



# Seguridad digital integral

Materiales para mejorar tus hábitos digitales.









## **Tutorial de Veracrypt**



Tomado de:



### Veracrypt: Cifra y oculta tus archivos gratis

redeszone.net/tutoriales/seguridad/veracrypt-cifra-archivos-gratis/



VeraCrypt es un software de código abierto para **cifrar archivos**, **carpetas**, **unidades USB extraíbles**, **discos duros completos**, **e incluso el disco duro donde se encuentra el propio sistema operativo** instalado. **VeraCrypt es multiplataforma**, actualmente es compatible con sistemas operativos Microsoft Windows, cualquier sistema basado en Linux, y también es compatible con macOS. Este software está basado en el popular **TrueCrypt 7.1a**. Debemos recordar que el proyecto TrueCrypt cerró, y ya no tendremos nuevas actualizaciones de dicho software. Sin embargo, VeraCrypt ha cogido el testigo e incorpora todas las características de TrueCrypt y muchas mejoras de seguridad y rendimiento.

#### Principales Características de VeraCrypt

Algunas de las principales características de VeraCrypt son las siguientes:

 Creación de discos cifrados virtuales en un simple archivo: podremos crear un archivo cifrado a modo de contenedor, en el cual esté toda la información importante. Este archivo lo podremos montar para su lectura y escritura con VeraCrypt, este método es ideal para moverlo a cualquier sitio e incluso para enviarlo por email, subirlo a un servidor FTP o Samba y más. Gracias a que tenemos un simple archivo que contiene toda la información confidencial, podremos guardarlo a buen recaudo grabándolo en un CD o DVD, e incluso copiarlo en un pendrive.

- Cifrado de dispositivos de almacenamiento extraíble como USB, tarjetas SD e incluso discos duros. En este caso, todo el dispositivo de almacenamiento extraíble estará complemente cifrado, Windows nos indicará que necesita formato el disco para poder leerlo, siempre debemos pinchar en cancelar y abrirlo con VeraCrypt, introduciendo la correspondiente clave de descrifrado.
- Cifrado de cualquier partición de estos dispositivos de almacenamiento extraíble.
- Cifrado de la partición o disco completo donde Windows esté instalado. Esto nos permite hacer exactamente la misma función que Bitlocker, cifrará el disco duro o SSD por completo, para que tanto el sistema operativo como todos nuestros archivos estén a salvo frente a posibles robos.
- El cifrado y el descifrado es automático y se hace en tiempo real, siendo completamente transparente al usuario.
- El cifrado y descifrado si utilizamos AES se puede acelerar si el procesador del equipo soporta AES-NI, proporcionando una mayor velocidad de lectura y escritura.
- Posibilidad de crear un volumen «oculto» para evitar que un posible atacante nos fuerce a revelar la contraseña del volumen (chantaje, extorsión etc.)

Una vez que ya conocemos sus principales características, vamos a ver cómo descargar e instalar VeraCrypt en nuestro ordenador con Windows 10 Pro.

#### 1. Descarga e instalación de VeraCrypt

Lo primero que tenemos que hacer es descargar VeraCrypt, la descarga se realiza directamente a través de la <u>página web oficial</u>, en la sección descargas: <u>Descargar</u> <u>VeraCrypt gratis</u>. En esta web vamos a poder descargar todas las versiones de VeraCrypt, tanto para Windows, Linux, macOS, FreeBSD e incluso directamente el código fuente.



Una vez descargado el programa, debemos instalarlo como cualquier programa. Nos saldrá un asistente de instalación que nos dará la opción de instalarlo en el propio equipo, o extraer VeraCrypt y usarlo de manera «portable», es decir, sin instalarlo en el

propio ordenador. Un detalle importante es que si vamos a cifrar el sistema completo o la partición donde está el sistema operativo, deberemos instalarlo obligatoriamente y no usarlo en modo «portable».

You must					M.
	accept these license terms	s before you can use, ex	tract, or install Ve	eraCrypt.	
MPORTAN	T: By checking the checkb and agree to them. Pleas	oox below, you accept the se click the 'arrow down'	ese license terms icon to see the r	and signify that est of the license	you
VeraCryp	t License				,
Software o ANY KIND WHO USE ACTION(S LICENSE. SOFTWAR	distributed under this licer . THE AUTHORS AND DIS S, COPIES, MODIFIES, OR ), ACCEPTING AND AGREI IF YOU DO NOT ACCEPT E, NOR ANY PART(S) THE	nse is distributed on an " TRIBUTORS OF THE SOF (RE)DISTRIBUTES ANY EING TO BE BOUND BY THEM, DO NOT USE, CO REOF.	AS IS" BASIS WI TWARE DISCLAI PART OF THE SO ALL TERMS AND PY, MODIFY, NO	THOUT WARRAN M ANY LIABILITY OFTWARE IS, BY CONDITIONS OF R (RE)DISTRIBUT	TTIES OF (. ANYONE SUCH THIS TE THE
VeraCrypt copy of bo	is multi-licensed under Ap th licenses can be found l	pache License 2.0 and th below.	e TrueCrypt Lice	nse version 3.0, a	a verbatim
I accep	t the license terms				
Crypt Inst	aller				
		Help	< Back	Next >	Cancel
_					
/eraCrypt	Setup 1 22			_	
	Setup 1.22				
izard Mo	de				VC.
izard Mo	de of the modes. If you are	not sure which to select,	use the default	mode.	<u>×</u>
Select one	de of the modes. If you are	not sure which to select,	use the default	mode.	<u>×</u>
Select one	de of the modes. If you are	not sure which to select,	use the default	mode.	¥.
Select one	de of the modes. If you are	not sure which to select,	use the default	mode.	~
Select one	de of the modes. If you are II Select this option if you	not sure which to select, want to install VeraCryp	use the default	mode.	~
izard Mo Select one Insta	de e of the modes. If you are II Select this option if you	not sure which to select, want to install VeraCryp	use the default	mode.	¥
<ul> <li>izard Mor</li> <li>Select one</li> <li>Insta</li> <li>Extra</li> </ul>	de e of the modes. If you are ll Select this option if you ect If you select this option, installed on the system. system drive. Selecting VeraCrypt in so-called p operating system under the extracted file 'VeraC	not sure which to select, want to install VeraCryp , all files will be extracte Do not select it if you in this option can be usefu portable mode. VeraCryp which it is run. After all Crypt.exe' (then VeraCryp	d from this system. t on this system. t on this system. for example, if t does not have t files are extracted of will run in port	mode. age but nothing v the system partiti you want to run o be installed on ed, you can direct able mode).	vill be ion or the tly run

Una vez que hayamos pinchado en «Install», nos saldrán las típicas opciones de instalación para todos los usuarios, creación de acceso directo en escritorio y también en el menú inicio. Una vez que haya terminado de instalar, nos recomendará seguir una pequeña guía para principiantes en VeraCrypt.

Vera	Count Coture 1	22			_	
	Crypt Setup 1.	22				
Setup	o Options					VC.
Her	e you can set va	arious options to co	ontrol the installation	process.		
P	lease select or t	ype the location w	here you want to inst	all the VeraCrypt	program files. If	the
S	pecified folder d	loes not exist, it wi	ill be automatically cro	eated.		
Ē	C:\Program File	s\VeraCrvpt\				Browse
	Install for al	lusers				
	Add VeraCry	pt to Start menu				
	Add VeraCry	pt icon to desktop	)			
	Associate th	e .hc file extension	with VeraCrypt			
	Create Syste	em Restore point				
raCry	pt Installer —					
Vera	Crypt Setup 1.	22	Help	< Back	Install	Cancel
Vera Insta Plea	Crypt Setup 1. I <b>lling</b> ase wait while V	22 eraCrypt is being i	Help	< Back	Install —	Cancel
Vera Plea Insta Insta Insta Addi Addi Addi Addi Addi Addi Addi Add	Crypt Setup 1. Illing ase wait while Va alling C:\Program alling C:\Program alling C:\Program ing registry entr ing con C:\Prog ing icon C:\Prog ing icon C:\Prog ing icon C:\User allation completo	22 eraCrypt is being i m Files\VeraCrypt\ m Files\VeraCrypt\ m Files\VeraCrypt\ m Files\VeraCrypt\ y Software\Classes y Softwar	Help Installed. docs\html\en\Wear-Li docs\html\en\Whirlpo docs\VeraCryptVolume s\VeraCryptVolume\Di s\VeraCryptVolume\Di s\VeraCryptVolume\Si s\.hc oft\Windows\Current\ t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu	< Back eveling.html ol.html Guide.chm efaultIcon hell\open\comman /ersion\Uninstall\V i\Programs\VeraCr i\Programs\VeraCr i\Programs\VeraCr i\Programs\VeraCr	Install d eraCrypt ypt\VeraCrypt.lr ypt\VeraCryptE: ypt\VeraCrypt V ypt\Uninstall Ve	Cancel
Vera Insta Insta Insta Addi Addi Addi Addi Addi Addi Addi Add	Crypt Setup 1. Illing ase wait while Va alling C:\Program alling C:\Program alling C:\Program ing registry entry ing icon C:\Prog ing icon C:\Prog ing icon C:\User allation complete	22 eraCrypt is being i m Files\VeraCrypt\ m Files\VeraCrypt\ m Files\VeraCrypt\ y Software\Classes y Software y Software\Classes y Software\Classes y Software y Software y Software y S	Help Installed. docs\html\en\Wear-Li docs\html\en\Whirlpo docs\VeraCryptVolume s\VeraCryptVolume\Di s\VeraCryptVolume\Di s\VeraCryptVolume\Si s\.hc oft\Windows\Current\ t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu	< Back eveling.html ol.html Guide.chm efaultIcon hell\open\comman /ersion\Uninstall\V i\Programs\VeraCr i\Programs\VeraCr i\Programs\VeraCr i\Programs\VeraCr	Install — d eraCrypt ypt\VeraCrypt.lr ypt\VeraCryptEs ypt\VeraCrypt V ypt\Uninstall Ve	Cancel
Vera Insta Plea Inst Inst Addi Addi Addi Addi Addi Addi Addi Add	Crypt Setup 1. Illing ase wait while Va alling C:\Program alling C:\Program alling C:\Program ing registry entr ing icon C:\Prog ing icon C:\Prog ing icon C:\Prog ing icon C:\User allation complete pt Installer	22 eraCrypt is being i m Files\VeraCrypt\ m Files\VeraCrypt\ m Files\VeraCrypt\ y Software\Classes y Softwar	Help Installed. docs\html\en\Wear-Lu docs\html\en\Whirlpo docs\VeraCryptVolume s\VeraCryptVolume\Di s\VeraCryptVolume\Si s\.hc oft\Windows\Current\ t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu t\Windows\Start Menu	< Back eveling.html ol.html Guide.chm efaultIcon hell\open\comman /ersion\Uninstall\V i\Programs\VeraCr i\Programs\VeraCr i\Programs\VeraCr	Install d eraCrypt ypt\VeraCrypt.lr ypt\VeraCryptEr ypt\VeraCrypt V ypt\Uninstall Ve	Cancel

VeraCrypt Setup 1 VeraCrypt has been Please consider main	1.22 n successfully installed aking a donation. You car	l n click Finish anyt	ime to close the ins		×
VeraCrypt	Setup If you have never used read the chapter Begi you want to view the	d VeraCrypt befo inner's Tutorial i tutorial?	ore, we recommen n the VeraCrypt U	id that you ser Guide. Do	×
		_	Sí	No	
VeraCrypt Installer —	ļ	Help	< Back	Finish	Cancel

Una vez que lo tenemos instalado, vamos a proceder a crear los diferentes volúmenes, el cifrado de discos USB, y también el cifrado completo del sistema operativo.

