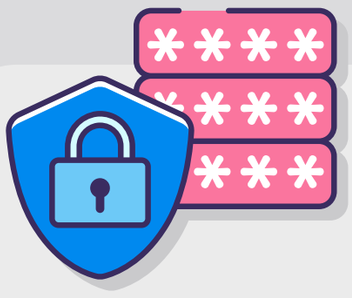
Cifrado de Sistema Operativo en Windows y Mac OS.



1. Cifrado

El cifrado es un proceso matemático que utiliza códigos y claves para comunicarnos de forma privada. A lo largo de la historia, la gente ha utilizado métodos cada vez más sofisticados de cifrado para enviarse mensajes entre sí con el objetivo de que no puedan ser leídos por cualquier persona además de los destinatarios.

Las primeras formas de cifrado a menudo eran operaciones simples que podían realizarse a mano, por ejemplo, el "cifrado César" de la antigua Roma. Hoy en día, las computadoras son capaces de realizar un cifrado mucho más complejo y seguro para nosotros. Los propósitos para los cuales la tecnología criptográfica existe se ha expandido más allá de los mensajes secretos; hoy en día, la criptografía se puede utilizar para otros fines, por ejemplo para verificar la autoría de los mensajes o la integridad de las descargas de software, o para navegar la Web anónimamente[1].

1.1. Importancia del Cifrado

1.1.1. Seguridad Digital y Código abierto

La Seguridad Digital es un proceso colectivo de medidas preventivas y reactivas para proteger nuestra información y la información de los demás. Las prácticas de cifrado se insertan dentro de la seguridad digital para proteger la información que almacenamos y la que fluye por los diversos medios por los que nos comunicamos.

Las cualidades del software libre, permiten que éste pueda ser distribuido, estudiado, modificado y usado libremente. Son estas cualidades las que permiten que el desarrollo e implementación de programas de cifrado, entre otros, continúen y se auditen por una comunidad que lo valida, y reporta a la comunidad usuaria que el software hace lo que dice hacer, y aportando en la resolución de problemas que las y los usuarios finales reportan.

En el cifrado, el código debe ser conocido y sólo la clave secreta debe permanecer resguardada del acceso público. Por lo tanto, hay un consenso de que el código debe ser abierto, sin embargo hay un debate sobre si sus implementaciones deben de ser de código abierto (público) o software propietario (secreto), ya que el software propietario decide en qué momento y quienes desarrollan la auditoría de su código, y por otro lado, en el software de código abierto se puede hacer en cualquier momento por cualquier persona que lo desee[2].

El software que no es libre (privativo) a menudo es *malware* (diseñado para maltratar a los usuarios). El software que no es libre está controlado por quienes lo han desarrollado, lo que los coloca en una posición de poder sobre los usuarios; esa es la injusticia básica. Habitualmente, esto suele realizarse mediante funcionalidades maliciosas[3]. Algunas de estas funcionalidades maliciosas, han sido documentadas[3] por la FSF (Free Software Foundation). También se documentó al menos un caso en que el gobierno solicitó a Apple romper el cifrado de un usuario específico, dicho proceso no se implementó por parte de Apple, pero sí de forma independiente lo cual permite saber de la vulnerabilidad del cifrado en dispositivos Apple[4].

1.2. Consideraciones de Seguridad

- **Capacidad computacional:** Con suficiente tiempo o recursos computacionales es posible adivinar la llave y descifrar el "mensaje", pero los algoritmos actuales de cifrado hacen muy difícil esta tarea.
- **Vulnerabilidades:** Las supuestas fallas en los sistemas de cifrado son más bien fallas en las aplicaciones que usan cifrado. Hasta ahora no se sabe que los últimos algoritmos de cifrado hayan sido rotos.
- **¡Advertencia!:** Si se pierde esta llave o la contraseña que la resguarda nadie ni siquiera tu podrás tener acceso a tus correos y archivos. Por esto es muy importante escoger una contraseña que te sea difícil de olvidar.
- **El punto más débil del cifrado es la contraseña.** Por esto, la contraseña debe ser fuerte, contener al menos 12 caracteres, utilizar mayúsculas y minúsculas, números, y caracteres especiales y debes cambiarla con cierta recurrencia.
- **El cifrado por si** mismo no te hace anónimo.

1.3 Cifrado de disco

Con el cifrado de disco, se protege tanto el sistema operativo (SO) programas instalados y datos personales. Se cifra para que no se pueda acceder al contenido mientras el dispositivo está apagado o (en algunas implementaciones) cuando se cierra la sesión. Sin el cifrado de disco, cuando alguien roba o accede sin autorización al dispositivo, podría leer archivos, acceder a cuentas en línea y robar la identidad digital de la persona propietaria. También podría instalar malware que le permita acceder de forma remota a las actividades realizadas dentro del dispositivo, por ello es importante mantener el sistema protegido con un programa Antivirus.

1.4 Cifrado transparente

El cifrado, puede funcionar de diversas maneras, dependiendo de cómo éste sea implementado. El cifrado transparente es una implementación utilizada por algunos programas de cifrado en que los datos son automáticamente cifrados o descifrados al mismo tiempo que son generados o guardados. Cuando se enciende el dispositivo, los archivos se vuelven accesibles inmediatamente después de que se proporciona una llave, dejándolos tan accesibles como en cualquier otro sistema que no esté cifrado. Así, ningún dato que esté almacenado en un disco cifrado puede ser leído sin proporcionar previamente la contraseña o el archivo clave[5]. En general, cada método en donde los datos se cifren de manera transparente durante la escritura y se descifren durante la lectura puede ser llamado cifrado transparente.

1.5 Cifrado de archivos

Además del cifrado de disco, es posible realizar el cifrado a archivos o crear contenedores cifrados. Esto puede realizarse de manera complementaria junto con el cifrado de disco, o en caso de no contar con este, se puede realizar como una medida de seguridad. Ambas implementaciones de cifrado dependen de programas específicos, por ejemplo, en sistemas operativos con GNU/Linux puede cifrar archivos con el programa GPG que viene integrado de forma nativa, es decir, como elemento esencial del sistema. Por otro lado, un ejemplo de programa con el cual se puede implementar el cifrado a través de contenedores es VeraCrypt (disponible para Windows, Mac OSy Linux) con el cual asignas cierto tamaño a un contenedor en el que podrás acceder en un proceso que incluye montar el contenedor cifrado y autenticar el acceso con una contraseña, proceso que se describe más adelante.

1.6 Recuperación de contraseñas

Los mecanismos de recuperación de contraseña pueden ser considerados esenciales para el uso de las soluciones de cifrado a través de métodos fáciles y a la vez seguros, que apliquen en el caso de olvidar una contraseña o casos más complejos dentro de empresas. Es indispensable que la gestión de estos mecanis-

mos de recuperación sean bien conocidos sobre todo por los y las usuarias finales, para proceder de manera adecuada cuando se requiere recuperar una contraseña, así como para proteger debidamente estos mecanismos y evitar que alguien sin autorización descifre estos dispositivos.

2. Cifrado de Sistema Operativo (SO)

De acuerdo al sistema operativo y a las características del equipo, puede ser más conveniente implementar cifrado con uno u otro programa. Por ejemplo, si el dispositivo cuenta con una versión de Windows con posibilidad de activar el cifrado nativo Bitlocker, ésta será la opción preferida a implementar , de otro modo habría que cifrar con otro software, por ejemplo Veracrypt. En el caso de dispositivos Apple, estos cuentan con un programa de cifrado nativo llamado FileVault a partir de la versión OS X Lion.

En la guía vamos a revisar los métodos para cifrar Windows con BitLocker y FileVault en Mac OS. En el caso de sistemas Linux es común que el cifrado se implemente cuando se está instalando el sistema. Además se guiará en el proceso de creación de contenedores cifrados con VeraCrypt, este proceso puede implementarse en sistemas GNU/Linux, Windows o MacOS y puede ser un mecanismo complementario para gestionar contenedores cifrados que protejan la información más sensible.

2.1 Cifrado en Windows con BitLocker

El cifrado de unidad BitLocker es una característica de protección de datos que se integra en el sistema operativo y previene de forma importante la exposición de datos en equipos perdidos, sustraídos o retirados inadecuadamente.

El módulo de plataforma confiable (TPM Trusted Platform Module) es un componente de hardware instalado en muchos equipos nuevos por los fabricantes de equipos. Funciona con BitLocker para ayudar a proteger los datos de usuario y para garantizar que un equipo no se haya manipulado mientras el sistema estaba sin conexión, es decir, puede ser usado para autenticar un hardware. Si el disco duro se elimina de ese dispositivo y se coloca en otro, el proceso de descifrado fallará[6].

Además del TPM BitLocker ofrece la opción de bloquear el proceso de inicio normal hasta que el usuario proporcione un número de identificación personal (PIN) o inserte un dispositivo extraíble, como una unidad flash USB, que contenga una clave de inicio. Estas medidas de seguridad adicionales proporcionan autenticación multifactor y la garantía de que el equipo no se inicia o reanuda desde la hibernación hasta que se ofrezca el PINo la clave de inicio correctos[7].

Versiones de Windows con BitLocker disponible[8]:

- Ediciones Ultimate y Enterprise de Windows Vista y Windows 7
- Ediciones Pro y Enterprise de Windows 8 y 8.1
- Ediciones Pro, Enterprise y Education de Windows 10

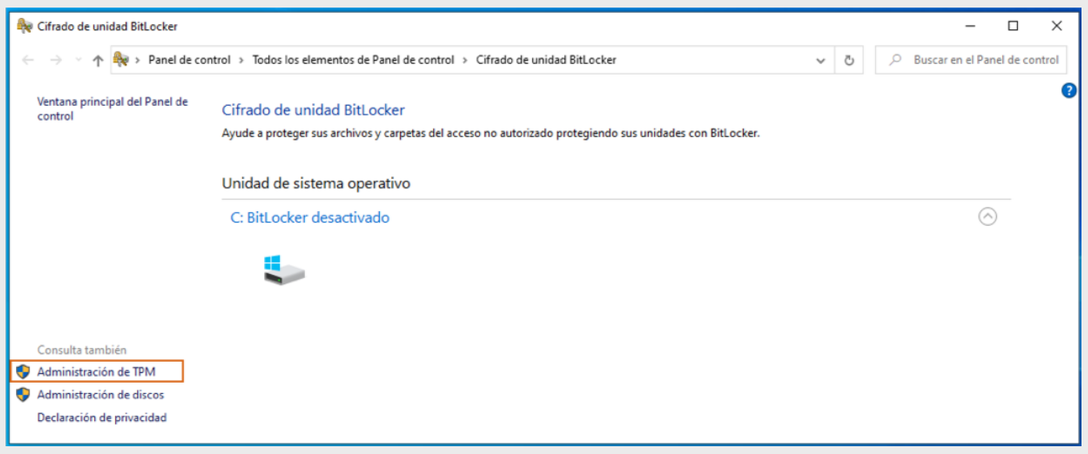
Cifrado de disco sin un chip TPM (Trusted Platform Module)

A partir de Windows 7, si no existe un chip TPM en el equipo, aún es posible que la unidad del sistema operativo sea cifrada sin TPM y USB. Se puede usar una contraseña como protector de la unidad del sistema operativo[7]. Para ello se debe habilitar una política de grupo (GPO, Group Policy, es una característica que controla el entorno de trabajo de las cuentas de usuario y del ordenador).

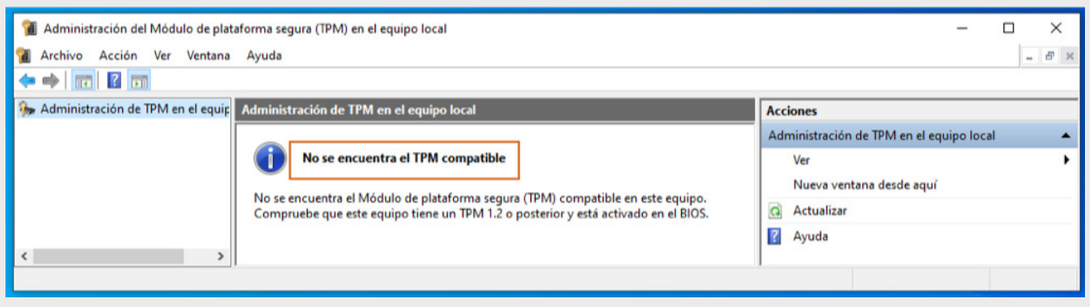
Verificar si el dispositivo cuenta con TPM

Dentro de “Panel de control” buscamos “Cifrado de unidad BitLocker”, ubica y abre el “Administrador de TPM.

