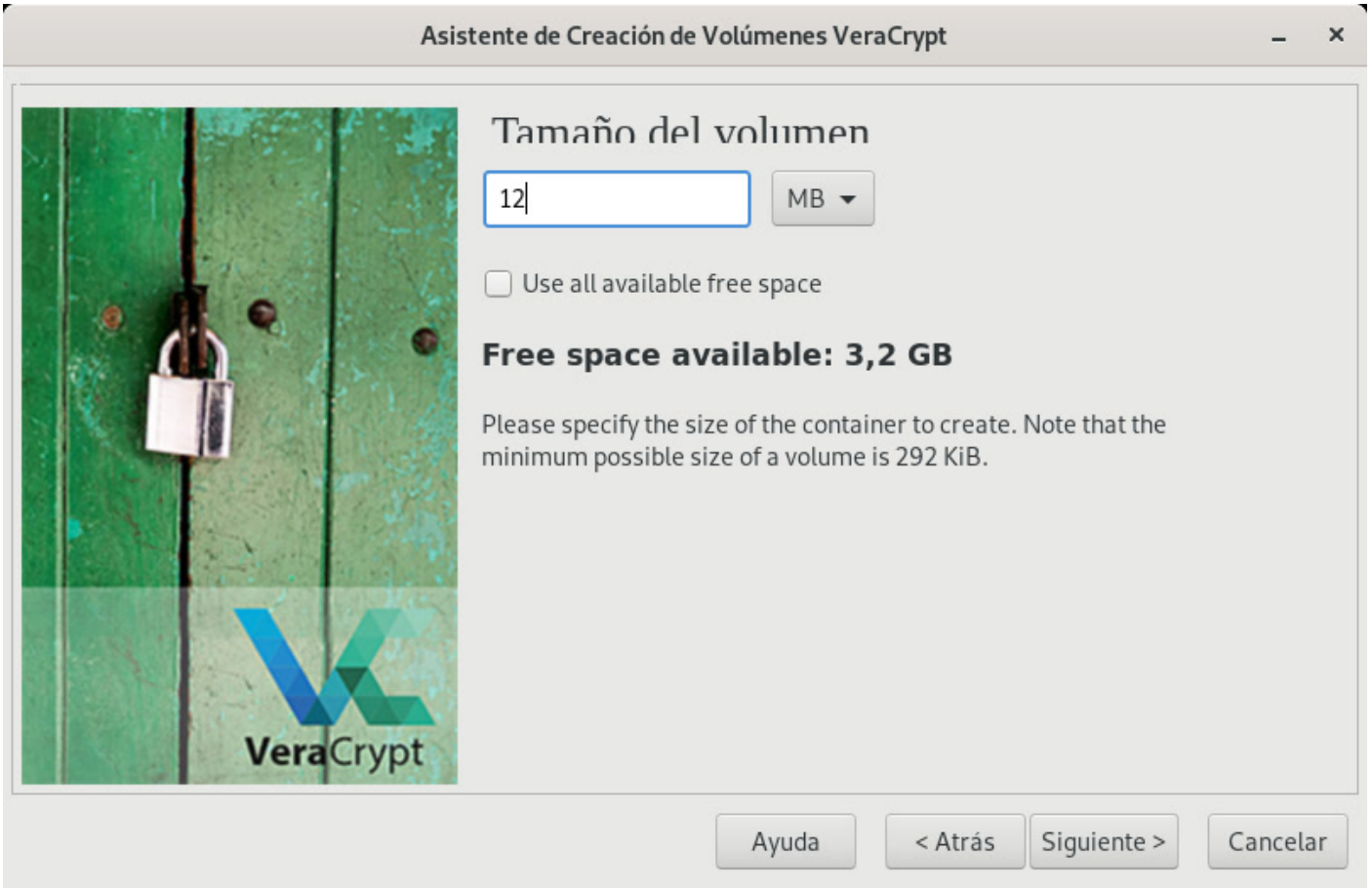
Aquí podemos elegir entra varios algoritmos de cifrado y algoritmos de hashing. Para cada uno de estos, aparece una breve descripción sobre el cifrado y en qué contextos se utiliza. Entre la variedad de algoritmos que ofrece VeraCrypt, es interesante comprobar su eficiencia pulsando el botón "Comparación" (y dentro de la

pantalla que aparece, de nuevo en el botón con el mismo nombre), que nos dice la rapidez con la que cifra y descifra:

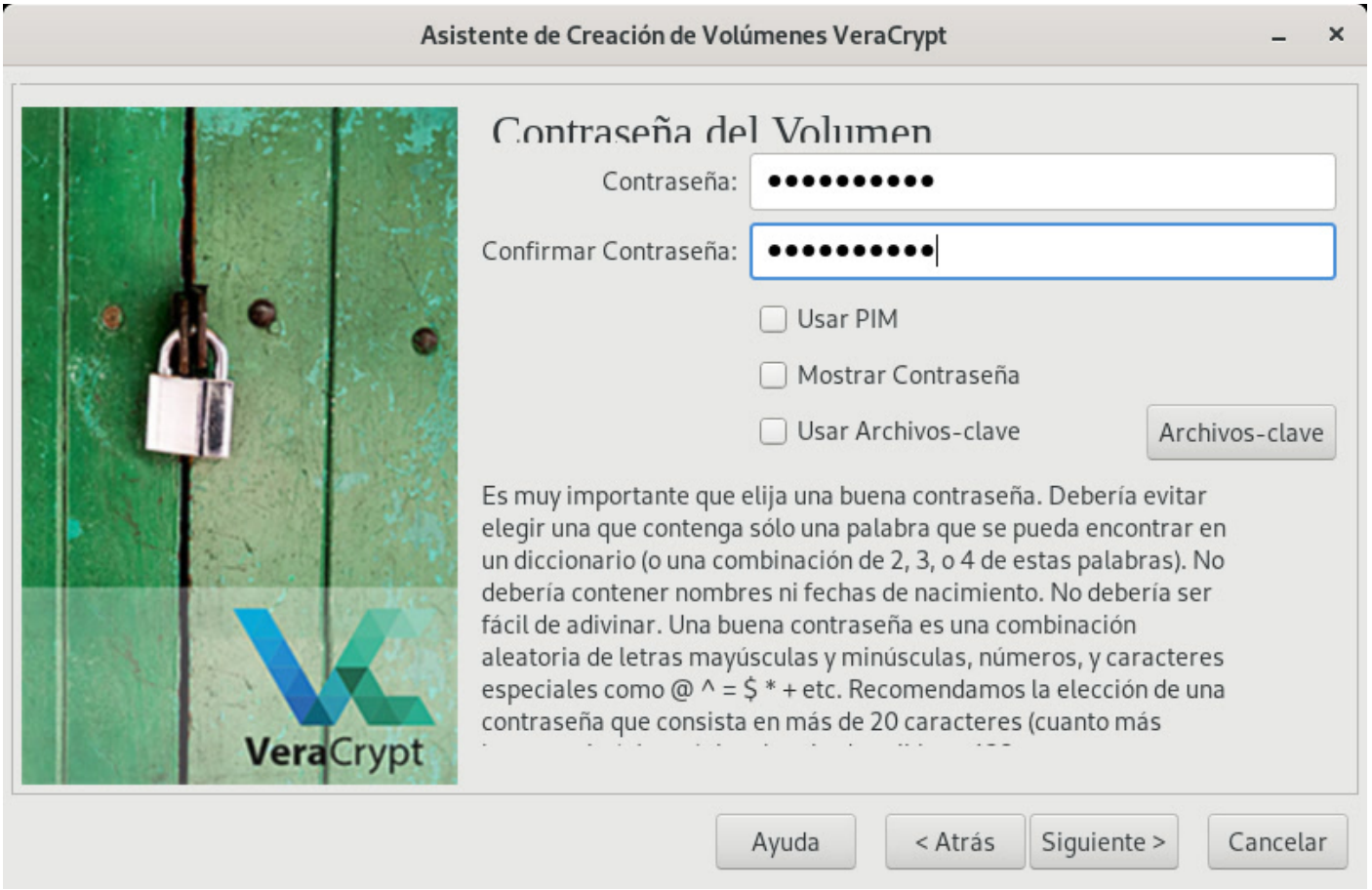


De entre todos los algoritmos, una combinación de cifrado AES y hashing con SHA-512 es más que suficiente, aunque animamos a explorar las características que ofrecen el resto de algoritmos. Una vez elegido el algoritmo, pulsamos en "Siguiente".

