Cifrado de Archivos Confidenciales de Acceso Restringido

Proceso

Gestión Estratégica de Tecnologías de la Información

Versión 01

07/10/2024

TABLA DE CONTENIDO

1. OBJETIVO

Proveer una capa adicional de seguridad para proteger información confidencial o sensible del Ministerio de Ambiente y Desarrollo Sostenible mediante el uso de algoritmos criptográficos a través de una herramienta de software.

2. ALCANCE

El cifrado de información (archivos, carpetas o discos) aplica para los activos de información en medio digital de todas las áreas y dependencias de los procesos del Ministerio, y estará disponible como control técnico por demanda del servicio, para quién así lo requiera en el Ministerio de Ambiente y Desarrollo Sostenible en el ejercicio de gestión de riesgos de seguridad de la información.

3. NORMAS Y DOCUMENTOS DE REFERENCIA

- Norma ISO 27001:2013
- Norma ISO 27002:2013
- Modelo de Seguridad y Privacidad – MSPI

4. ROLES Y RESPONSABILIDADES

Roles	Responsabilidades
Jefe Oficina TIC	• Aprobar la documentación. • Aprobar el uso de software de cifrado. • Custodiar copia de los sobres sellados con contraseñas de recuperación de acceso a información cifrada. No se recibirán sobres abiertos o transparentes que puedan identificar fácilmente su contenido. Se recomienda el uso de sobres de seguridad para documentos.
Equipo de Seguridad de la Información	• Mantener actualizado este documento. • Socializar y transferir conocimiento al personal pertinente en el uso de este documento y la herramienta de software. • Investigar nuevas tendencias relacionadas con el tema. • Considerar el contenido de este documento en la aplicación de gestión de riesgos de seguridad.
Plataforma de Gestión y Mesa de Asistencia - GEMA	• Gestionar las solicitudes de casos mediante la herramienta de Gestión y Mesa de Asistencia. • Notificar al Equipo de Seguridad y jefe de la Oficina TIC, sobre usuarios que hagan uso inadecuado de las herramientas de este documento, y de tendencias estadísticas de casos que puedan tener un comportamiento anómalo alineado con este documento o con incumplimiento o la violación las políticas especificas de seguridad de la información. • Llevar inventario detallado de los equipos donde se ha implementado el cifrado de información.
Líder de proceso / jefe / coordinador	• Exhortar a sus equipos de trabajo a participar en las socializaciones convocadas por el equipo de Seguridad de la Información de la Oficina TIC.

Roles	Responsabilidades
	• Instruir a sus colaboradores a aplicar y hacer un uso adecuado de este documento como un control técnico en la protección de la confidencialidad de información altamente confidencial o sensible cuando se requiera de acuerdo como el cumplimiento normativo vigentes así lo requiera o durante un periodo de transición especial que requiera confidencialidad antes de ser dado a conocer de forma pública o para un grupo específico de personas. • Custodiar copia de los sobres sellados con contraseñas de recuperación de acceso a información cifrada. No se recibirán sobres abiertos o transparentes que puedan identificar fácilmente su contenido. Se recomienda el uso de sobres de seguridad para documentos.
Colaboradores y otras partes interesadas	• Asistir a las socializaciones que el Equipo de Seguridad de la información de la Oficina TIC convoca. • Analizar en los procesos internos de trabajo la pertinencia de aplicabilidad el contenido de este documento en el manejo de la información potencialmente confidencial o que contenga datos sensibles. • Solicitar mediante la Plataforma de Gestión y Mesa de Asistencia el cifrado de información confidencial.
Oficina de Control Interno	• Realizar acompañamiento en el proceso de recuperación y acceso a archivos, carpetas o unidades de disco cifradas en casos en los que un usuario responsable de la información deje la entidad por cualquier motivo o se niegue a permitir su acceso. • Realizar auditorías de funcionalidad de este documento y de eficacia de recuperación de acceso a información cifrada mediante la llave guardada en sobre sellado. El sobre se abrirá en presencia de los auditados y equipo acompañante de Seguridad de la Información y la Oficina TIC.

5. METODOLOGIA

Identificación de información que se requiere cifrar.

El líder de proceso, jefe o coordinador de cualquier área del Ministerio designará un colaborador o equipo de trabajo, quien(es) debe(n) identificar y seleccionar de los activos de información existes en medio digital, la información confidencial que requiera de elementos de protección adicionales como el descrito en este documento y otros de ser necesario de acuerdo con la evaluación de riesgos que se presente.