#### 2. Creación de un volumen cifrado «normal»

Lo primero que vamos a hacer es crear un volumen cifrado «normal», sin introducir dentro de él un volumen oculto.

En el menú principal de VeraCrypt procedemos a pinchar sobre «**Crear Volumen**«, para posteriormente seleccionar la opción «**Crear un contenedor de archivos cifrado**«. Una vez hecho esto, deberemos elegir si queremos crear un volumen VeraCrypt común, o un volumen VeraCrypt oculto, nosotros vamos a seleccionar la primera opción: **Crear un volumen VeraCrypt común**.

Para crear un contenedor, deberemos seleccionar una ruta y un nombre de archivo, pinchamos en «**Seleccionar archivo**» para ubicar el archivo que nosotros queramos donde nosotros queramos.

₩ VeraCrypt Volúmenes Sistema Favoritos	Herramientas Co	nfiguración Avuda	_	Página Web
Unid Volumen A: B: E: F: G: H: J: J: K: L: M: N: O:		Tamaño Algoritmo de cifrado	Tipo	Y digina (Veb
Crear Volumen	Propieda	des del Volumen	Borra	Caché
Volumen		~	Seleccion	ar Archivo
VeraCrypt No guardar nu	unca historial	Herramientas de volumen	Selecciona	r Dispositivo
Montar	Montar Autom.	Desmontar Todo		Salir

🐱 VeraCrypt	- 🗆 🗙
Volúmenes Sistema Favoritos Herramientas Configuración A	yuda Página Web
🐸 Asistente de creación de Volumen VeraCrypt	– 🗆 🗙
Asistente de C Crea un disco cifrac para usuarios sin es Más información	reación de Volúmenes or de archivos cifrado do virtual dentro de un archivo. Recomendado xperiencia.
<ul> <li>Cifrar partición/uni Cifra una partición/uni Cifra una partición/uni Unidad flash). Opcio</li> <li>Cifrar la partición/uni Cifra una partición/uni Cifra la part</li></ul>	idad secundaria en cualquier unidad interna o externa (ej: onalmente, crea un volumen oculto. unidad del sistema entera nidad donde Windows está instalado. era acceder al sistema, leer y escribir á que introducir la contraseña antes de Opcionalmente, crea un sistema oculto. bre cifrado del sistema
Ayuda Montar Montar Autom. Desm	< Atrás Siguiente > Cancelar ontar Todo Salir





Una vez que ya tenemos configurado nuestro volumen VeraCrypt, deberemos seleccionar dos aspectos muy importantes: el cifrado simétrico para asegurar la confidencialidad, y el algoritmo de hashing para comprobar la integridad de los archivos.

En el desplegable tendremos la posibilidad de seleccionar una gran cantidad de algoritmos de cifrado simétrico, por defecto es AES, de hecho, si nuestra CPU soporta AES-NI (AES por hardware) tendremos un grandísimo rendimiento. Si pinchamos en «Comparación» podremos ejecutar un «benchmark» para comprobar cuál de todos es el más rápido.

Una vez que hayamos elegido el algoritmo de cifrado simétrico (nosotros hemos elegido **AES**), tendremos que elegir el algoritmo de hashing. Por defecto es **SHA512**, uno de los más seguros actualmente, así que elegimos este.

🐱 Asistent	te de creación de Vo	lumen VeraCrypt			- 0	×
		Algo Algo AE Sea Tw Cal	ciones de cif ritmo de Cifrado S S rpent ofish mellia zwechik	frado	Probar licado en 1998) qu cias gubernament ida hasta el nivel d , 14 rondas	ie ales Alto
	Vera	AE AE Sei Sei Crypt	S(Twofish) S(Twofish(Serpent)) rpent(AES) rpent(Twofish(AES)) ofish(Serpent) mellia(Kuznyechik) znyechik(Twofish) mellia(Serpent) znyechik(AES) znyechik(Serpent(Ca	mellia))	Comparación algoritmos hash	
		[	Ayuda	< Atrás	Siguiente > Ca	ncelar
✓ Asiste	VeraCrypt - Compara Benchmark: Algori Orden: Veloc Algoritmo	ación de algoritmos itmo de Cífrado 🛛 🗸 idad Media (Descendie Cifrado	de cifrado Buffer: endo) v Descifrado	50 MB Media	<ul> <li>Comparación</li> <li>Cerrar</li> </ul>	×
					La veloci ( <sup>1</sup> ad se ve afectada por la carga de la CPU y las características del dispositivo de almacenamiento. Éstas pruebas tienen lugar en RAM.	lto
						-

Asiste	Benchmark: Algoritmo de (	Cifrado 🗸	]	Buffer: 50 MB	~	
	Orden: Velocidad Med	lia (Descendi	endo)	~		
1	Algoritmo	Cifrado	Descifrado	Media	Comparación	
	AES	2.3 GB/s	2.4 GB/s	2.3 GB/s		a
anna anna	Camellia	635 MB/s	640 MB/s	637 MB/s	Cerrar	les
	Twofish	453 MB/s	443 MB/s	448 MB/s		lto
	Serpent	435 MB/s	438 MB/s	436 MB/s	La valocidad co vo	
	AES(Twofish)	378 MB/s	379 MB/s	378 MB/s	afectada por la	
	Serpent(AES)	375 MB/s	372 MB/s	374 MB/s	carga de la CPU y	
	Kuznyechik	368 MB/s	315 MB/s	341 MB/s	las características	1
	Kuznyechik(AES)	321 MB/s	2/6 MB/s	299 MB/s	del dispositivo de	
	Camellia(Serpent)	259 MB/s	262 MB/s	201 MB/s	almacenamiento.	-
	Camelila(Kuznyechik)	233 MD/S	211 MD/S	222 MD/S	Éstas pruebas	
	Corport(Twofish(AEC))	221 MD/S	222 MD/S	222 MD/S	tienen lugar en	
	AES(Twofish(Serpent))	202 MD/S	204 MB/s	203 MD/S	RAM.	
	AES(Twonsh(Serpent))	203 MB/s	200 MD/S	201 MB/s		-
	Kuznyechik (Serpent (Camellia	1) 154 MB/c	141 MB/c	147 MB/c		
	Ruzhyechik(Serpent(Camenia	)) 134 110/5	141 110/5	147 110/5		
						celar
	Paralalización 4 bilos		AEC	colorado por barduaros	Cí	

🐱 Asistente de creación de Volumen VeraCrypt	- 🗆 ×
Algoritmo de C	s de cifrado
AES	Y Probar
Algoritmo ap podría ser us de EEUU par Secreto. Clav (AES-256). E <u>Más informac</u>	robado por FIPS (Rijndael, publicado en 1998) que sado por departamentos y agencias gubernamentales a proteger información clasificada hasta el nivel Alto ve de 256-bit, bloque de 128-bit, 14 rondas I modo de operación es XTS.
Algoritmo Has	h
VeraCrypt	v Información de algoritmos hash
Whirlpool	
SHA-256	
Streebog	
Ayuda	a < Atrás Siguiente > Cancelar

Ahora tendremos que configurar el tamaño del volumen cifrado VeraCrypt que estamos creando, y definir una contraseña (autenticación con algo que sabemos) o bien crear una clave criptográfica (autenticación con algo que tenemos). Nosotros hemos elegido la

primera opción, una contraseña, y si la clave no es muy larga nos avisará que es recomendable que sea más compleja debido a que podrían atacar el contenedor por fuerza bruta o diccionario.

100	ОКВ	● MB	⊖gb	Отв
El espacio libre Especifique el tamañ Si crea un contenedo especificará su máxin Tenga en cuenta que es 292 KB. De un vol	en la unidad o del contenedo or dinámico (arc mo tamaño posi e el mínimo tam lumen NTFS, el	C:\ es 6 or que de hivo disp ble. año posib mínimo e	sea crear. erso), este p ble de un vo s 3792 KB.	parámetro Iumen FAT
			♦_	
Aunda	< Atric	Sigu	iente >	Cancelar
	100 El espacio libre d Especifique el tamañ Si crea un contenedo especificará su máxin Tenga en cuenta que es 292 KB. De un vol	100 OKB El espacio libre en la unidad Especifique el tamaño del contenedo Si crea un contenedor dinámico (arc especificará su máximo tamaño posi Tenga en cuenta que el mínimo tam es 292 KB. De un volumen NTFS, el	100 OKB OMB El espacio libre en la unidad C:\ es 6 Especifique el tamaño del contenedor que des Si crea un contenedor dinámico (archivo dispuespecificará su máximo tamaño posible. Tenga en cuenta que el mínimo tamaño posible es 292 KB. De un volumen NTFS, el mínimo es	100       KB       MB       GB         El espacio libre en la unidad C:\ es 68.13 GB         Especifique el tamaño del contenedor que desea crear.         Si crea un contenedor dinámico (archivo disperso), este pespecificará su máximo tamaño posible.         Tenga en cuenta que el mínimo tamaño posible de un voles 292 KB. De un volumen NTFS, el mínimo es 3792 KB.



active Archives have			×
Archivo-llave			Aceptar Cancelar PRECAUCIÓN: isi pierde un archivo-llave o si cambian sus primero 1024 KB, será imposible montar los volúmenes que usan ese archivo-llave!
Añadir Archivos Añadir Ruta	Archivos Token	Eliminar	Eliminar todo
Usar archivo-llave <u>Más in</u> Asistente de creación de Volumen V	nformación /eraCrypt	Generar Arc	hivo-llave Aleatorio
Usar archivo-llave <u>Más in</u> Asistente de creación de Volumen V	nformación /eraCrypt Contraseña del V	Generar Arcl	hivo-Ilave Aleatorio

Cuando hayamos configurado la contraseña, deberemos elegir el sistema de archivos del contenedor cifrado. Si no vamos a introducir archivos mayores de 4GB, podremos seleccionar FAT, de lo contrario, podremos elegir exFAT o NTFS. Es muy importante

«mover el ratón» para crear la suficiente aleatoriedad en las claves, una vez que la barra esté en verde, pinchamos en «Formatear» para iniciar el proceso.

