

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 1 de 32

**IDEAM – INSTITUTO DE HIDROLOGÍA, METEOROLOGIA Y ESTUDIOS
AMBIENTALES**

INSTRUCTIVO PARA EL CIFRADO DE DATOS

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 2 de 32

TABLA DE CONTENIDO

	PAGINAS
INTRODUCCIÓN	3
MARCO LGEAL	4
OBJETIVOS	6
ALCANCE	7
DEFINICIONES	7
POLÍTICAS DE OPERACIÓN	8
CIFRADO DE DATOS PARA WINDOWS	10
CIFRADO DE DATOS PARA LINUX	20

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 3 de 32

INTRODUCCIÓN

- La información es considerada el activo más valioso en una organización, por tanto, la protección en cuanto a su confidencialidad, integridad y disponibilidad se ha vuelto indispensable en las entidades públicas y privadas; la seguridad de la información brinda las herramientas que permitirán salvaguardar datos e información sensible, confidencial, privada y pública de las entidades logrando así evitar fugas de información por medios no oficiales, además la protege ante posibles alteraciones en su contenido o pérdida de la misma, de no ser así, acarrearía inconvenientes de tipo legal o administrativo o sancionatorios para la organización.
- El riesgo siempre está presente, por tanto, es imprescindible que las organizaciones cuenten con sistemas y herramientas que le permitan evitar o reducir la materialización de los mismos, para así garantizar la protección de la información.
- Las amenazas informáticas aprovechan las vulnerabilidades existentes en los diferentes sistemas de información; la organización puede verse comprometida a diferentes ataques y nuevas formas de intrusión y daño a su infraestructura tecnológica y por supuesto a la información, algunos de estos ataques o amenazas son: Phishing, Malware, Suplantación, Accesos no Autorizados, ingeniería social y demás que con el avance tecnológico se pueden ir presentando; por tanto, tomar medidas necesarias frente a estas posibles amenazas, le permitirá a la organización proteger sus activos y lograr el cumplimiento de sus objetivos misionales y de negocio.
- Implementar protocolos de seguridad fortalecerá a la organización en sus procesos y evitará que se pierda la trazabilidad de la información en todos sus niveles, generando compromiso por parte de los funcionarios en cuanto a la importancia de preservar y conservar la información de manera segura.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 4 de 32

Marco legal

El 5 de enero de 2009, el congreso de la República de Colombia promulgo la ley 1273 “Por medio se, modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la Protección de la información y de los datos” – y se preservan integralmente los sistemas que utilicen las tecnologías de la información preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. 1. Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. 2. Capítulo Segundo: De los atentados informáticos y otras infracciones.

CAPITULO PRIMERO

Artículo 269 A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 36 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269 C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis meses (36) a setenta y dos (72) meses.

Artículo 269 D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, venda, intercambie, envíe, compre

	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 5 de 32

intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas p determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que l ley obliga a quien sustraiga e “intercepte” dichos datos a pedir autorización al titular de los mismos.

Artículo 269 G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrollo, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

CAPITULO SEGUNDO

Artículo 269 I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 23[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas de en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

Artículo 269 J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. 28

28 LEY 1273 DE 2009 (Enero 05) {En línea} {12 de marzo de 2018} disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

OBJETIVOS:

Objetivo General:

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 6 de 32

- Definir lineamientos para el cifrado de información digital almacenada en medios removibles, evitando potenciales pérdidas y/o fugas de información clasificada como crítica en la entidad.

Objetivos Específicos:

- Orientar a los funcionarios de IDEAM, para la apropiación y uso adecuado de los medios de almacenamiento extraíbles (removibles), como parte de las estrategias de prevención de incidentes de seguridad de la información.
- Establecer procesos y/o actividades para la ejecución de los controles de cifrado de información.
- Asegurar los principios de Integridad, Confidencialidad y Disponibilidad de la información del IDEAM, según ISO 27001.
- Aplicar la seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados que constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información
- Garantizar la confidencialidad la información (no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados).
- Preservar la integridad de la información (mantenimiento de la exactitud y completitud de la información y sus métodos de proceso)
- Mantener la disponibilidad de la información (acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran)

ALCANCE

Este instructivo está dirigido a toda la entidad (IDEAM) a nivel nacional donde realiza la prestación de sus servicios, brindando orientación necesaria frente a la solicitud y lineamientos para el cifrado de información digital almacenada en medios removibles.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 7 de 32

DEFINICIONES

Amenaza: suceso que tiene la posibilidad de causar daño o pérdida, la cual puede presentarse en forma de destrucción, robo o divulgación, modificación de datos, perfeccionamiento de las técnicas de ingeniería social, ataques a nivel mundial.

Algoritmo: secuencia de pasos lógicos que se realizan para realizar una acción o proceso.

Autenticación: proceso de verificación o comprobación de la identidad de algo a alguien.

Ciberdelito: operación ilícita realizada a través de internet o que tiene como objeto destruir o dañar un ordenador, redes de internet o medios electrónicos

Ciberseguridad: acción caracterizada por tratar de minimizar las amenazas o riesgos a una infraestructura tecnológica

Cifrado: proceso de ocultar o codificar información importante para evitar que personas no autorizadas puedan acceder a ellas, se aplica también a los dispositivos de E/S como USB, discos extraíbles y entre otros.

Confidencialidad: acción de guardar la privacidad de documentos, información o datos que solo le interesan a las entidades o las partes interesadas.

Open Source: es un software en base a código abierto, el cual en su mayoría se puede conseguir de forma gratuita.

Protección: conjunto de acciones que pretenden salvaguardar la seguridad de algo a alguien.

Riesgos: es el evento de que una amenaza se pueda manifestar o se produzca.

Robo de datos: es la pérdida de la información importante para la empresa, el cual puede ser causado por un empleado o por un ataque informático.

Software libre: son todos los programas informáticos los cuales su código fuente puede ser estudiado, modificado y utilizado libremente con cualquier fin.

Vulnerabilidad: son las pequeñas debilidades que se pueden presentar en una infraestructura informática, las cuales pueden ser aprovechadas para causar daños por robo de información.

POLÍTICAS DE OPERACIÓN

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 8 de 32

A continuación, se especifican las políticas de operación para la solicitud, autorización y uso de medios removibles:

1. La solicitud para el uso de medios removibles deberá realizarse formalmente a través de la mesa de servicios, adjuntando el formato XXXXX debidamente diligenciado, igualmente también se requiere la autorización por parte del jefe inmediato de la dependencia y del jefe de oficina de informática.
2. En el formato adjunto se definen las condiciones y requisitos para la autorización y uso de medios removibles.
3. La solicitud será evaluada por el grupo de arquitectura empresarial TI y seguridad de la información GAESI, donde se emitirá un concepto técnico, la autorización o negación de la solicitud según el caso, se notificará a los dos días de haber recibido la solicitud
4. En caso de requerimientos por entes de control se evaluará la solicitud y se contemplarán las respectivas excepciones.
5. En caso de transferencia de información institucional se dispondrá de los repositorios y medios dispuestos por la oficina de informática para el intercambio de información.
6. El uso de medios removibles deberá emplear métodos para el cifrado de información, para ello la oficina de Informática deberá indicar los medios de cifrado, esto con el fin de evitar la pérdida y fuga de información institucional de carácter clasificada o reservada.
7. Se deberá realizar un escaneo por medio de una herramienta de gestión de seguridad (antivirus), cada vez que haga la conexión de un medio removable a los equipos de cómputo de IDEAM.
8. El cifrado de medios removibles atiende a las políticas de seguridad de la información y el cumplimiento de las mismas, cualquier incumplimiento será investigado por la Oficina de Informática y se tomarán las acciones respectivas.
9. No se permite la ejecución de programas y/o aplicación no autorizadas almacenadas en los medios removibles.
10. Es responsabilidad del usuario, propender por la confidencialidad y no divulgación de la información institucional, además deberá asegurar que ninguna otra persona manipule los medios removibles autorizados. Cabe recordar que la autorización únicamente será otorgada a funcionarios y contratistas de la Entidad.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 9 de 32

11. La oficina de Informática realizará el monitoreo frente al uso de medios removibles, en caso de evidenciarse comportamientos inadecuados o alteraciones en la infraestructura tecnológica de IDEAM, se tomarán las medidas necesarias en caso de ocurrencia de algún incidente lo que podría implicar el bloqueo y suspensión del uso de medios removibles.

12. La oficina de Informática, a través del grupo de Arquitectura Empresarial TI y Seguridad de la Información, realizaran un control de auditoria frente al uso de medios removibles en la Entidad.

13. El cifrado de medios removibles obedece a los estándares de la industria, por tanto, el profesional o profesionales de la Oficina de Informática determinarán la mejor solución de cifrado.

14. En caso de pérdida, daño, afectación del medio removible, o cualquier novedad relacionada con el mismo, es deber del funcionario o custodio del medio removible informar inmediatamente a la Oficina de Informática para tomar las acciones respectivas.

DESARROLLO:

A continuación, se describen las acciones para realizar el cifrado de datos en los medios removibles:

Proceso de Cifrado de Datos.

Cifrado de datos para WINDOWS.

La herramienta para realizar el proceso de cifrado de datos se denomina BitLocker, esta herramienta está disponible y puede ser ejecutada en sistemas operativos Microsoft en versiones Profesional, Ultimate y Enterprise, la cual permitirá asegurar la protección de datos de IDEAM.