Cifrado de Sistema Operativo en Windows y Mac OS

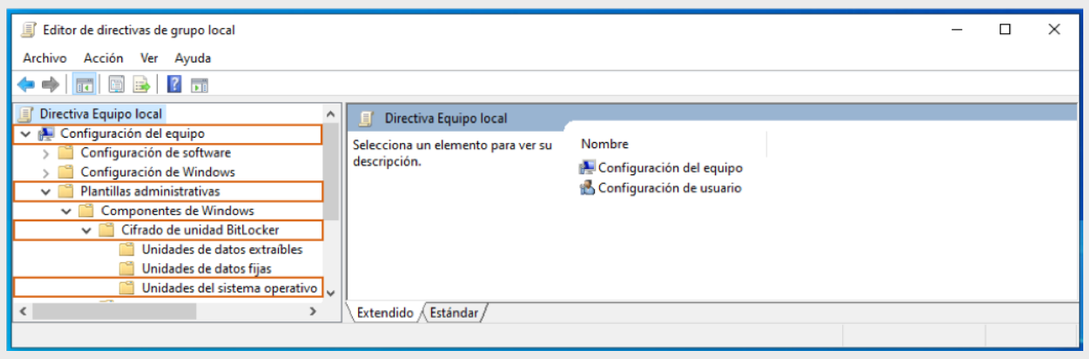


Si el mensaje es “No se encuentra el TPMcompatible”, debe habilitarse la opción de BitLocker sin TPM

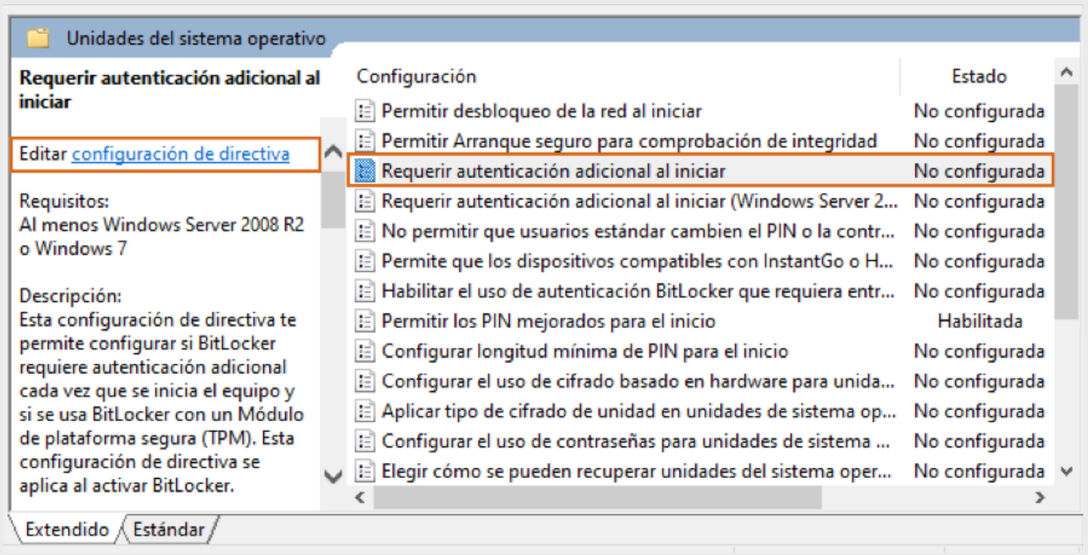


Habilitar BitLocker sin TPM

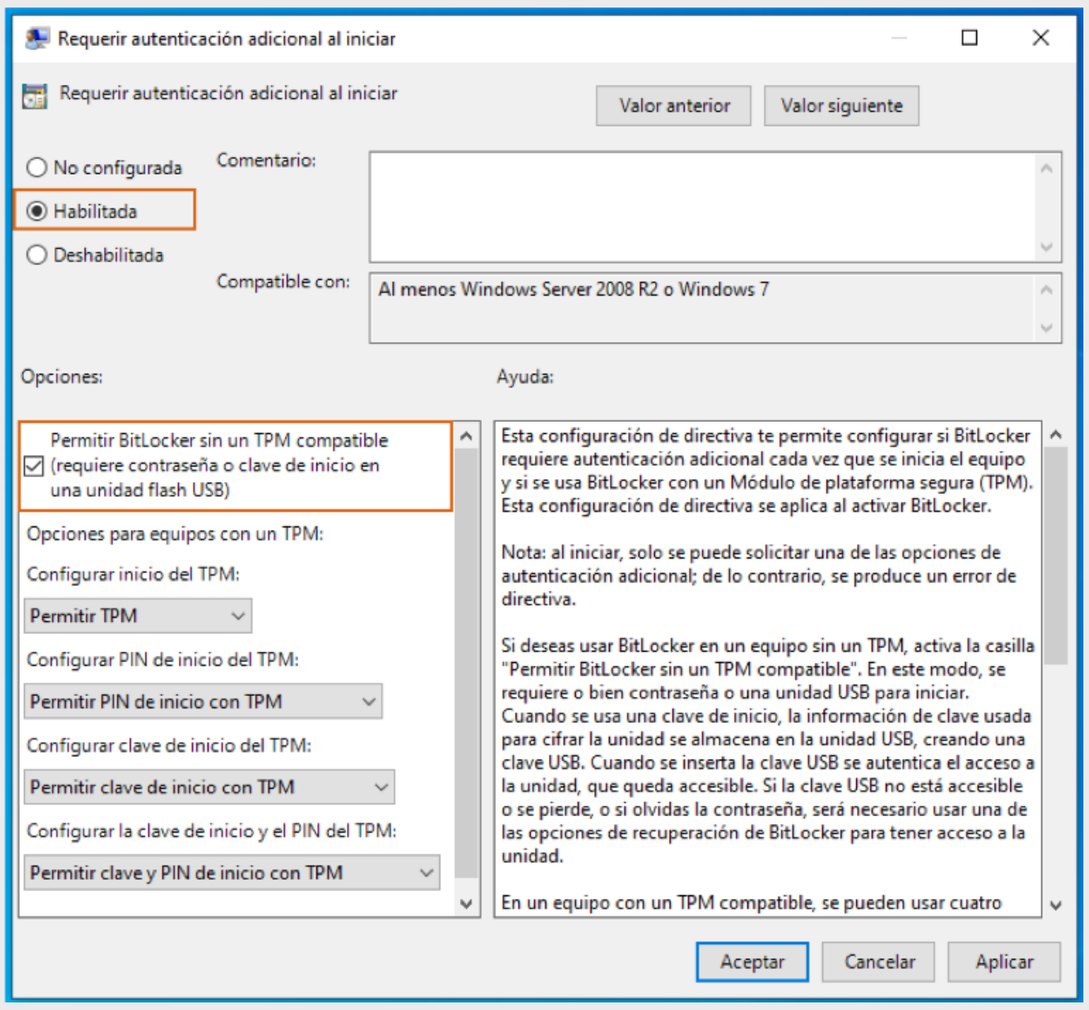
Abrir el “Editor de objetos de directiva de grupo”, el cual puedes encontrar buscándolo desde “Inicio” como “gpedit” y accede hasta la configuración llamada “Unidades del sistema operativo”.



Dentro de “Unidades del sistema operativo”, seleccionar “Requerir autenticación adicional al iniciar” y “Editar configuración de directiva”.

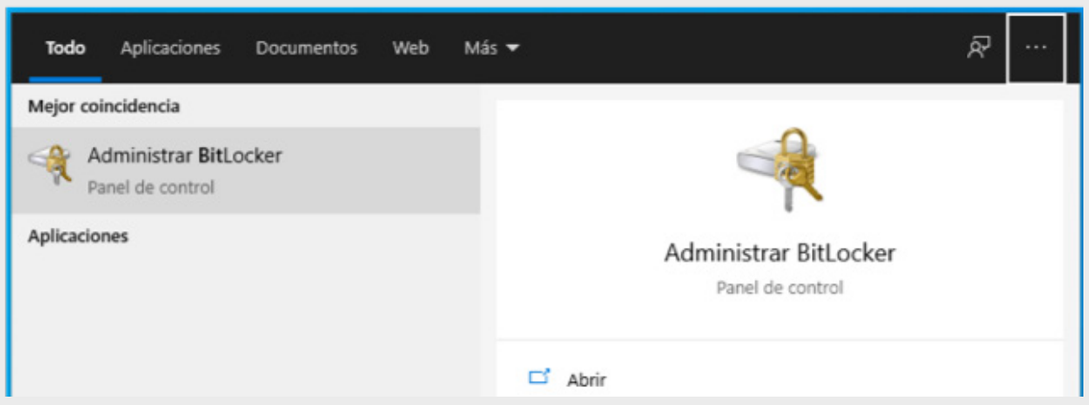


Una vez dentro se habilita y se asegura de seleccionar “Permitir BitLocker sin un TPM compatible”, finalmente “Aplicar” y “Aceptar”. Después de habilitar esta política, es posible activar BitLocker aún cuando el dispositivo no cuente con un TPM o un TPM compatible.

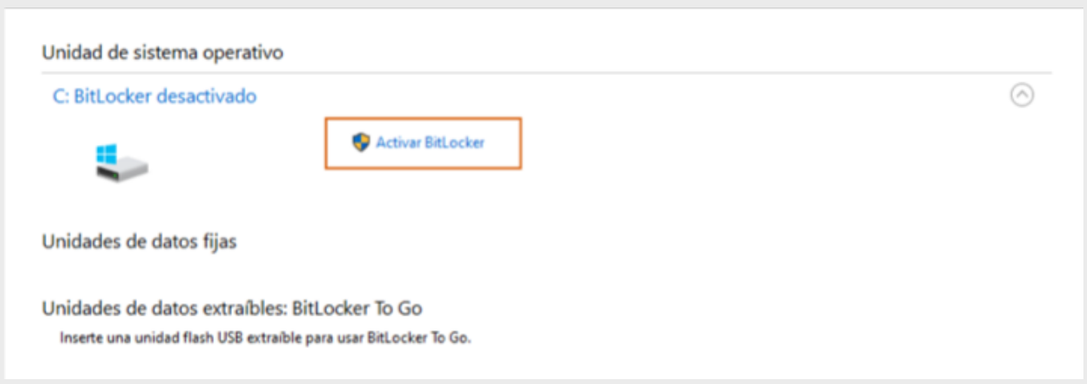


Activar BitLocker

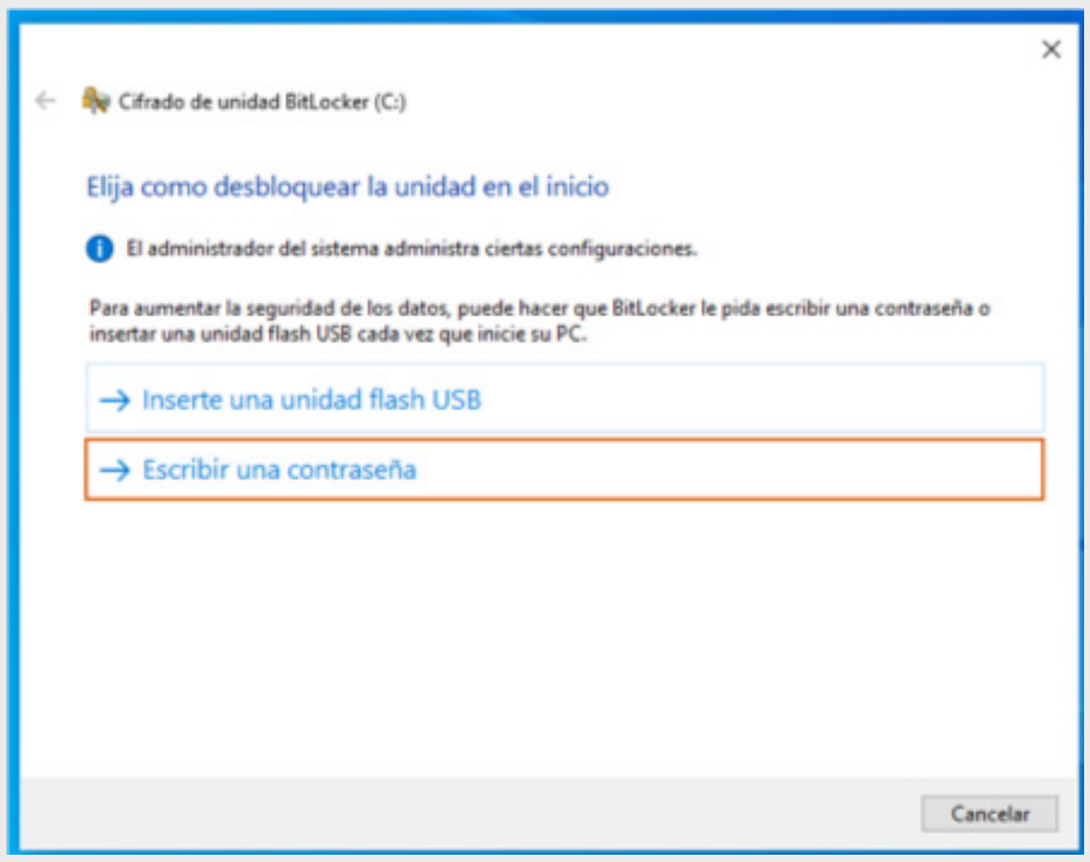
1. Accede al “Administrador de BitLocker” desde la tecla de “Inicio”.