Cuando el proceso termine, pinchamos en «Salir», o en «Siguiente» si queremos crear otro volumen.

🐱 Asistente de creación de Volumen VeraC	Crypt		-	X
	Formato de Opciones Sistema de FAT	el volumen Cluster Po	r defec 🗸 🔲 [	Dinámico
	Pool Aleatorio: Clave Cabecera: Clave Maestra:	++*,-,**,- *************************	-/-*+-*,./*, *********************************	**+,.*/ □ ********
	Hecho	Velocidad	Ouedan	ADOITAF
VeraCrypt	IMPORTANTE: Mu ventana. Cuanto r significativamente Luego haga clic e Aletoriedad Obte	ieva el ratón al azar nás lo mueva, mejor la fuerza criptográfi n 'Formatear' para ci nida De Movimientos	todo lo posible de . Esto incrementa ca de las claves d rear el volumen. de Ratón	ntro de esta e cifrado.
			-	
	Ayuda	< Atrás	Formatear	Cancelar
↘ Asistente de creación de Volumen VeraC	rypt		_	□ X
	Formato de Opciones Sistema de FAT NTF FAT Pool Aleato exF/ Clave Cabec(Ning Clave Maestra:	cluster Po	r defec ~ [] [	Dinámico + . + / * * * * * * *
				Abortar
	Hecho	Velocidad	Quedan	
VeraCrypt	IMPORTANTE: Mu ventana. Cuanto r significativamente Luego haga clic e	eva el ratón al azar nás lo mueva, mejor la fuerza criptográfi n 'Formatear' para cr	todo lo posible de . Esto incrementa ca de las claves d rear el volumen.	ntro de esta e cifrado.
	Aletoriedad Obte	nida De Movimientos	de Ratón	
	Ayuda	< Atrás	Formatear	Cancelar

🗴 Asistente de creación de Volumen Vera	Crypt	- 🗆 X
	Opciones Sistema de FAT Cluster Por defec	✓ Dinámico
Asistente de creac	nión de Volumen VeraCrypt ×	Abortar Quedan 0 s sible dentro de esta ementa claves de cifrado. umen.
	Aletoriedad Obtenida De Movimientos de Rate Ayuda < Atrás Forr	ón matear Cancelar
🐱 Asistente de creación de Volumen Vera	Crypt	– 🗆 X
	Volumen creado El volumen VeraCrypt ha sido creado y está lis crear otro volumen VeraCrypt haga clic en Sig en Salir.	sto para usarse. Si desea guiente. Si no, haga clic
	Avuda - Atrás Sigui	ianta > Salir

Ahora que ya hemos creado el volumen cifrado «normal», vamos a «montarlo» para poder acceder a él y empezar a cifrar nuestros archivos.

#### 3. Montaje del volumen cifrado «normal» creado anteriormente

Para montar un volumen cifrado, debemos tener en cuenta que hemos debido de crearlo anteriormente. Simplemente debemos pinchar sobre «Seleccionar archivo», buscamos el volumen cifrado, elegimos una ruta en nuestro Windows para su montaje y pinchamos en «MONTAR».

🧏 VeraCrypt			_	□ ×
Volúmenes Sistema Favoritos	Herramientas Cor	nfiguración Ayuda		Página Web
Unid Volumen A: B: E: F: G: H: J: X: L: M: N: O:	T	Famaño Algoritmo de cifrado	Тіро	~
Crear Volumen	Propiedad	es del Volumen	Borrar	Caché
VeraCrypt	nca historial	✓ Herramientas de volumen	Selecciona Seleccionar	r Archivo Dispositivo
Montar	Montar Autom.	Desmontar Todo		Salir





¥ Vera	Crypt	invoritor Horromiontos Co	opfiguración Avuda	— 🗌	X
Unid A: B: F: G: H: I: J: K: L: M: N:	Volumen		Tamaño Algoritmo de cifrado	Тіро	
Volume	Crear Volumen en C:\User	Propieda rs\Br_n\VeraCrypt_RedesZone	ides del Volumen	Borrar Caché Seleccionar Archiv	0
VeraC	ypt 🔽 No g	ardar nunca historial	Herramientas de volumen	Seleccionar Disposit	ivo
	Montar	Montar Autom.	Desmontar Todo	Salir	

Cuando pinchemos en «Montar», nos va a pedir la contraseña de acceso o la clave criptográfica para abrirlo. Automáticamente VeraCrypt se encargará de abrir el contendor cifrado, montarlo en la unidad elegida, y hacerlo accesible.

Torunner	nes Sistema Favoritos Herramient	tas Configuración Ayuda	Página	Web
Unid A: B: E:	Volumen	Tamaño Algoritmo de cifrado	Тіро	^
=G:	troduzca contraseña para C:\Users\	Bron\VeraCrypt_RedesZone		1
-I:	trodazea contrasena para ettosenst	bron (verderypt_hedes2one		_
=J: =K:	Contraseña:		Aceptar	
⇒L: ⇒M	PKCS-5 PRF: Autodetección	Modo TrueCrypt	Cancelar	
=N:	Usar PIM			
	Guardar contras	eñas y archivos en caché		*
	Mostrar contrase	eña		
	Usar archivo-llav	Archivos-Ilave	Opciones Montaje	
Volum	en			-
	C:\Users\Bron\VeraCrypt_Rede	esZone v	Seleccionar Archivo	
	Teans .	Herramientas de volumen	Seleccionar Dispositive	0
VeraC	No guardar nunca historial			_

A: B:	Volumen		Tamaño Algoritmo de cifrado	Тіро	
E: F:				1	
H Intr	oduzca contras	eña para C:\Users\Bro	n\VeraCrypt_RedesZone	+	
л: К:	Contraseña:	•••••		Aceptar	
L: M	PKCS-5 PRF:	Autodetección	Modo TrueCrypt	Cancelar	
N:					
		Guardar contraseña	s v archivos en caché		h
		Guardar contraseña	s y archivos en caché		
		Guardar contraseña Mostrar contraseña Usar archivo-llave	s y archivos en caché Archivos-llave	Opciones Montaje	
olumer	1	Guardar contraseña Mostrar contraseña Usar archivo-llave	s y archivos en caché Archivos-llave	Opciones Montaje	
blumer	C:\Users\I	Guardar contraseña Mostrar contraseña Usar archivo-llave Bron\VeraCrypt_RedesZo	s y archivos en caché Archivos-llave	Opciones Montaje Seleccionar Archivo	
olumer VeraCryp	C:\Users\I	Guardar contraseña Mostrar contraseña Usar archivo-llave Bron\VeraCrypt_RedesZo	s y archivos en caché Archivos-llave one ~ Herramientas de volumen	Opciones Montaje Seleccionar Archivo Seleccionar Dispositiv	/0

🐱 VeraCŋ	ypt		_		×
Volúmene	s Sistema Favoritos Herramientas	Configuración Ayuda		Página	Web
Unid V A: B: E: F:	/olumen	Tamaño Algoritmo de cifrado	Tipo		^
G: H: J: K: L: M: N: G:	VeraCrypt Por Este proceso puede llevar mucho tie	r favor, espere mpo y VeraCrypt puede parece que	e no respond	de.	
Volumen			Dong	r-cocrié	
VeraCrypt	C:\Users\Bron\VeraCrypt_RedesZon	Herramientas de volumen	Seleccion	nar Archivo ar Dispositiv	/0
	Montar Montar Autom.	Desmontar Todo		Salir	

nid Vo A:	lumen		Tamaño Algoritmo de cifr	ado Tipo	agina we
в. E: C:\ T.	\Users\Bron\VeraCrypt_F	RedesZone	99 MB AES	Normal	
G: H:					
I: ]:					
К:					
L:					
M-					
M: N:					
M: N: O:					
M: N: O:					
M: N: O: Cre	ear Volumen	Propied	ades del Volumen	Borrar Cad	:hé
M: N: O: Cre	ear Volumen	Propied	ades del Volumen	Borrar Cad	ché
M: N: O: Cre olumen	ear Volumen C:\Users\Bron\Vera	Propied Crypt_RedesZone	ades del Volumen	Borrar Cac	ché rchivo
M: N: O: Cre olumen	ear Volumen C:\Users\Bron\Vera ☑ No guardar nunc	Propied Crypt_RedesZone a historial	ades del Volumen e Herramientas de volum	Borrar Cad Seleccionar A en Seleccionar Dis	ché archivo apositivo

En «Equipo» nos aparecerá un nuevo disco local E, que es el volumen cifrado. Todo lo que copiemos en este «Disco local E» estará cifrado con AES, el cifrado y descifrado se realiza en tiempo real y «al vuelo».

✓ Carpetas (7)				
Descargas		5	Escritorio	Imágenes
Música	Objetos 3D		Vídeos	
imes Dispositivos y unidades (3) $-$				
Disco loca 68,0 GB d	I (C:) Isponibles de	D:)	Disco local (E:) 98,9 MB disponibles de	
✓ Ubicaciones de red (1)				
		-		
		20		

Si queremos desmontar la unidad, simplemente pinchamos en «**Desmontar todo**«, o con click derecho sobre la unidad y pinchar en «Desmontar».

🐱 VeraCrypt	-	
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda		Página Web
Unid Volumen Tamaño Algoritmo de cifrado	Тіро	^
⇒F:		
G:		
<b>]</b> :		
-K:		
aL: aM·		
<b>■</b> 0:		~
Crear Volumen Propiedades del Volumen	Borrar	Caché
Volumen		
C:\Users\Bron\VeraCrypt_RedesZone	Selecciona	r Archivo
VeraCrypt No guardar nunca historial Herramientas de volumen	Seleccionar	Dispositivo
		]
Montar Montar Autom. Desmontar Todo	3	Salir

Una vez que ya sabemos cómo crear y montar un volumen cifrado VeraCrypt normal, vamos a explicar el volumen cifrado oculto.

#### 4. Creación de un volumen cifrado «oculto»

En esta sección vamos a crear un volumen cifrado, dónde meteremos nuestros datos, pero dentro de él crearemos uno OCULTO, os explico en qué consiste esto.