En la siguiente pantalla seleccionamos el tamaño del volumen que queremos crear, expresado en KiB, MiB o GiB que, más o menos (no explicaremos aquí la diferencia), corresponden a kilobytes, megabytes y gigabytes, respectivamente. Seleccionamos el tamaño teniendo en cuenta la cantidad de datos que vamos a meter. Por ejemplo, si es para almacenar un solo Word y subirlo a la nube o pasárselo a alguien, seguramente baste con 1 MiB (habría que mirar primero el tamaño del archivo), mientras que si se pretenden almacenar, por ejemplo, unos cuantos documentos o libros, habrá que valorar qué tamaño darle, tal vez de varios GiB. En cualquier caso, siempre es deseable minimizar el tamaño, para que no ocupe tanto y se descifre antes:



Una vez pulsado en "Siguiente", nos pedirá que introduzcamos la clave de cifrado dos veces:

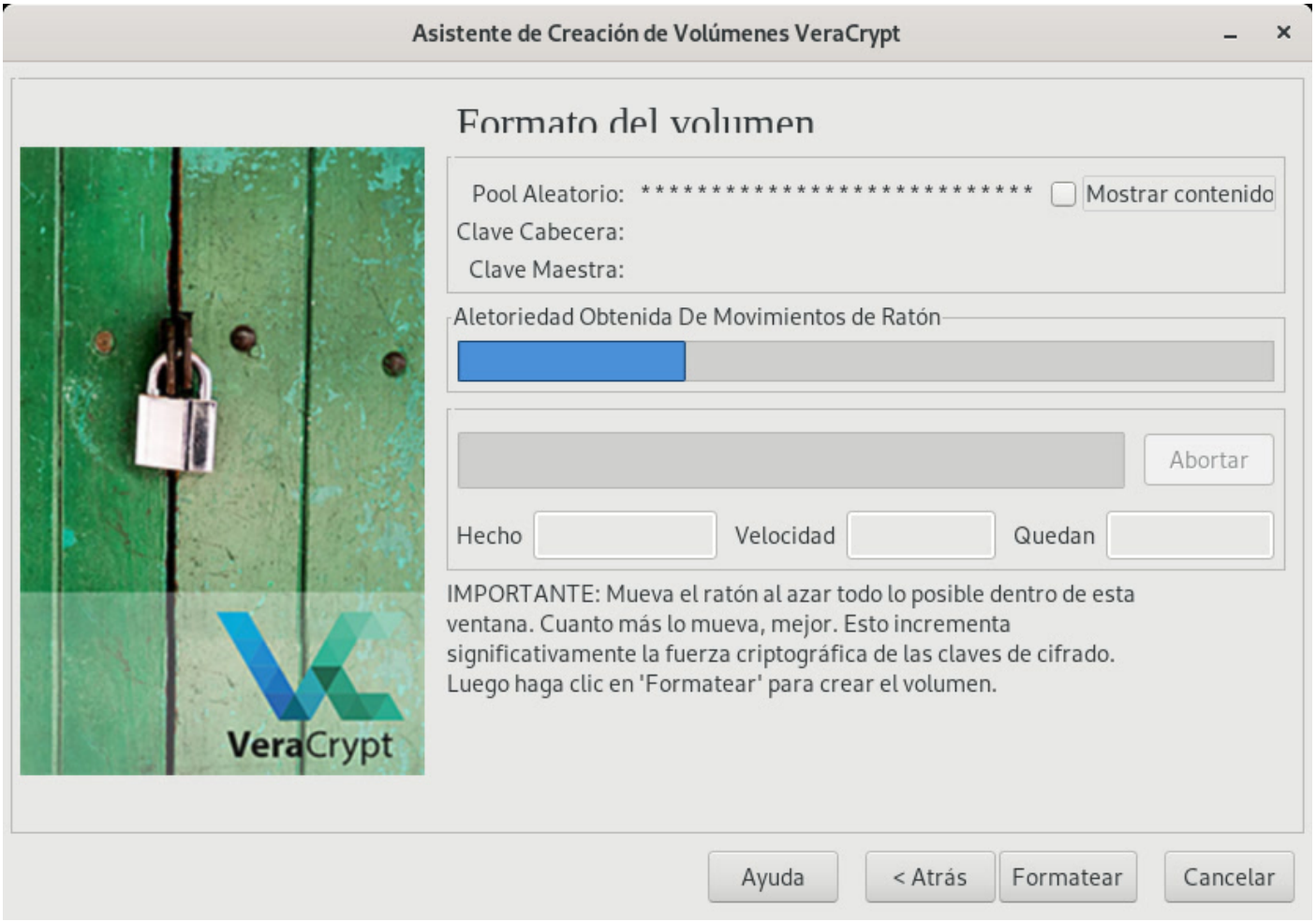


También existe la opción de utilizar un número de PIM, que básicamente funciona como un número más que conocer e introducir aparte de la clave de cifrado, para aumentar la seguridad, pero no es estrictamente necesario utilizarlo. En esta guía no exploraremos los "keyfiles" o Archivos-Clave.

Una vez introducida la contraseña (y el PIM, si se ha decidido usarlo), pulsamos en "Siguiente".

En la próxima pantalla, nos pedirá el tipo de sistema de archivos. Para aumentar la compatibilidad con diferentes sistemas operativos, utilizaremos la opción "FAT" y pulsaremos en "Siguiente":

Llegamos a la pantalla final, en la que hay que generar la cadena de datos aleatorios que se utilizarán para encriptar el volumen. Para ello, se presenta la manera de hacerlo moviendo el cursor del ratón de forma aleatoria por la pantalla de VeraCrypt. Es recomendable, aunque no necesario, que la barra de estado llegue hasta el final. Una vez logrado esto, se pulsa en "Formatear":



Cuando el proceso termine, se habrá creado un archivo en la ruta y con el nombre que habíamos especificado. Aparecerá una ventana en la que nos preguntará por crear otro volumen o terminar. Si no queremos crear más volúmenes, pulsamos en "Salir". Más adelante veremos cómo descifrar el volumen y utilizarlo.