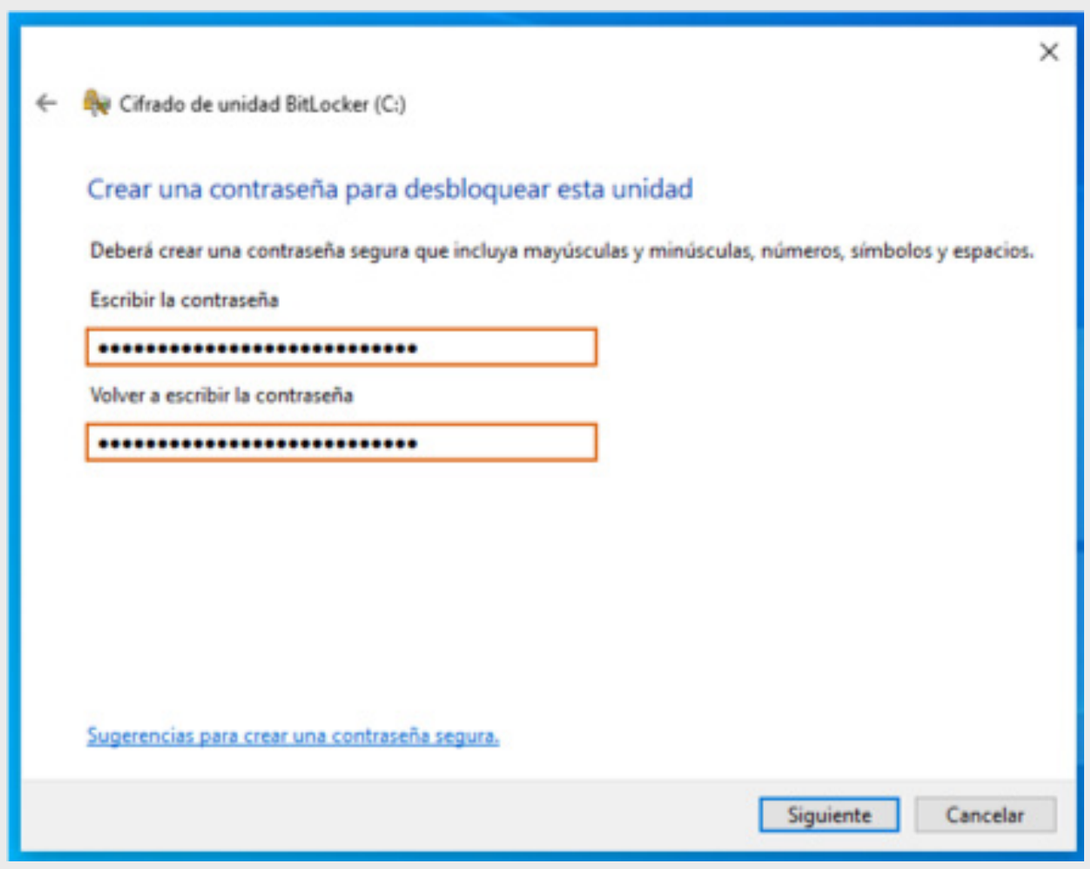


2. Selecciona “Activar BitLocker”.

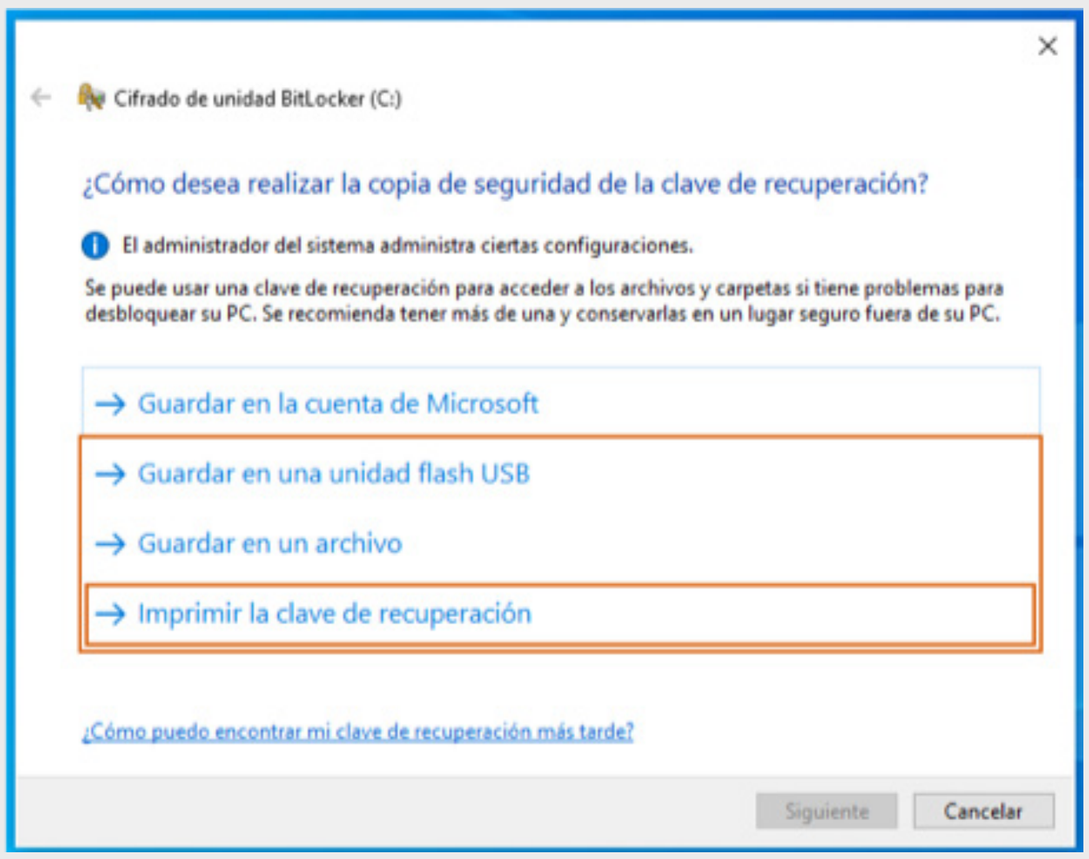


3. Una vez que se abre el programa de "Cifrado de unidad BitLocker", solicita seleccionar una opción para desbloquear el sistema una vez que este esté cifrado. Puede elegirse la que parezca más adecuada, sin embargo, se recomienda usar la opción de "Escribir una contraseña", debido a que es más práctico que insertar una USB. Después de esto, se escribe la contraseña en los dos campos disponibles, la segunda vez se escribe para verificar que es la que deseamos y la hemos escrito bien.

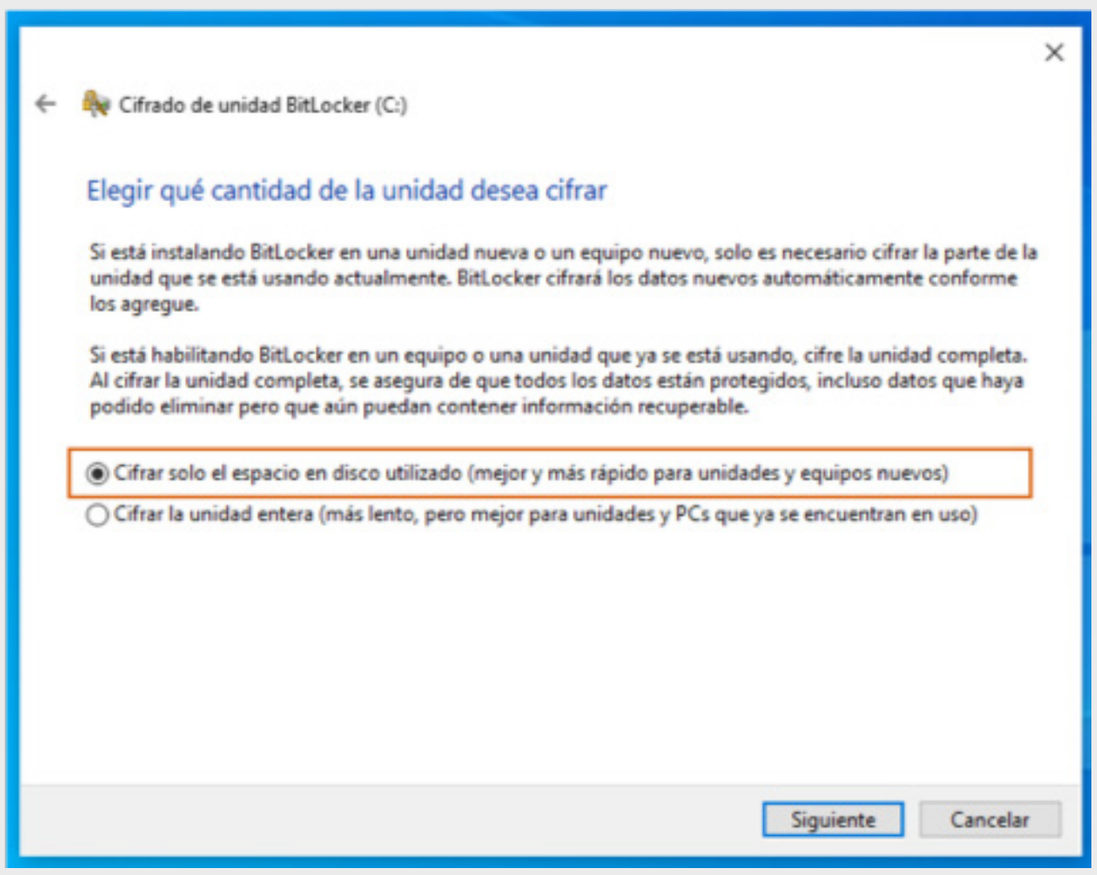




4. Las opciones para resguardar la clave de recuperación recomendadas son las enmarcadas (la opción de "Guardar en la cuenta de Microsoft" no se recomienda para no centralizar la información). La opción "Guardar en una unidad flash USB" y "Guardar en un archivo", solicitarán un dispositivo externo donde poder colocar el archivo de recuperación. También es posible imprimir la clave ya sea en papel o en un archivo PDF, el cual deberás resguardar.