- Volumen normal: para acceder tendrás que meter la contraseña, por ejemplo 112233, entonces en Windows se montará un nuevo disco local, tal y como habéis visto anteriormente.
- Volumen oculto: para acceder tendrás que meter otra clave que hayas puesto anteriormente, por ejemplo 11223344 y se montará SÓLO el volumen oculto

¿Para qué sirve el volumen cifrado oculto? Para guardar los archivos más importantes en su interior, como claves de bancos, emails, documentos confidenciales etc. ¿Por qué no guardar esto en el volumen normal si está cifrado? Para evitar que alguien amenace nuestra integridad física (nos haga daño), nos chantajee o extorsione, ya que, de esta forma, podremos darle la clave del volumen cifrado «normal», pero no la del volumen oculto, y ellos no pueden saber de ninguna manera si hay un volumen oculto o no. Un detalle muy importante que debemos tener en cuenta es lo siguiente: imaginemos que el volumen normal es de 50Mb, y el oculto de 25Mb, si tú llenas 26Mb de datos o más en el volumen normal, estás sobrescribiendo los datos del volumen oculto (ya sean archivos o espacio en blanco si no lo has llenado por completo), así que cuidado, dejad margen.

El proceso de creación del volumen cifrado oculto es muy similar al «normal». En el menú principal de VeraCrypt procedemos a pinchar sobre «**Crear Volumen**«, para posteriormente seleccionar la opción «**Crear un contenedor de archivos cifrado**«. Una vez hecho esto, deberemos elegir «**Volumen VeraCrypt oculto**«, y si estás creando un volumen nuevo, pinchamos en «Modo normal» para que todo funcione más rápido.

🐱 Vera	Crypt			_		$\times$
Volúme	nes Sistema Favorito	os Herramientas Co	onfiguración Ayuda		Página	Web
Unid A: B: E:	Volumen		Tamaño Algoritmo de cifrado	Tipo		^
F: G: H: J: J: K: L: M: N: O:						>
Volum	Crear Volumen	Propieda	ades del Volumen	Borrar	Caché	Ľ
	c		~	Seleccion	ar Archivo	
Vera	No guardar	nunca historial	Herramientas de volumen	Selecciona	Dispositiv	0
	Montar	Montar Autom	Desmontar Todo		Calir	

Massistente de creación de Volumen VeraCrypt





Х



Para crear un contenedor, deberemos seleccionar una ruta y un nombre de archivo, pinchamos en «**Seleccionar archivo**» para ubicar el archivo que nosotros queramos donde nosotros queramos. Una vez elegido, vamos a «configurar» el volumen externo, es decir, el volumen «normal», seleccionando el cifrado simétrico, hash y también el tamaño.





Ayuda

< Atrás

Siguiente >

Cancelar

Seistente de creación de Volumen Vera	Crypt Tamaño del v	volumen e	_ xterno	
	200 El espacio libre e	) ⊖KB (€ n la unidad C	MB GB	⊖тв
VeraCrypt	Especifique el tamaño volumen externo y lue mínimo tamaño posibl crear un volumen ocu	del volumen ext go un volumen o e para un volum lto es 340 KB.	terno (primero crea oculto en su interio en en el que se pr	ará un xr). El retenda
	Ayuda	< Atrás	Siguiente >	Cancelar

Pondremos una contraseña o una clave criptográfica como antes os hemos explicado, también elegimos el sistema de archivos, y pinchamos en «Formatear».

	Contraseña:	a del Volumo 112233 112233	en Externo	
VeraCrypt	Elija una contrase que ud. podrá rev IMPORTANTE: La que elegirá para o Nota: La longitud	Usar archivo-llave Mostrar contraseñ Usar PIM ña para el volumen o velar a un enemigo s contraseña debe ser el volumen oculto. máxima posible de la	a externo. Esta será i es obligado a hac sustancialmente d a contraseña es 64	nivos-llave la contraseña erlo. liferente de la caracteres.
	Ayuda	< Atrás	Siguiente >	Cancelar





Una vez que hayamos creado el volumen externo, procedemos a crear el volumen oculto, y es que el asistente de configuración es exactamente igual que para el volumen externo, tendremos que configurar el cifrado, hash y también el tamaño (aunque en este caso tenemos un límite que depende del volumen normal creado anteriormente). VeraCrypt nos permite crear un volumen externo e interno con diferente cifrado y hash, no hay problema porque el volumen externo esté con AES, y el interno esté con una combinación de AES con otros algoritmos de cifrado simétrico.



Ayuda

< Atrás

Siguiente >

VeraCrypt

Cancelar



	Tamaño del v	olumen o	oculto	
	100 El tamaño máxim este volumen es	OKB ( o posible de 197.16 MB.	●MB ◯GB volumen oculto	⊖тв рага
VeraCrypt	Especifique el tamaño posible de un volume como NTFS). El máxin el volumen oculto se r	o del volumen oc n oculto es 40 KE no tamaño posib nuestra más arri	ulto. El mínimo tam 3 (o 3664 KB si se f le que puede espec ba.	naño ormatea cificar para
	Ayuda	< Atrás	Siguiente >	Cancelar

Sistente de creación de Volumen Vera	Crypt		· 🗆 🗙
	Contraseña de Contraseña: 11223 Confirmar: 11223 Usa Mos Usa	l Volumen Ocult 344 344 r archivo-llave trar contraseña r PIM	O Archivos-Ilave
VeraCrypt	Elija una contraseña par elija una buena contrase sólo una palabra que se combinación de 2, 3, o 4 nombres ni fechas de na buena contraseña es un minúsculas, números, y Recomendamos la elecc 20 caracteres (cuanto m 64 caracteres.	a el volumen oculto. Es muy aña. Debería evitar elegir una pueda encontrar en un dico i de estas palabras). No debe acimiento. No debería ser fác a combinación aleatoria de la caracteres especiales como ( ión de una contraseña que c iás larga, mejor). La máxima < Atrás Siguiente >	importante que a que contenga ionario (o una ería contener cil de adivinar. Una etras mayúsculas y @ ^ = \$ * + etc. onsista en más de longitud posible es
	, , , ucu	organization of galance of	
Se Asistente de creación de Volumen Vera	iCrypt	-	· 🗆 🗙
i in the second second	Contraseña de	I Volumen Ocult 344	0
Asistente de creación de	e Volumen VeraCrypt	>	hivos-llave
AVISO: ¡Las c técnicas de f Recomendan caracteres. ¿Seguro que	ontraseñas cortas son fáci uerza bruta! nos la elección de una cor desea utilizar una contras	iles de romper usando ntraseña de más de 20 eña corta?	portante que le contenga ario (o una contener e adivinar. Una s mayúsculas y = \$ * + etc. ista en más de gitud posible es
	2	ií No	
	Ayuda	< Atrás Siguiente >	Cancelar

Assence de creación de volumen vera	Formato d Opciones Sistema de FA	el volumen o r v Cluster Po	r defec 🗸 📿 Fo	ormato Rápido
	Pool Aleatorio: Clave Cabecera: Clave Maestra:	+/-+-,*+.+,/+* **********************************	**************	, -++  ****** ******
	Hecho	Velocidad	Quedan	
VeraCrypt	IMPORTANTE: M ventana. Cuanto significativament Luego haga clico	ueva el ratón al azar t más lo mueva, mejor. e la fuerza criptográfi en 'Formatear' para cr	codo lo posible den Esto incrementa ca de las claves de ear el volumen.	tro de esta e cifrado.
	Aletoriedad Obt	enida De Movimientos	de Ratón	
	Ayuda	< Atrás	Formatear	Cancelar

Al finalizar la configuración del volumen oculto, nos va a informar que debemos tener mucho cuidado con sobrescribir los datos, tal y como os hemos explicado anteriormente. Una vez que hayamos creado el volumen oculto, pinchamos en «Finalizar».

Se Asistente de cre	ente de creación de Volumen VeraCrypt	×
	El volumen oculto VeraCrypt ha sido creado con éxito y está listo para ser usado. Si todas las instrucciones han sido seguidas y las precauciones y requisitos listados en la sección "Precauciones y Requisitos de Seguridad Concernientes a los Volúmenes Ocultos" de la Guía del Usuario de VeraCrypt han sido seguidos, debería ser imposible demostrar que el volumen oculto existe, incluso si el volumen externo está montado.	ato Rápido -+* **** ****
	AVISO: SI NO PROTEGE EL VOLUMEN OCULTO (PARA INFORMARSE SOBRE CÓMO HACERLO, VAYA A LA SECCIÓN "PROTECCIÓN DE VOLÚMENES OCULTOS CONTRA DAÑOS" EN LA GUÍA DEL USUARIO DE VERACRYPT), NO MODIFIQUE EL VOLUMEN EXTERNO. DE LO CONTRARIO, ¡PODRÍA SOBRESCRIBIR Y DAÑAR EL VOLUMEN OCULTO!	de esta rado.
	Aceptar	Cancelar



Ahora vamos a montar este volumen cifrado oculto, y vais a ver cómo diferenciarlos.

#### 5. Montaje del volumen cifrado «oculto» creado anteriormente

El montaje del volumen oculto se realiza como antes, seleccionamos el volumen cifrado, seleccionamos una unidad para su montaje e introducimos la contraseña.

- 1. Si introducimos la contraseña del volumen «normal», se montará ese volumen.
- 2. Si introducimos la contraseña del volumen «oculto», se montará el volumen oculto.



		Tamaño Algoritmo de cifrado	Тіро
:			
:			
Introduzca contra	aseña para C:\Users\Bro	n\VeraCrypt_RedesZone_OCUL	TO
Contraseña	a:		Aceptar
PKCS-5 PRI	: Autodetección	V Modo TrueCrypt	Cancelar
1:	_		
	Usar PIM		
	Guardar contraseña	s y archivos en caché	
	Mostrar contrasena	Analytican Harra	Oncience Mentric
	Usar archivo-llave	Archivos-Ilave	Opciones Montaje
lu			Coloccionar Archivo
C:\Users	Bron\VeraCrypt_RedesZor	ne_OCULTO ~	Seleccional Archivo

veracryp	t		_	×
<u>V</u> olúmenes	<u>Sistema</u> Favor <u>i</u> tos <u>H</u> erramie	entas Configuración Ayuda	Pá	gina <u>W</u> eb
Unid Vol	umen	Tamaño Algoritmo de cifrado	Tipo	^
= <mark>E: C:\</mark>	U\VeraCrypt_RedesZone_OCUL	TO 199 MB AES	Normal	
⇒F: ⇒G:				
H:			T	
=];			/	
=K:			/	
eL:			*	
=N:				
=0:				¥
Crea	ar Volumen	Propiedades del <u>V</u> olumen	Borrar Cac	hé
Volumen				
	Cullingers Bron Wars Count Ba			
XC	C:\Users\bron\veraCrypt_Re	edesZone_OCULTO ~	Seleccionar Ar	chivo
VeraCrypt	✓ No guardar nunca historia	edesZone_OCULTO ~	Seleccionar A	oositivo
VeraCrypt	No guardar nunca historia Montar Montar A	utom.	Seleccionar Ar Seleccionar Disp Salin	oositivo

VeraCrypt				-	
lúmenes	Sistema Favoritos Her	ramientas Co	onfiguración Ayuda		Página Wel
Unid Volu A:	umen		Tamaño Algoritmo de cifrado	Tipo	
E: C:\l	J\VeraCrypt_RedesZone	_OCULTO	99 MB AES	Oculto	
=G: =H: =I: =J:				1	
K: L: M: N: O:					
EK: L: N: O: <u>C</u> rea	ar Volumen	Propieda	ades del <u>V</u> olumen	Borrar	Caché
=K: =L: =M: =N: =O: 	ar Volumen	Propieda	ades del <u>V</u> olumen	Borrar	Caché
=K: =L: =M: =N: =O: 	ar Volumen C:\Users\Bron\VeraCr	Propieda ypt_RedesZone	ades del <u>V</u> olumen	Borrar	Caché ar A <u>r</u> chivo
K: L: N: O: Crea Volumen	ar Volumen C:\Users\Bron\VeraCn ☑ No guardar nunca h	Propieda ypt_RedesZone	ades del <u>V</u> olumen	<u>Borrar</u> Selecciona Seleccionar	Caché ar A <u>r</u> chivo r Dispositivo

Una vez que ya sabemos cómo crear volúmenes cifrados ocultos y cómo montarlos en una unidad, vamos a ver cómo podemos cifrar una unidad de almacenamiento extraíble entera.