Solicitud del servicio de cifrado

La solicitud del servicio de cifrado de archivos o carpetas o unidades de disco se realiza mediante solicitud del área funcional y debe ser realizada directamente por el jefe del área solicitante y estar dirigida al jefe de la oficina TIC mediante un caso en la Plataforma de Gestión y Mesa de Asistencia, quien designará al o los responsables de la aplicación de este documento.

En el cuerpo de la solicitud, se debe describir al o los usuarios autorizados del área funcional y la(s) respectiva(s) placa(s) de inventario del (los) equipo(s) con información objeto de ser protegida, y una descripción breve del activo de información a proteger.

Instalación del software de cifrado

El personal autorizado de la Oficina TIC debe instalar y configurar el aplicativo para que pueda ser usado.

Configuración de carpeta de cifrado o capsula

El personal autorizado de la Oficina TIC debe crear una carpeta y configurarla de acuerdo con los requerimientos.

Configuración de llave de acceso

El personal autorizado de la Oficina TIC debe configurar el acceso a la carpeta con la que además se realizará el cifrado de la información.

El usuario autorizado o designado responsable de la información debe digitar la contraseña en el software de cifrado cuando el personal de la Oficina TIC lo indique, y debe escribir la contraseña en dos hojas en blanco las cuales deben ser almacenadas y selladas en un sobre~~)~~, los sobres serán entregados uno al jefe del área y el otro al jefe de la OTIC, esto con el fin de mantener el gobierno sobre la información y poder recuperarla ante cualquier eventualidad futura.

Dicho sobre, podrá ser abierto en caso de ausencia del usuario y requerimiento urgente de la información por parte del jefe del área. De igual manera, el sobre podrá ser objeto de auditoria por parte de la Oficina de Control Interno, del Equipo de Seguridad de la Información o de cualquier auditoría interna o externa autorizada por el Ministerio con el fin de constatar que la contraseña del sobre y la contraseña del aplicativo coincidan y el acceso a la información es factible.

6. PASOS

PASO 1.

Para usar el aplicativo https://veracrypt.de/en/Downloads.html se debe seleccionar el icono “VeraCrypt.exe”.

PASO 2:

Debería aparecer la ventana principal de VeraCrypt. Haga clic en **Crear volumen** (marcado con un rectángulo rojo para mayor claridad). Como se observa en la figura 1.

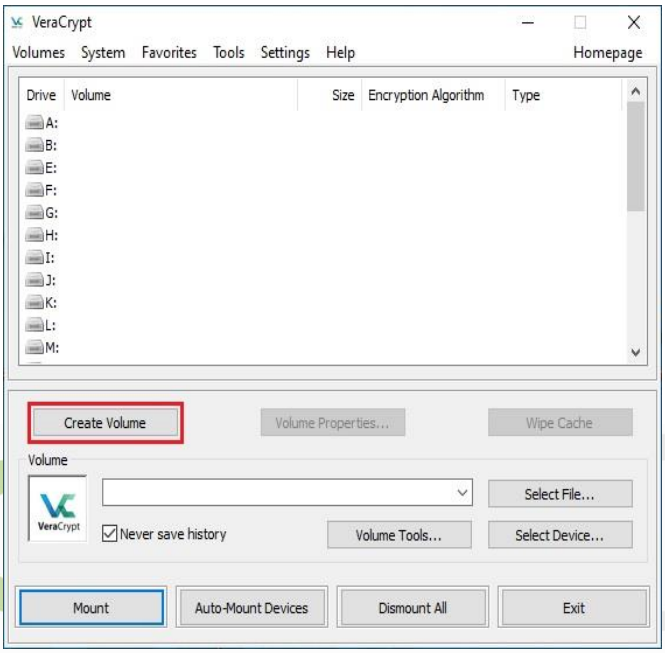

Ilustración 1 Crear un volumen; Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 3:

Debería aparecer la ventana del Asistente de Creación de Volúmenes de VeraCrypt. En este paso se debe elegir el sistema de cifrado que se requiere que cree VeraCrypt. Por ejemplo, en un volumen de VeraCrypt puede residir en un archivo o contenedor, en una partición o unidad. En este tutorial, elegiremos la primera opción y crearemos un volumen VeraCrypt dentro de un archivo.

Como la opción está seleccionada de forma predeterminada, puede hacer clic en **Siguiente (**Next).

Nota:
En los siguientes pasos, las capturas de pantalla mostrarán solo la parte derecha de la ventana del asistente.

Ilustración 2ventana del Asistente de Creación de Volúmenes de VeraCrypt; Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 4:

En este paso debe elegir si desea crear un volumen VeraCrypt estándar u oculto. En este tutorial, elegiremos la primera opción y crearemos un volumen VeraCrypt estándar. Como la opción está seleccionada de forma predeterminada, puede hacer clic en **Siguiente (**Next**)**.