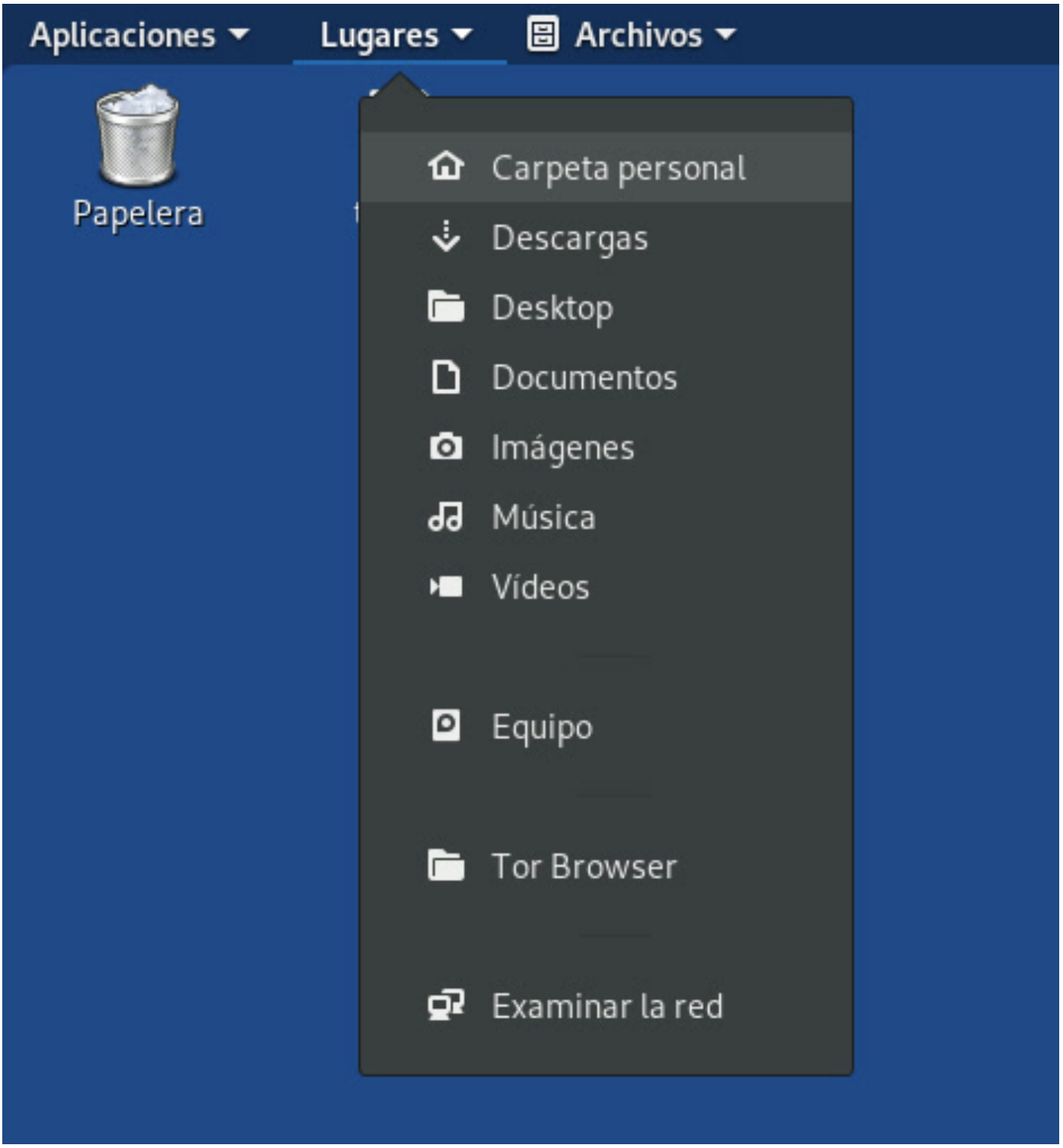
Soporte cifrado

Un soporte es un disco duro, una unidad de almacenamiento USB, una tarjeta micro SD o cualquier dispositivo análogo. En este caso, el volumen cifrado no consistirá en un archivo, sino en un soporte entero o una partición del mismo. Por cuestión de simplicidad, lo explicaremos cifrando una unidad USB entera.

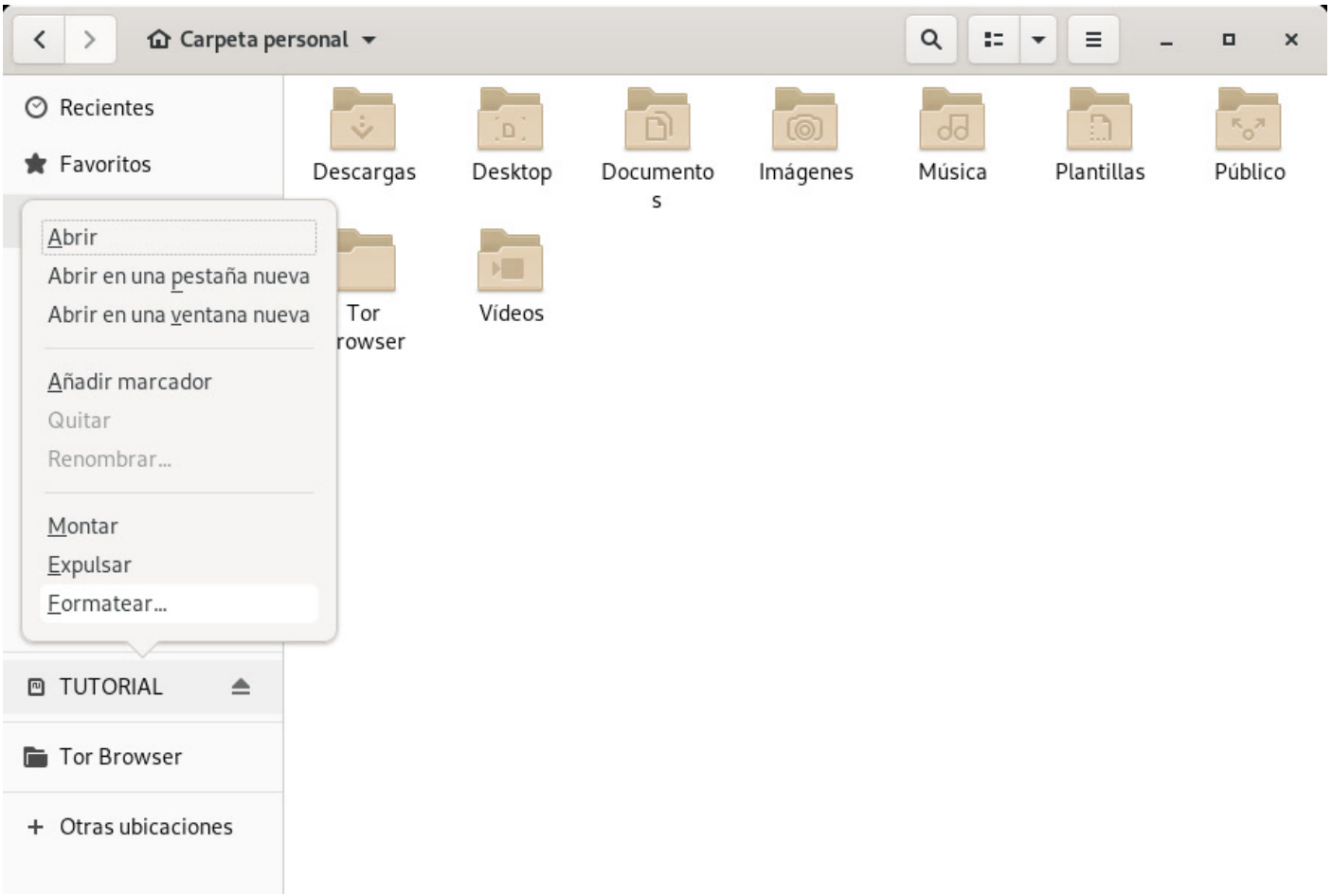
Antes de nada, es recomendable formatear el soporte que vamos a cifrar, aunque no es estrictamente necesario. No explicaremos aquí cómo hacerlo en cada sistema operativo, ya que en Internet hay una infinidad de guías que lo explican. Explicaremos cómo hacerlo en Tails con una unidad USB:

Aviso: formatear una unidad borrará todos los archivos que contenga. Recomendamos revisar bien que la unidad esté vacía o valorar si no nos importa perder los archivos que contiene.

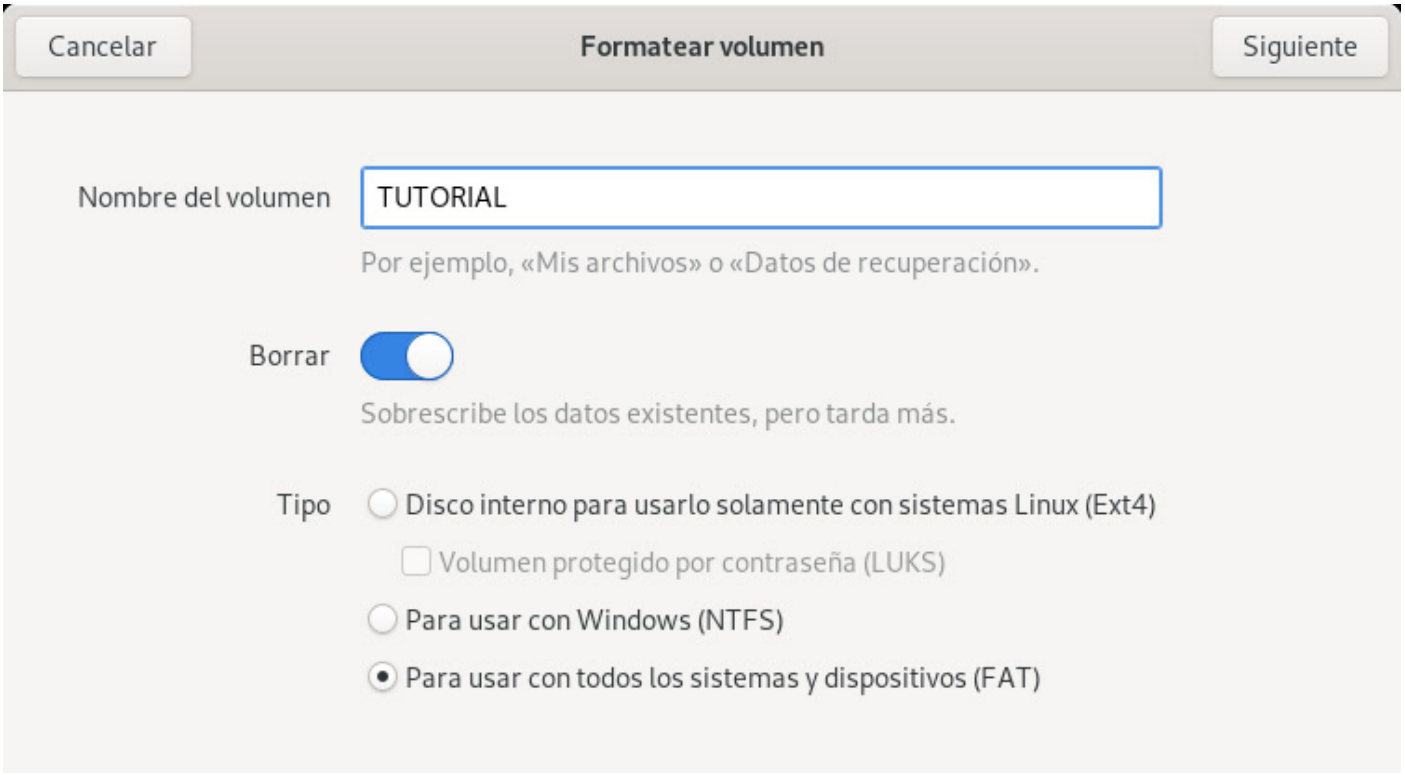
Pulsamos en "Lugares" y abrimos, por ejemplo, la ruta de "Carpeta personal":