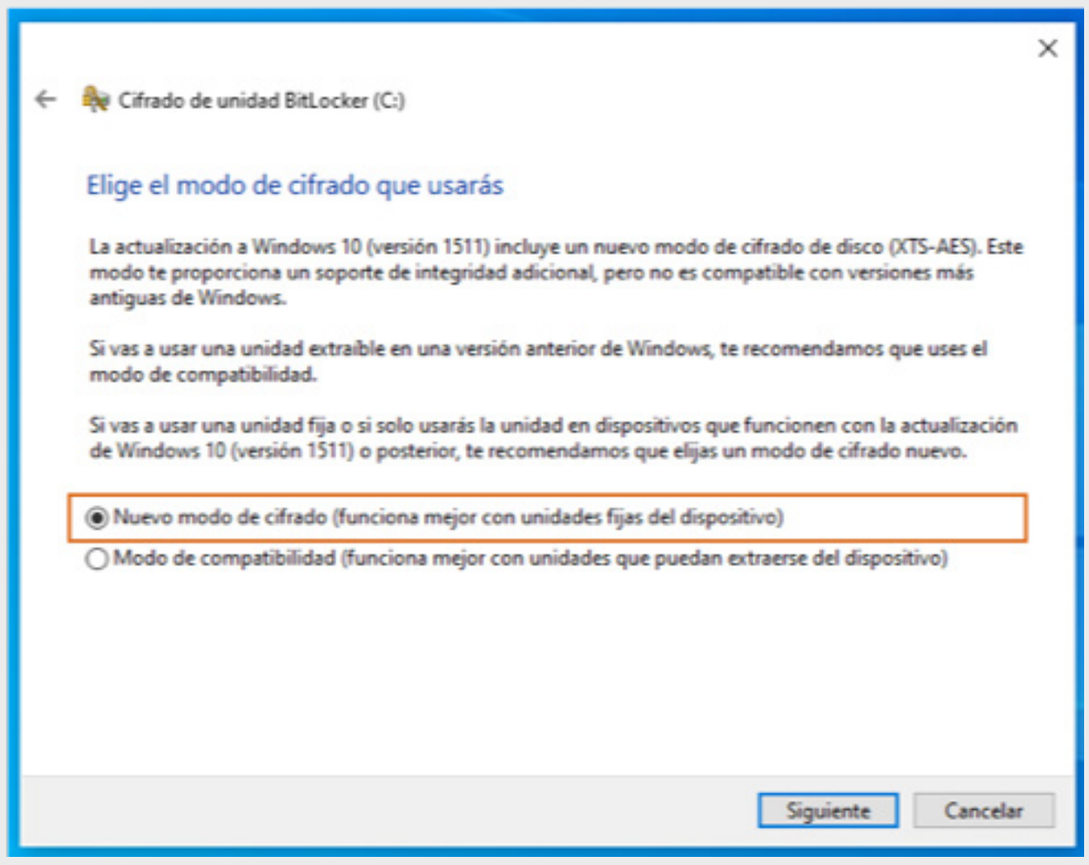


5. Las opciones siguientes dependen del estado de uso de tu dispositivo, si es nuevo o si tiene tiempo de uso. Como menciona el texto, si el dispositivo es nuevo, selecciona la primera opción, de otro modo, seleccionar la segunda (para ejemplos prácticos de la guía se selecciono la primera, selecciona la que corresponda a tu caso).

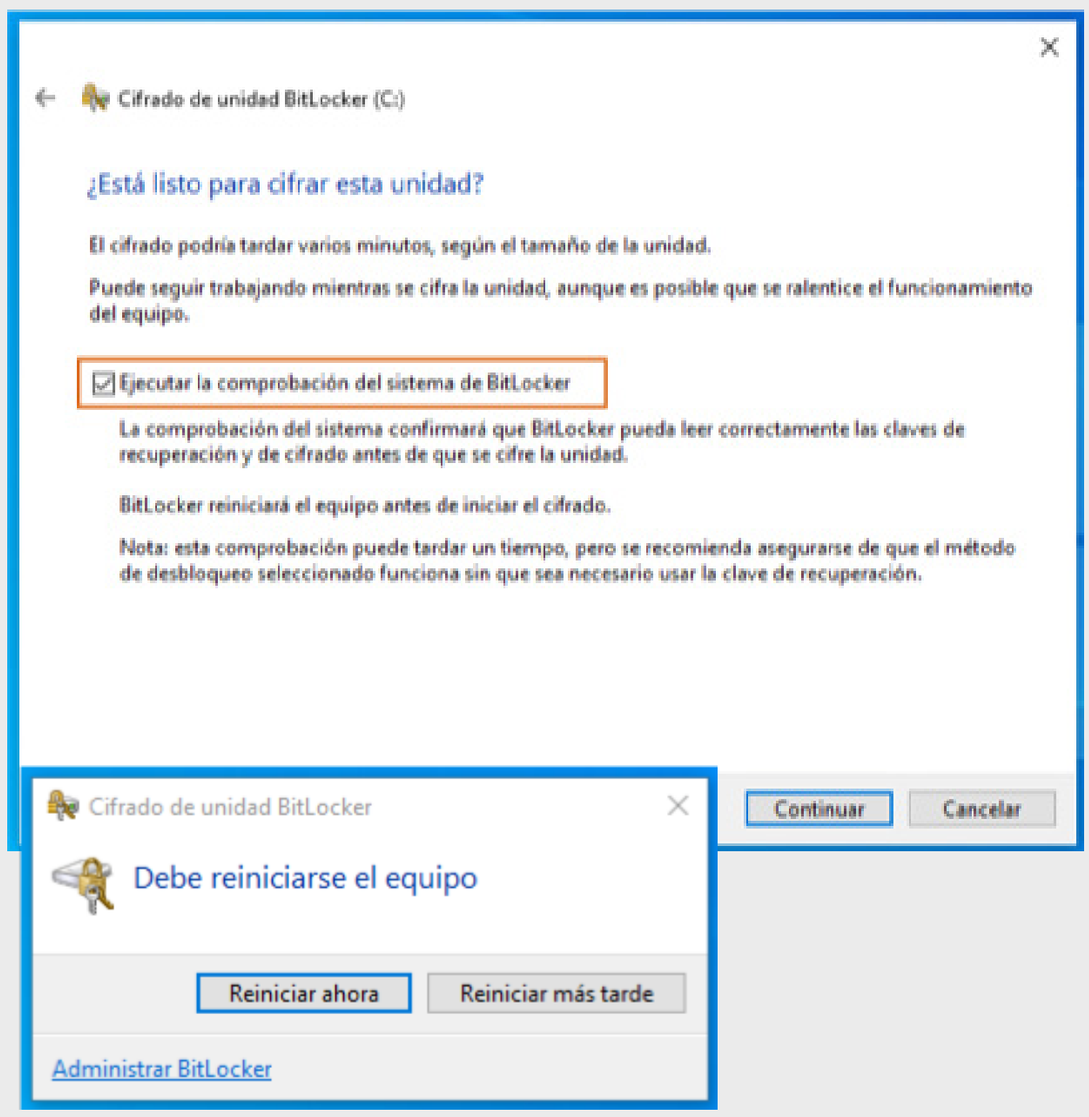


Cifrado de Sistema Operativo en Windows y Mac OS

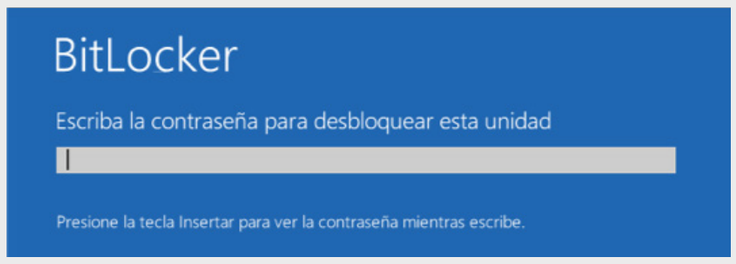
6. La siguiente opción también dependerá de la versión de sistema del dispositivo, pero básicamente puede elegirse la primera opción si el disco a cifrar no pretende ser extraído del dispositivo.



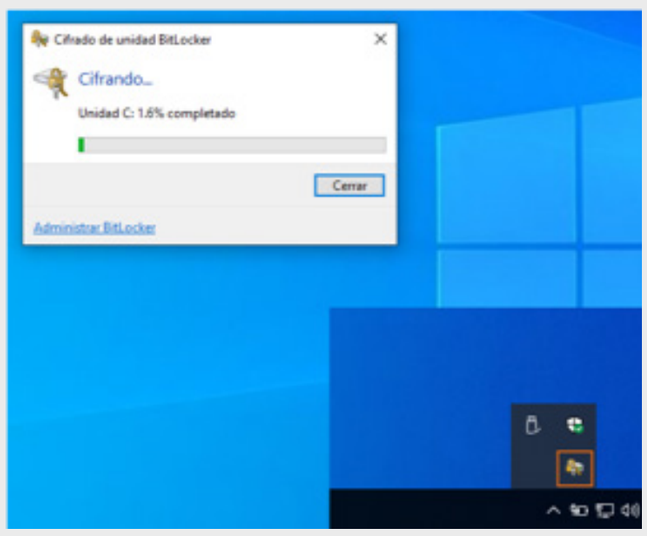
7. Finalmente, "Ejecutar la comprobación del sistema de BitLocker" permite verificar que se puede acceder a las claves de recuperación y reinicia el sistema para iniciar con el cifrado de disco.



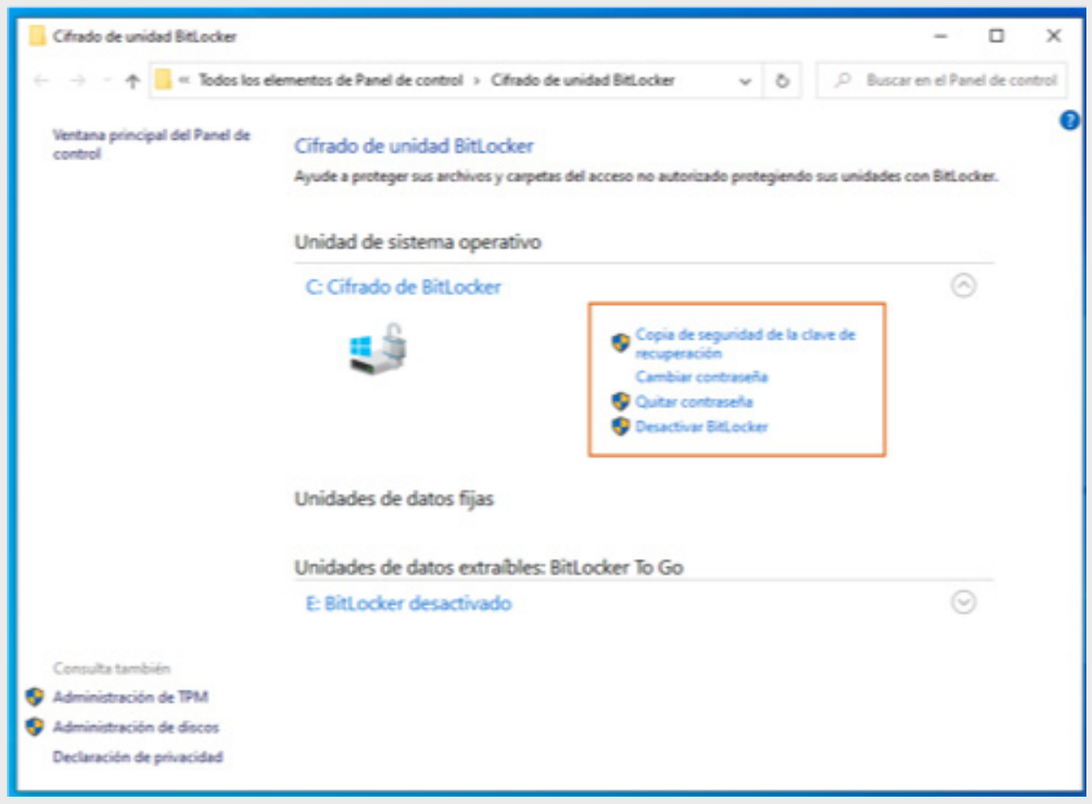
8. Al iniciar el sistema se solicita la contraseña de cifrado que en el paso 3 se ha tecleado.



9. Se puede acceder al estado del cifrado desde la barra de estado, seleccionando el icono de BitLocker.



10. Una vez que se ha terminado de activar el "Cifrado de unidad BitLocker", es posible acceder a las opciones de gestión.



Recuperación de contraseña BitLocker

El archivo impreso o resguardado contendrá un texto como el de abajo, con el cual es posible recuperar el acceso al disco cifrado en caso de olvidar la contraseña entre otros casos. Puedes consultar el proceso de recuperación en la documentación oficial[9].

> Clave de recuperación de Cifrado de unidad BitLocker
> Para comprobar que esta es la clave de recuperación correcta, compara el comienzo del
> siguiente identificador con el valor de identificador que se muestra en tu equipo.
> Identificador: 94225ED3-8C4C-47B9-A41F-09FDE9ABCD
> Si el identificador anterior coincide con el que se muestra en el equipo, usa la siguiente clave para desbloquear la unidad.
> Clave de recuperación:
> 576180-582857-105908-495286-449317-288904-263362-123456
> Si el identificador anterior no coincide con el que se muestra en el equipo, esta no es la clave correcta para desbloquear la unidad.
> Prueba con otra clave de recuperación o visita https://go.microsoft.com/fwlink/?LinkID=0123456 para obtener ayuda adicional.

2.2 Cifrado de disco en macOS

El cifrado de disco de FileVault (versión 2 actualmente) utiliza el cifrado XTS-AES-128, con una clave de 256 bits para ayudar a impedir el acceso no autorizado a la información en el disco de arranque.