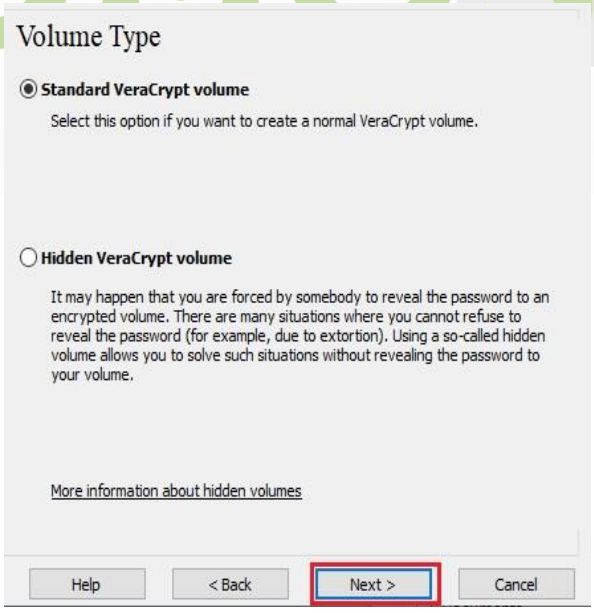

Ilustración 3Crear un volumen estándar Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 5:

En este paso se tiene que especificar en dónde se quiere crear el volumen VeraCrypt (contenedor de archivos). Tenga en cuenta que un contenedor VeraCrypt es como cualquier archivo normal. Se puede, por ejemplo, mover o eliminar como cualquier archivo normal. También necesita un nombre de archivo, que elegirá en el siguiente paso. Haga clic en **Seleccionar archivo (**Select File…**)**.

Debería aparecer el selector de archivos estándar de Windows (mientras que la ventana del Asistente de Creación de Volúmenes de VeraCrypt permanece abierta en segundo plano).

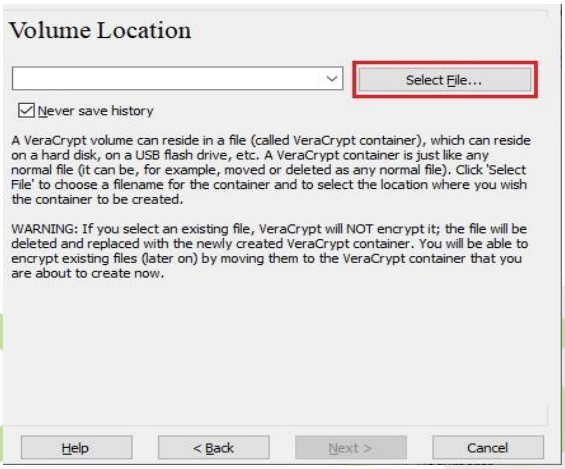

Ilustración 4Seleccionar archivo; Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 6:

Crearemos nuestro volumen VeraCrypt en la carpeta C:*Data*\ y el nombre del archivo del volumen (contenedor) será *MyVolume.hc,* como se puede ver en la figura 5, a continuación.

NOTA: Tanto la ruta la carpeta C:\Data\ y el nombre del archivo del volumen (contenedor) MyVolume.hc, pueden cambiar de acuerdo con las políticas de TI, en cuanto al uso y configuración de los equipos de cómputo de Ministerio que determine la Oficina TIC.

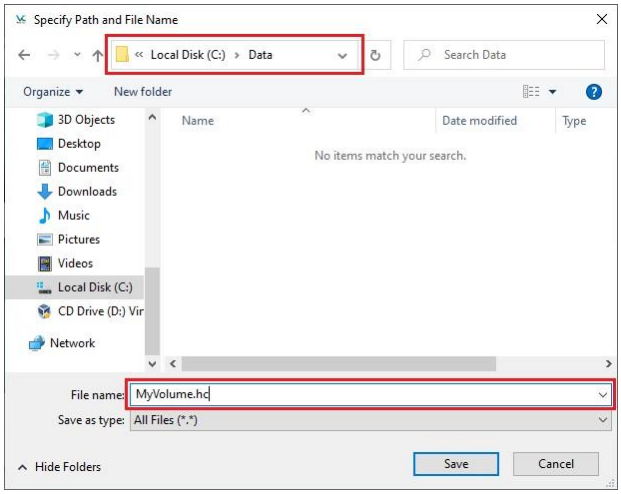

Ilustración 5Crearemos nuestro volumen VeraCrypt; Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Por supuesto, puede elegir cualquier otro nombre de archivo y ubicación que desee (por ejemplo, en una memoria USB). Tenga en cuenta que el archivo *MyVolume.hc* aún no existe – VeraCrypt lo creará.