	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 10 de 32

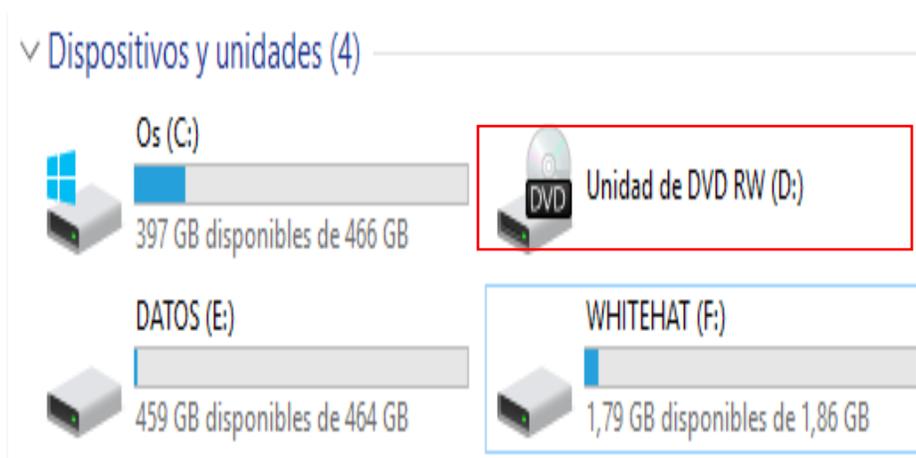
Paso 1:

Disponer de la autorización para el uso de medios removibles por parte del grupo de arquitectura empresarial y seguridad de la información.

- Generación formal de la solicitud a través de la mesa de servicio

Paso 2:

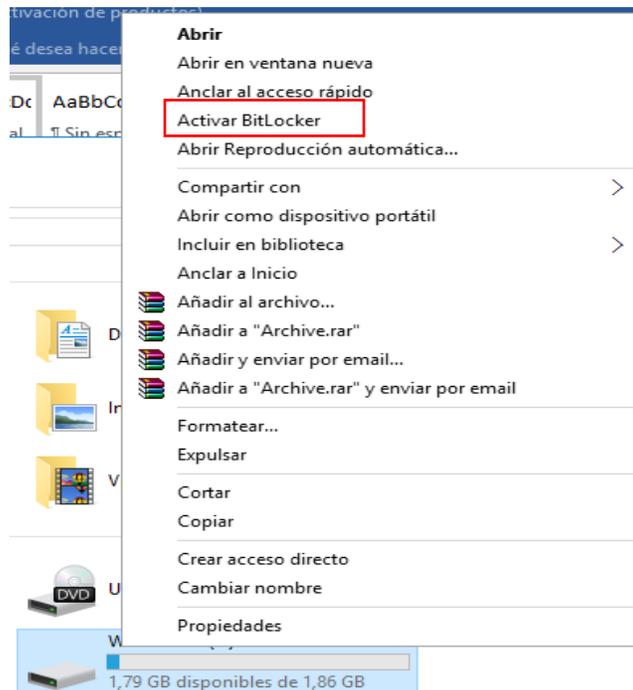
Una vez otorgada la autorización, el usuario deberá conectar al equipo de cómputo el medio removible (UBS, Discos Externo, Entre otros), el cual será objeto del proceso de cifrado de datos.



Paso 3:

Una vez conectado el medio removible al equipo de cómputo de IDEAM, deberá pulsar click derecho sobre el icono de memoria USB, Disco externo, entre otros, y selecciona la opción Activar BitLocker.

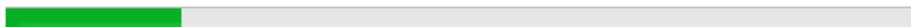
	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 11 de 32



Luego de seleccionar la opción de activar BitLocker esperar mientras se ejecuta la herramienta.

Iniciando BitLocker

Espere mientras BitLocker inicializa la unidad.



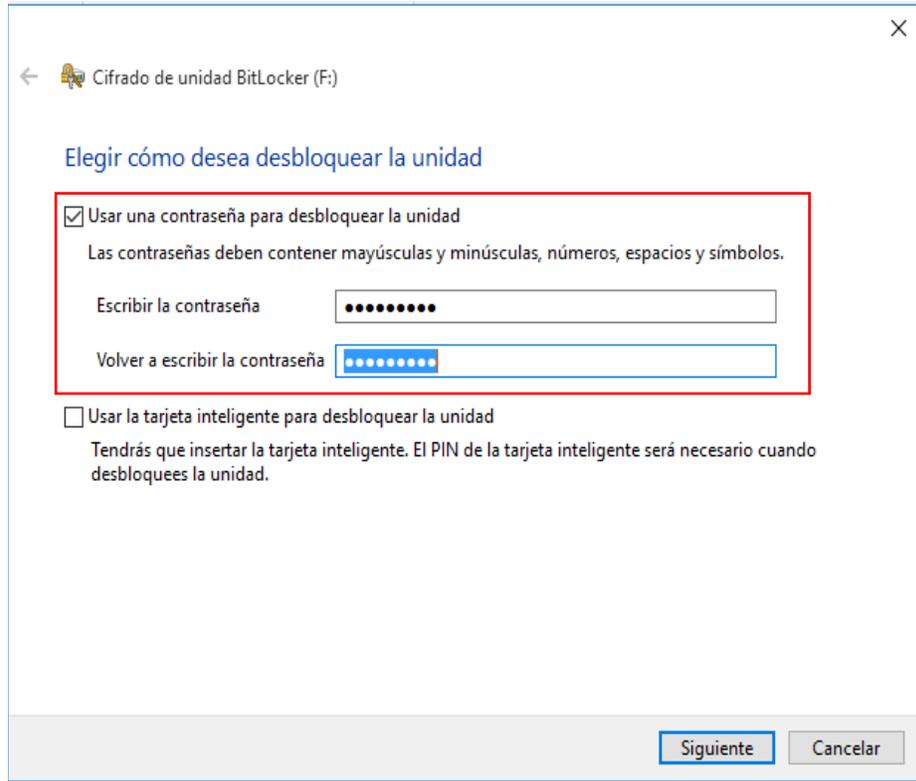
 No quites la unidad durante la instalación de BitLocker.

Paso 4:

La ventana principal de la herramienta solicitará que el usuario seleccione el método de acceso o desbloqueo de unidad de almacenamiento.

- Es recomendable seleccionar la opción: Usar una contraseña para desbloquear la unidad.
- El usuario deberá generar y asignar una contraseña segura.
- Esta contraseña es indispensable que sea recordada por el usuario y que esta no sea descuidada y/o desatendida o expuesta en lugares visibles.

	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 12 de 32



← Cifrado de unidad BitLocker (F:)

Elegir cómo desea desbloquear la unidad

Usar una contraseña para desbloquear la unidad
Las contraseñas deben contener mayúsculas y minúsculas, números, espacios y símbolos.

Escribir la contraseña

Volver a escribir la contraseña

Usar la tarjeta inteligente para desbloquear la unidad
Tendrás que insertar la tarjeta inteligente. El PIN de la tarjeta inteligente será necesario cuando desbloques la unidad.

- Una vez generada y asignada la contraseña pulsar click en el botón siguiente.

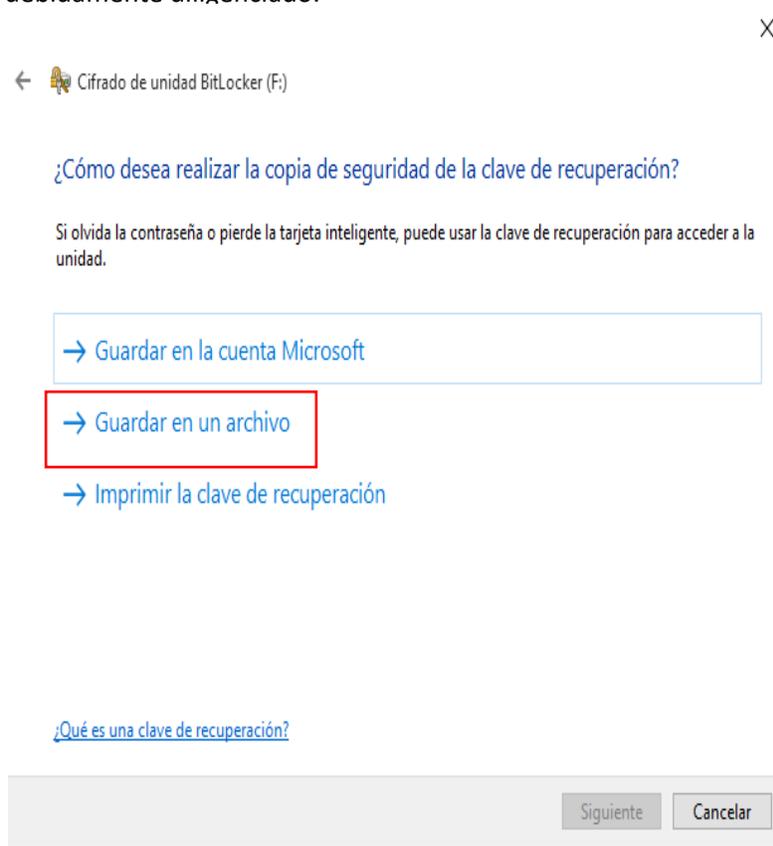
Paso 5:

Como se indicó en el paso anterior la contraseña asignada no deberá ser desatendida (olvidada), en caso de suceder la herramienta permite generar un método de recuperación de la misma.

- La herramienta generará un archivo plano en el cual se encontrará un código que nos permitirá realizar un proceso de recuperación, es importante tener presente que este es el único método para poder acceder a la información en caso de olvidar la contraseña.
- Este archivo plano deberá conservarse y custodiarse adecuadamente en caso de olvidar la contraseña y a su vez perder este archivo no será posible acceder a la información, lo cual representaría una pérdida potencial de la misma.