## 6. Cifrado de un dispositivo de almacenamiento extraíble (USB, tarjeta SD, disco duro externo)

Lo primero que tenemos que hacer es introducir el dispositivo de almacenamiento extraíble en nuestro ordenador. Una vez introducido, pinchamos en «**Crear Volumen**«, y seleccionamos «**Cifrar partición/unidad secundaria**» ya que vamos a cifrar una partición que no tiene el sistema operativo. Una vez seleccionada esta opción, elegimos entre «**Volumen VeraCrypt común**» o «**Volumen VeraCrypt oculto**«, nosotros hemos seleccionado la primera opción para simplificar, pero podéis seleccionar la segunda opción con las mismas características que justo antes os hemos explicado.

úmonos Sistema Favor	ritos Horramiontas Configuración Avuda	Dágina W
umenes sistema ravo		ragina w
Jnid Volumen #A: #B:	Tamaño Algoritmo de cifrado	Тіро
iG:		
H:		
1: 1):		
к:		
M:		
N:		
O:		
<u>Crear</u> Volumen	Propiedades del Volumen	Borrar Caché
olumen	-	
	~	Seleccionar Archivo
		Seleccional Alchivo
No avord		
Mo guard.	ar nunca historial Herramientas de volumen	Seleccionar Dispositivo
⊻] No guard	ar nunca historial Herramiențas de volumen	Seleccionar Dispositivo
Montar	Ar nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo	Seleccionar Dispositivo Salir
Montar	Ar nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo	Seleccionar Dispositivo
Montar	Ar nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo	Seleccionar Dispositivo
Montar Asistente de creación de	Ar nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt	Seleccionar Dispositivo Salir
Montar Asistente de creación de	Anistorial     Herramiențas de volumen       Montar Autom.     Desmontar Todo	Seleccionar Dispositivo
Montar Asistente de creación de	Ar nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt Asistente de Creación de	Seleccionar Dispositivo Salir – – Volúmenes
Montar Asistente de creación de	Ar nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt Asistente de Creación de O Crear un contenedor de archivos cifr	Seleccionar Dispositivo Salir – – Volúmenes rado
Montar Asistente de creación de	An nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt Asistente de Creación de O Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de	Seleccionar Dispositivo Salir – – Volúmenes rado e un archivo. Recomendado
Montar	ar nunca historial       Herramiențas de volumen         Montar Autom.       Desmontar Todo         Volumen VeraCrypt       Asistente de Creación de Crea un disco cifrado virtual dentro de para usuarios sin experiencia.	Seleccionar Dispositivo Salir – – Volúmenes rado e un archivo. Recomendado
Montar Asistente de creación de	An nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt Asistente de Creación de O Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia. Más información	Seleccionar Dispositivo Salir – – Volúmenes rado e un archivo. Recomendado
Montar Asistente de creación de	An nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt Asistente de Creación de O Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia. Más información O Cifrar partición/unidad secundaria Cifra una partición en cualquier unidad	Seleccionar Dispositivo Salir Salir Volúmenes ado e un archivo. Recomendado
Montar Asistente de creación de	An nunca historial Herramiențas de volumen Montar Autom. Desmontar Todo Volumen VeraCrypt Asistente de Creación de O Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia. Más información O Cifrar partición/unidad secundaria Cifra una partición en cualquier unidad unidad flash). Opcionalmente, crea un	Seleccionar Dispositivo Salir – – Volúmenes rado e un archivo. Recomendado
Montar Asistente de creación de	Montar Autom.  Montar Autom.  Desmontar Todo  Volumen VeraCrypt  Asistente de Creación de  Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia.  Más información  Cifrar partición/unidad secundaria Cifra una partición en cualquier unidad unidad flash). Opcionalmente, crea un Cifrar la partición/unidad del sistem	Seleccionar Dispositivo Salir Salir Volúmenes rado e un archivo. Recomendado d interna o externa (ej: volumen oculto.
Montar Asistente de creación de	Montar Autom.  Montar Autom.  Desmontar Todo  Volumen VeraCrypt  Asistente de Creación de  Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia.  Más información  Cifrar partición/unidad secundaria Cifra una partición en cualquier unidad unidad flash). Opcionalmente, crea un Cifra la partición/unidad del sistem Cifra la partición/unidad donde Windo	Seleccionar Dispositivo Salir Salir Volúmenes ado e un archivo. Recomendado d interna o externa (ej: volumen oculto.
Montar Asistente de creación de	Montar Autom.  Montar Autom.  Desmontar Todo  Volumen VeraCrypt  Asistente de Creación de  Crear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia.  Más información  Cifrar partición/unidad secundaria Cifra una partición en cualquier unidad unidad flash). Opcionalmente, crea un  Cifra la partición/unidad donde Windo Cualquiera que quiera acceder al siste archivos, etc. tendrá que introducir la	Seleccionar Dispositivo Salir Salir Volúmenes rado e un archivo. Recomendado d interna o externa (ej: volumen oculto. a entera ws está instalado. ma, leer y escribir contraseña antes de
Montar Asistente de creación de	Montar Autom.  Montar Autom.  Desmontar Todo  Volumen VeraCrypt  Asistente de Creación de  Orear un contenedor de archivos cifr Crea un disco cifrado virtual dentro de para usuarios sin experiencia.  Más información  Orifrar partición/unidad secundaria Cifra una partición en cualquier unidad unidad flash). Opcionalmente, crea un Orifrar la partición/unidad del sistem Cifra la partición/unidad donde Windo Cualquiera que quiera acceder al siste archivos, etc. tendrá que introducir la arrancar Windows. Opcionalmente, crea	Seleccionar Dispositivo Salir Salir Volúmenes rado e un archivo. Recomendado d interna o externa (ej: volumen oculto. a entera ws está instalado. ma, leer y escribir contraseña antes de ea un sistema oculto.
Montar Asistente de creación de	Montar Autom.	Seleccionar Dispositivo Salir Salir Volúmenes ado e un archivo. Recomendado d interna o externa (ej: volumen oculto. a entera ws está instalado. ma, leer y escribir contraseña antes de ea un sistema oculto.

Ayuda

< Atrás

Siguiente >

Cancelar



Ahora debemos elegir el dispositivo a cifrar, si estamos introduciendo una unidad de almacenamiento extraíble, vamos a poder seleccionar su propia partición. En nuestro caso hemos introducido un pendrive que ha sido montado en la unidad E: por el sistema operativo, con un tamaño de 3,7GB. Cuando hayamos elegido la partición del dispositivo a cifrar, pinchamos en «**Aceptar**«.



20.00						
ARCHINE)	Dispositivo	Unidad	Tamaño	Etiqueta		
Real	Disco Duro 0:		476 GB			
	\Device\Harddisk0\Part	ition1	549 MB			Dispositiv
	\Device\Harddisk0\Part	ition2 C:	119 GB			
	\Device\Harddisk0\Part	ition3	910 MB			
	(Device (Harddisku (Part	Ition4 D:	200 GD			eden ser
and the second second	Disco extraíble 1:		3.7 GB			ondo,
	\Device\Harddisk1\Part	ition1 E:	3.7 GB			ser
	_					
						tro de
						discos
						do por
						es la
						<b>)</b> .
					<b>_</b>	
				_	-	

Cuando hayamos elegido el dispositivo, tenemos dos opciones para elegir:

- Crear volumen cifrado y formatearlo: esta opción es recomendable seleccionarla siempre y cuando lo que haya en el pendrive esté vacío, o que no nos importe que se formatee el dispositivo. Esta opción es muy rápida, y formatea todo el dispositivo.
- **Cifrar partición conservando datos**: este proceso es mucho más largo, ya que se encarga de cifrar el propio contenido sin pérdida de datos.

Una vez elegido el modo de creación de volumen, deberemos **elegir las diferentes opciones de cifrado simétrico, y también hashing**. Por supuesto, en esta ocasión **no podremos elegir el tamaño del volumen** ya que el tamaño viene dado por el propio tamaño del dispositivo de almacenamiento extraíble. Sistente de creación de Volumen VeraCrypt



	Algoritmo de Cifrado	)
	AES	Y Probar
	Algoritmo aprobado por FIPS ( podría ser usado por departam de EEUU para proteger informa Secreto. Clave de 256-bit, bloq (AES-256). El modo de operacio <u>Más información en AES</u> Algoritmo Hash	Rijndael, publicado en 1998) que ientos y agencias gubernamentales ación clasificada hasta el nivel Alto ue de 128-bit, 14 rondas ón es XTS. Comparación
	5HA 512	forma sida da alas situa a bash
<b>Vera</b> Crypt	SUM-212 V IU	

X



De cara a la autenticación para acceder a los datos, podremos introducir la típica contraseña de paso, o también elegir una clave criptográfica para acceder al propio dispositivo cifrado. Si seleccionamos una contraseña que sea muy corta, nos avisará que no es recomendable de cara a la seguridad.

Una vez elegida la autenticación, procedemos a «mover» el ratón para aumentar la aleatoriedad del volumen y pinchamos en «Formatear». Por último, nos avisará que todos los datos almacenados se perderán.