IMPORTANTE: Tenga en cuenta que VeraCrypt *no* cifrará ningún archivo existente (al crear un contenedor de archivos VeraCrypt). Si selecciona un archivo existente en este paso, se sobrescribirá y se reemplazará por el volumen recién creado (por lo que el archivo sobrescrito se *perderá*, *no* se cifrará). Podrá cifrar los archivos existentes (más adelante) moviéndolos al volumen VeraCrypt que estamos creando ahora.

Seleccione la ruta deseada (donde desea que se cree el contenedor) en el selector de archivos. Escriba el nombre del archivo contenedor deseado en el cuadro **Nombre de archivo**.

Haga clic en **Guardar**.

La ventana del selector de archivos debería desaparecer. En los siguientes pasos, volveremos al Asistente de Creación de Volúmenes de VeraCrypt.

Tenga en cuenta que después de copiar los archivos no cifrados existentes en un volumen VeraCrypt, debe borrar de forma segura los archivos originales sin cifrar. Existen herramientas de software que se pueden utilizar con el fin de borrar de forma segura (muchas de ellas son gratuitas).

PASO 7:

En la ventana Asistente para la creación de volúmenes, haga clic en **Siguiente (**Next**)**.

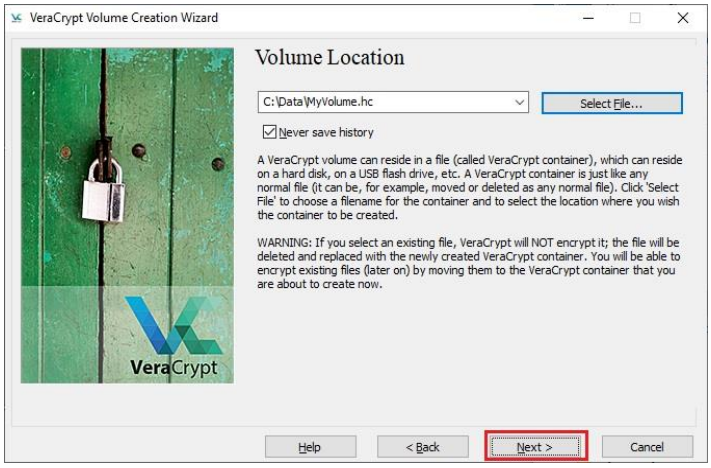

Ilustración 6Vista Asistente para la creación de volúmenes; Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 8:

Aquí puede elegir un algoritmo de cifrado y un algoritmo hash para el volumen. Si no está seguro de qué seleccionar aquí, puede utilizar la configuración predeterminada y hacer clic en **Siguiente.**

Ilustración 7Algoritmo de cifrado y un algoritmo hash; Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 9:

Aquí especificamos para el ejemplo, que deseamos que el tamaño de nuestro contenedor VeraCrypt sea de 250 megabytes. Por supuesto, puede especificar un tamaño diferente. Después de escribir el tamaño deseado en el campo de entrada (marcado con un rectángulo rojo), haga clic en **Siguiente** (Next).

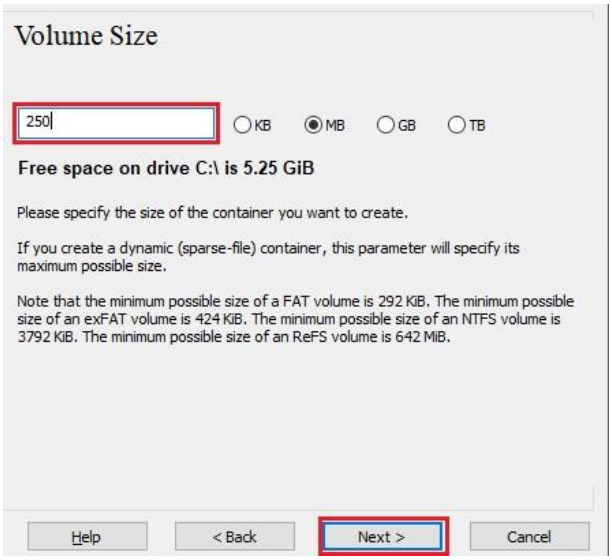

Ilustración 8Tamaño de contenedor; Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 10:

Este es uno de los pasos más importantes. Aquí hay que elegir una buena contraseña de volumen. Lea atentamente la información que se muestra en la ventana del Asistente sobre lo que se considera una buena contraseña.

