

# Protección de la información en mi ordenador. VeraCrypt aplicación para cifrar y proteger la información

La manera de evitar los problemas derivados de que la información privada quede expuesta a personas no autorizadas es sencilla: basta con **cifrar la información**, es decir, almacenarla codificada de tal forma que no pueda acceder a ella alguien que no conozca la **contraseña de cifrado**.

Muchas son las ocasiones en que nos interesa cifrar un archivo:

- Documentos privados almacenados en un ordenador que compartimos o son accesibles a otras personas.
- Documentos almacenados en un portátil, en una unidad usb u otro soporte externo que puede ser susceptible de robo o pérdida.
- Documentos confidenciales adjuntados en un correo electrónico. Los correos que enviamos a través de internet pueden fácilmente ser interceptados por terceras personas. Por otro lado, mientras éstos permanecen en un servidor, pueden estar accesible a terceras personas.

En situaciones como las anteriores puede ser obligado cifrar los documentos. Por supuesto es obligatorio cuando estamos trabajando con datos personales de ficheros declarados de nivel medio-alto de la Universidad de Zaragoza en la Agencia de Protección de Datos .

**VeraCrypt** es una herramienta sucesora de *TrueCrypt*, aplicación discontinuada por sus desarrolladores, que nos permite crear un volumen cifrado que podemos trasladar con seguridad.

Los datos almacenados en un volumen cifrado por **VeraCrypt** quedan ocultos y protegidos de tal forma que sólo se puede acceder a ellos conociendo la contraseña que permite montar un volumen de disco como una unidad/disco virtual. Por ello, es muy importante conocer y **no olvidar dicha contraseña.** 

*VeraCrypt* es un desarrollo de software libre, que se encuentra disponible para los sistemas Windows, Linux y MacOSX

## Instalación de VeraCrypt

Lo primero que haremos será descargarnos la aplicación de la web oficial <u>https://veracrypt.codeplex.com/</u> desde la sección *Download* y elegir la última versión estable para nuestra plataforma.

## Uso de la aplicación VeraCrypt



Cuando lanzamos la aplicación ésta será la pantalla principal de funcionamiento. Lo que haremos es crear en un fichero de nuestro equipo un volumen/unidad de disco, o también en un dispositivo USB, Dropbox, GoogleDrive, ...puesto que se trata de usar un fichero para convertirlo en un volumen.

Seleccionaremos la opción "Create Volume"

olumes/	System	Favorites	Tools	Settings	Help				Home	page
Drive	Volume					Size	Encryption alg	orithm	Type	
<u></u> Е;										
]:										
— К:										=
- M:										
-N:										
_0:										
=P:										
Q:										
R:										
S:										
S:										
S:										÷
	Create Volu	me		Volume 1	Properties.			Wipe	Cache	-
S: T:	Create Volui	me		Volume 1	Properties.	** .		Wipe	Cache	]
S: T: Volume	Create Volu	me		Volume 1	Properties.	**		Wipe	Cache	
S: T: Volume	Create Volu	me		Volume P	Properties.		•	Wipe	Cache : File	-
S: T: Volume	Create Volur	me	tory	Volume 1	Properties.		• [ s,	Wipe ( Select Select D	Cache : File Device	
S: T: Volume	Create Volur	me	tory	Volume P	Properties.	 me Tool	•	Wipe ( Select Select D	Cache File Device	



Elegiremos donde queremos crear el volumen, **en un fichero cifrado**, en una partición en un "drive". En este tutorial elegiremos la primera opción, opción por defecto, y marcaremos **Next**.

VeraCrypt Volume Creation Wizard	VeraCrypt Volume Creation Wizard © Create an encrypted file container Creates a virtual encrypted disk within a file. Recommended for
	<ul> <li>inexperienced users.</li> <li>More information</li> <li>Encrypt a non-system partition/drive</li> <li>Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.</li> <li>Encrypt the system partition or entire system drive</li> <li>Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files. etc., will need to enter the correct password each time</li> </ul>
	before Windows boots. Optionally, creates a hidden system.       More information about system encryption       Help     < Back

Creamos un **volumen de tipo común**. En este tutorial elegiremos la primera opción, opción por defecto, y marcaremos **Next** 



0	Standard VeraCrypt volume
	Select this option if you want to create a normal VeraCrypt volume.
0	Hidden VeraCrypt volume
	It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
	More information about hidden volumes

Seguimos el asistente para la creación de volúmenes y decidimos en que unidad y que nombre de fichero le vamos a dar para contener nuestro volumen/unidad de disco . **Seleccionaremos el fichero:** 



En este tutorial el fichero sobre el que se creara el "volumen" VeraCrypt lo llamamos



