Encriptar una parte o todo nuestro disco duro o pendrive.

Introducción: Desde las versiones de Windows 8.1 PRO y Windows 10, se ofrece una herramienta propia del sistema operativo llamada **BITLOCKER**, con la que es posible la realización de encriptación de discos duros y pendrives. Mientras el resto de personas como las que utilizamos Windows 8.1 Home u otro sistema operativo, estamos "huertanos" de esa herramienta, lo que nos obliga a la utilización de otras aplicaciones que a mi punto de vista son más completas que las propias de Windows. En el mercado hay cientos de este tipo de herramientas, pero he escogido la herramienta llamada VeraCrypt que es gratuita, con muchas opciones, fácil de utilizar y muy potente.

¡Empecemos!

Nos dirigiremos a la página web oficial: <u>https://www.veracrypt.fr/en/Downloads.html</u>



Hay 2 versiones, la que se instala en el equipo y la Portable, que es la que preferiremos utilizar puesto que podremos encriptar y desencriptar nuestros archivos desde nuestro pendrive en cualquier PC. Lo único importante aquí es recordar la contraseña de nuestros almacen encriptado.

Vamos a hablar de almacen encriptado como método más útil y necesario para una informática básica y de hogar. Con este método podemos encriptar caulquier archivo de forma muy segura.

Paso 1: Empecamos abriendo el archivo y ejecutarlo que nos descomprimirá en la carpeta elegida los archivos necesarios para el funcionamiento del programa.



Pulsaremos doble clic con el ratón al archivo correspondiente:

- VeraCrypt-x64.exe para ordenadores basados en microprocesadores de 64 bits.
- **VeraCrypt.exe** para ordenadores basados en microprocesadores de 32 bits.

Paso 2: Ya teniendo el programa abierto, deberemos pulsar en el botón Create Volume.

×				Ver	raCryp	t	-	. 🗆 🗡
Volumes	System	Favorites	Tools	Settings	Help			Homepage
Drive	Volume				Size	Encryption Algorithm	Туре	^
P:								
Q:								
T:								
₩0.								
W:								
								_
<u>ج</u> ۲:								~
		_						
	Create Volur	ne		Volume	Propert	es	Wipe C	ache
Volume	; 							
						~	Select F	ile
VeraC	Vet 🗸 Ne	ever save hist	ory		۷	olume Tools	Select De	vice
				- Davies		Diaman All		1
	Mount		Jto-Moun	t Devices		Dismount All		

Paso 3: Nos aparecerá un cuadro con un asistente que nos hará automáticamente la opción que señalemos:



Crear un almacén encriptado (la opción que vamos a ver: Puedes crear un almacén encriptado en cualquier parte y con el tamaño que quieras; no debe pasar el tamaño total del dispositivo físico en donde se va a crear y crearlo no implica que puedas crear otros archivos visibles y sin encriptar alrededor del almacen encriptado)

Encriptar una partición de un disco duro que no pertenece al sistema (Si tenemos 1 disco duro grande particionado (dividido) en 2 partes, una parte será del sistema (Donde estará el sistema operativo Windows) y la otra parte que aunque depende de Windows para crear archivos y gestionar sus funciones, no pertenece al sitema de Windows y es entonces cuando se puede utilizar toda esa unidad para encriptarla. (Aconsejo hacer una copia de seguridad de todos tus documentos importantes)

Encriptar la partición del sistema o toda la unidad del sistema entera: Según lo explicado anteriormente, encriptaremos todo el sistema Windows en nuestro PC. **Nada Recomendable para personas con pocos conocimientos.** (Aconsejo hacer una copia de seguridad de todos tus documentos importantes)





No entraremos en más explicaciones avanzadas. Quien quiera puede seleccionar las opciones que mejor le convenga siempre que haya leído y comprendido las acciones y consecuencias de las mismas y la posible pérdida de datos si se equivoca o no es un usuario medio – avanzado en conocimientos de informática.

Seleccionaremos Standard VeraCrypt Volume y pulsamos en el botón NEXT.

Paso 5: Ahora vamos a seleccionar dónde vamos a crear el almacén (dicho almacén se podrá copiar, cortar y pegar en otras unidades, pero ahora debemos elegir uno)

Yo seleccionaré como localización de creación del almacén un pendrive en donde llevaré el almacén y el programa portable para encriptar y desencriptar mis archivos)



Paso 6: Habiendo seleccionado mi pendrive denominado WHITE_PEN (F:) como se observaen la imagen, escribiré en Nombre (franja amarilla) el nombre de nuestro almacén al que he denominado PRIVATE y luego pulsaré el botón Guardar.