En la barra lateral de la ventana nos aparecerá la unidad USB, sobre la que haremos clic derecho y luego pulsaremos en "Formatear...":



Es muy importante asegurarse de que hemos seleccionado la unidad correcta y de que hemos guardado todos los archivos que queremos conservar en algún otro lado, ya que el formateo borrará todos los datos dentro de la unidad seleccionada. Introducimos un nombre, en este ejemplo será "TUTORIAL", seleccionamos la casilla de "Borrar", seleccionamos la casilla de tipo "FAT" y pulsamos en "Siguiente":



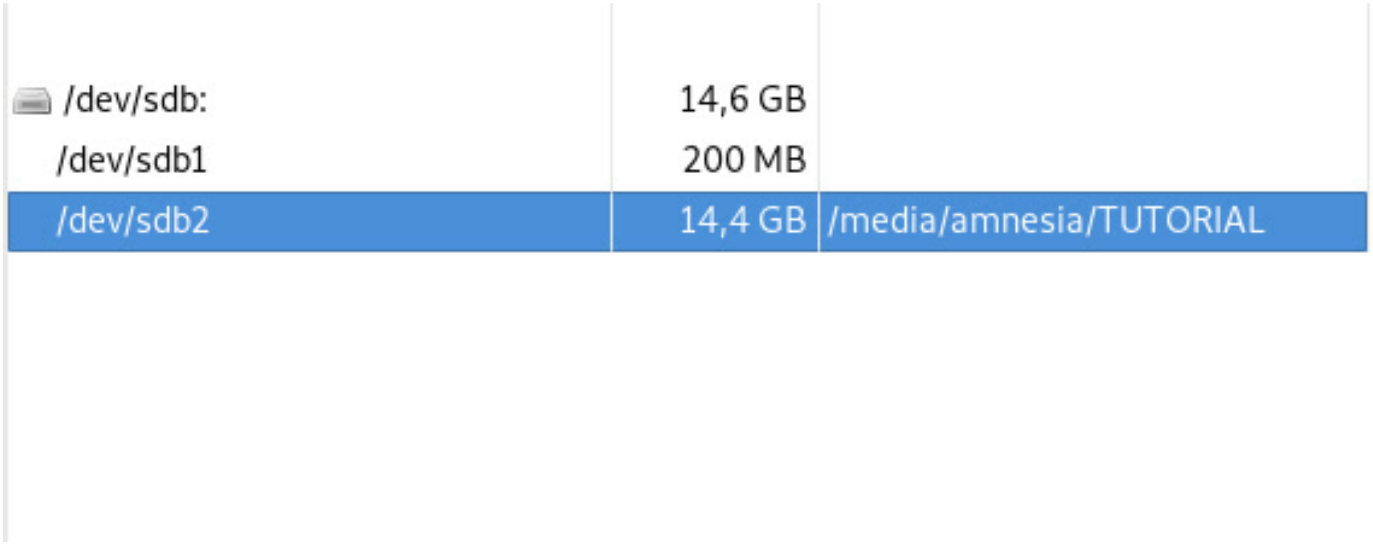
Nos aparecerá una advertencia y si estamos seguros de que hemos seleccionado bien la unidad de almacenamiento, pulsamos en "Formato" y comenzará el proceso de formateo.

Una vez formateado el soporte, procedemos a cifrarlo.

Aviso: al igual que el formateo, cifrar un soporte con VeraCrypt borrará todos los archivos que contenga, por lo que, de nuevo, recomendamos revisar bien que la unidad esté vacía o valorar si no nos importa perder los archivos que contiene.

En la pantalla principal de VeraCrypt, pulsamos en el botón "Crear Volumen", seleccionamos la opción "Cifrar partición/unidad secundaria" y pulsamos en "Siguiente":

De momento, al igual que en al apartado anterior, utilizaremos la opción "Volumen VeraCrypt común" y pulsaremos en "Siguiente". Ahora nos pedirá seleccionar la unidad de almacenamiento que queremos cifrar. En MacOS y GNU/Linux estarán nombrados de la siguiente forma y habrá que escoger el que tenga el nombre que le hemos puesto tras formatear y que tenga tamaño parecido al de nuestra unidad de almacenamiento. En este caso "/dev/sdb2":



Aceptamos y avanzamos de paso:

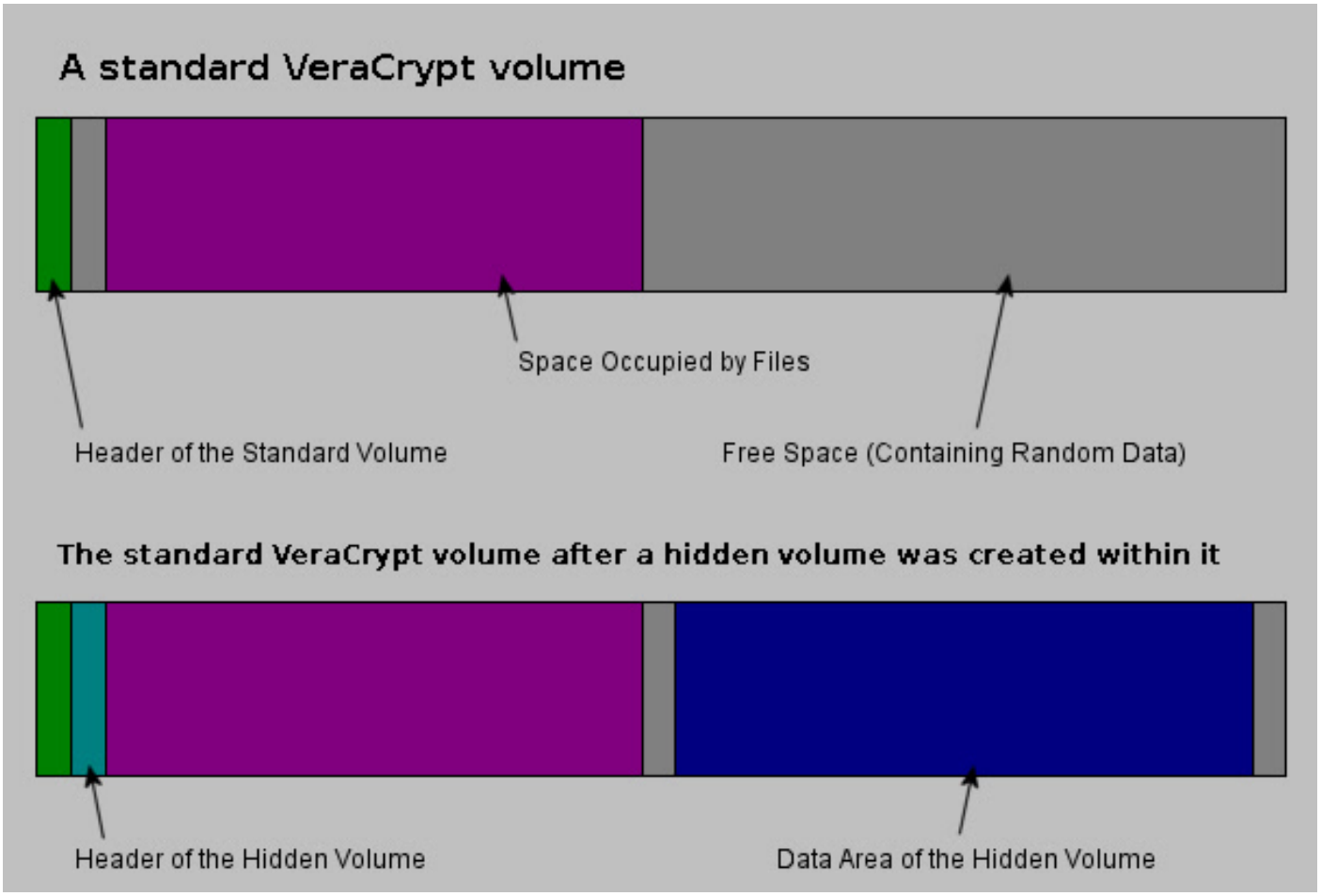
En este siguiente paso, nos preguntará si queremos almacenar archivos mayores o menores de 4 GB. Seleccionamos la opción y pulsamos en "Siguiente":