🗴 Asistente de creación de 1	Volumen VeraCrypt –	- 🗆 🗙
Ve	Contraseña del Volumen Contraseña: 112233 Confirmar: 112233 Usar archivo-llave Mostrar contraseña Usar PIM Es muy importante que elija una buena contraseña. Usar PIM Es muy importante que elija una buena contraseña. elegir una que contenga sólo una palabra que se pu un diccionario (o una combinación de 2, 3, o 4 de el debería contener nombres ni fechas de nacimiento. de adivinar. Una buena contraseña es una combina letras mayúsculas y minúsculas, números, y caracte @ ^ = \$ * + etc. Recomendamos la elección de un consista en más de 20 caracteres (cuanto más larga máxima longitud posible es 64 caracteres.	Archivos-llave Debería evitar ueda encontrar en estas palabras). No No debería ser fácil ción aleatoria de eres especiales como a contraseña que a, mejor). La
▲ Asistente de creación de <sup>1</sup>	Ayuda < Atrás Siguiente Volumen VeraCrypt -	> Cancelar
	Contraseña del Volumen Contraseña: 112233	

Sí

< Atrás

Ayuda

No

Siguiente >

Cancelar

🐱 Asistente de creación de Volumen Vera	Crypt		-	×
- Minimize	Formato d	el volumen		
ADDANSS.	Opciones			
	Sistema de FA	T ∨ Cluster Po	r defec \vee 🗌 Fo	ermato Rápido
	Pool Aleatorio: Clave Cabecera: Clave Maestra:	-+*+,*+-/**/-* ******************************	-*,-,.*,+/-/ ***********************************	* . / , ++ 🗋
				Abortar
	Hecho	Velocidad	Quedan	
II veraciypt	Aletoriedad Obte Ayuda	enida De Movimientos < Atrás	de Ratón Formatear	Cancelar
☑ Asistente de creación de Volumen Vera	aCrypt		—	×
- Ministeries	Formato d	el volumen		
	Opciones			
	Sistema de FA	Cluster Por	r defec 🗸 📃 Fo	ormato Rápido
Asistente de creación de Ve	olumen VeraCrypt		×	*+/+
AVISO: ¡TODOS I PARTICIÓN '\Dev SE PERDERÁN (f	LOS ARCHIVOS ACT vice\Harddisk1\Part NO SERÁN CIFRADC	UALMENTE ALMACE ition1' (E:) SERÁN BC DS)!	ENADOS EN ORRADOS Y	bortar
¿Seguro que de	sea continuar con e	l formato?		o de esta
		Sí	No	frado.
	Avuda	< Atrás	Formatear	Cancelar

Cuando el proceso termine, **nos avisará que la unidad E no va a ser accesible**, ya que en esta unidad es el propio sistema operativo donde «coloca» el dispositivo de almacenamiento extraíble. Una vez que nosotros montemos este dispositivo en VeraCrypt, e introduzcamos la contraseña de acceso, sí vamos a poder acceder sin ningún tipo de problema.

Cuando el proceso termine (la duración depende sobre todo del tamaño y velocidad de la unidad USB), nos avisará que todo está correcto, y pinchamos en «Salir».

Aistente       Aistente de creación de Volumen VeraCrypt         Aistente el creación de Volumen VeraCrypt       Aistente asignada al mismo!         Aistente el creación de Volumen No puede ser montado al mismo!       Aistente asignada al mismo!         Aistente el creación de Volumen No puede ser montado e una letra de unidad E:, la cual está actualmente asignada al mismo!       Aistente asignada al mismo!         Aistente reación de Volumen Naga clic en Montar Autom," en la ventana Dispositivo, seleccione esta partición/dispositivo y puese de de la deventana, cuanto más de mundad E:, la cual está actualmente asignada al mismo!       Aistente de creación de Volumen No puede ser montado en una letra de unidad diferente, que podrá elegir de la lista de la ventana principal de VeraCrypt.       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistente asignada al mismo!       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistente asignada al mismo!       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistente asignada al mismo!       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistente asignada al mismo!       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistente asignada al mismo!       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistente asignada al mismo!       Aistente asignada al mismo!         Aistente asignada al mismo!       Aistene asignada al mismo!       Aistente asignada a	Asistente de creación de Volum	nen VeraCrypt –	
Pool Aleatorio: : / /		Opciones Sistema de FAT Cluster Por defec	Formato Rápido
Abortar Hecho 2.469% Velocidad 8.6 MB/s Queda 7 minutos MPORTANTE: Mueva el ratón al azer todo lo posible dentro de esta significativamente la fuerza criptográfica de las claves de cifrado. Luego haga clic en "formatear" para crear el volumen. Aletoriedad Obtenida De Movimientos de Ratón Ayuda < Atrás Formatear Asistente Asistente de creación de Volumen VeraCrypt Asistente de creación de Volumen VeraCrypt MPORTANTE: ¡Tenga presente que este volumen NO puede ser montado/accedido usando la letra de unidad E:, la cual está actualmente asignada al mismo! Para montar este volumen, haga clic en 'Montar Autom.' en la ventana principal de VeraCrypt (o también, en dicha ventana, clic en 'Seleccionar Dispositivo'; seleccione esta partición/dispositivo y pulse 'Seleccionar Dispositivo'; seleccione esta partición/dispositivo y pulse 'exe de unidad E: de bería usarse sólo en caso de que necesiterá eliminar el cifrado de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de la quindad E: debería usarse sólo en caso de que necesiterá eliminar el cifrado de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de la partición/unidad (p.e. si ya no necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de zequipor (o' Mi PC) y seleccione "Formatear". De otro modo, la letra de unidad E: nunca debería ser usada (a menos que		Pool Aleatorio:         //-**, -, ., *+**//           Clave Cabecera:         ************************************	,,,*-+ 🗋
Hecho       2.469%       Velocidad       8.6 MB/s       Quedan       7 minutos         MPORTANTE:       Mueva el ratón al azar todo lo posible dentro de esta significativamente la fuerza criptográfica de las claves de cífrado. Luego haga clic en "Formatear" para crear el volumen.       Altrias       Cancelar         Aguda       < Atrás			Abortar
Importante:		Hecho 2.469% Velocidad 8.6 MB/s Queda	n 7 minutos
Asistente       Asistente de creación de Volumen VeraCrypt       X         Asistente de creación de Volumen VeraCrypt       X         IMPORTANTE: ¡Tenga presente que este volumen NO puede ser montado/accedido usando la letra de unidad E:, la cual está actualmente asignada al mismo!       ato Rápido         Para montar este volumen, haga clic en 'Montar Autom.' en la ventana principal de VeraCrypt (o también, en dicha ventana, clic en 'Seleccionar Dispositivo', seleccione esta partición/dispositivo y pulse 'Montar'). El volumen será montado en una letra de unidad diferente, que podrá elegir de la lista de la ventana principal de VeraCrypt.       0 s         La letra original de unidad E: debería usarse sólo en caso de que necesitará cifrado). En ese caso, haga clic derecho en la letra de unidad E: en la lista de 'Equipo' (o 'Mi PC') y seleccione 'Formatear'. De otro modo, la letra de unidad E: nunca debería ser usada (a menos que la elimine, como se describe p.e. en la FAQ de VeraCrypt, y la asigne a otra partición/dispositivo).		Ayuda < Atrás Formatear	Cancelar
	Asistente de creació Asistente de creació IMPORTA montado actualme Para mon ventana 'Seleccio 'Montar' que pod La letra o necesite necesita unidad E De otro n menos q y la asign	ón de Volumen VeraCrypt ANTE: ¡Tenga presente que este volumen NO puede ser o/accedido usando la letra de unidad E:, la cual está ente asignada al mismo! ntar este volumen, haga clic en 'Montar Autom.' en la principal de VeraCrypt (o también, en dicha ventana, clic en onar Dispositivo', seleccione esta partición/dispositivo y pulse ). El volumen será montado en una letra de unidad diferente, lrá elegir de la lista de la ventana principal de VeraCrypt. original de unidad E: debería usarse sólo en caso de que eliminar el cifrado de la partición/unidad (p.e. si ya no rá cifrado). En ese caso, haga clic derecho en la letra de E: en la lista de 'Equipo' (o 'Mi PC') y seleccione 'Formatear'. modo, la letra de unidad E: nunca debería ser usada (a que la elimine, como se describe p.e. en la FAQ de VeraCrypt, ne a otra partición/dispositivo).	× ato Rápido ,*-+ ,**** oortar 0 s de esta rado.

			^
	Opciones Sistema de FAT	defec 🗸 🖂 F	ormato Rápido
Asistente de cread	Pool Aleatorio: //-**,-,., ción de Volumen VeraCrypt	*+**//,- × ******	,,*-+ [] ****** *****
El volu	ımen VeraCrypt ha sido creado con éxit	o. Quedan	Abortar 0 s
	Aceptar Aletoriedad Obtenida De Movimientos	ementa claves de umen. de Ratón	e cifrado.
	Ayuda < Atrás	Formatear	Cancelar
🐱 Asistente de creación de Volumen Vera	Crypt	-	×
inter a	M. how on a factor		
	volumen creado		
	VOIUMEN Creado El volumen VeraCrypt ha sido creado y crear otro volumen VeraCrypt haga clic en Salir.	está listo para us en Siguiente. Si i	arse. Si desea no, haga clic
VeraCrypt	Volumen Creado El volumen VeraCrypt ha sido creado y crear otro volumen VeraCrypt haga clic en Salir.	está listo para us en Siguiente. Si	arse. Si desea no, haga clic

Ahora ya tendremos nuestra unidad de almacenamiento perfectamente cifrada, y para usarla, deberemos «montarla» en el propio «VeraCrypt».

#### 7. Montaje del dispositivo de almacenamiento extraíble cifrado

El montaje del dispositivo de almacenamiento extraíble cifrado es realmente fácil y sencillo, ahora pinchamos en «**Seleccionar Dispositivos**«, elegimos la partición que antes hemos elegido, introducimos la contraseña de acceso y automáticamente se nos montará en otra unidad para poder acceder a los datos.