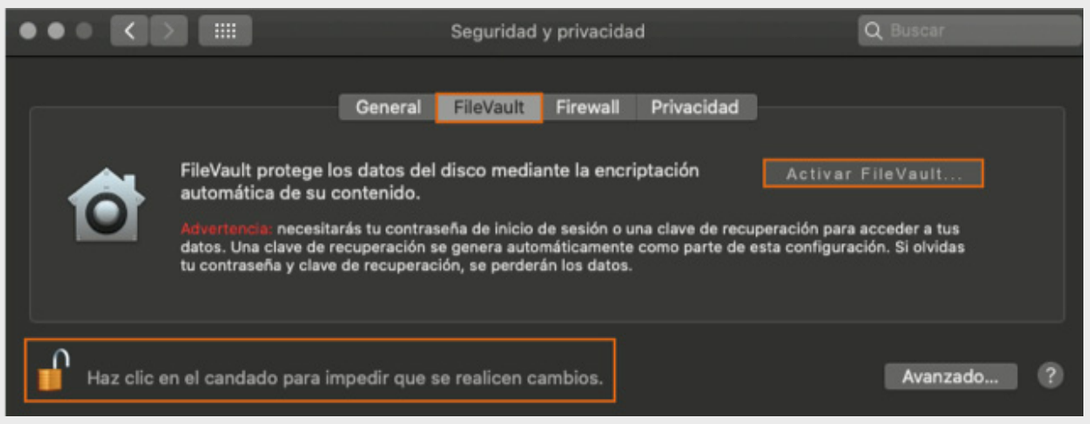
El cifrado XTS-AES es un modo de cifrado por bloques. En 2010, el Instituto Nacional de Estándares y Tecnología añadió el modo XTS a la lista de modos de cifrado por bloques AES. Por lo que es el modo de cifrado por bloques más reciente que se ha diseñado como alternativa a otros modos de cifrado por bloques disponibles. Elimina las posibles vulnerabilidades asociadas con algunos de los ataques de canal lateral10más sofisticados que podrían usarse para explotar las deficiencias de otros modos[11].

Activar FileVault

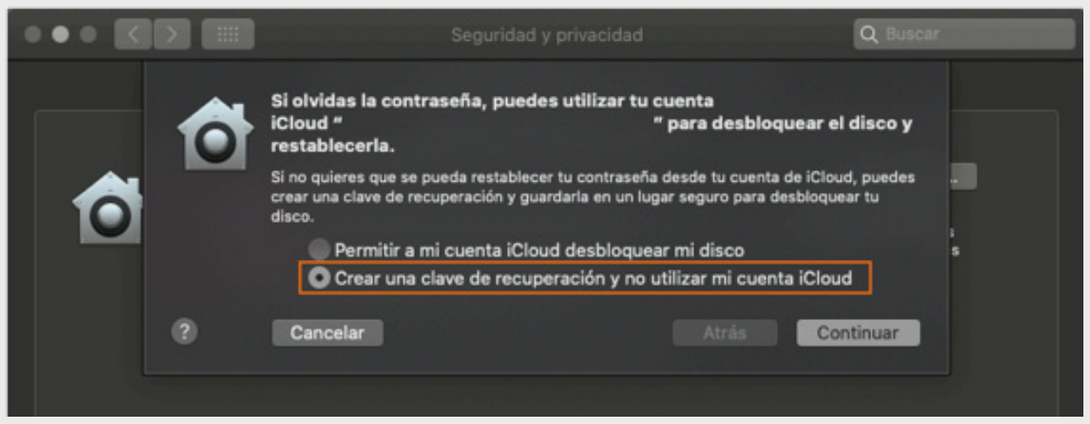
FileVault 2 está disponible en OS X Lion o posterior. Una vez activado, el dispositivo requerirá siempre la contraseña de tu cuenta.

1. Acceder a “Preferencias del sistema”, a este accedes desde el “Finder” o a través del menú “Apple” y seleccionar “Seguridad y privacidad”.

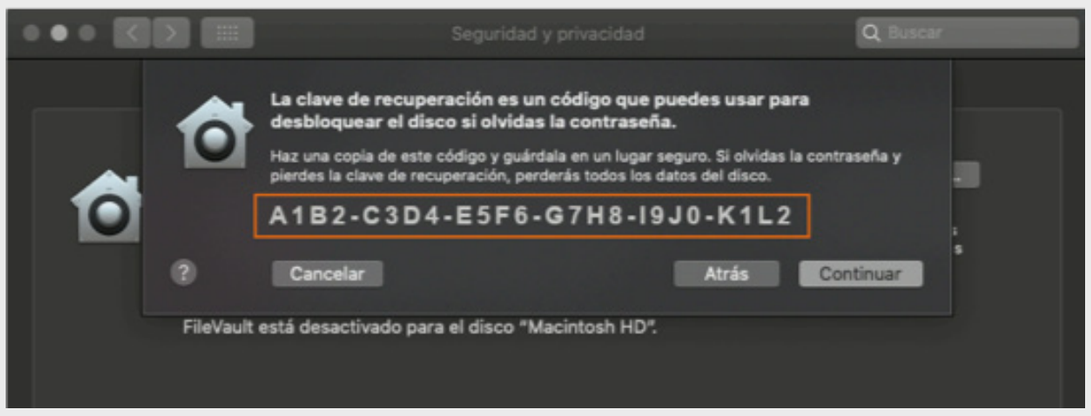
2. Dentro de “Seguridad y privacidad”, seleccionar la pestaña “FileVault”, hacer clic en el candado para desbloquear los permisos y poder realizar la activación de FileVault, ello requerirá que ingreses usuario y contraseña con permisos de administración. Una vez desbloqueado, hacer clic en “Activar FileVault”.



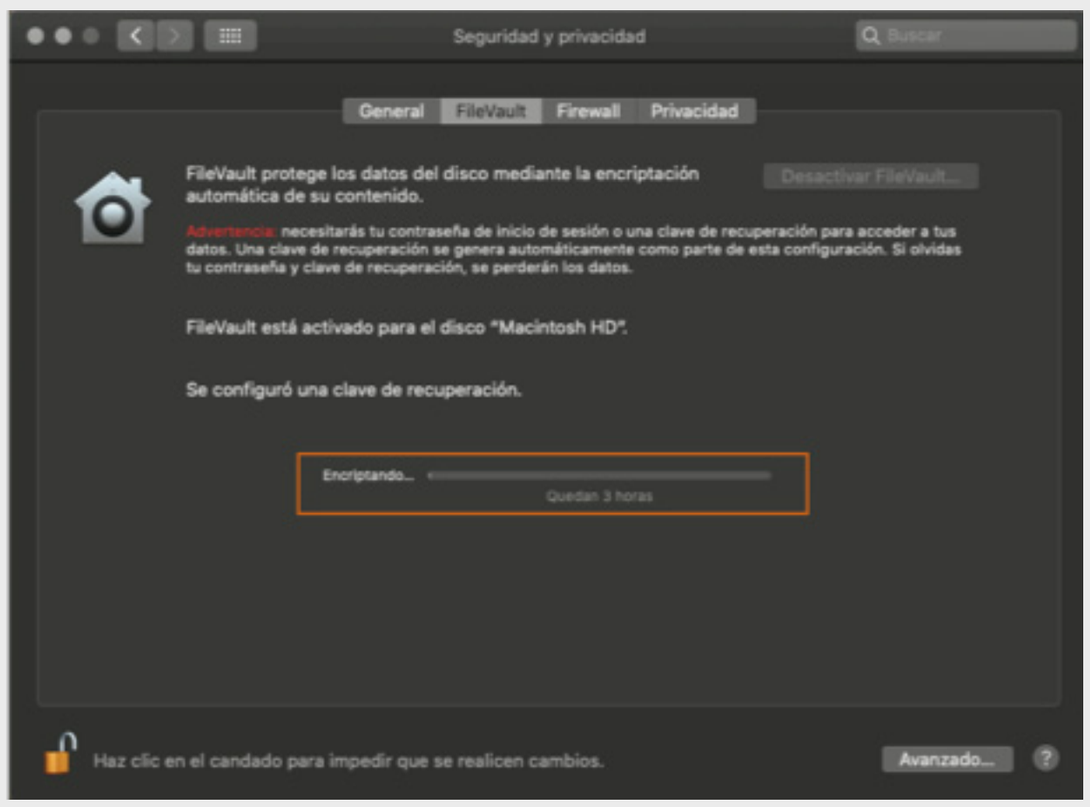
3. Se debe seleccionar el tipo de resguardo que se hará de la clave de recuperación, la opción que recomendamos es “Crear una clave de recuperación y no utilizar mi cuenta iCloud”, para no centralizar la información en tu cuenta de iCloud.



4. Ese tipo de resguardo genera una clave que deberás almacenar de manera segura, y has clic en “Continuar”. Esta clave la puedes resguardar en una USB de uso exclusivo, un dispositivo cifrado, un gestor de contraseñas como “KeePassXC”, etc. asegúrate de guardar varias copias.



5. El cifrado se produce en segundo plano mientras usas la Mac y solo cuando la Mac está activa y enchufada a una toma de CA. Puedes consultar el progreso en la sección de “FileVault” en las preferencias de “Seguridad y privacidad”. Todos los archivos nuevos que creas se cifran automáticamente a medida que se guardan en el disco de arranque. Cuando se completa la configuración de FileVault y reinicias la Mac, debes usar la contraseña de tu cuenta para desbloquear el disco y permitirle a la Mac que complete el inicio[12].



Para restablecer tu contraseña o cambiar la clave de recuperación de FileVault, desactivar FileVault y obtener más información, consulta la documentación oficial[13].

2.3 Cifrado de Archivos con Veracrypt

VeraCrypt es un programa de código abierto, que sirve para cifrar y ocultar datos que se consideren sensibles, empleando para ello diferentes algoritmos de cifrado, o una combinación de estos. Crea un volumen cifrado accesible a través de un archivo (como si este fuera la puerta de acceso), además es posible realizar cifrado de disco y unidades externas. Es un programa multiplataforma, es decir, está disponible su instalación para sistemas Windows, MacOS y GNU/Linux.

En VeraCrypt es posible crear dos tipos de volúmenes cifrados: ocultos y estándar.

Estándar[14]:

- Contenedor: Un volumen alojado en un archivo de VeraCrypt es un archivo normal, que puede residir en cualquier tipo de dispositivo de almacenamiento.
- Partición del sistema: Una partición VeraCrypt es una partición del disco duro cifrada con VeraCrypt.

Ocultos[15]:

- Un volumen de VeraCrypt se crea dentro de otro volumen de VeraCrypt (dentro del espacio libre). Incluso cuando el volumen exterior está montado, debería ser imposible probar si hay un volumen oculto dentro de él o no, porque el espacio libre de cualquier volumen de VeraCrypt siempre está lleno de datos aleatorios cuando se crea el volumen y ninguna parte del volumen oculto puede distinguirse de los datos aleatorios.

Descarga el programa de acuerdo al sistema operativo del dispositivo desde el sitio oficial: https://www.veracrypt.fr/en/Downloads.html.