Cuando nos pida elegir el tipo de formato, seleccionaremos el formato "FAT", ya que es el más compatible con los diferentes sistemas operativos. En cuanto al formato rápido, es recomendable seleccionarlo, pero como ya hemos formateado previamente la unidad que estamos utilizando, no hace falta hacer uso de esta opción:

A partir de aquí, todos los pasos son idénticos al apartado anterior, donde explicábamos como crear un contenedor cifrado.

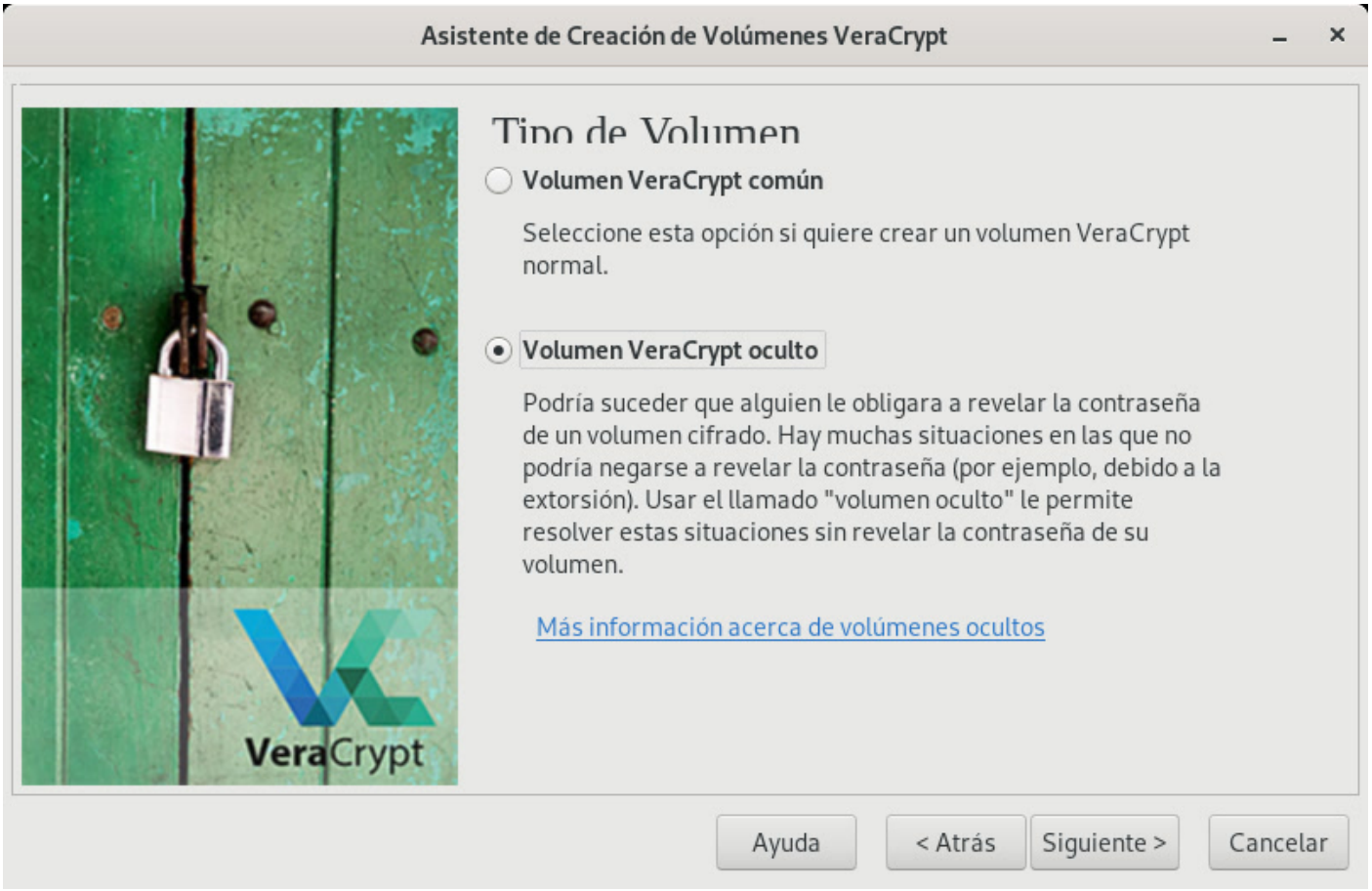
Volumen cifrado oculto

Un volumen cifrado oculto consiste en que, en un mismo volumen (contenedor o unidad de almacenamiento), existen dos volúmenes, cada uno con una clave de cifrado propia. Como ya hemos dicho, esto sirve para despistar a la policía, ya que si piden la clave de cifrado, el militante puede proveer la de la parte no sensible del volumen, es decir, la que no está oculta, mientras que guarda en esta última los archivos sensibles.



El proceso para crear un volumen cifrado oculto, es el siguiente:

En la pantalla principal de VeraCrypt hay que pulsar en "Crear Volumen", seleccionar si queremos cifrar un contenedor o un unidad como se ha explicado en los apartados anteriores, pero esta vez seleccionaremos la opción "Volumen VeraCrypt oculto":



Siguiendo los pasos explicados en los partados anteriores, seleccionamos el archivo en el que crear el contenedor o la unidad de almacentamiento, el algoritmo de cifrado, el tamaño, introducimos la contraseña (que será la del volumen no oculto), seleccionamos el tipo de formato ("FAT"), movemos el ratón por la pantalla y pulsamos en "Formatear". Es posible que en alguno de estos pasos nos pida la contraseña de administrador que, por supuesto, la introduciremos.