🗴 Vera	Crypt			_	×
Volúmei	nes Sistema Favorito	os Herramientas Co	nfiguración Ayuda		Página Web
Unid A: B:	Volumen		Tamaño Algoritmo de cifrado	Tipo	^
F: G: H: J: K: L: N: O: P:					~
Value	<u>C</u> rear Volumen	Propieda	des del <u>V</u> olumen	Borrar	Caché
Volum				Selecciona	r A <u>r</u> chivo
VeraC	No guardar r	nunca historial	Herramiențas de volumen	Seleccionar	Dįspositivo
	Montar	Montar Autom	Desmontar Todo		Calir

Coloccionar Dartic		Tamaño Algori	tmo de cifrado	Tipo
Seleccionar Partic	ión o Dispositivo			×
Dispositivo	Unidad Ta	maño Etiqueta		
Disco Duro 0:	4	76 GB		
\Device\Harddisk	0\Partition1 54	19 MB		
\Device\Harddisk	0\Partition2 C: 1	19 GB		
\Device\Harddisk	0\Partition3 9	LO MB		
\Device\Harddisk	0\Partition4 D: 2	00 GB		
Disco outroíble 1		7 CP		
Disco extraible 1:	1\Partition1 E:	7 GB		
incree (naradisk.		./ 00		
	7			
	<b>\</b>			
	<b>\</b>			
	•		<b>M</b>	
			Acentar	Cancelar

nia	Volumen		Tamaño Algoritmo de cifrado	Tipo	1
A: 8-					
F:					
G:					
H: [·					4
): Inti	roduzca contras	eña para \Device\Har	ddisk1\Partition1		
<:	Contracaña			Accestor	
 1:	Contrasena:			Aceptar	
V:	PKCS-5 PRF:	Autodetección	Modo TrueCrypt	Cancelar	
): I					
5.					
>: -		Usar PIM			
>:		Usar PIM Guardar contraseña	s y archivos en caché		
): 		Usar PIM Guardar contraseña Mostrar contraseña	s y archivos en caché		
): 		Usar PIM Guardar contraseña Mostrar contraseña Usar archivo-llave	s y archivos en caché Archivos-Ilave	Opciones Montaje	
):  u	Device	Usar PIM Guardar contraseña Mostrar contraseña Usar archivo-llave	s y archivos en caché Archivos-llave	Opciones Montaje	
	\Device\Ha	Usar PIM Guardar contraseña Mostrar contraseña Usar archivo-llave	s y archivos en caché Archivos-Ilave	Opciones Montaje Seleccionar Archivo	
	\Device\Ha	Usar PIM Guardar contraseña Mostrar contraseña Usar archivo-llave rddisk1\Partition1	s y archivos en caché Archivos-Ilave ✓ Herramientas de volumen	Opciones Montaje Seleccionar Archivo Seleccionar Dispositiv	0
ilu VeraCrypt	\Device\Ha ✓ No guard	Usar PIM Guardar contraseña Mostrar contraseña Usar archivo-llave rddisk1\Partition1 dar nunca historial	s y archivos en caché Archivos-Ilave ✓ Herramientas de volumen	Opciones Montaje Seleccionar Archivo Seleccionar Dispositiv	0

VeraCryp	ot			-		Х
olúmenes	Sistema Favoritos	Herramientas Co	onfiguración Ayuda		Página	Web
Unid Vo ≔A:	Jumen		Tamaño Algoritmo de cifrado	Тіро		^
B: G: H: I: J: K: L:	evice\Harddisk1\Parti	tion1	3.7 GB AES	Normal		
=M: =N: =O: =P:	ear Volumen	Propieda	ades del <u>V</u> olumen	Borrar	· Caché	Ŷ
M: N: O: P: Volumen	ear Volumen	Propieda	ades del <u>V</u> olumen	<u>B</u> orrar	Caché	Ŷ
M: N: O: P: Volumen	ear Volumen \Device\Harddisl	Propieda <1\Partition1	ades del <u>V</u> olumen	<u>B</u> orrar Selecciona	Caché ar A <u>r</u> chivo	Ŷ
M: N: O: P: Volumen	ear Volumen \Device\Harddisl	Propieda k1\Partition1 unca historial	ades del <u>V</u> olumen ~ Herramien <u>t</u> as de volumen	Borrar Selecciona Seleccionar	Caché ar A <u>r</u> chivo r D <u>i</u> spositive	~

Al montar la unidad, veremos algo como lo siguiente:

- Unidad de USB E: es el propio dispositivo hardware (pendrive)
- Disco local F: es el dispositivo cifrado que hemos «montado» con VeraCrypt.



Una vez que terminemos de leer o escribir en dicho disco cifrado, procedemos a desmontarlo pinchando en «Desmontar» sobre la unidad que nosotros queramos, o bien en «**Desmontar todo**» si es que solo tenemos uno o queremos desmontar todas las unidades que tengamos en ese instante.

🐱 VeraCrypt			X
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda		Página <sup>1</sup>	Web
	<b>T</b> .		
Unid Volumen l'amano Algoritmo de cifrado	Про		^
A:			
E: \Device\Harddisk1\Partition1 37 GB AFS	Normal		
■G:	Reimer		
H:			
I:			
<b>a</b> ]:			
<i>■</i> K:			
M:			
			•
Corres Velumen	Daman	Carala A	
<u>Crear volumen</u> Propiedades del <u>v</u> olumen	Dorrar	Lache	
Volumen			
	<u>.</u>		
	Selecciona	r Archivo	
VeraCrypt	Seleccionar	Dispositiv	
	Seleccional	Dispositive	,
Desmontar Montar Autom. Desmontar Todo		Salir	

Ahora que ya sabemos cómo crear una unidad de almacenamiento extraíble cifrada, y que sabemos cómo montarla, vamos a cifrar el sistema operativo entero.

### 8. Cifrado de todo el sistema operativo (cifrar la partición/unidad del sistema entera) en VeraCrypt

Este proceso lo debemos realizar con mucho cuidado, ya que de lo contrario podríamos perder toda la información. Es recomendable realizar una copia de seguridad completa de nuestro PC con programas como Acronis True Image o similares, y sobre todo, no olvidar la clave de acceso al sistema que pongamos en VeraCrypt.

Lo primero que debemos hacer es pinchar en «**Crear Volumen**«, y posteriormente elegir «**Cifrar la particion/unidad del sistema entera**«. Una vez dentro, tenemos dos opciones principales:

- Normal: se cifra con una clave de paso o una clave criptográfica en un volumen con el sistema operativo nuestro.
- Oculto: se cifra el sistema operativo dentro de un volumen oculto para evitar una extorsión, de esta forma, podremos poner una clave y acceder a un sistema operativo que no sea el «bueno».

Nosotros hemos elegido el modo «normal». A continuación, también nos da la opción de «**Cifrar la partición de Windows**«, o bien pinchar en «**Cifrar toda la unidad**» si queremos realizar justo esto.

🐱 Vera	Crypt					-		×
Volúmer	nes Sistema F	avoritos H	erramientas	Configura	ición Ayuda		Página	Web
Unid =A: =B: =F: =G: =H: =I: =J: =K: =L: =M: =N:	Volumen			Tamaño	Algoritmo de cifrado	Tipo		^
Volum	Crear Volumen	L	Propi	edades del	Volumen	Borrar	Caché	•
	с 🗆				~	Seleccion	ar Archiv	D
VeraC	√ No g	uardar nunc	a historial	Herra	amientas de volumen	Selecciona	r Dispositi	vo
	Montar		Montar Autom.		Desmontar Todo		Salir	



🐱 VeraCrypt			- 🗆 X
Se Asistente de creación de V	olumen VeraCrypt		- 🗆 🗙
Ver.	Área a © Cifrar la Selecci instala ejecud O Cifrar to Selecci sistem con to en la co Cualqui almaci correci ser us: Windo	Cifrar a partición de Windows ione esta opción para cifra do el sistema operativo Wi ión. oda la unidad ione esta opción si desea o a Windows en ejecución en das sus particiones, será ci que residirá el Cargador de aiera que desee acceder a enado en la unidad, debera ta cada vez que se inice el ada para cifrar una unidad ws no está instalado ni se	er la partición donde está indows que hay ahora mismo en cifrar la unidad en la que el stá instalado. La unidad entera, ifrada excepto la primera pista e Arranque VeraCrypt. un sistema o archivo á introducir la contraseña sistema. Esta opción no puede l secundaria o externa si arranca desde ella.
	Ay	vuda < Atrás	Siguiente > Cancelar
Montar	Montar Autom.	Desmontar Todo	Salir

Si nuestro equipo incorpora varios sistemas operativos con multi arranque, tendremos que elegir la opción correspondiente. De lo contrario, elegimos la opción de «**Arranque simple**» tal y como hemos hecho nosotros.

Cuando hayamos terminado de configurar el volumen para el sistema operativo, nos queda seleccionar el algoritmo de cifrado simétrico, el algoritmos de hashing y la clave de autenticación o clave criptográfica.



terescipt.	- L X
S Asistente de creación de Volur	men VeraCrypt – 🗆 🗙
	Contraseña:       •••••••         Confirmar:       •••••••         Usar archivo-llave       Archivos-llave         Mostrar contraseña       Usar PIM         Star PIM       Star explantation de 2, 3, o 4 de estas palabras). No debería contener nombres ni fechas de nacimiento. No debería ser fácil de adivinar. Una buena contraseña es una combinación aleatoria de letras mayúsculas y minúsculas, números, y caracteres especiales como (@ ^ = \$ * + etc. Recomendamos la elección de una contraseña que consista en más de 20 caracteres (cuanto más larga, mejor). La máxima longitud posible es 64 caracteres.
Montar	Ayuda < Atrás Siguiente > Cancelar
Pioritar	Pontal Autom. Desmontal Todo Salir
🐱 VeraCrypt	- T ×
Velómere Cistere Francisco	Hamminata Castinomitás Annula Dásias Mala
Sint Francisco Francisco Sector Secto	men VeraCrypt – 🗆 X
Asistente de creación de Volur	Men VeraCrypt     Contraseña   creación de Volumen VeraCrypt   WISO: ¡Las contraseñas cortas son fáciles de romper usando écnicas de fuerza bruta!   Recomendamos la elección de una contraseña de más de 20 caracteres.   Seguro que desea utilizar una contraseña corta?     Sí   No     Sí     No
Asistente de creación de Volur Asistente de creación de Volur Asistente de Asistente de Asistent	Men VeraCrypt     Contraseña   creación de Volumen VeraCrypt   AVISO: ¡Las contraseñas cortas son fáciles de romper usando écnicas de fuerza bruta!   Recomendamos la elección de una contraseña de más de 20 caracteres.   Seguro que desea utilizar una contraseña corta?     Sí   No     Sí   No     Ayuda        Ayuda

Una vez configurado por completo el volumen, se crearán las claves internas, y nos recomendará crear un disco de rescate por si ocurre algún tipo de problema, poder recuperar toda la información, aunque siempre vamos a tener que introducir la contraseña de acceso.