Instalación en GNU/Linux

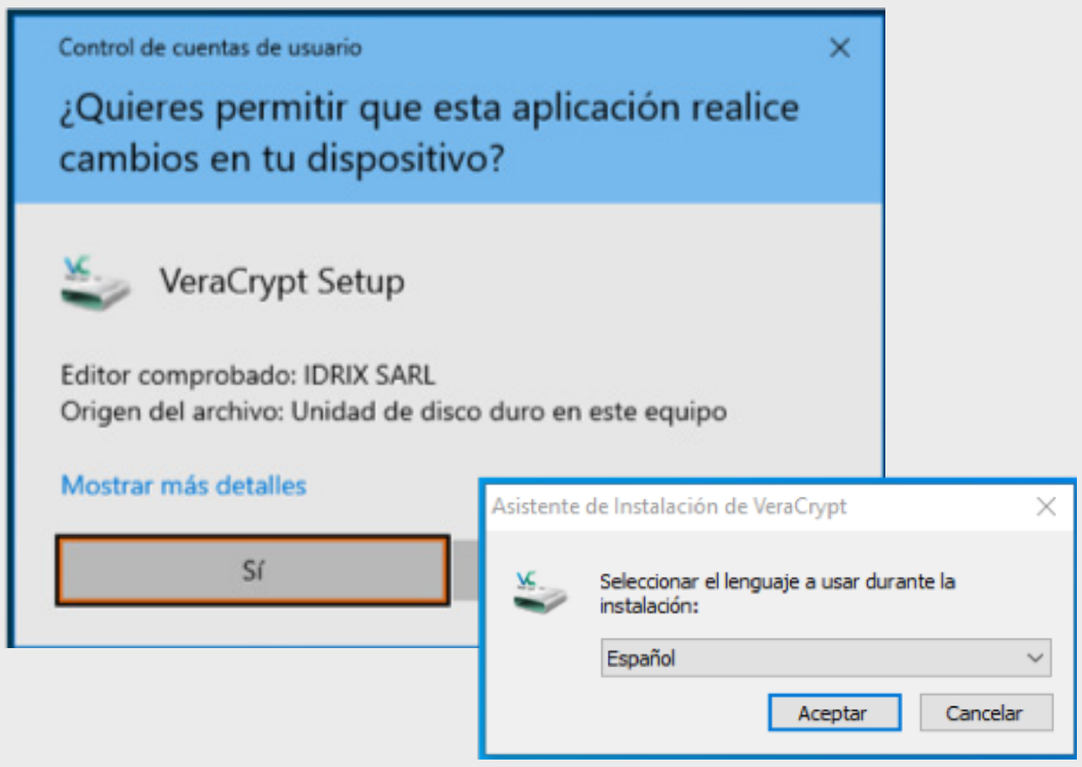
Instala de acuerdo al sistema operativo con que cuenta tu dispositivo. En el caso de GNU/Linux, para demostración se utiliza Debian 10. Para instalarlo ejecuta en una terminal el siguiente comando:

```
$ sudo dpkg -i Descargas/veracrypt-1.24-
Update4-Debian-10-amd64.deb
```

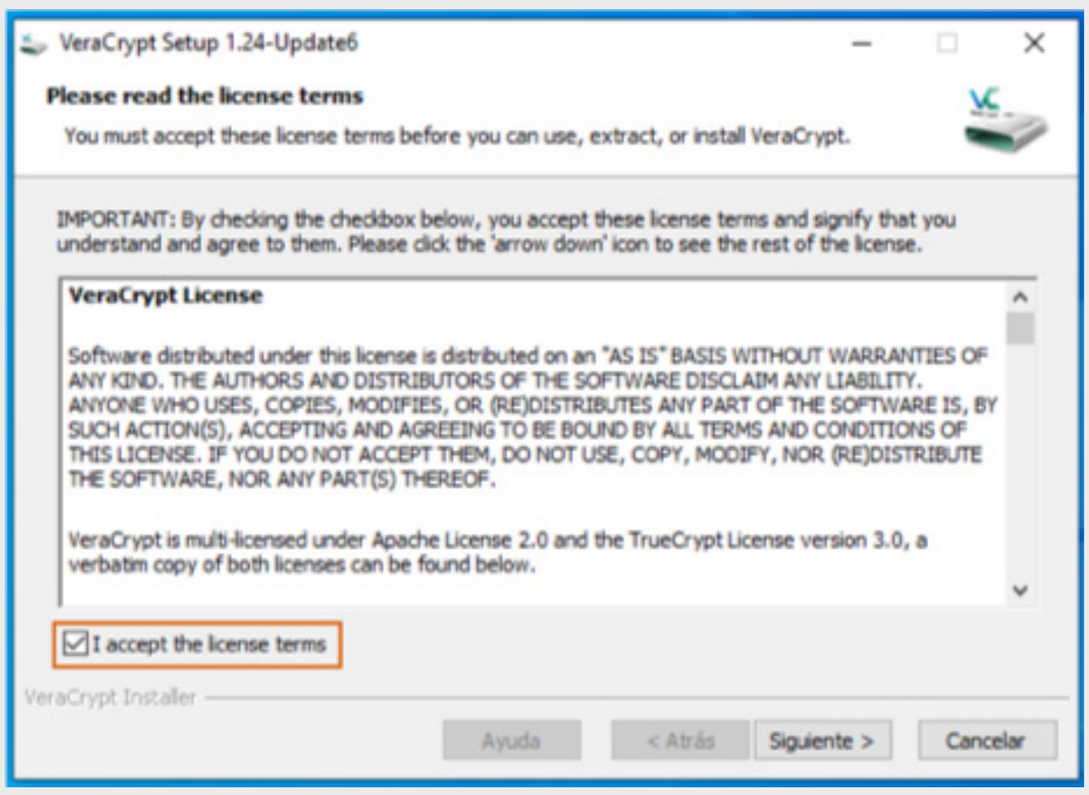
Te solicitará la contraseña de tu usuario/a para realizar la instalación.

Instalación en Windows 10

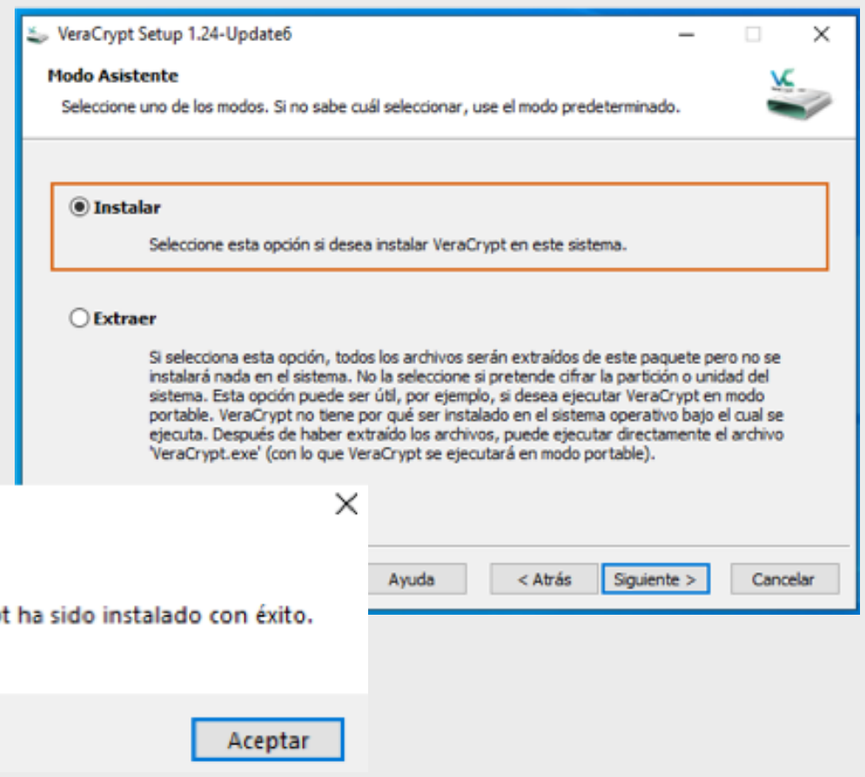
1. Ejecuta en instalador, permite la instalación de VeraCrypt y selecciona el idioma.



2. Acepta los revisa y acepta los términos de la licencia.

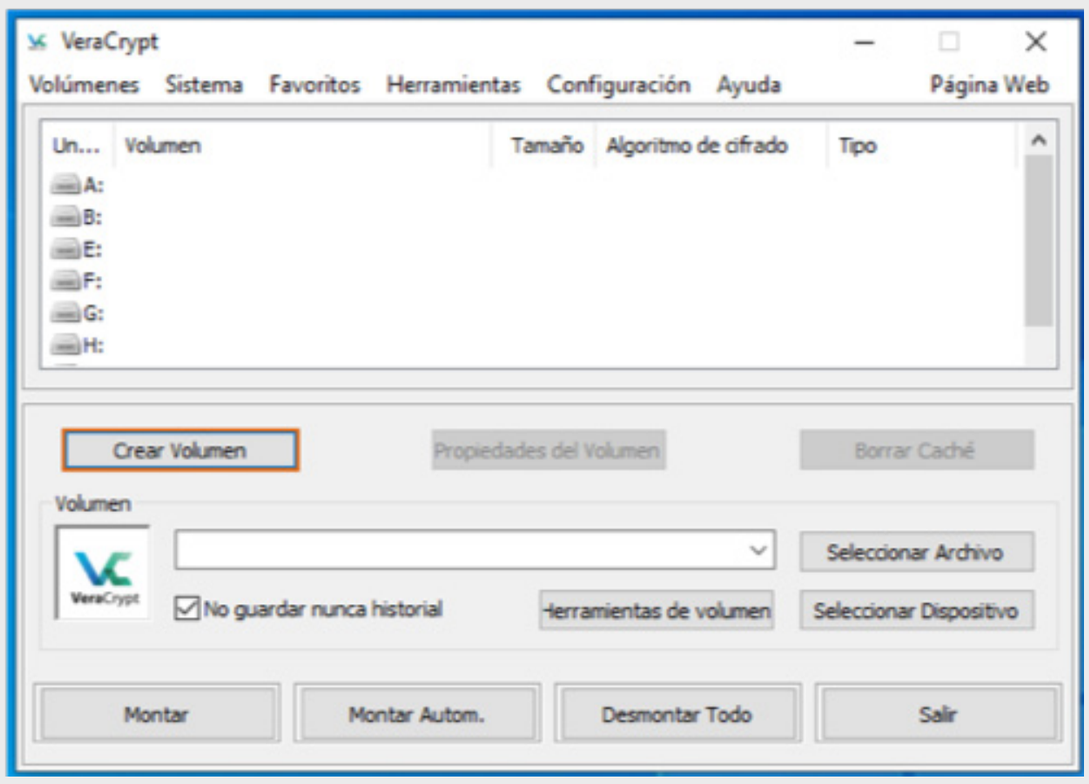


3. Existen dos formas básicas en las que es posible utilizar VeraCrypt, cuando se ha instalado como cualquier otro programa en nuestro dispositivo, o es posible usarlo de forma portable, es decir, este puede ejecutarse pero a través de los archivos de descarga, sin la necesidad de instalarlo. Existe una variedad de programas que funcionan así y una ventaja es que es la posibilidad de usarlo sin tener permisos de administración para instalarlo, entre otras. En este caso, se opta por "Instalar" con la ruta predeterminada. Al finalizar, VeraCrypt envía un mensaje de instalación exitosa.



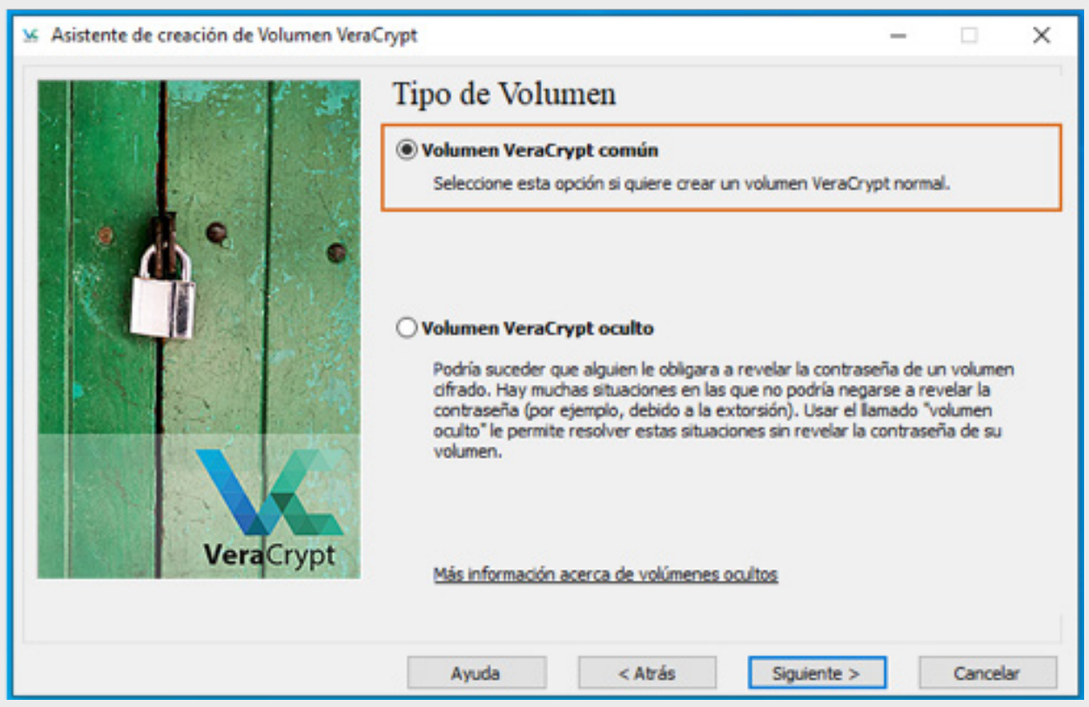
Creación de un volumen estándar de tipo contenedor