Cuando haya terminado el formateo, nos aparecerá un mensaje como este, en el que pulsaremos en "Siguiente":

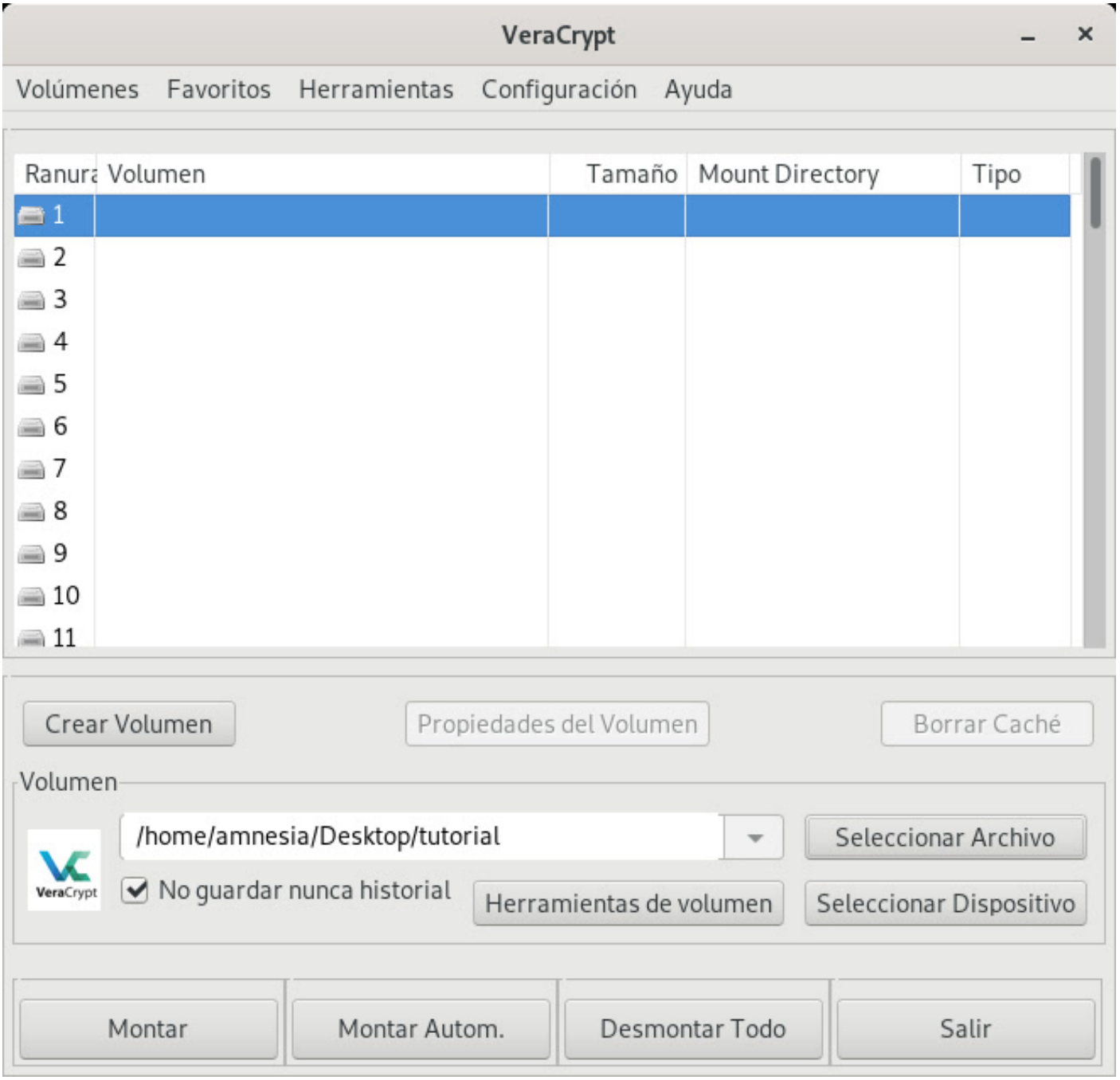
En la próxima pantalla pulsamos en "Siguiente" y realizamos los mismos pasos que en los otros apartados, desde seleccionar algoritmo hasta mover el ratón por la pantalla. El único paso que cambiará un poco será el de introducir el tamaño del volumen oculto, que dependerá del espacio disponible en el volumen no oculto. A la hora de introducir la contraseña, es importante recordar que tendrá que ser diferente a la del volumen no oculto.

Una vez seguidos todos los pasos, ya habremos creado un contenedor o unidad de almacenamiento con un volumen oculto (en el que guardaremos los documentos sensibles) y otro no oculto (en el que guardaremos documentos no tan ocultos, a modo de señuelo).

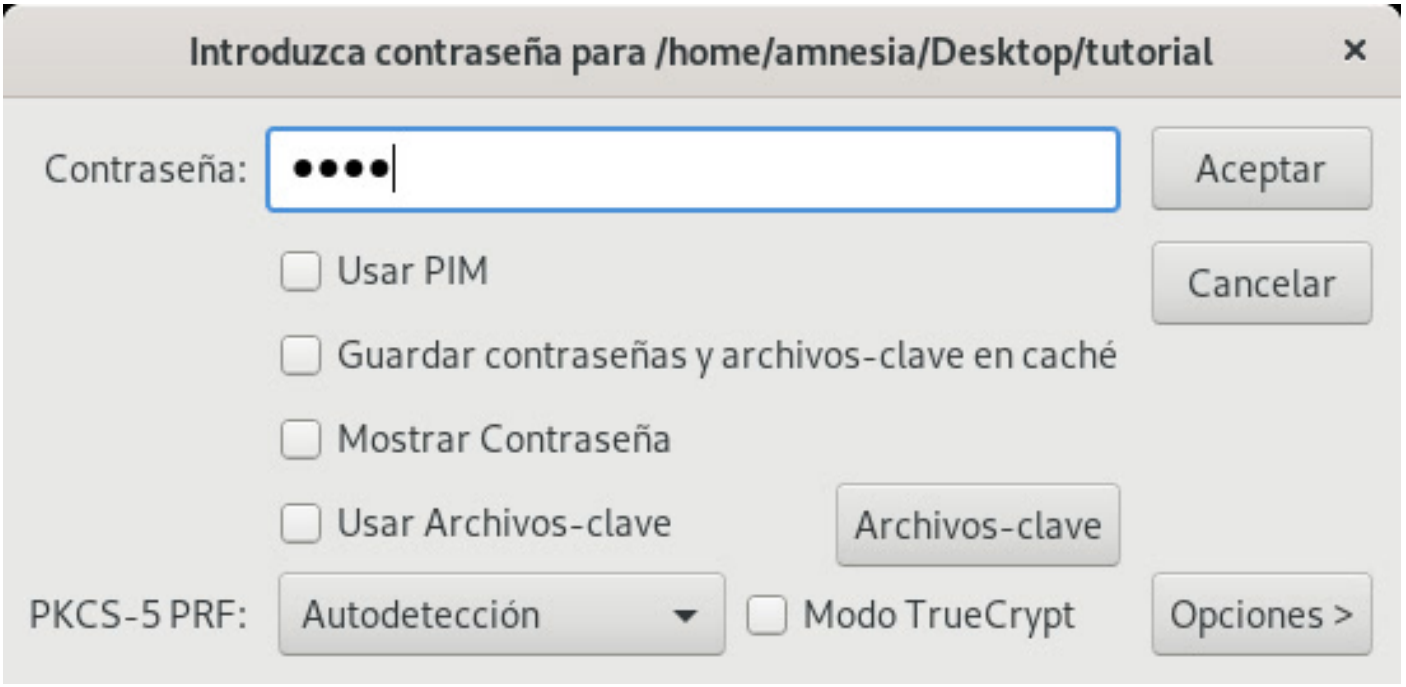
Descifrado de volúmenes VeraCrypt

Los volúmenes de VeraCrypt, como hemos dicho, son como unos cajones. Se descifran, se realizan acciones dentro de él (meter archivos, sacarlos, editarlos, etc.) y luego se cierran, cifrándolos de nuevo. Para descifrar un volumen VeraCrypt:

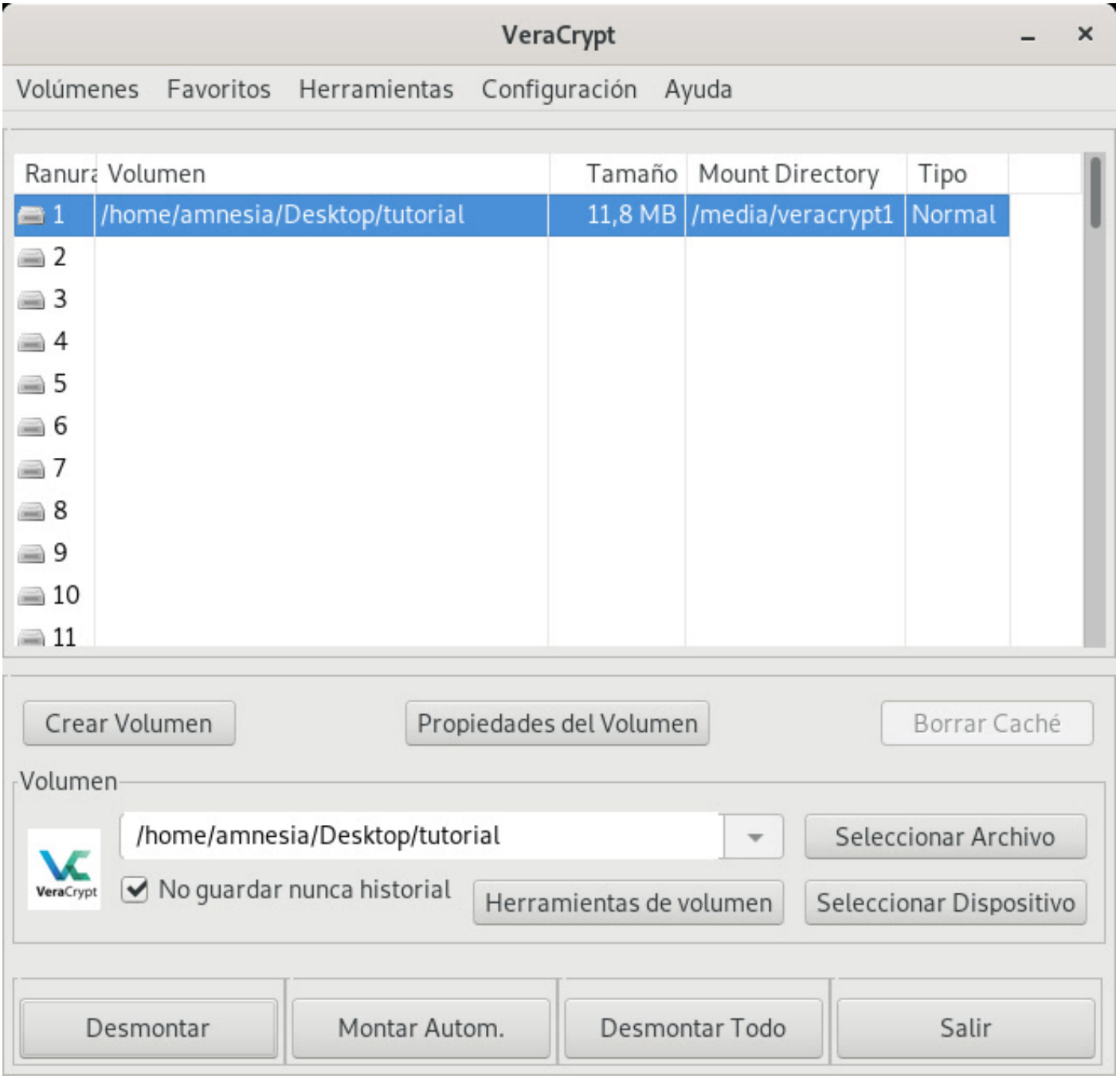
En la pantalla principal de VeraCrypt, pulsar en "Seleccionar archivo", si lo que queremos descifrar es un contenedor, o pulsar en "Seleccionar dispositivo", si lo que queremos es descifrar una unidad de almacenamiento, por ejemplo, una unidad USB. En este caso, desbloquearemos el contenedor creado anteriormente. Por lo tanto, lo seleccionamos:



Una vez cargado el archivo o el dispositivo, seleccionamos una ranura de la lista que hay en el recuadro superior (normalmente ya hay una seleccionada) y pulsamos en el botón de "Montar" (abajo a la izquierda). Se nos abrirá una ventana pidiéndonos la clave (también el PIM si lo hemos configurado al crear el contenedor). Solo tendremos que introducir la clave (y el PIM si lo hemos configurado) y pulsar en "Aceptar" (es posible que nos pida la contraseña de administrador):



Terminado el paso anterior, si ha resultado exitoso, veremos que en la ranura que habíamos seleccionado anteriormente ahora aparece una ruta. Para abrir el contenedor, hacemos doble click sobre esa ranura (en la imagen está marcada en azul):



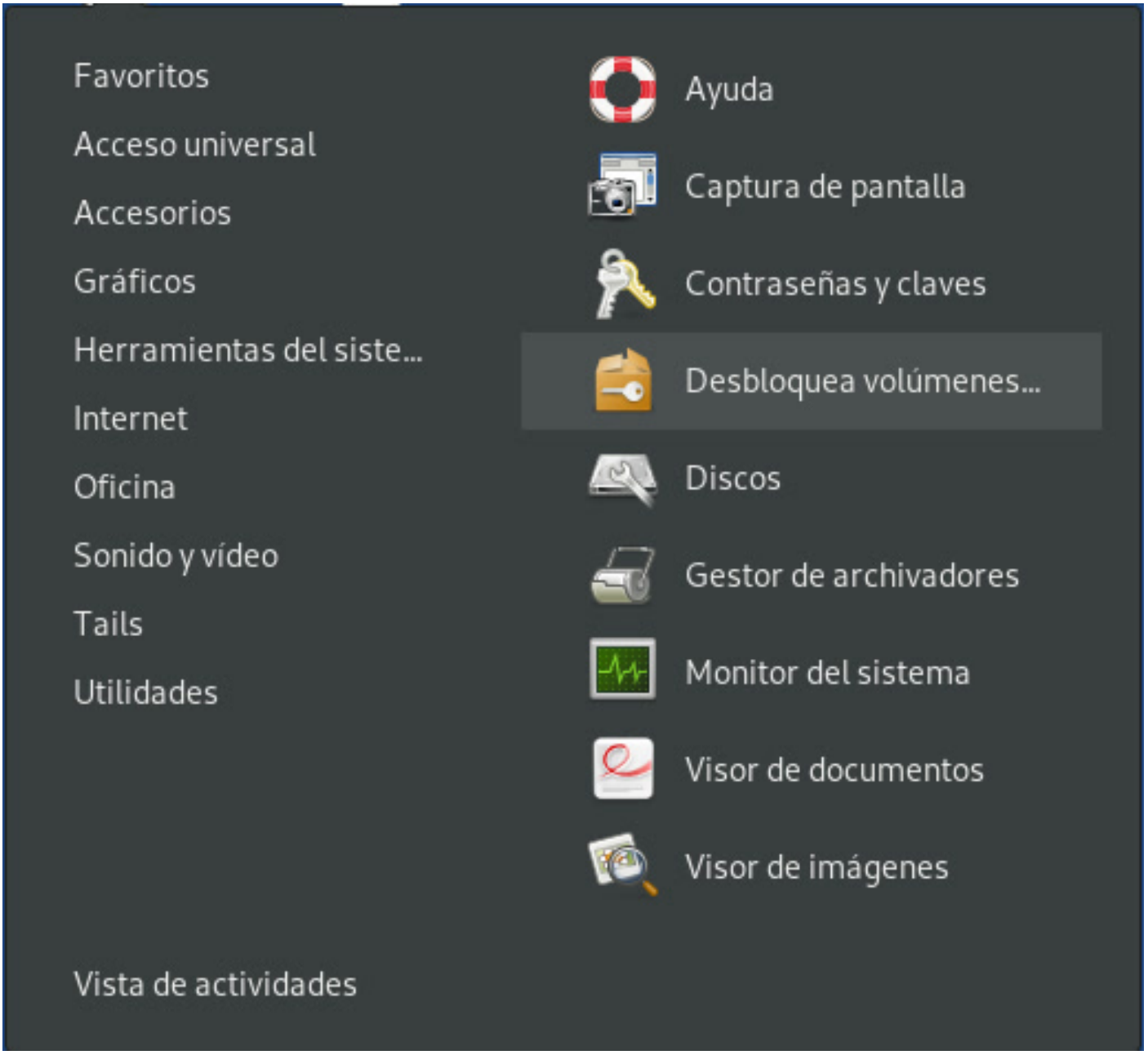
También veremos este contenedor montado como si fuese una unidad de almacenamiento más en el sistema (a través del explorador de archivos).

En caso de querer montar otro contenedor, realizaremos los mismos pasos, pero seleccionando una ranura libre.