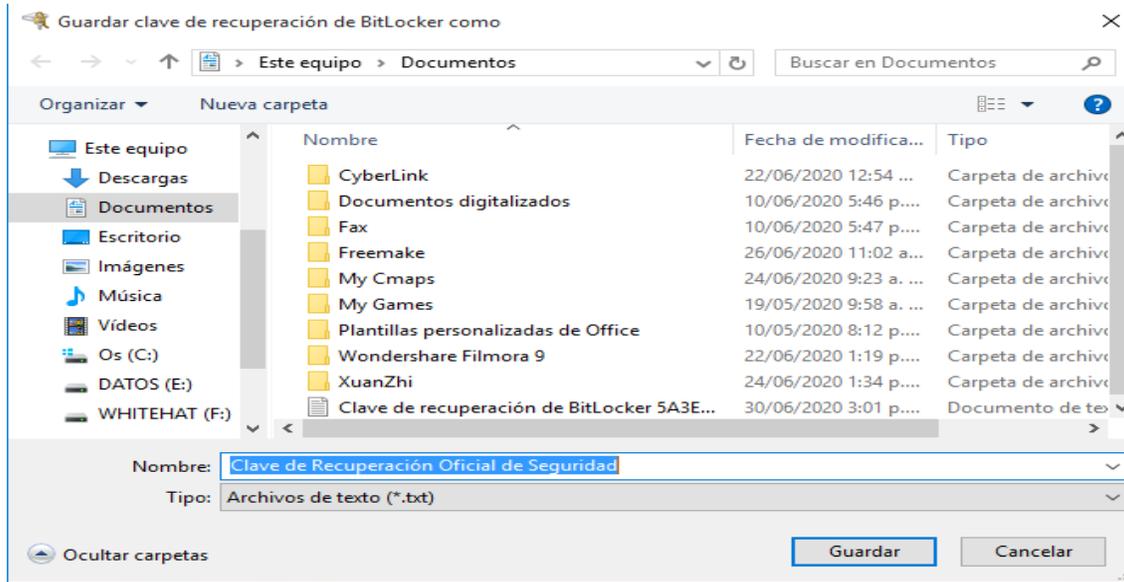
	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 13 de 32

- Como medida preventiva una vez generado este archivo deberá ser emitirse una copia al grupo de Arquitectura Empresarial y Seguridad de la información, donde se preservará la confidencialidad, integridad y disponibilidad de la información.
- En caso de requerir la restauración del acceso mediante el archivo plano deberá solicitarse formalmente a través de la mesa de servicios con el formato debidamente diligenciado.



Lo recomendable al usuario es seleccionar la opción Guardar en un archivo, esta opción permitirá guardar el archivo de recuperación de acceso, en ubicación determinada del equipo de cómputo.

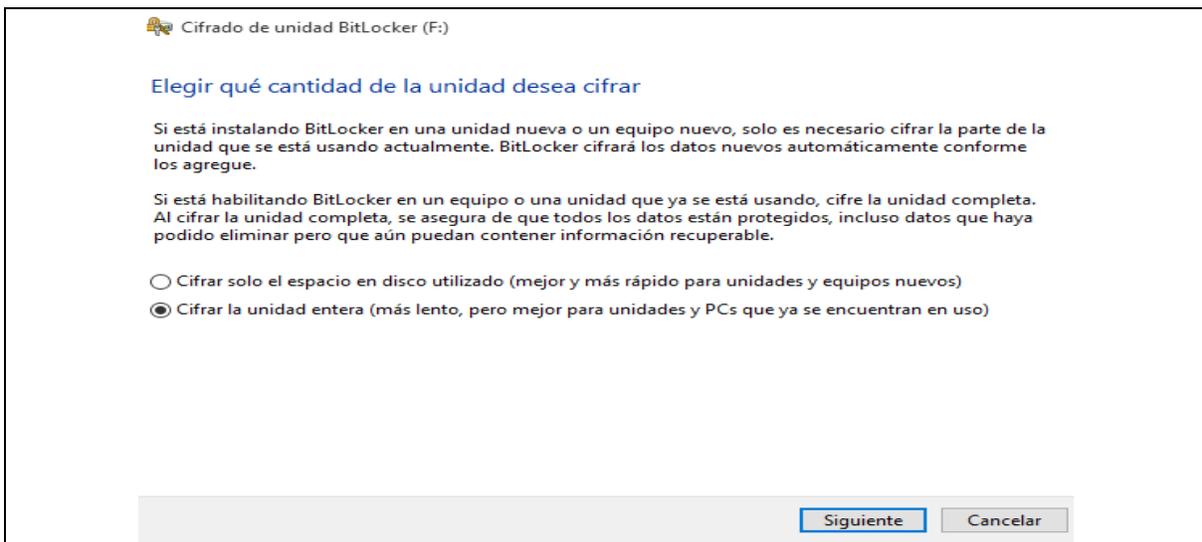
	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 14 de 32



- Se sugiere que el usuario conserve una copia de seguridad del archivo plano una vez finalizada la configuración.

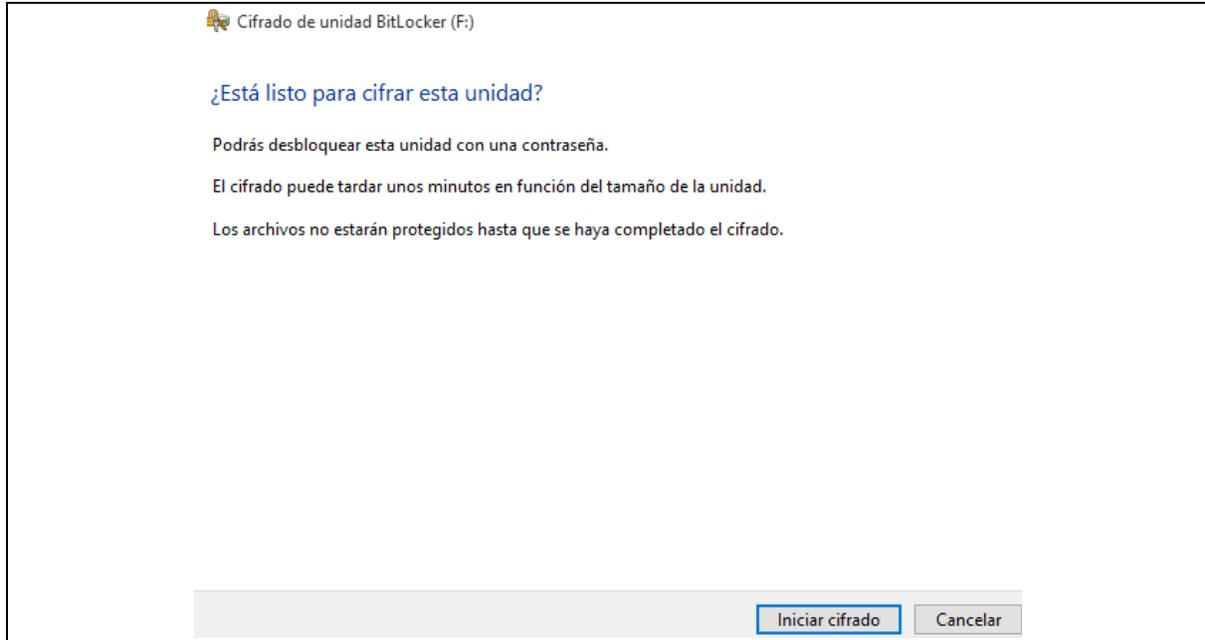
Paso 6:

- Se deberá seleccionar la opción Cifrar la unidad entera y pulsar click en el botón siguiente como se muestra a continuación:



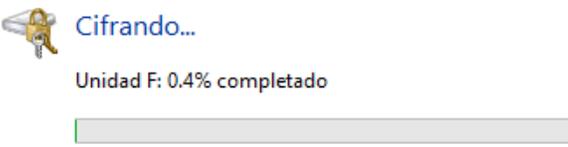
	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 15 de 32

- Seguidamente seleccionar la opción iniciar cifrado.



- Posteriormente inicia el proceso de cifrado de la unidad de almacenamiento, los tiempos serán acordes a la capacidad de almacenamiento del medio removible y de la información contenida en este.

Cifrado de unidad BitLocker

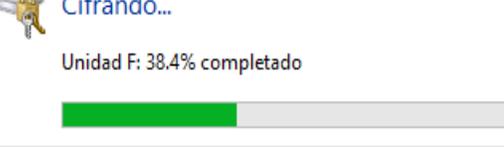


Unidad F: 0.4% completado

[Pausa](#)

! Pause el cifrado antes de quitar la unidad para evitar que se dañen los archivos de la unidad.

[Administrar BitLocker](#)



Unidad F: 38.4% completado

[Pausa](#)

! Pause el cifrado antes de quitar la unidad para evitar que se dañen los archivos de la unidad.

[Administrar BitLocker](#)

Cifrado de unidad BitLocker



 Se completó el cifrado de F:

[Cerrar](#)

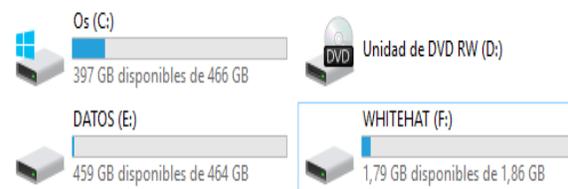
[Administrar BitLocker](#)

- La herramienta confirmara que ha finalizado el proceso de cifrado de datos.

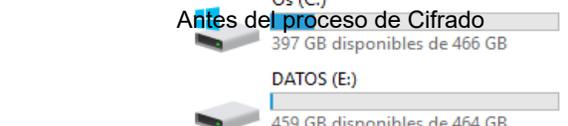
Paso 7:

Finalizado el proceso de cifrado el medio de almacenamiento ya se encuentra protegido mediante la contraseña asignada previamente.