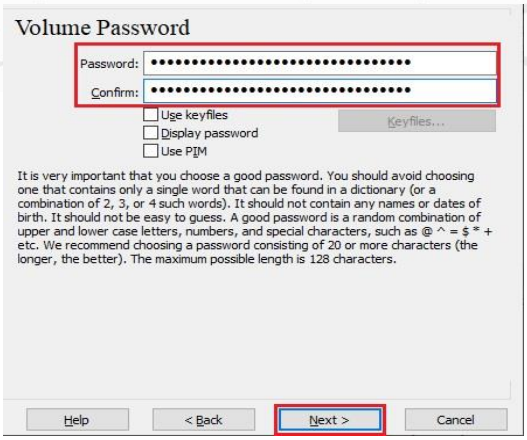

Ilustración 9Elección de contraseña; Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Después de elegir una buena contraseña, escríbala en el primer campo de entrada. A continuación, vuelva a escribirlo en el campo de entrada situado debajo del primero y haga clic en **Siguiente (**Next**)**.

La contraseña elegida para el acceso a este software no debe ser la misma que se usa para acceder al correo electrónico institucional, ni igual a otras contraseñas de uso personal. Una buena contraseña o contraseña segura, se destaca por su longitud mínima de 12 caracteres, que combine letras

mayúsculas, minúsculas, caracteres especiales y números. Se sugiere usar un software de generación de contraseñas, que el Equipo de Seguridad de la Información puede sugerirle.

Nota: El botón **Siguiente** se desactivará hasta que las contraseñas de ambos campos de entrada sean las mismas.

PASO 11:

Mueva el ratón lo más aleatoriamente posible dentro de la ventana del Asistente para la creación de volúmenes al menos hasta que el indicador de aleatoriedad se vuelva verde. Cuanto más tiempo muevas el ratón, mejor (se recomienda moverlo durante al menos 30 segundos). Esto aumenta significativamente la fuerza criptográfica de las claves de cifrado (lo que aumenta la seguridad).

Haga clic en **Format**.

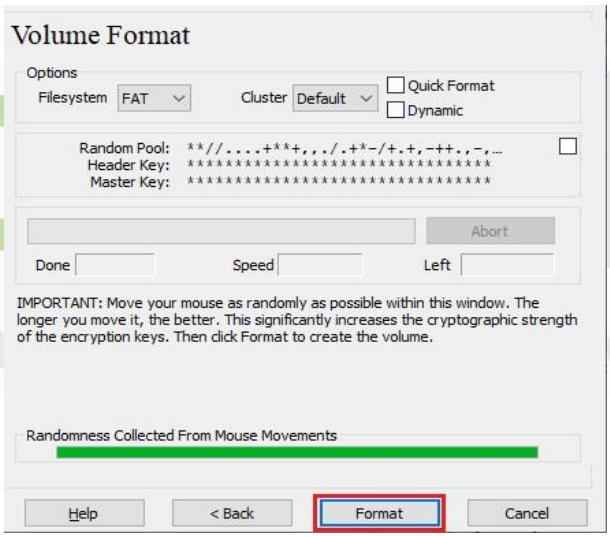

Ilustración 10 Volumen de formato; Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Debería comenzar la creación del volumen. VeraCrypt ahora creará un archivo llamado *MyVolume.hc* en la carpeta C:*Data*\ (como especificamos en el Paso 6). Este archivo será un contenedor VeraCrypt (contendrá el volumen VeraCrypt cifrado). Dependiendo del tamaño del volumen, la creación del volumen puede tardar mucho tiempo. Una vez que finaliza, aparecerá el siguiente cuadro de diálogo, haga clic en **OK** para cerrar el cuadro:

PASO 12:

Acabamos de crear con éxito un volumen VeraCrypt (contenedor de archivos). En la ventana del Asistente de Creación de Volúmenes de VeraCrypt, haga clic en **Salir (**Exit**)**. La ventana del asistente debería desaparecer.

Ilustración 11: Volumen creado; tomado de :https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

En los pasos restantes, montaremos el volumen que acabamos de crear. Volveremos a la ventana principal de VeraCrypt (que aún debería estar abierta, pero si no lo está, repita el Paso 1 para iniciar VeraCrypt y luego continúe desde el Paso 13).

PASO 13:

Seleccione una letra de unidad de la lista (marcada con un rectángulo rojo). Esta será la letra de la unidad en la que se montará el contenedor VeraCrypt.

Nota: En este tutorial, elegimos la letra de unidad M, pero, por supuesto, puede elegir cualquier otra letra de unidad disponible. Siga las sugerencias e instrucciones del personal designado de la Oficina TIC.