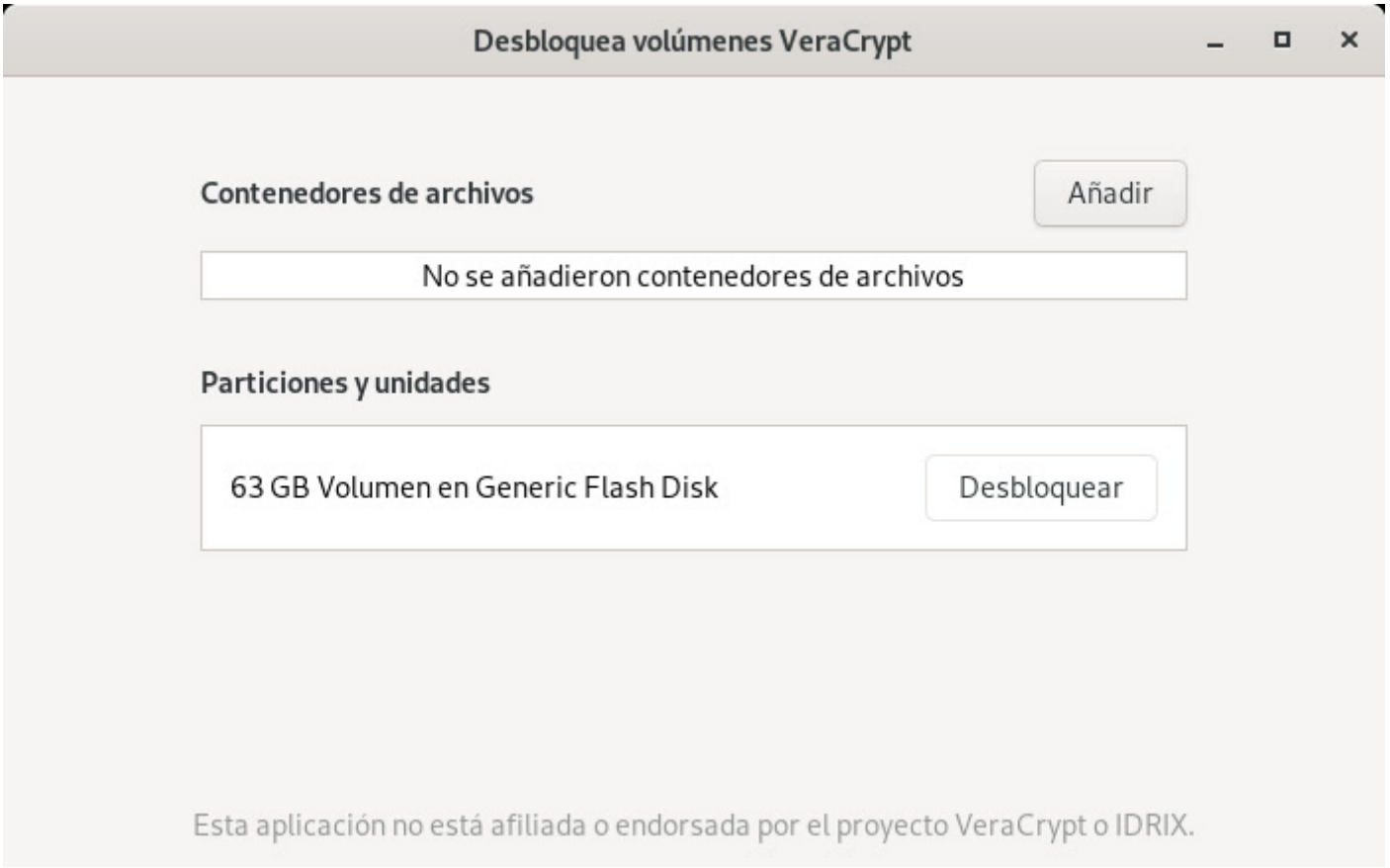
Cuando terminemos de usar el contenedor, en la pantalla principal de VeraCrypt, seleccionaremos la ranura y pulsaremos en "Desmontar".

Una ventaja de usar Tails, es que trae instalada una utilidad para desbloquear (pero no crear) archivos y unidades VeraCrypt, de tal forma que no tengamos que instalar VeraCrypt cada vez que iniciamos Tails y queramos desbloquear un archivo o unidad.

Para acceder a esta herramienta, hay que pulsar en la sección de aplicaciones (a la izquierda del todo en la barra superior de Tails) y lo encontraremos en la sección de "Utilidades", con el nombre "Desbloquea volúmenes VeraCrypt":



Si bien la interfaz gráfica no es la misma, es bastante intuitiva. Dispone de una sección para cargar archivos y otra para cargar dispositivos. De hecho, si se conecta, por ejemplo, una unidad USB cifrada con VeraCrypt, automáticamente aparecerá para ser desbloqueada en la sección de dispositivos:



Para desbloquear, aparecerá una ventana parecida a la de la aplicación de Veracrypt, en la que se solicitará la contraseña y otros campos en caso de que apliquen.

Limitaciones

Como hemos ido dejando caer, existe alguna limitación en cuanto al cifrado se refiere, de la que hay que advertir.

En primer lugar, los algoritmos de cifrado no son infalibles en cuanto a su diseño y su implementación. Por un lado, en cuanto al diseño, los algoritmos de cifrado son algoritmos matemáticos que no son necesariamente perfectos y que pueden romperse de diversos modos. Algunos de estas formas de romperlos son el Time-Memory Trade-Off (TMTO), los ataques de diccionario, los ataques de fuerza bruta, claves inseguras por propiedades criptoanalíticas, etc. En cuanto a las vulnerabilidades en la implementación, básicamente consisten en que los algoritmos están mal programados, por muy seguros que sean teóricamente, y permiten ataques específicos según el fabricante o desarrollador.

En segundo lugar, aunque los algoritmos de cifrado mantienen los archivos cifrados en reposo, cuando un archivo se descifra, este puede quedar almacenado en un directorio temporal del sistema operativo, pueden quedar trazas en la RAM y si el dispositivo está comprometido (pinchado por la policía), una vez descifrado, el archivo será legible por el atacante. Este tipo de amenazas son difíciles de evitar por un usuario estándar, pero existen algunas formas de evitarlo. Para mitigar el hecho de que se almacenen en algún directorio temporal, es mejor utilizar Tails, tal y como explicábamos en nuestra guía sobre Tor, ya que al apagar la computadora se eliminará toda la información generada durante la sesión, porque se almacena en la memoria RAM y el propio sistema operativo Tails realiza acciones de borrado, aunque no del todo infalibles. Para evitar el problema de que quede almacenada información en la memoria RAM, pueden utilizarse técnicas de *shredding*, aunque no son muy accesibles para un usuario estándar y, en un futuro, podríamos desarrollar una herramienta para hacerlo. Por ahora, una solución bruta es la de utilizar la computadora como se utilizaría de normal, de tal forma que la RAM vaya pisando datos antiguos, y la forma de acelerar este proceso es utilizando programas que consuman mucha RAM: el navegador, ver vídeos en Internet, jugar a videojuegos, etc. Son soluciones brutas, pero pueden valer.

En tercer lugar, es conocido que el desarrollo de la capacidad computacional provoca que las claves de cifrado puedan adivinarse de forma cada vez más rápida, sobre todo con las computadoras cuánticas que, aunque aún están en pañales, en un futuro podrían adivinar claves de cifrado en muy poco tiempo. Por ahora las computadoras actuales y las de desarrollo previsible en los próximos años son muy limitadas para poder adivinar claves con longitudes razonables y es este el criterio que principalmente se usa (por parte de empresas, organismos gubernamentales y por la ciberseguridad en general) para determinar si un algoritmo es seguro o no. Aquí, con longitud no nos referimos a la longitud de la clave que una o uno escribiría para cifrar un archivo, sino a la longitud de clave que utiliza un determinado algoritmo. Por ejemplo, AES-128 (AES con longitud de clave de 128 bits) es menos seguro que AES-256, usando ambos una misma contraseña de usuario que no tiene que tener una longitud de 128 o 256 bits (por ejemplo, "contraseña123"). Otro criterio para medir la seguridad de una clave es su entropía, propiedad que nos informa sobre la imprevisión de una clave; cuanta más entropía, mejor es la clave.

Por todas estas limitaciones, siempre es mejor reducir la cantidad de datos sensibles que almacenamos, aunque estén cifrados. Del mismo modo que es recomendable almacenarlo en soportes extraíbles para poder esconderlos o deshacerse de ellos. En

cualquier caso, el cifrado de la información sensible es siempre un buen aliado y, por tanto, es mejor utilizarlo que no utilizarlo.

Colectivo 406