×		Specify Path and	l File Name			×
€ ∋ - ↑ -	🖕 🕨 Este equipo	WHITE_PEN (F:)	× ¢	Buscar en WHITE_PE	:N (F:)	ρ
Organizar 👻 N	ueva carpeta				• •	0
 Documento Escritorio Imágenes Música Router Voda Router Voda Vídeos Vídeos OS (C:) Almacen (D Unidad de E WHITE_PEN Descargas (afor afor DVD J (F: G:)	Ningún elemen	to coincide con el c	riterio de búsqueda.		
Nombre:	PRIVATE					~
Tipo:	All Files (*.*)					~
) Ocultar carpetas				Guardar	Cancelar	

Paso 7: Se nos confirmará el lugar y el nombre de nuestro almacén encriptado:





Sera VeraCr	ypt Volume Creation Wizard 🛛 🚽 🔍 🗡
	Encryption Options
	AES Test FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
VeraCrypt	More information on AES Benchmark Hash Algorithm
	Help < Back Next > Cancel

Algoritmo AES: Es la más estandarizada y siempre es más fácil solucionar posibles problemas que puedan ocurrir en la encriptación, y el tipo de "troceado" del algoritmo, donde seleccionaremos el estándar . Se pueden escoger otros tipos de encriptación, cada cual el que le mejor le convenga.

Paso 9: Seleccionemos ahora el tamaño de nuestro almacén a encriptar (ojo, una vez realizado no se podrá aumentar o achicar su tamaño, aunque siempre queda en crear un almacén nuevo si nos equivocamos al hacer este.

El programa te pedirá el tamaño el tamaño en varias unidades y abajo (*en el recuadro azul*) te dice la capacidad total del dispositivo para que no te pases de tamaño y calcules que vas a necesitar. Mi Pendrive tiene 976,99 MB (1 GB) por lo que seleccionaré un pequeño espacio para llevar algunos archivos importantes con datos personales. 200 MB, será para mi una buena elección. Si se me pierde el pendrive, mis datos estarán a salvo o si se lo dejo a un amigo para que me pase alguna foto, no podrá ver ni acceder a mi almacen.



Aqui vemos un ejemplo de nuestra elección. Lógicamente deberemos pulsar en **NEXT** para continuar...



Paso 10: Ahora viene la decisión más importante y por la cual, la seguridad de nuestros archivos van a ser seguros o no.

En el manual ya he explicado anteriormente que consideraciones debemos tener en cuenta para crear una contraseña adecuada y segura para nuestros propósitos. Yo he puesto como password "micurso" y aunque no es para nada una contraseña segura, nos servirá para realizar este ejemplo.

SeraCi	rypt Volume Creation Wizard 🛛 🚽 🔍 🗙
	Volume Password Password: ••••••• Confirm: ••••••• Use keyfiles Keyfiles Display password Use PIM
VeraCrypt	It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ $^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.
	Help < Back Next > Cancel

Continuaremos pulsando el botón **NEXT**.

Como ejemplo podemos ver como el propio programa me avisa de que la contraseña es muy fácil para "hackearla" con el método de diccionarios de "Fuerza bruta". No obstante si dices que estás de acuerdo pulsando SI, el programa continuará...



Paso 11: Aquí veremos como se crea el almacén encriptado. **IMPORTANTE: mientras se crea el volumen debes mover el puntero del ratón por toda la pantalla de la forma mas aleatoria posible.**

R	VeraCr	ypt Volume Creation Wizard 🛛 🚽 🔍 🗡
		Options Filesystem FAT Cluster Default Dynamic Random Pool: *++*.*-+,/.,/*,/+*/+/*.*.+-,* Header Key: Master Key:
	Vera Crypt	Abort Done Speed Left IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume. Randomness Collected From Mouse Movements
		Help < Back Format Cancel

Aqui veremos los mensajes que indican que nuestro almacén encriptado ha sido creado con éxito.





Pulsaremos en el botón Aceptar.

-ı -·· -· [* OS (C:) 95,0 GB disponibles de 260 GB Almacen (D:) 7,38 GB disponibles de 195 GB Unidad de DVD RW (E:) 4,38 GB disponibles de 4,38 GB WHITE_PEN (F:) 776 MB disponibles de 977 MB Descargas (G:) 161 GB disponibles de 298 GB PortableApps.com (J:) 635 MB disponibles de 28,6 GB - -👝 l ⊋ 📗 🗡 👳 l F:\ Inicio Compartir Vista • Ж] Mover a 🔻 🗙 Eliminar 🝷 P W... Propiedades 🥳 A Seleccionar Copiar Pegar Nueva 📋 Copiar a 🔻 📺 Cambiar nombre 5 carpeta Portapapeles Organizar Nuevo Abrir Buscar en ... 🔎 ► Este equipo → WHITE_PEN (F:) € 🦻 ד ↑ v C 🔋 Vídeos 🝺 Vínculos 👰 Este equipo 🚺 Descargas Documentos PRIVATE 膭 Escritorio 📄 Imágenes 🚺 Música ᢪ Router Vodafone Fi Ҏ Router Vodafone Fi 📑 Vídeos 📥 OS (C:) 👝 Almacen (D:) 💿 Unidad de DVD RW - WHITE_PEN (F:) 👝 Descargas (G:) 🔊 DartshleAnns com 1 elemento 👘 1 elemento seleccionado 200 MB :::: 🔊

Ahora podemos comprobar como se ha creado nuestro almacén.