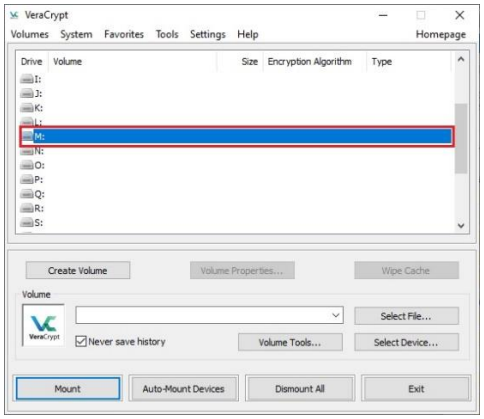

Ilustración 12 Selección de unidad; Tomado de: https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 14:

Haga clic en **Seleccionar archivo (**Select File…**)**. Debería aparecer la ventana de selección de archivos estándar

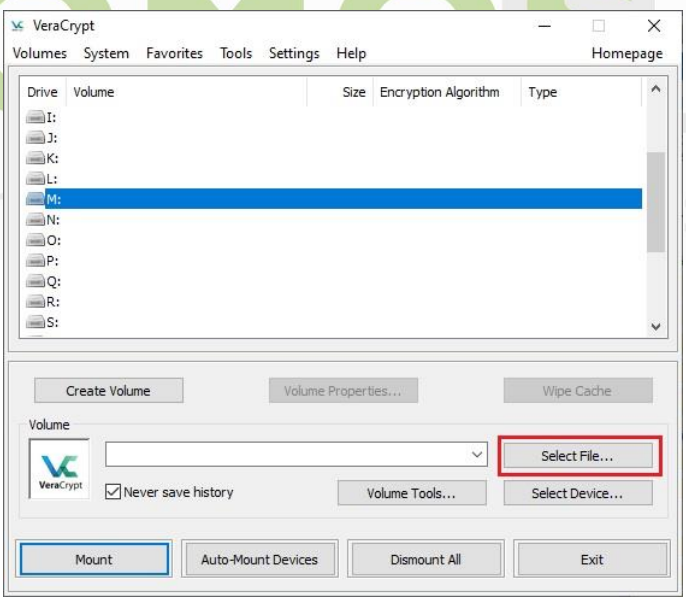

Ilustración 13 Seleccionar archivo; Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 15:

En el selector de archivos, busque el archivo contenedor (que creamos en los pasos 6 a 12) y selecciónelo. Haga clic en **Abrir (**Open**)** (en la ventana del selector de archivos). La ventana del

selector de archivos debería desaparecer. En los siguientes pasos, volveremos a la ventana principal de VeraCrypt.

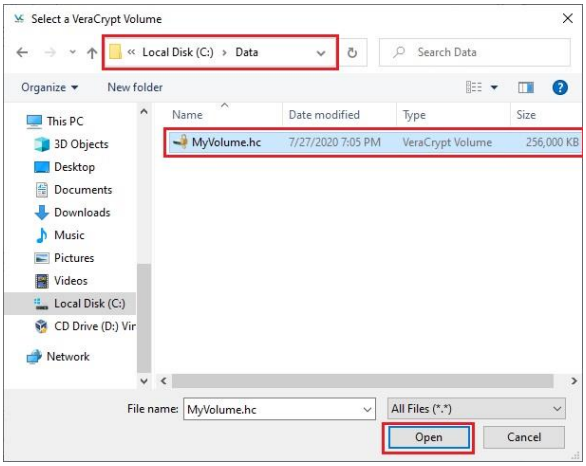

Ilustración 14 Apertura de volumen: Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 16:

En la ventana principal de VeraCrypt, haga clic en **Montar (**Mount**)**. Debería aparecer la ventana de diálogo de solicitud de contraseña.

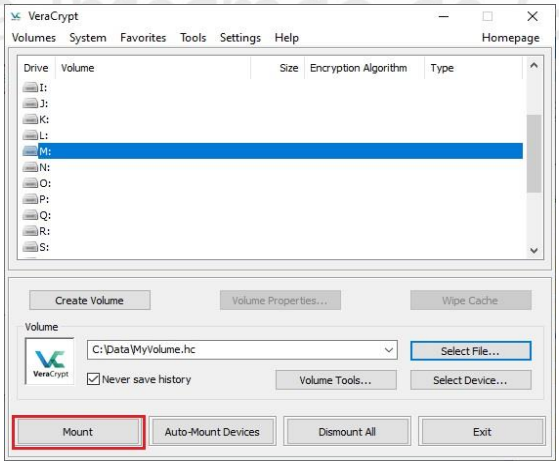

Ilustración 15 Montar volumen; Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 17:

Escriba la contraseña (que especificó en el paso 10) en el campo de entrada de contraseña (marcado con un rectángulo rojo).