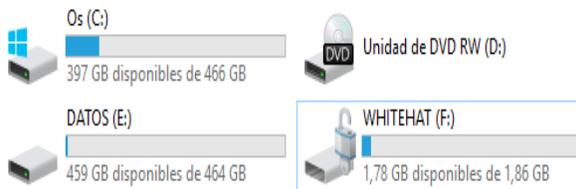
Dispositivos y unidades (4)



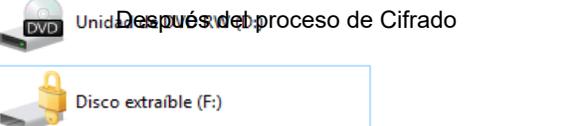
Antes del proceso de Cifrado



Dispositivos y unidades (4)

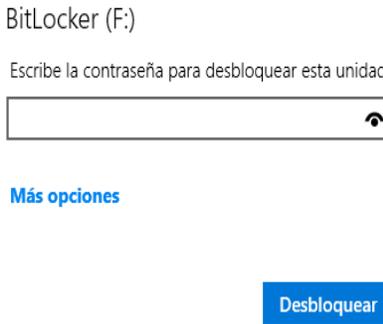


Después del proceso de Cifrado



	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 17 de 32

- El proceso de cifrado y asignación de contraseña solo deberá realizarse una sola vez, sin embargo, cada vez que se requiera acceder a la información si se deberá ingresar la contraseña asignada por el usuario.



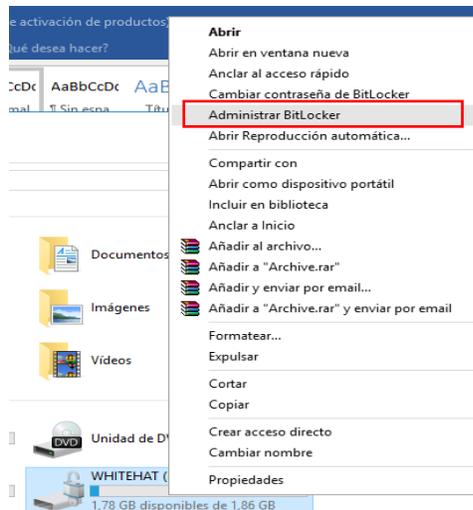
Desactivar cifrado de datos

Paso 1: Para desactivar el cifrado de datos, el usuario deberá notificar al grupo de Arquitectura Empresarial y Seguridad de la Información, a través de la mesa de servicio con el diligenciamiento del formato respectivo.

- Esta solicitud será evaluada y notificada al usuario.
- Se da por entendido que, si el usuario requiere solicitar la desactivación del cifrado de información, es porque no requiere hacer uso del medio removible, por tal razón se restringirán los puertos USB del equipo de cómputo de IDEAM.

Paso 2:

- Sobre el medio de almacenamiento conectado al equipo de cómputo, pulsar click derecho y seleccionar la opción administrar BitLocker.



	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 18 de 32

Seleccionar la Opción desactivar BitLocker.

Cifrado de unidad BitLocker

Ayude a proteger sus archivos y carpetas del acceso no autorizado protegiendo sus unidades con BitLocker.

Unidad de sistema operativo

Os (C:) BitLocker desactivado

Unidades de datos fijas

DATOS (E:) BitLocker desactivado

Unidades de datos extraíbles: BitLocker To Go

WHITEHAT (F:) BitLocker activado



- Copia de seguridad de la clave de recuperación
- Cambiar contraseña
- Quitar contraseña
- Agregar tarjeta inteligente
- Activar desbloqueo automático
- Desactivar BitLocker**

Cifrado de unidad BitLocker

Desactivar BitLocker

Se descifrá la unidad. Esto puede tardar bastante tiempo, pero puede seguir usando su equipo durante el proceso de descifrado.

Desactivar BitLocker

Cancelar



Cifrado de unidad BitLocker



Descifrando...

Unidad F: 93.0% completado



Pausa

⚠ Pause el descifrado antes de quitar la unidad para evitar que se dañen los archivos de la unidad.

Administrar BitLocker

Cifrado de unidad BitLocker



Se completó el descifrado de F:.

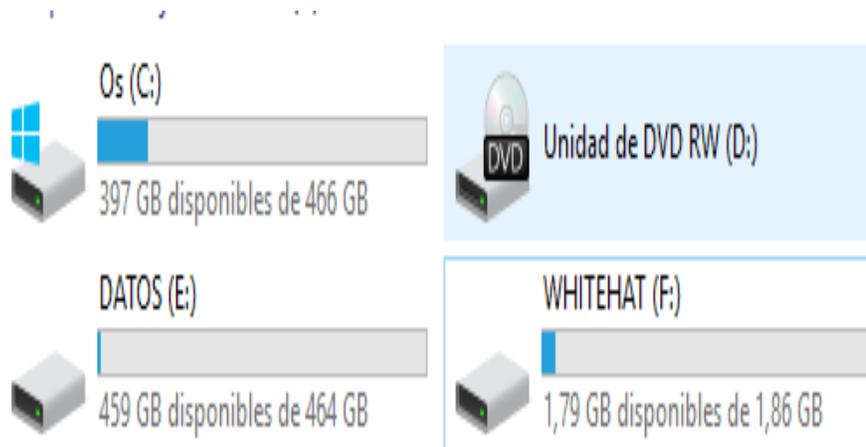
Cerrar

Administrar BitLocker

- El proceso de desactivación de cifrado será acorde a la capacidad de almacenamiento y la información alojada en el medio removible.

	INSTRUCTIVO PARA CIFRADO DE DATOS	Código: E-GI-I010
		Versión: 1.0
		Fecha emisión: 24/03/2022
		Página 19 de 32

- Finalmente, la memoria USB, disco externo, entre otros retornara a su estado inicial (sin control de cifrado).



Cifrado de datos para Linux

Para cifrar archivos en Linux podemos trabajar con el comando GPG, suele venir instalado por defecto en casi en todos los sabores de Linux, en caso de no estar debe estar disponible en sus directorios de instalación dentro del mismo sistema operativo.

Con este comando se puede encriptar archivos importantes de alto impacto para el IDEAM procedemos de la siguiente manera:

- Llamamos una terminal para trabajar en forma de meta comando
 - Digitamos en la terminal lo siguiente con la sintaxis que se indica a continuación
- ```
gpg -c nombre del archivo.txt
```
- pedirá una contraseña para encriptarlo, se puede también hacer para un directorio también
- Al hacer lo anterior se genera un archivo binario gpg

Para desencriptar los archivos o directorios se procede de la siguiente manera:

- Tecleamos `gpg -d nombre del archivo.gpg`, pedirá la contraseña especificada al encriptarlo

Se tiene otra manera de hacer la criptografía de las unidades de USB con el software VERACRYPT y requiere mucho la participación del administrador de la máquina, debido a que se maneja ciertos comandos que requiere ser administrador para poder trabajar con el usuario root de estas máquinas, se muestra a continuación la forma de instalar en las máquinas este software para el cifrado en los sistemas operativos Linux.

|                                                                                                                                                         |                                          |                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
| <br>Instituto de Hidrología,<br>Meteorología y<br>Estudios Ambientales | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                                                                                         |                                          | Versión: 1.0                  |
|                                                                                                                                                         |                                          | Fecha emisión: 24/03/2022     |
|                                                                                                                                                         |                                          | Página <b>20</b> de <b>32</b> |

Antes de instalar el VERACRYPT se debe tener en cuenta si se está trabajando con un sistema de 32 bits o 64 bits, vamos a proceder a instalarlo paso por paso

### **Paso 1**

En la máquina donde se va instalar el VERACRYPT debemos abrir una ventana como de terminal

### **Paso 2**

Al interior de este ejecutamos el siguiente comando uname -m

- Si estás operando un sistema de 32 bits, en la ventana abierta nos mostrará i686 o i386
- Si estás operando un sistema de 64 bits, nos mostrará x86\_64

### **Paso 3.**

Se debe navegar en la URL VERACRYPT en VERACRYPT en

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

### **Paso 4**

En la parte o sección donde se menciona Otras descargas disponibles, se hace clic, se hace clic en la versión más nueva de la aplicación configuración de VERACRYPT para Linux, actualmente, es configuración VERACRYPT para Linux 1.16 pero los lanzamientos futuros tendrán números de versiones más altos), después de haber descargado VERACRYPT, se puede instalar haciendo lo siguiente:

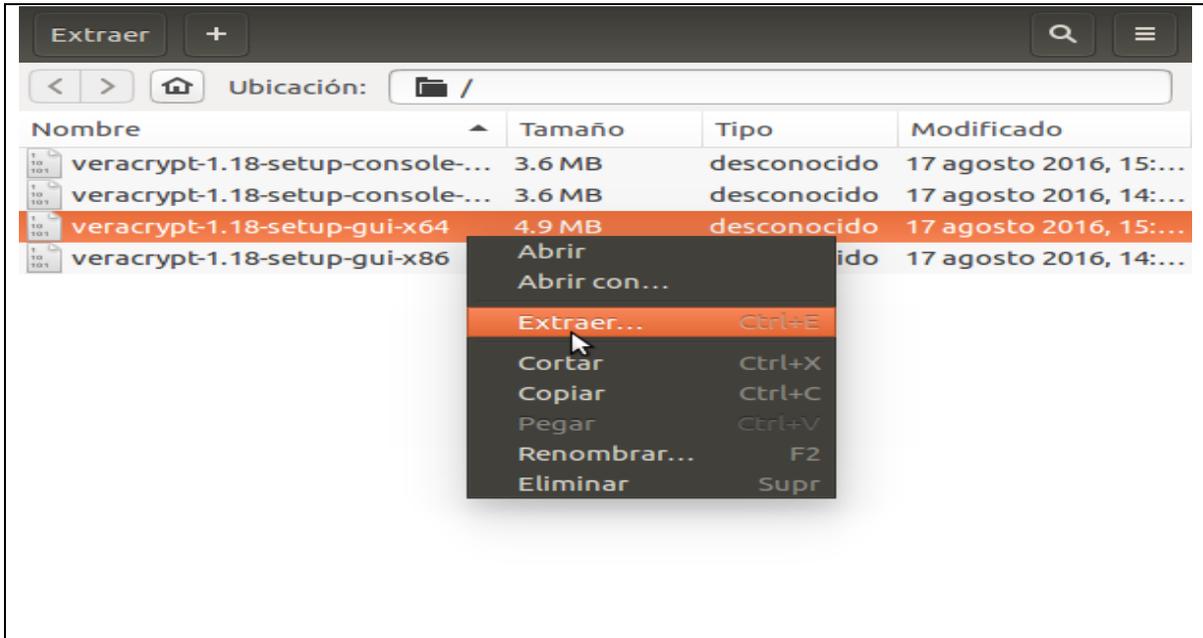
### **Paso 5**

Se inicia con el administrador de archivos o la ventana donde se muestren los directorios como son mostrados en el explorador de Windows se busca donde esta descargado el VERACRYPT

### **Paso 6.**

Haz doble clic en el archivo que se descargó en el Paso4.