Paso 12: Ahora pasaremos algunos archivos a nuestro almacén criptado para mantenerlos seguros. Empezamos abriéndolo, pero para poder abrirlo y nuestro sistema lo reconozca, lo tenemos que convertir en una unidad (G,H,N,Z,X...)

Veamos como lo hacemos con el propio programa.

<u>w</u>		Ver	aCryp	t	_ □	×
Volumes System F	avorites Tools	Settings	Help		Home	page
Drive Volume			Size	Encryption Algorithm	Туре	^
A:						
H:						
I:						
M:						
0:						
P:						
						•
Create Volume		Volume F	Properti	es	Wipe Cache	
Volume						
	/ATE			~	Select File	
VeraCrypt VeraCrypt	er save history		۷	olume Tools	Select Device	
Mount	Auto-Moun	t Devices		Dismount All	Exit	

El Programa de por si nos da ya unidades disponibles para poder escoger la que queramos (No están usadas por el sistema) **EN Select File...** Pulsaremos para seleccionar nuestro almacén, al que llamamos PRIVATE y guardamos en nuestro pendrive en la unidad **F**:

Habiendo realizado todos estos pasos ya podemos dar al botón **MOUNT** con el que convertiremos nuestro almacén encriptado en la unidad que seleccionamos, la **H**: para trabajar en ella.

Paso 13: Para continuar nos pedirá el password (Contraseña) que le pusimos, en este caso "micurso" y pulsaremos en OK.

	Enter password f	or F:\PRIVATE	
Password:			ОК
PKCS-5 PRF:	Autodetection V	TrueCrypt Mode	Cancel
	Use PIM Cache passwords and keyfile Display password Use keyfiles	s in memory Keyfiles	Mount Options

En este momento podremos ver como nuestro almacén encriptado **PRIVATE** se ha convertido en una unidad con la letra **H**:

Σ¢				Ver	aCryp	t		-		
Volumes	s System	Favorites	Tools	Settings	Help				Home	page
Drive	Volume				Size	Encryption Algorit	hm	Туре		^
A:										
H:	F:\PRIVATE			1	99 MB	AES		Normal		
I:										
E:										
M:										
0:										
P:										J
	Create Volur	ne		Volume I	Propert	es		Wipe Ca	ache	
Volume										
	F:\P	RIVATE				~		Select F	ile	
VeraC	rypt 🗹 Ne	ever save his	tory		٧	olume Tools		Select De	vice	
	Dismount	A	uto-Moun	t Devices		Dismount All		E	Xit	
Volume	Create Volur F:\P rypt V Dismount	ne RIVATE ever save his	tory uto-Moun	Volume I	Propert	ies olume Tools Dismount All		Wipe Ca Select F Select De	ache ile vice	

Paso 14: Vemos como en nuestro sistema Windows hay una nueva unidad con la letra H:



Podemos utilizar la unidad como si fuera un pendrive o disco duro y podremos poner los archivos que queramos (**ojo tenemos sólo 200 MB**) ya que lo configuramos de esa forma.

Paso 15: Ya hemos metido en esa unidad todos los archivos que queremos encriptar y vayan seguros en cualquier medio, discos duros, pendrives,... Es hora de cerrar nuesto almacén para que nadie tenga acceso a mis archivos.

Si vemos el programa, deberemos seleccionar nuestra unidad (bien definida en la interfaz) y pulsaremos el botón **Dismount**.



Paso 16: Ya nuestra unidad **H:** (la del almacén encriptado) ha desaparecido y si sólo podemos abrir el pendrive donde tenemos el almacén **PRIVATE**. Sólo vemos ese archivo y ningún otro archivo que estuvimos manipulando y guardando en **PRIVATE**. **PRIVATE** es un archivo cerrado y no puedes ver nada de lo que hay dentro de él sino lo haces con los medios apropiados (**Programa VeraCrypt**) y la contraseña usada ("micurso")



Pero aunque no lo creas y no lo veas, PRIVATE tiene 3 documentos que pusimos anteriormente...