1. Abrir VeraCrypt, y hacer clic en "Crear Volumen".

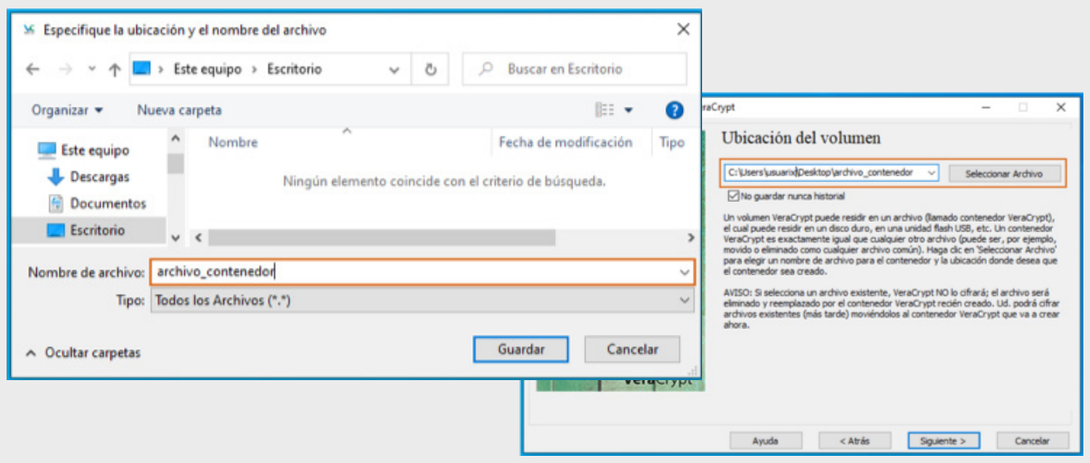


2. Se abrirá el "Asistente de Creación de Volúmenes VeraCrypt". Hay tres acciones que pueden realizarse a partir de aquí, la creación de un contenedor, cifrado de una partición, y cifrado del sistema. Selecciona la primera. Para más información sobre las otras opciones puedes recurrir a la documentación[14].

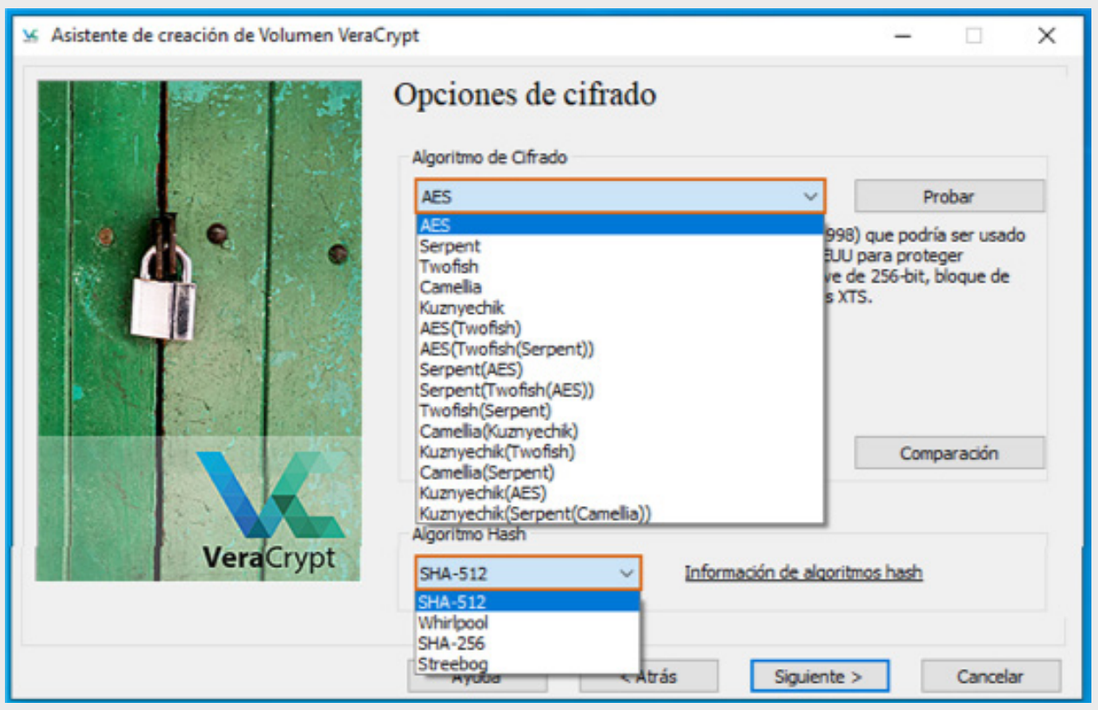
3. El contenedor permite habilitar dos tipos de contenedores, uno común y uno oculto. Selecciona "Volumen VeraCrypt común".



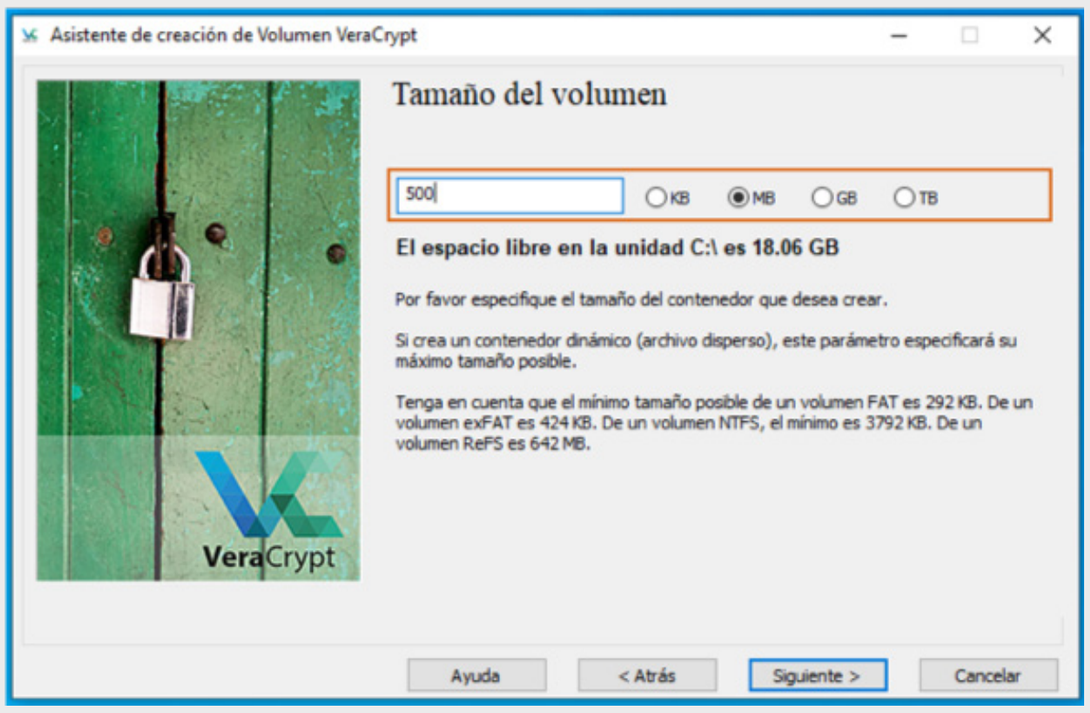
4. Especifica la ruta en el sistema del archivo contenedor del volumen.



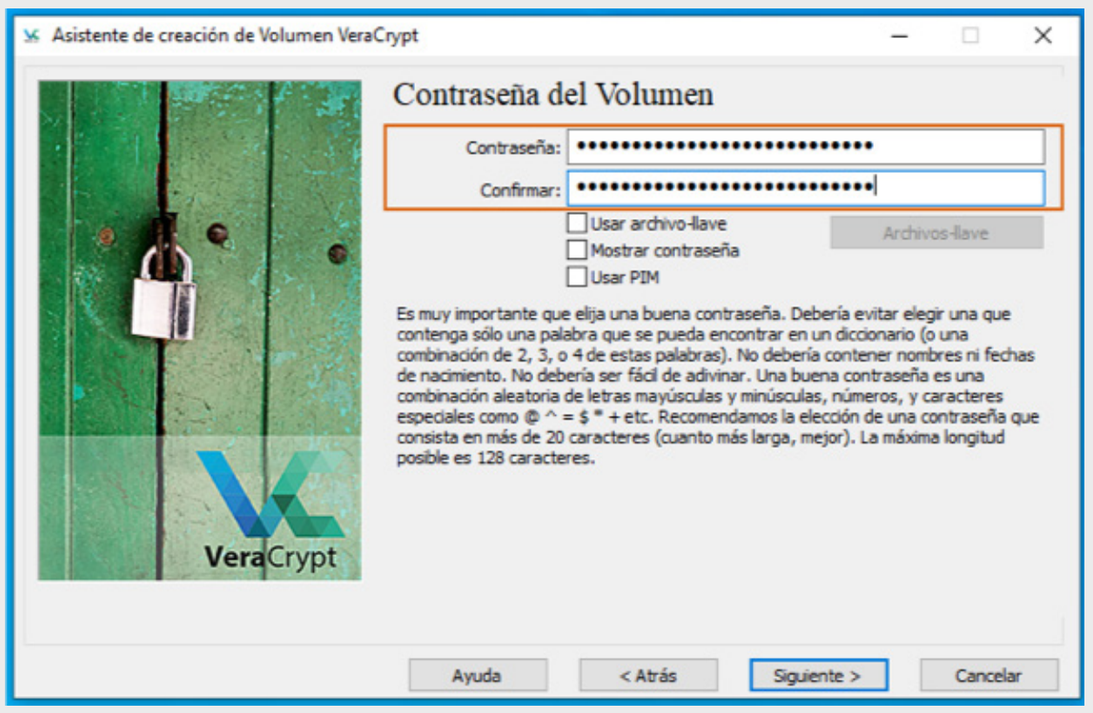
5. Como puedes ver, existen diversos algoritmos de cifrado y de hash que VeraCrypt soporta, ofrece la posibilidad de elegir entre quince combinaciones de algoritmos, algunos de cifrado individuales y otros de combinaciones en cascada, además soporta cinco funciones hash diferentes. Las opciones predeterminadas son AES y SHA-512, las cuales utilizaremos. Por una lado AES (Advanced Encryption Standard, Estándar de Encriptación Avanzado) es uno de los algoritmos más populares usados en criptografía simétrica, y SHA-2 (Secure Hash Algorithm, Algoritmo de Hash Seguro) es parte de una familia de funciones hash una de cuyas funciones es SHA-512. VeraCrypt se basa en la criptografía simétrica para cifrar los datos, y emplea transformaciones unidireccionales (funciones hash) para proteger la clave de cifrado de los datos binarios con la contraseña del usuario.



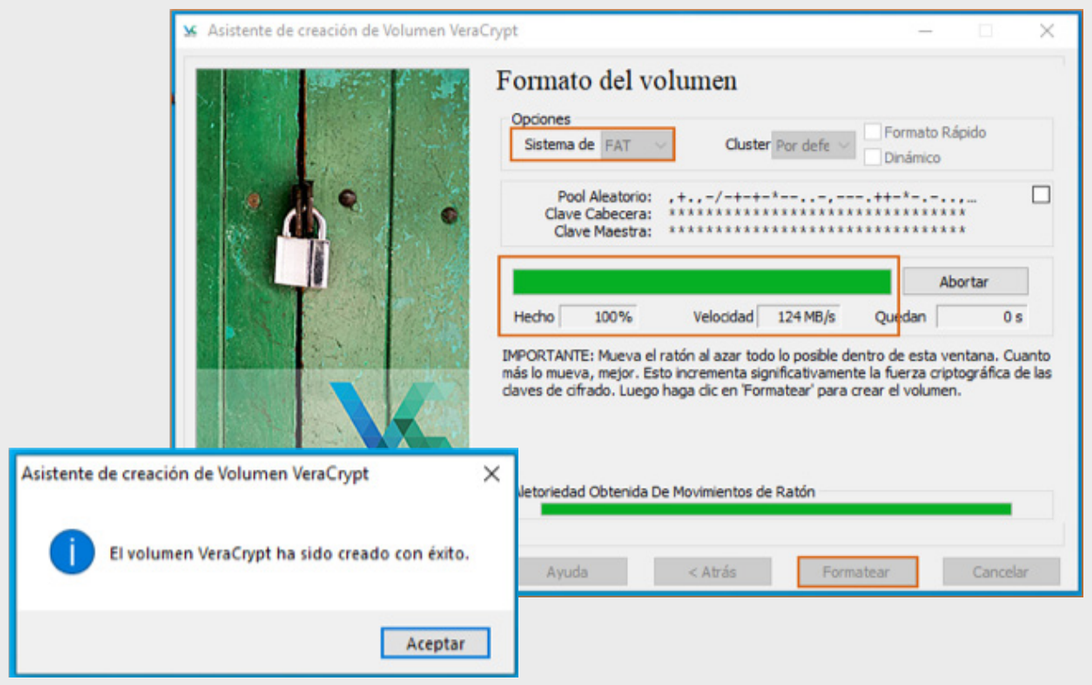
6. Ahora es momento de elegir el tamaño de tu contenedor. Dependiendo de la versión disponible para tu sistema operativo, puede haber o no, habilitada la opción para expandir el volumen. Puedes verificar si existe esta opción en el menú "Herramientas", donde si se encuentra habilitado verás "Expansor de volúmenes", así puedes asignar un espacio mesurado y expandirlo si llegara a ser necesario.