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>21</b> de <b>32</b> |



#### **Paso 7.**

Haz clic derecho en la utilidad de configuración de VERACRYPT que sea correcta para tu sistema y se elige extraer

- Para un sistema de 32 bits, actualmente es veracrypt-1.16-setup-gui-x86
- Para un sistema de 64 bits, actualmente es veracrypt-1.16-setup-gui-x64

#### **Paso 8.**

Escoge una ubicación para el archivo de configuración de VERACRYPT y haz clic en Extraer

#### **Paso 9.**

Cuando la extracción esté hecha, haz clic en cerrar, cerramos el Administrador de archivos

#### **Paso 10**

Encuentra la carpeta en la que se ha extraído el archivo de configuración de VERACRYPT, en este punto, tal vez debas cambiar las preferencias de tu navegador de archivos con la finalidad de iniciar el propio instalador.

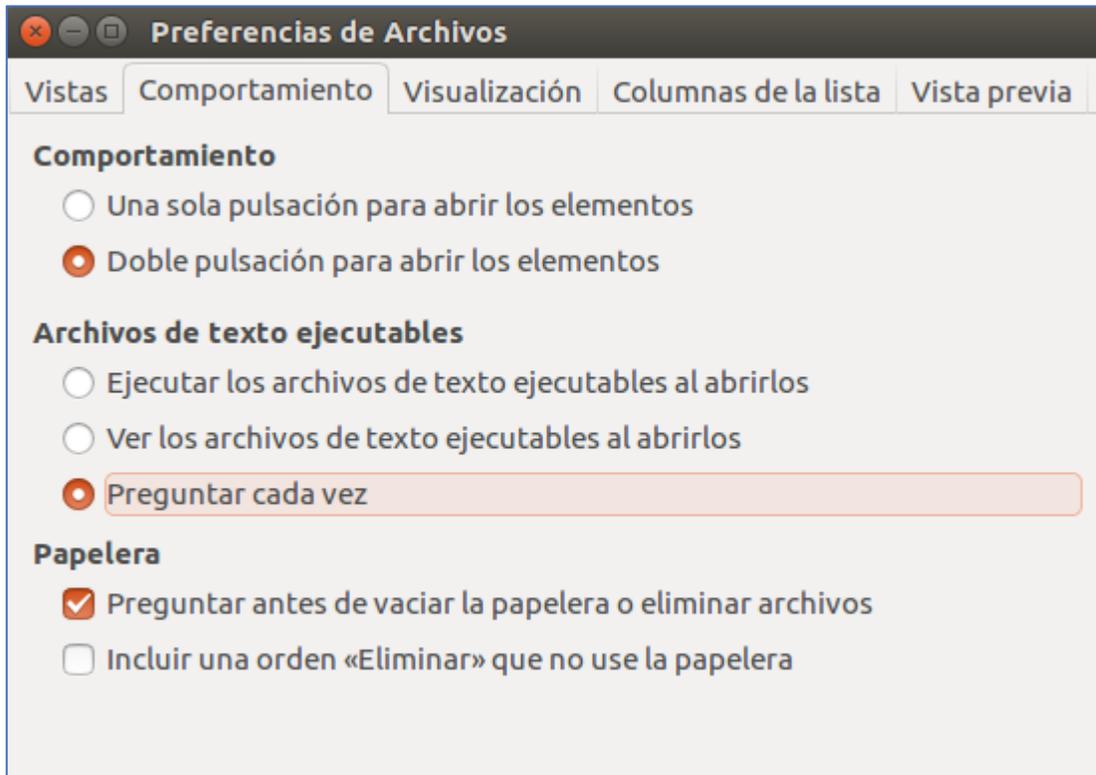
#### **Paso 11**

Haz clic en editar en el menú de tu navegador de archivos y se elige preferencias para abrir la pantalla de preferencias

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>22</b> de <b>32</b> |

### Paso 12

Haz clic en la pestaña comportamiento



### Paso 13

Debajo de archivos de texto ejecutables, asegurar de que pregunte cada vez esté marcado

### Paso 14

Haz clic en cerrar

### Paso 15

Se hace doble clic en el archivo de configuración de VERACRYPT, para escoger si se quiere mostrar el archivo de configuración o Ejecutarlo

### Paso16

Haz clic en ejecutar para iniciar el instalador de VERACRYPT

### Paso 17

Haz clic en instalar VERACRYPT para mostrar los términos de la licencia

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>23</b> de <b>32</b> |

### Paso 18

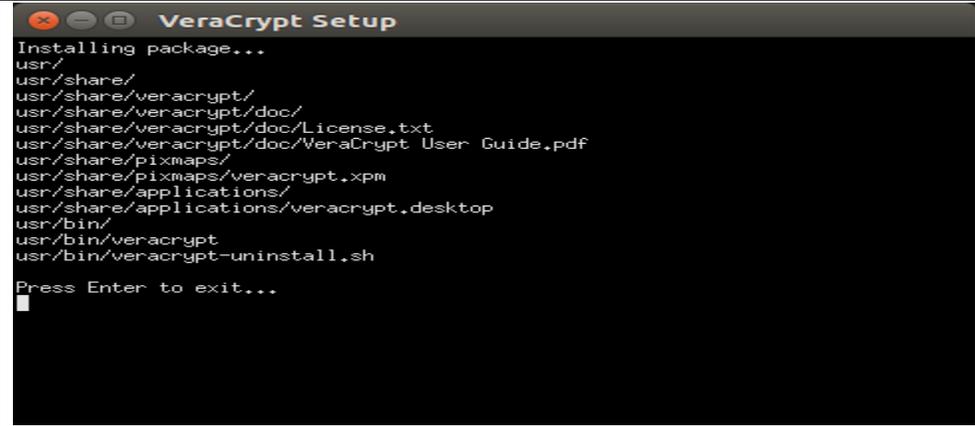
Se deben leer los términos de la licencia de VERACRYPT y se hace clic en Acepto y estoy de acuerdo con cumplir los términos de la licencia

### Paso 19

Se clic en OK

### Paso 20

Se escribe la contraseña que se usa para iniciar la sección en la máquina donde se esta instalando y se presiona Aceptar para completar la instalación de VERACRYPT



```

VeraCrypt Setup
Installing package...
usr/
usr/share/
usr/share/veracrypt/
usr/share/veracrypt/doc/
usr/share/veracrypt/doc/License.txt
usr/share/veracrypt/doc/VeraCrypt User Guide.pdf
usr/share/pixmaps/
usr/share/pixmaps/veracrypt.xpm
usr/share/applications/
usr/share/applications/veracrypt.desktop
usr/bin/
usr/bin/veracrypt
usr/bin/veracrypt-uninstall.sh
Press Enter to exit...