V Marg Count	— — V
Asistente de creación de Volumen V	VeraCrypt – 🗆 🗙
	Claves Generadas Las claves, sal y otros datos han sido generados con éxito. Si quiere generar nuevas claves, presione Volver y luego Siguiente. Si no, presione Siguiente para continuar. Clave Cabecera: ************************************
Montar Mor	Ayuda < Atrás Siguiente > Cancelar ntar Autom. Desmontar Todo Salir
VeraCrypt	
Asistente de creación de Volumen	VeraCrypt — 🗆 🗙
	<ul> <li>Disco de Rescate</li> <li>Antes de cifrar una partición, debe crear una Disco de Rescate de VeraCrypt (VeraCrypt Rescue Disk - VRD), el cual sirve los siguientes propósitos: <ul> <li>Si se daña el Cargador de VeraCrypt, llave maestra u otro dato crítico, el VRD le permite restaurarlo (no obstante, será preciso introducir la contraseña correcta).</li> <li>Si Windows se daña y no puede iniciar el sistema, el VRD le permitirá descifrar permanentemente la partición antes de que Windows inicie.</li> <li>El VRD contiene una copia de seguridad del cargador de arranque EFI y le permitirá restaurarlo si fuera preciso.</li> </ul> </li> <li>La imagen ZIP del Disco de Rescate VeraCrypt se creará en la ubicación especificada abajo.</li> </ul>
VeraCryp	t Saltar la verificación del Disco
	C:\Users\RedesZone\Documents\VeraCrypt Rescue Examinar
	Ayuda < Atrás Siguiente > Cancelar
Montar Mo	ntar Autom. Desmontar Todo Salir

S VeraCrypt		_	×
Se Asistente de creación de Volumen	VeraCrypt	_	
	Disco de Rescate d La imagen ZIP del Disco de Res este fichero: C:\Users\RedesZone\Document Ahora debería extraerlo en una formateada con el sistema de f ubicación segura para posterior IMPORTANTE: Tenga en cuenta directamente en el directorio ra letra de unidad de la memoria debe crear una carpeta E:\EFI Haga clic en Siguiente para cor	Creado scate ha sido creada y alr ts\VeraCrypt Rescue Disk. a memoria USB que haya ficheros FAT/FAT32 o mov r uso. a que el fichero zip debe aíz de la memoria USB. P USB es E:, la extracción e en la memoria USB. ntinar.	macenada en zip sido verlo a una extraerse or ejemplo, si la del fichero zip
	Ayuda < P	siguiente >	Cancelar
Montar M	ontar Autom. Desmontar Te	odo Sal	lir

También tenemos la posibilidad de seleccionar la política si borramos algún archivo dentro del propio sistema operativo, y es que nos va a permitir utilizar diferentes métodos de borrado seguro, ideal para mantener nuestra privacidad.



	✓ VeraCrypt —	ining W	×
×	Asistente de creación de Volumen VeraCrypt —		×
	Asistente de creación de Volumen VeraCrypt           AVISO: Tenga en cuenta que cuando elige p.e. el modo de borrado de 3 pasadas, el tiempo necesario para cifrar la partición/unidad será unas 4 veces mayor. Asimismo, si elige el modo de 35 pasadas, tardará unas 36 veces más (podría incluso tardar varias semanas).           Sin embargo, recuerde que el borrado NO se realizará después de que la partición/unidad esté cifrada por completo. Cuando la partición/unidad esté cifrada por completo. Cuando la ningún dato. Cualquier dato que se escriba será cifrado al vuelo en memoria primero, y sólo entonces el dato (cifrado) será escrito en el disco (por lo tanto el rendimiento NO será afectado).           ¿Seguro que desea usar el modo de borrado?	×	a. Esto que d no ede blos de nicas uno de ga en nidad sin
	Sí No		
	Ayuda < Atrás Siguiente >	Ca	ncelar
	Montar Montar Autom. Desmontar Todo Sali	r	

Una vez configurado el modo de borrado, pinchamos en «probar», pinchamos en «sí» y posteriormente en «aceptar». De manera automática VeraCrypt se encargará de cifrar todo nuestro disco duro, y nos pedirá reiniciar el sistema operativo.



🖌 Ver	raCrypt			_		Х	
¥ Asiste	VeraCrypt						×
	<ul> <li>Si los pasos anterio de que se inicie Wind ordenador. Si la pant la sección 'Controles configurada para arr su ordenador, pulse una pantalla de configura pantalla de configura primero (para obtem- contacte con el equip ordenador. La pantal 'Opciones de Repara 'Restaurar cargador su ordenador. Windo Tenga en cuenta que (nadio aundo iniciono)</li> </ul>	res no funcionan o si la p dows), introduzca el Disco talla del Disco de Rescate de Teclado' de la pantalla ancar desde discos duros F2 o Supr (en cuanto vea iguración BIOS. Si dicha p sar F2 o Supr reiteradam ación de la BIOS, configur er información sobre cóm co de soporte técnico del la del Disco de Rescate Va ción' pulsando F8 en su teo original del sistema'. Lueg ws debería iniciar con no e los pasos anteriores NO	antalla del Cargador de de Rescate VeraCrypt o VeraCrypt no aparece ( del Disco de Rescate), antes que desde unidad la pantalla de inicio de pantalla de configuración ente en cuanto se reinic e su BIOS para que arri- o hacerlo, vaya a la doci fabricante para obtener eraCrypt debería aparece colado. Desde el menú 'C o extraiga el Disco de R rmalidad (siempre que r	Arranque VeraCrypi en su unidad CD/DV o si no ve 'Opciones es posible que su Bi des CD/DVD. Si ése la BIOS), y espere h n no aparece, reinici cie el ordenador. Cue anque desde la unid umentación de su Bi asistencia). Luego r cer ahora. En dicha p Opciones de Reparad tescate de su unidad no esté cifrado).	t no apareco D y reinicie de Reparao IOS esté es el caso, r nasta que ag ie el ordena ando aparez lad de CD/D IOS/placa b reinicie su pantalla, sel ción', selecco I CD/DVD y	e (antes su ción' en reinicie parezca idor otra cca una DVD ase o leccione ione reinicie	^
	siguen los pasos ante	eriores).				230 31 30	
	Recuerde que inclus de descifrar la partic	o si pierde su Disco de Re ión o unidad del sistema s	scate VeraCrypt y un at sin la contraseña correc	acante lo encuentra, ta.	, éste NO se	erá capaz	~
			Imprimir		A	Aceptar	
		0		1.05			
	Montar	Montar Autom.	Desmontar To	odo	Salir		

Al reiniciar el sistema operativo, tendremos que introducir nuestra contraseña de acceso, y dejar en blanco la segunda opción (por defecto), y automáticamente entraremos en el sistema operativo nuestro como siempre.

PlatformInfo create Unsupported Password: \_

PlatformInfo create Unsupported Password: \* PIM (Leave empty for default): \_\_\_

PlatformInfo create Unsupported Password: \* PIM (Leave empty for default): Authorizing... Success Start θ 644874240 len θ



Tal y como habéis visto en este completo tutorial, VeraCrypt es una de las formas más fácil y rápidas para crear contenedores cifrados, cifrar dispositivos USB o discos duros enteros, e incluso cifrar la partición donde almacenamos nuestro sistema operativo. Un aspecto muy importante cuando vayamos a usar VeraCrypt, es elegir correctamente el algoritmo de cifrado simétrico, nuestra recomendación es AES por varios motivos:

- Es actualmente el estándar, y no se conocen vulnerabilidades
- Los procesadores nuevos incorporan el juego de instrucciones AES-NI, esto significa que tendremos aceleración de cifrado por hardware, de tal forma que tengamos una gran velocidad de lectura/escritura.

Para que veáis la gran diferencia de rendimiento entre un procesador SIN AES-NI, y un procesador con AES-NI, en la siguiente imagen podéis ver el rendimiento que obtenemos con un procesador Intel i5 760 del año 2010, el cual no tiene esta tecnología, y, por tanto, obtendremos una velocidad de lectura/escritura muy baja:

Sort Method: Mean Spe	ed (Descend	ding)	$\checkmark$	
Algorithm	Encryption	Decryption	Mean	Benchmark
Twofish	696 MB/s	709 MB/s	702 MB/s	
Serpent	580 MB/s	658 MB/s	619 MB/s	Close
Camellia	614 MB/s	607 MB/s	610 MB/s	
AES	551 MB/s	558 MB/s	554 MB/s	
Twofish(Serpent)	320 MB/s	352 MB/s	336 MB/s	Speed is affecte
Serpent(AES)	285 MB/s	298 MB/s	292 MB/s	storage device
AES(Twofish)	291 MB/s	292 MB/s	291 MB/s	characteristics.
Kuznyechik	242 MB/s	226 MB/s	234 MB/s	These tests tak
Serpent(Twofish(AES))	198 MB/s	217 MB/s	207 MB/s	place in RAM.
AES(Twofish(Serpent))	202 MB/s	208 MB/s	205 MB/s	

Si utilizamos nuestro nuevo procesador AMD Ryzen 7 3800X que sí tiene la tecnología AES-NI, podremos ver que llegamos fácilmente a más de 10GB/s de velocidad, por supuesto, actualmente no hay disco duro o SSD capaz de gestionar tan altas velocidades:

	Comparación: Algoritmo de C	ifrado 🗸		Buffer: 100 MB	v
-	Orden: Velocidad Medi	a (Descendie	ndo)	~	
ar	Algoritmo	Cifrado	Descifrado	Media	Comparación
	AES	11.3 GB/s	10.2 GB/s	10.7 GB/s	
	Twofish	3.1 GB/s	3.1 GB/s	3.1 GB/s	Cerrar
	Serpent	2.6 GB/s	2.7 GB/s	2.6 GB/s	
	AES(Twofish)	2.3 GB/s	2.6 GB/s	2.4 GB/s	
	Camellia	2.3 GB/s	3/s 2.3 GB/s 2.3 GB/s	La velocidad se	
	Serpent(AES)	1.8 GB/s	2.3 GB/s	2.1 GB/s	ve afectada por la
	Kuznyechik	1.6 GB/s	1.4 GB/s	1.5 GB/s	carga de la CPU y
1	Twofish(Serpent)	1.4 GB/s	1.4 GB/s 1.3 GB/s	1.4 GB/s 1.3 GB/s	del dispositivo de almacenamiento.
	Serpent(Twofish(AES))	1.3 GB/s			
	AES(Twofish(Serpent))	1.3 GB/s	1.3 GB/s	1.3 GB/s	
<b>D</b> [ [ [	Kuznyechik(AES)	1.5 GB/s	1007 MB/s	1.2 GB/s	Éstas pruebas
	Camellia(Serpent)	1.1 GB/s	1.1 GB/s	1.1 GB/s	tienen lugar en
	Kuznyechik(Twofish)	1.1 GB/s	924 MB/s	1003 MB/s	RAM.
	Camellia(Kuznyechik)	968 MB/s	854 MB/s	911 MB/s	
	Kuznyechik(Serpent(Camellia)	) 72 <mark>2 M</mark> B/s	669 MB/s	696 MB/s	
_					

Aunque este último procesador es mucho más potente, la diferencia sustancial la encontramos en el «AES acelerado por hardware», ya que es cuando realmente notamos una grandísima diferencia entre ambos procesadores.

Hasta aquí hemos llegado con nuestro manual de instalación, configuración y creación de volúmenes de VeraCrypt para almacenar de manera segura nuestros datos. Esperamos que os haya gustado y os recomendamos <u>visitar la documentación oficial</u> <u>del software VeraCrypt</u> donde encontraréis toda la información sobre esta fantástica herramienta.