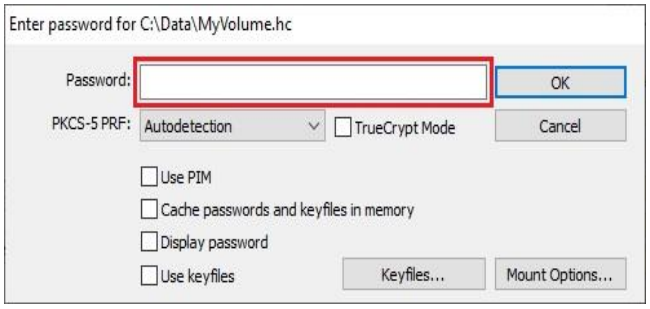

Ilustración 16 Inserción de contraseña: Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

PASO 18:

Seleccione el algoritmo PRF que se utilizó durante la creación del volumen (SHA-512 es el PRF predeterminado utilizado por VeraCrypt). Si no recuerda qué PRF se utilizó, simplemente déjelo configurado en "detección automática", pero el proceso de montaje llevará más Hora. Haga clic en **Aceptar (**OK**)** después de ingresar la contraseña.

Ilustración 17 Selección de algoritmo: Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Ahora VeraCrypt intentará montar el volumen. Si la contraseña es incorrecta (por ejemplo, si la escribió incorrectamente), VeraCrypt te lo notificará y tendrá que repetir el paso anterior (escriba la contraseña de nuevo y haga clic en **Aceptar (**OK**)**. Si la contraseña es correcta, se montará el volumen.

PASO FINAL:

Acabamos de montar con éxito el contenedor como un disco virtual M: El disco virtual está completamente cifrado (incluidos los nombres de los archivos, las tablas de asignación, el espacio libre, etc.) y se comporta como un disco real. Puede guardar (o copiar, mover, etc.) archivos en este disco virtual y se cifrarán sobre la marcha a medida que se escriban.

Si abre un archivo almacenado en un volumen VeraCrypt, por ejemplo, en un reproductor multimedia, el archivo se descifrará automáticamente en la RAM (memoria) sobre la marcha mientras se lee.

Importante: Tenga en cuenta que cuando abra un archivo almacenado en un volumen VeraCrypt (o cuando escriba/copie un archivo a / desde el volumen VeraCrypt) no se le pedirá que introduzca la contraseña de nuevo. Debe introducir la contraseña correcta solo al montar el volumen.

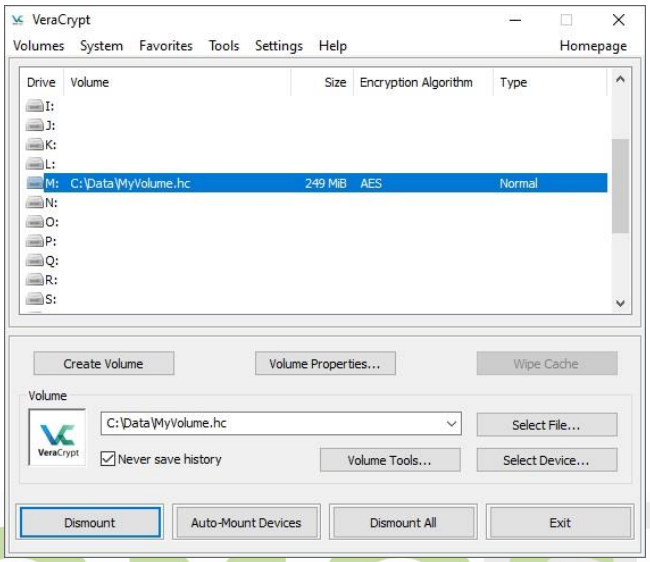

Ilustración 18 Montar contenedor: Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Para abrir el volumen montado, por ejemplo, puede seleccionarlo en la lista como se muestra en la captura de pantalla anterior (selección azul) y luego haciendo doble clic en el elemento seleccionado. También puede buscar el volumen montado de la misma manera que normalmente navega por cualquier otro tipo de volúmenes. Por ejemplo, abriendo la lista '*Equipo*' (o '*Mi PC*') y haciendo doble clic en la letra de la unidad correspondiente (en este caso, es la letra M).