```

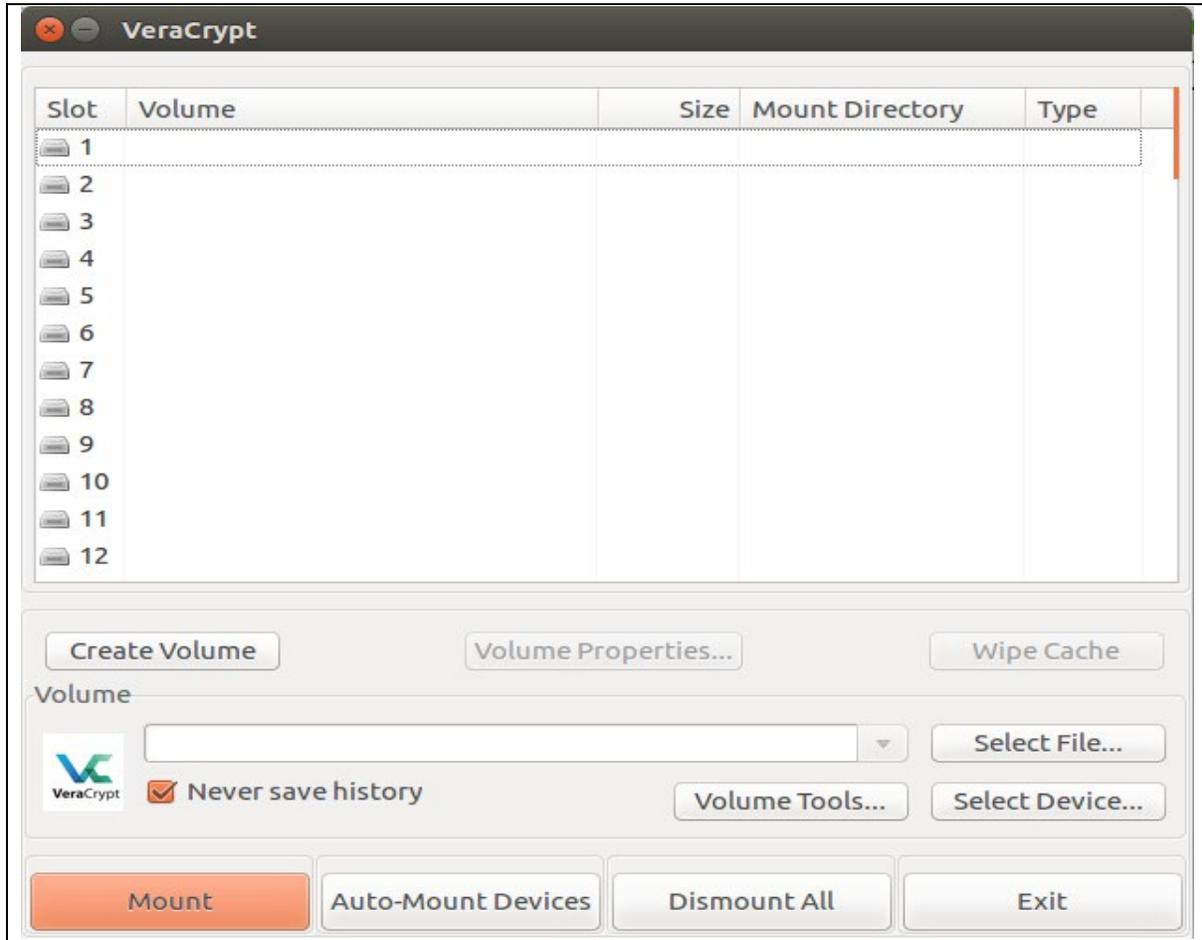
### CREAR UN VOLUMEN ESTÁNDAR

Para comenzar a usar esta herramienta se trabaja de dos formas una es volúmenes ocultos y volúmenes estándar,

- Los volúmenes estándar protegen los archivos con una contraseña que se debe ingresar con la finalidad de acceder a ellos
- Los volúmenes ocultos tienen dos contraseñas. Con la una de las dos se puede abrir un volumen estándar señuelo donde se debe guardar los archivos menos sensibles de los que se puede ceder de ser necesario. Ingresar la otra contraseña abrirá el volumen oculto que contienen verdaderamente sensibles

### Paso 1

Se inicia VERACRYPT para abrir la ventana principal de la aplicación



**Paso 2** Haz clic en crear volumen para activar la siguiente ventana de creación de VeraCrypt

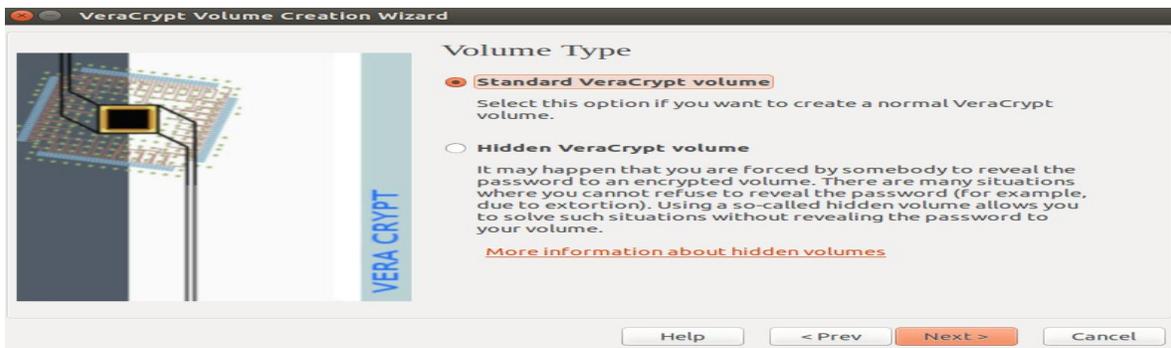


|                                                                                   |                                          |                           |
|-----------------------------------------------------------------------------------|------------------------------------------|---------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010         |
|                                                                                   |                                          | Versión: 1.0              |
|                                                                                   |                                          | Fecha emisión: 24/03/2022 |
|                                                                                   |                                          | Página 25 de 32           |

Un archivo contenedor de VeraCrypt es un volumen encriptado que se almacena dentro de un solo archivo. Este contenedor se puede renombrar, mover, copiar o borrar como cualquier otro archivo.

### Paso 3

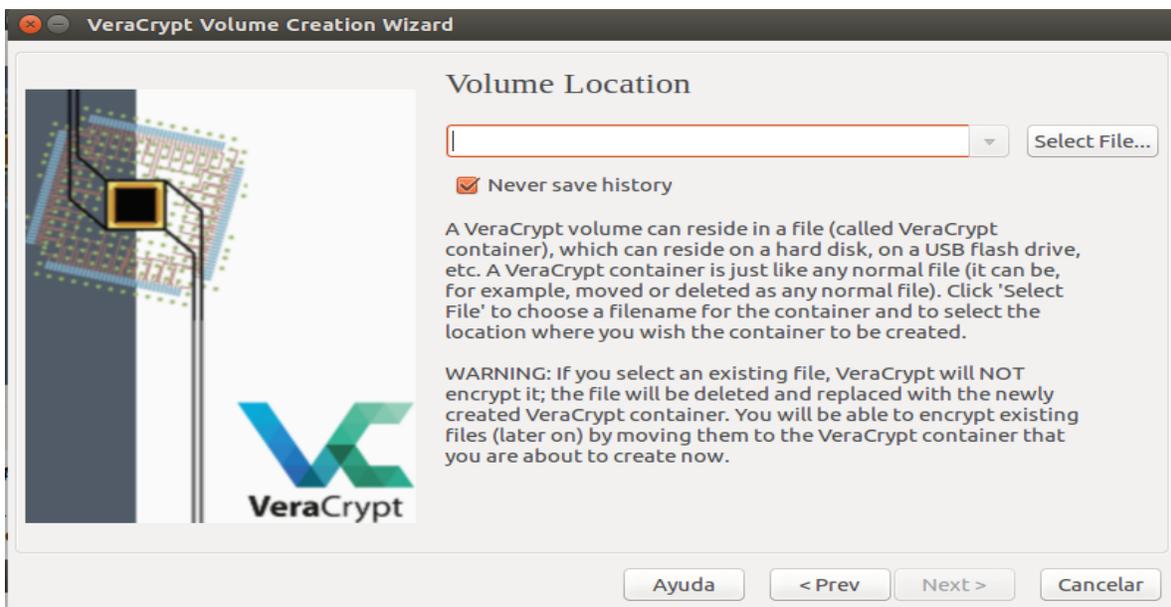
Se hace clic en el siguiente para elegir el tipo de volumen que quieres crear



La ventana de asistente para crear tipo de volumen de VeraCrypt te permite especificar si se quiere crear un volumen estándar u oculto

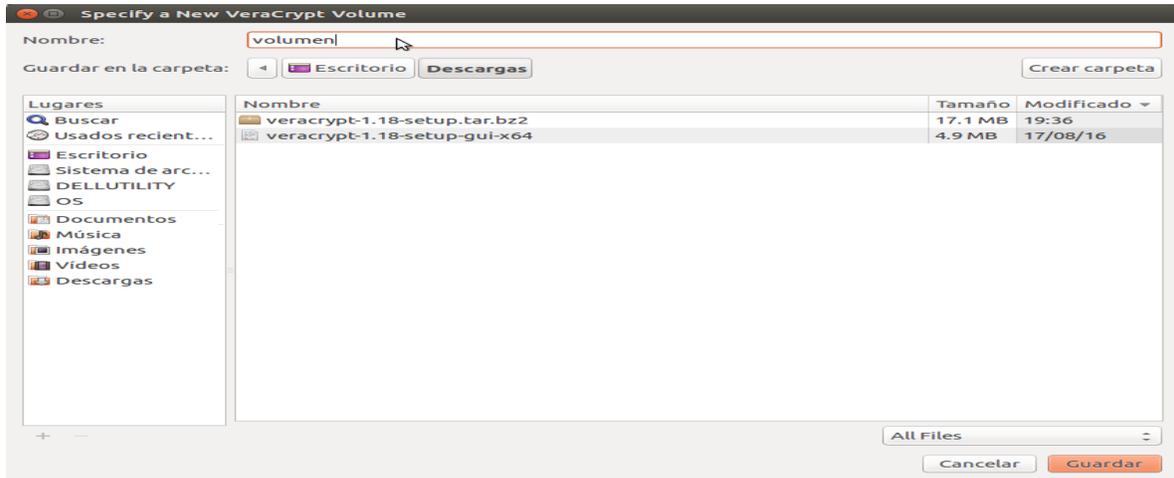
### Paso 4

Nos aseguramos de que el volumen estándar de VeraCrypt esté marcado y se hace clic en siguiente para elegir un nombre y ubicación para el archivo contenedor de VeraCrypt



**Paso 5** Se hace clic en Elegir archivo, para escoger una ubicación para tu archivo contenedor de Veracrypt y especifique un nombre