7. Escribe una contraseña, puedes seguir algunas recomendaciones de la infografía de generación y gestión segura de contraseñas. Existe la posibilidad de utilizar un archivo-llave y/o un PIM. El archivo-llave es un archivo cuyo contenido se combina con la contraseña, puede usarse cualquier archivo sin importar el tamaño aunque solo será procesado en el hash el primer MB[15], la cuestión de usar un archivo-llave radica en que podría eliminarse dicho archivo por error y causar la pérdida de acceso al contenedor, por lo cual debe evaluarse esta estrategia. El PIM (Personal Iterations Multiplier, multiplicador de iteraciones personal) es un "valor secreto" que debe ser introducido junto con la contraseña, y si este falla, no se permite montar el volumen. Por otro lado, utilizar un número largo de dígitos provee una mayor seguridad pero también resulta en tiempos más largos de espera al montar el volumen[16].

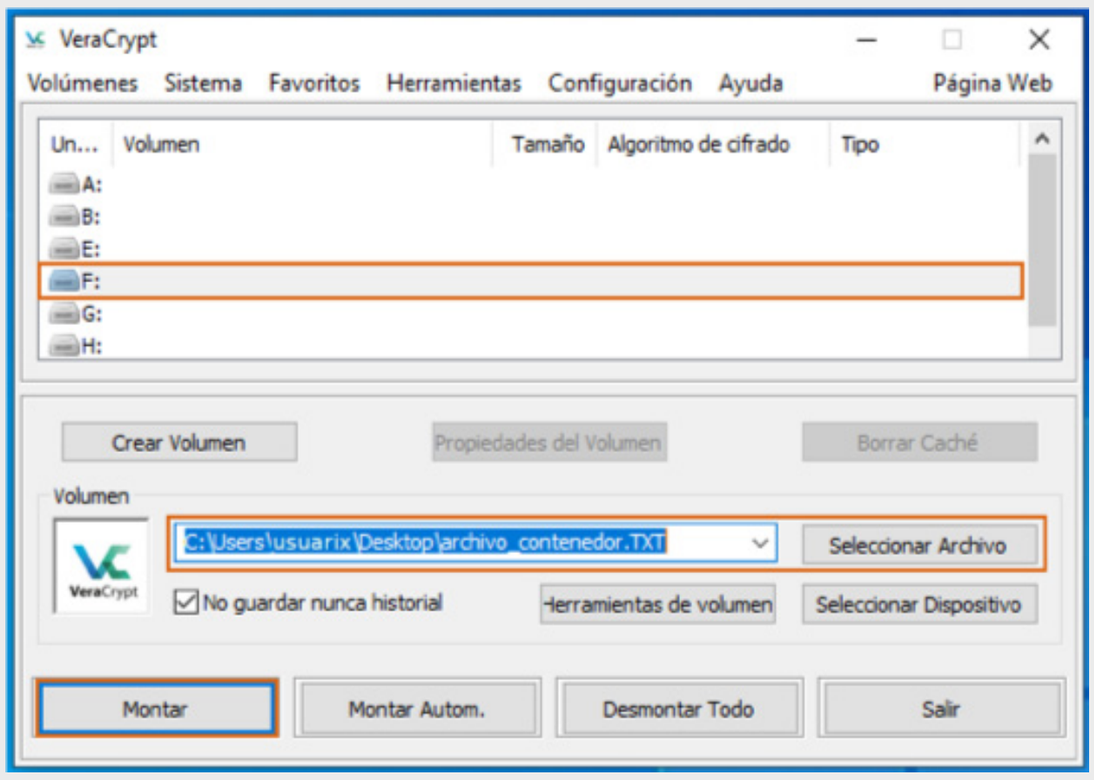


8. En este punto es importante considerar qué tipo de archivos se requieren resguardar en este contenedor ya que FAT soporta archivos de hasta 4GB, si por ejemplo es deseable resguardar videos o archivos de otro tipo con un tamaño mayor a 4GB, la opción a elegir será NTFS o exFAT. Para caso práctico selecciona FAT. En este paso será importante que muevas el cursor como se indica para generar aleatoriedad al algoritmo en la generación de las llaves. Una vez finalizado dicho proceso (la barra se colorea de verde), hacer clic en "Formatear". Al finalizar el proceso, se notifica con un mensaje "El volumen VeraCrypt ha sido creado con éxito".

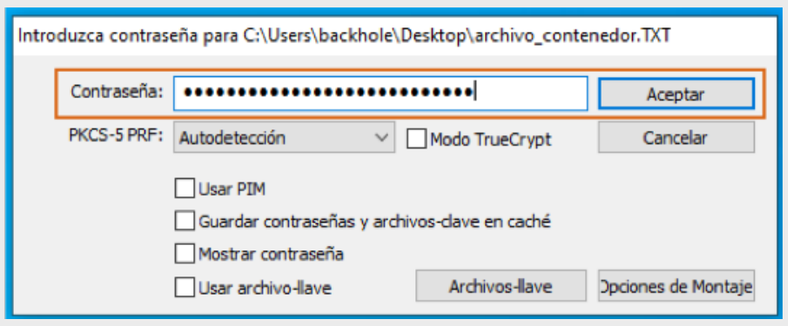


Montar el volumen

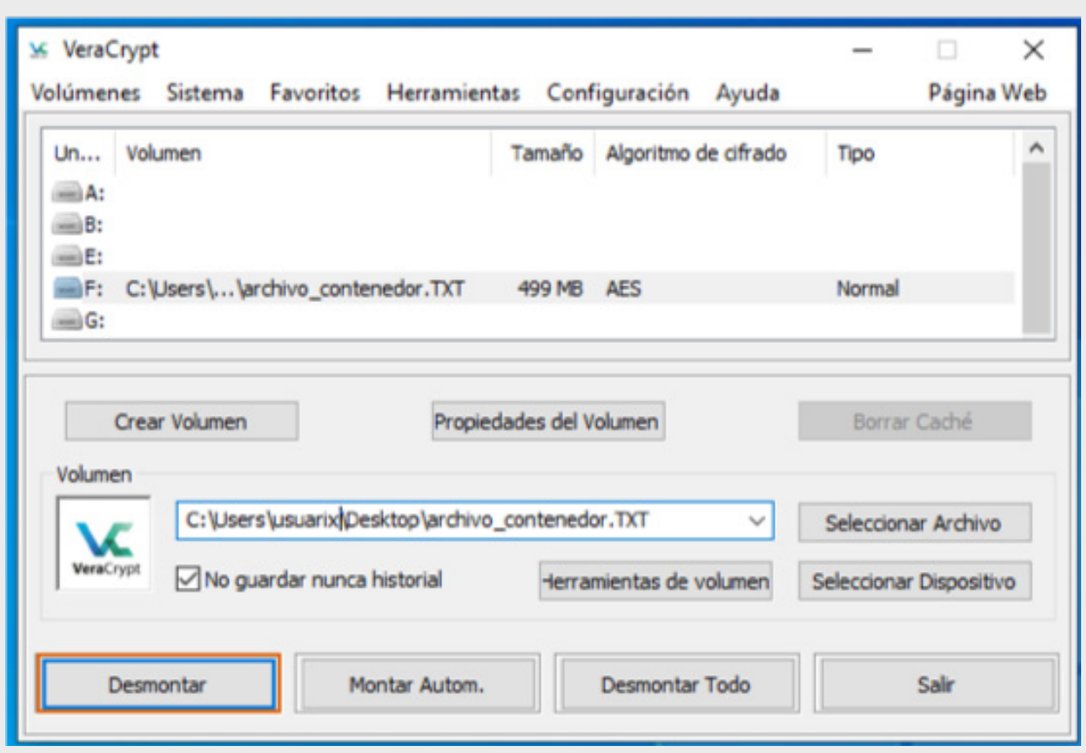
9. Seleccionar alguna letra de las disponibles, el archivo-llave y hacer clic en Montar.



10. Introducir la contraseña (y archivo-llave y/o PIM si así se configuro), para montar el volumen.



11. Se puede acceder al contenedor desde la unidad (letra en mayúscula), en este caso "F:". Y una vez concluido el uso del contenedor, este se puede desmontar.



Referencias

1 "anonimatoycifrado-eff-11.pdf". Consultado: may 11, 2020. [En línea]. Disponible en: https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf.

2 "Seguridad de Software de Código Abierto", *Wikipedia, la enciclopedia libre*. abr. 24, 2020, Consultado: may 11, 2020. [En línea]. Disponible en: https://es.wikipedia.org/w/index.php?title=Seguridad_de_Software_de_C%C3%B3digo_Abierto&oldid=125474002.

3 "gnu.org". https://www.gnu.org/proprietary/malware-microsoft.html (consultado may 11, 2020).

4 "Apple Challenges FBI: All Writs Act Order (CA)", *Electronic Frontier Foundation*, feb. 26, 2016. https://www.eff.org/cases/apple-challenges-fbi-all-writs-act-order (consultado may 11, 2020).

5 "Cifrado de disco - Wikipedia, la enciclopedia libre", Wikipedia. https://es.wikipedia.org/wiki/Cifrado_de_disco#Cifrado_de_disco_vs._Cifrado_a_nivel_de_archivos_del_sistema (consultado may 05, 2020).

6 DulceMontemayor, "Trusted Platform Module Technology Overview (Windows 10) - Microsoft 365 Security". https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview (consultado may 12, 2020).

7 Dansimp, "BitLocker (Windows10) - Microsoft 365 Security". https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/bitlocker-overview (consultado may 12, 2020).

8 "BitLocker", *Wikipedia*. abr. 19, 2020, Consultado: may 12, 2020. [En línea]. Disponible en: https://en.wikipedia.org/w/index.php?title=BitLocker&oldid=951848322.

9 "Opciones de recuperación en Windows 10". https://support.microsoft.com/es-co/help/12415/windows-10-recovery-options (consultado may 13, 2020).

10 "Ataque de canal lateral", *Wikipedia, la enciclopedia libre*. mar. 12, 2020, Consultado: may 12, 2020. [En línea]. Disponible en: https://es.wikipedia.org/w/index.php?title=Ataque_de_canal_lateral&oldid=124202598.

11 "El modo de cifrado de bloque AES-XTS se utiliza en las unidades Flash USB mejor encriptadas de Kingston", *Kingston Technology Company*. https://www.kingston.com/es/solutions/data-security/xts-encryption (consultado may 12, 2020).

12 "Usar FileVault para encriptar el disco de arranque de tu Mac", *Apple Support*. https://support.apple.com/es-lamr/HT204837 (consultado may 12, 2020).

13 "Utilizar FileVault para encriptar el disco de arranque del Mac", *Apple Support*. https://support.apple.com/es-es/HT204837 (consultado may 11, 2020).

14 "VeraCrypt - Free Open source disk encryption with strong security for the Paranoid". https://www.veracrypt.fr/en/Downloads.html (consultado may 13, 2020).

15 "VeraCrypt - Free Open source disk encryption with strong security for the Paranoid". https://www.veracrypt.fr/en/Keyfiles.html (consultado may 14, 2020).

16 "VeraCrypt - Free Open source disk encryption with strong security for the Paranoid". Consultado: may 14, 2020. [En línea]. Disponible en: https://www.veracrypt.fr/en/Personal%20Iterations%20Multiplier%20%28PIM%29.html.

17 "Cifrado (criptografía)", *Wikipedia, la enciclopedia libre*. abr. 28, 2020, Consultado: may 14, 2020. [En línea]. Disponible en: https://es.wikipedia.org/w/index.php?title=Cifrado_(