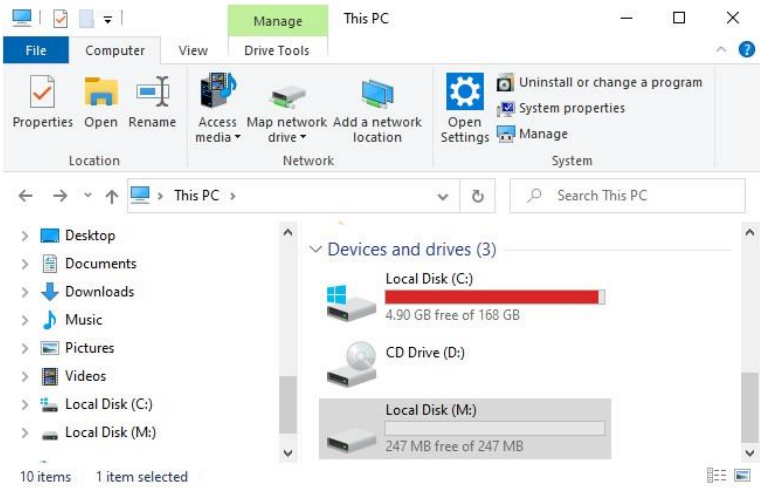

Ilustración 19 Disco local Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Puede copiar archivos (o carpetas) hacia y desde el volumen VeraCrypt de la misma manera que los copiaría a cualquier disco normal (por ejemplo, mediante simples operaciones de arrastrar y soltar).

Los archivos que están siendo leídos o copiados desde el volumen cifrado VeraCrypt se descifran automáticamente sobre la marcha en RAM (memoria). Del mismo modo, los archivos que están siendo escritos o copiados en el volumen VeraCrypt son automáticamente cifrados sobre la marcha en la RAM (justo antes de ser escritos en el disco).

Tenga en cuenta que VeraCrypt nunca guarda ningún dato descifrado en un disco – sólo los almacena temporalmente en la RAM (memoria). Incluso cuando el volumen está montado, los datos almacenados en el volumen siguen cifrados. Al reiniciar Windows o apagar el equipo, el volumen se desmontará y todos los archivos almacenados en él serán inaccesibles (y cifrados).

Incluso cuando el suministro de energía se interrumpe repentinamente (sin el apagado adecuado del sistema), todos los archivos almacenados en el volumen serán inaccesibles (y cifrados). Para hacerlos accesibles de nuevo, tiene que montar el volumen. Para ello, repita los pasos 13 a 18.

Si desea cerrar el volumen y hacer que los archivos almacenados en él sean inaccesibles, reinicie el sistema operativo o desmonte el volumen. Para hacerlo, siga estos pasos

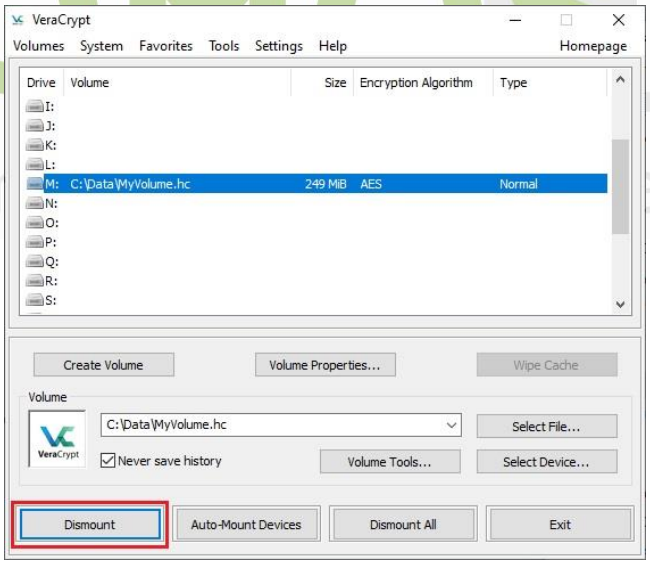

Ilustración 20 Desmontar unidad Tomado de https://veracrypt.de/en/Beginner%27s%20Tutorial.htm

Seleccione el volumen de la lista de volúmenes montados en la ventana principal de VeraCrypt (marcado con un rectángulo rojo en la captura de pantalla anterior) y luego haga clic en **Desmontar** (también marcado con un rectángulo rojo en la captura de pantalla anterior). Para que los archivos almacenados en el volumen vuelvan a ser accesibles, tendrá que montar el volumen. Para ello, repita los pasos 13 a 18.

7. TÉRMINOS Y DEFINICIONES

Cápsula de cifrado: Espacio en Disco destinado para el almacenamiento de información.

Cifrado: Es un procedimiento que utiliza un algoritmo y una clave para transformar un mensaje o archivo brindando protección al mismo.

Veracrypt: Software usado para el cifrado de archivos y carpetas.