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>26</b> de <b>32</b> |



### Paso 6

Se navega a la carpeta en la que quisieras crear el contenedor

### Paso 7

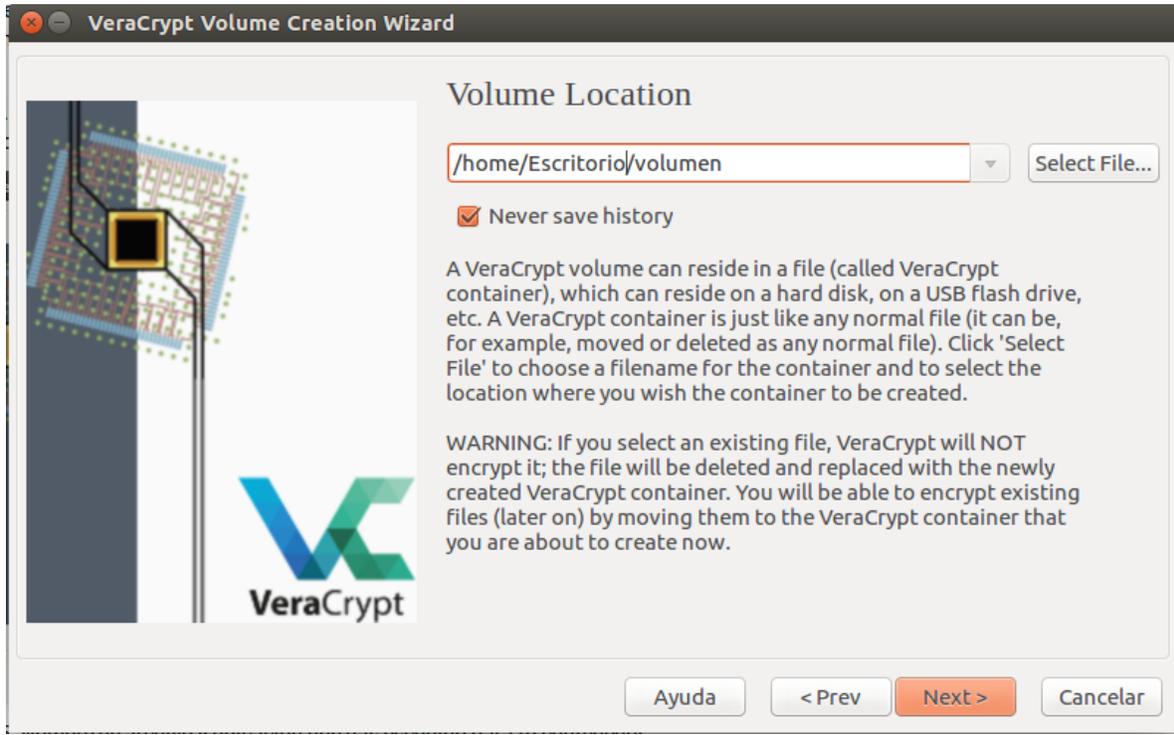
Escoge un nombre de archivo para el contenedor y se escribe en el campo en la parte de arriba de la ventana, se recomienda no elegir un archivo que exista y asegurar recordar dónde se ubicó el contenedor y el nombre con el cual fue llamado

En el ejemplo, se ha creado un contenedor llamado volumen en el escritorio, el contenedor puede tener cualquier nombre y cualquier extensión, por ejemplo, se puede llamar recetas.docx o vacaciones.mpg con la esperanza de que un observador de Microsoft Word casual pensará que es un documento o un archivo de video de Microsoft Word, esta es una manera en que puedes ayudar o disimular la existencia de un contenedor de VeraCrypt pero no funcionará con alguien que tenga el tiempo y los recursos para buscar minuciosamente en el dispositivo

Si se quiere crear un contenedor de VeraCrypt en un dispositivo de almacenamiento USB, simplemente navega al dispositivo, en vez de ir a la carpeta de la máquina se escoge un nombre del archivo

### Paso 8

Se hace clic en guardar una vez que se haya determinado una ubicación y escogido un nombre para tu archivo contenedor de VeraCrypt



**Paso 9**

Se hace clic en Siguiete para configurar las opciones de encriptación

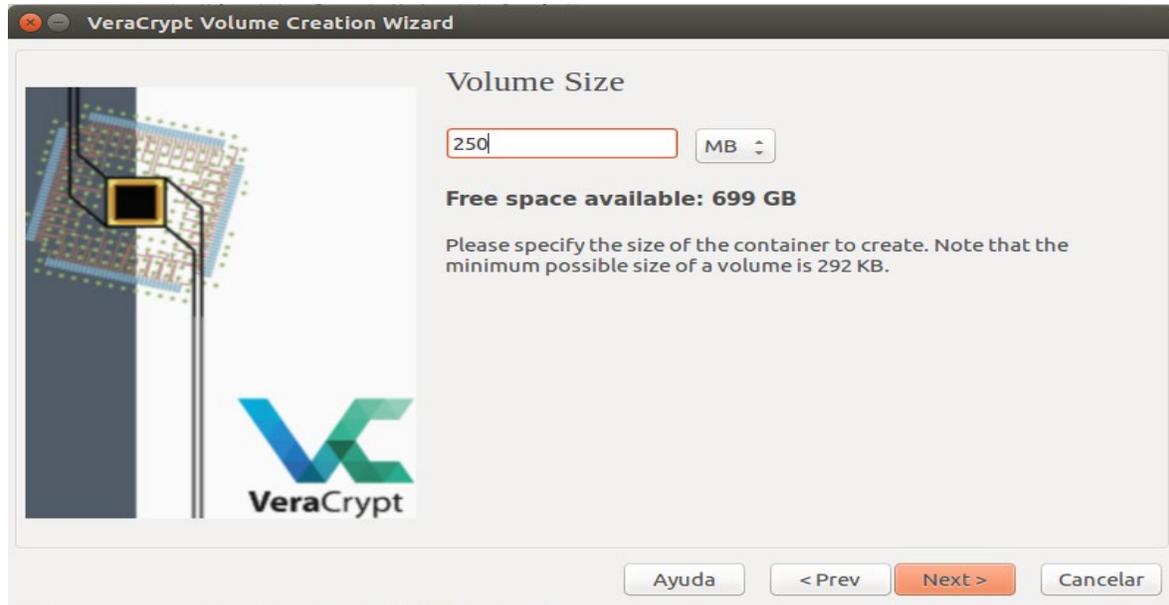


Acá se puede escoger un método específico o algoritmo a usar cuando se encriptes y desencriptes los archivos almacenados dentro del contenedor VeraCrypt, las opciones por defecto se consideran seguras, así que probamente se debe dejar como son mostradas

**Paso 10**

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>28</b> de <b>32</b> |

Se hace clic en siguiente para elegir un tamaño de volumen



La ventana de tamaño de volumen permite especificar el tamaño del contenedor que

se está creando. En el ejemplo se crea un volumen de 250 MB, pero tal vez se quiera especificar un tamaño diferente se evalúa la cantidad de archivos y más importante, el tipo de archivos que se van a guardar o almacenar en el volumen encriptado. Los archivos de imagen y videos, en particular, pueden llenar un contenedor VeraCrypt pequeño rápidamente.

Dato: Si se va a crear tener varias copias de seguridad del archivo contenedor en un cd, SE DEBE ELERGIR UN TAMAÑO DE 700 MB o menos, para una copia de seguridad en un DVD se debe ser 4.5 o menos. Al querer cargar el archivo contenedor en un servicio de almacenamiento en línea, se debe determinar un tamaño razonable desacuerdo con la velocidad de la conexión de internet.

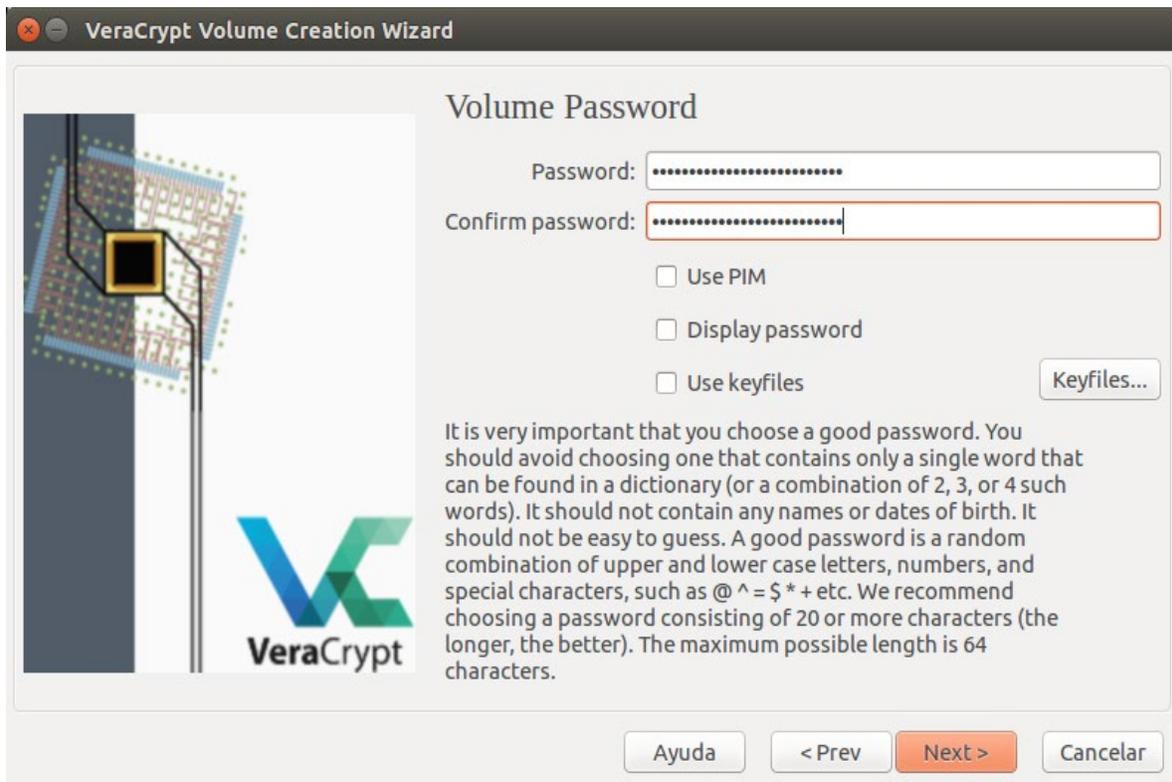
### **Paso 11**

Se escribe le tamaño del volumen que se quiere crear, se asegura de elegir un valor correcto para kb, MB, GB o TB

### **Paso 12**

Se hace clic en siguiente para elegir una contraseña

|                                                                                   |                                          |                           |
|-----------------------------------------------------------------------------------|------------------------------------------|---------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010         |
|                                                                                   |                                          | Versión: 1.0              |
|                                                                                   |                                          | Fecha emisión: 24/03/2022 |
|                                                                                   |                                          | Página 29 de 32           |



**IMPORTANTE** Elegir una contraseña fuerte es uno de los pasos más importantes que vas a llevar a cabo al crear un volumen VeraCrypt. Cuanto más sea la contraseña, mejor. Se puede usar el KeePassX

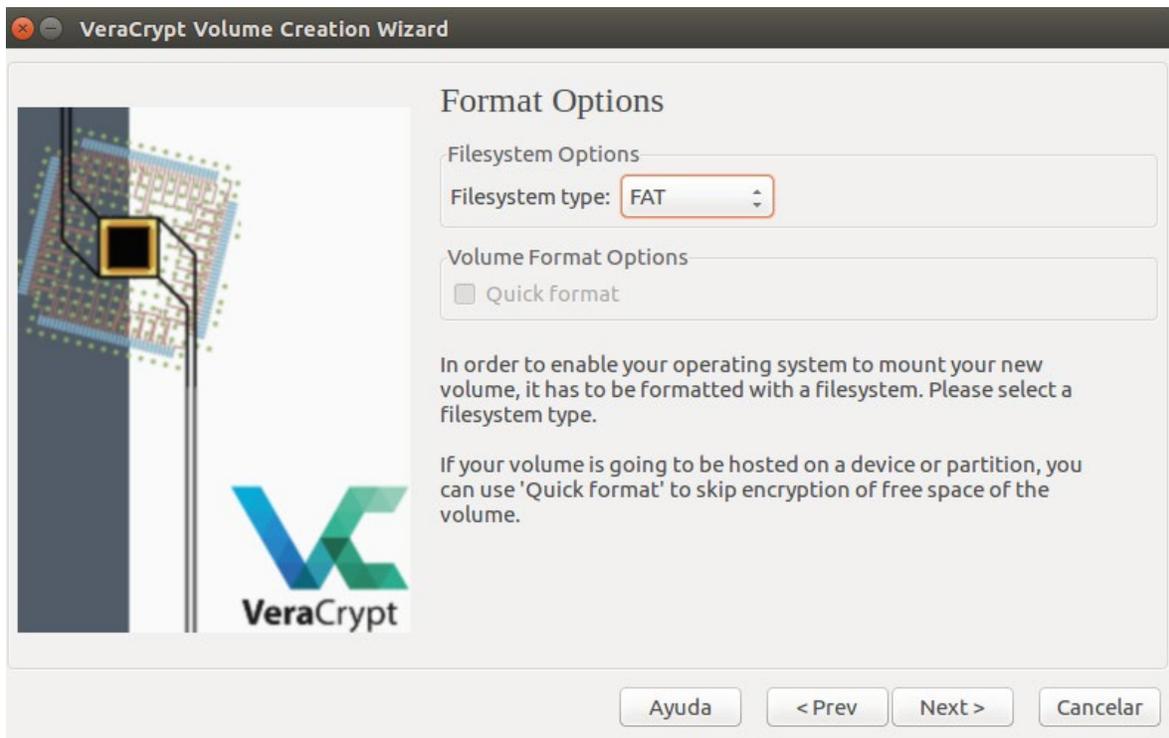
### Paso 13

Se escribe la contraseña y luego vuelve a escribirla en el campo Confirmar para activar el botón Siguiente

### Paso 14

Se hace clic en Siguiente para elegir un tipo de sistema de archivos

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>30</b> de <b>32</b> |

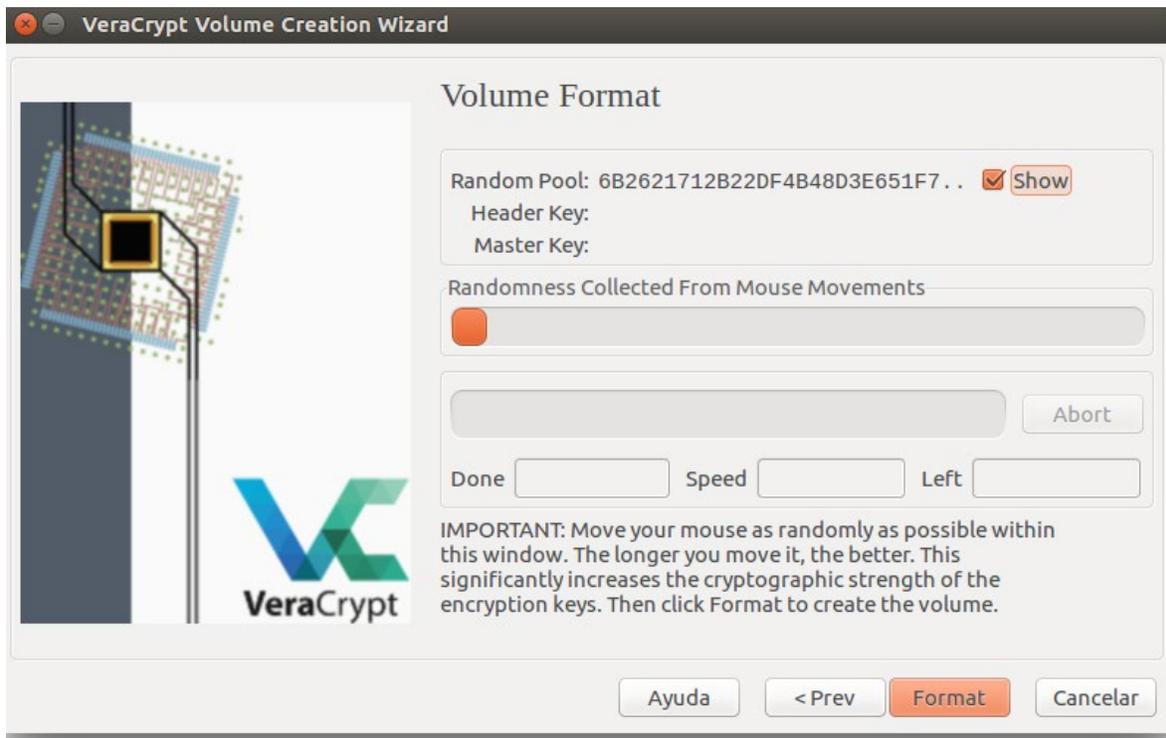


Nota: El valor por defecto es FAT el cual funcionara para la mayoría de personas y es compatible con computadoras Windows, Mac OS X y Linux. Sin embargo, si se quiere almacenar archivos de más de 4 GB como único archivo, entonces se debe elegir un tipo diferente de sistema de archivos. En Linux Ext2 solamente funcionara en computadoras de Linux y NTFS funcionarán la mayoría de computadoras con Windows y en la mayoría de computadoras de Linux

### Paso 15

Se hace clic en Siguiete luego de escoger un tipo de sistema de archivos adecuado

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>31</b> de <b>32</b> |

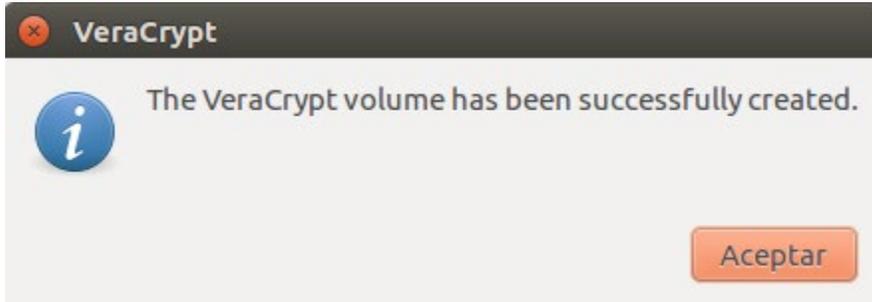


VeraCrypt ya está listo para crear un volumen estándar encriptado dentro de un archivo contenedor. Si se mueve el mouse dentro de la ventana del asistente de creación de volumen VeraCrypt se producirá información aleatoria que ayudará a fortalecer la encriptación

#### **Paso 16**

Haga clic en Formato para empezar a crear el volumen estándar, VeraCrypt le dirá cuando haya terminado de crear el volumen encriptado

|                                                                                   |                                          |                               |
|-----------------------------------------------------------------------------------|------------------------------------------|-------------------------------|
|  | <b>INSTRUCTIVO PARA CIFRADO DE DATOS</b> | Código: E-GI-I010             |
|                                                                                   |                                          | Versión: 1.0                  |
|                                                                                   |                                          | Fecha emisión: 24/03/2022     |
|                                                                                   |                                          | Página <b>32</b> de <b>32</b> |



Y ya se puede comenzar a usar el volumen estándar

#### HISTORIAL DE CAMBIOS

| Versión | Fecha         | Descripción       |
|---------|---------------|-------------------|
| 1.0     | 24/ 03 / 2022 | Documento Inicial |

|                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                            |                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ELABORÓ:</p>  <p>Carlos Eduardo Pedraza Tafur<br/>Oficina Informática</p> | <p>REVISÓ:</p>  <p>Eduardo Ramírez Acosta<br/>Coordinador del grupo<br/>GAESI</p>  <p>Guillermo Ojalora<br/>Oficial de Seguridad</p> | <p>APROBÓ:</p>  <p>Alicia Barón<br/>Jefe Oficina Informática</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|