# *F:\Data\* y el nombre del "volumen" será My Volume.



Organize 👻 New folde	er			9== •	0
Git	* Na	me		Date modified	
Pictures		No items	match your search.		
Videos					
👰 Computer	E				
Local Disk (C:)					
Local Disk (F:)	+ +	III			
File name: My Vo	olume				
Save as type: All File	es (*.*)				
Hide Folders			Save	Cancel	

## Seleccionaremos el tipo de cifrado

X

Q



ES		•	Test
ed by U.S. gover assified informatic 28-bit block, 14 ro ore information or	nment departme on up to the Top ounds (AES-256). <u>n AES</u>	nts and ager Secret level. Mode of ope	cies to protect 256-bit key, ration is XTS. Benchmark
ash Algorithm			

A continuación elegimos el **tamaño** para nuestro **volumen**/ unidad virtual. Será el adecuado a nuestras necesidades.





Se nos pide una **contraseña**. Hay que tener presente que dicha contraseña será la que en el futuro usaremos para montar y usar el volumen que estamos creando.

G				
<u>C</u> ommi	Use keyfiles Display password Use PIM	Keyfiles		
iot contain any re juess. A good pa ase letters, num etc. We recomme characters (the lo haracters.	ames or dates of birth. It sl issword is a random combina bers, and special characters and choosing a password colo onger, the better). The max	hould not be easy to ation of upper and low s, such as @ ^ = \$ * - nsisting of 20 or more timum possible length is		



### Procedemos a dar formato al volumen creado:

Filesystem FA	T  Cluster Defa	ult 🔻 🔲 Dynamic
Random Pool: Header Key: Master Key:	F8507E4453BAA3A7	783A67899F7C7676B 🗹
		Abort
Done	Speed	Left
IPORTANT: Mo indow. The lon creases the cr	ove your mouse as rando ger you move it, the bet yptographic strength of	omly as possible within this tter. This significantly the encryption keys. Then

Al finalizar el formato que puede llevar más de 30 segundos, aparecerá el siguiente diálogo que cerraremos marcando OK

VeraCrypt	Volume Creation Wizard
i	The VeraCrypt volume has been successfully created.
	ОК



La aplicación nos permite crear otro volumen si seleccionamos Next. Si no lo deseamos saldremos de la misma marcando **Exit** 

Volume Cre	eated		
The VeraCrypt volu wish to create anot Exit.	me has been crea her VeraCrypt vo	ated and is read lume, click Next	y for use. If you . Otherwise, <mark>dick</mark>
Help	< Back	Next >	Exit



## Y ya podemos proceder a usar la unidad creada:

Desde la aplicación VeraCrypt, elegimos una letra para asignar a la unidad

olumes	System	Favorites	Tools	Settings	Help				Home	page
Drive	Volume					Size	Encryption a	lgorithm	Type	-
E:										
K:										TE
N.										
0:										
-P:										
Q:										
-R:										
R:										
R: S: T:										
R: S: T:										Ŧ
R:		1		r						
R: S: T:	ireate Volur	ne		Volume 1	Properties.	n.]		Wipe	Cache	
R: S: T: Volume	reate Volur	ne		Volume 1	Properties.			Wipe	Cache	
R: S: T: Volume	reate Volur	ne		Volume R	Properties.	**		Wipe	Cache	
R: S: T: Volume	reate Volur	ne		Volume P	Properties.	**	•	Wipe	Cache t File	
R: S: T: Volume	ireate Volur	ne	tory	Volume I	Properties.	me Tool	• [ s]	Wipe Select Select [	Cache t File Device	
R: S: T: Volume	reate Volur	ne	tory	Volume F	Properties.	me Tool	• [ s	Wipe Select Select [	Cache t File Device	
R: S: T: Volume	reate Volur	ne	tory	Volume 1	Properties.	me Tool	s	Wipe Select Select [	Cache t File Device	-



Seleccionamos el volumen creado.

/olumes	System	Favorites	Tools	Settings	Help				Home	page
Drive	Volume					Size	Encryption	algorithm	Type	*
<u></u> Е:										
, ]:										
— K:										E
M:										
-N:										
0:										
=P:										
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1										
- Q.										
R:										
R:										
R:										
■ €. ■ R: ■ S: ■ T:										-
R: S: T:	reate Volun	ne		Volume	Properties.	]		Wipe	Cache	
R: S: T:	reate Volun	ne		Volume F	Properties		[	Wipe	Cache	
R: S: T:	reate Volun	ne		Volume P	Properties			Wipe	Cache	
R: S: T:	reate Volun	ne		Volume F	Properties		[	Wipe	Cache t File	
R: S: T:	reate Volun	ne	tory	Volume I	Properties.	me Tool		Wipe Select Select I	Cache t File Device	
R: S: T: Volume	reate Volun	ne	tory	Volume P	Properties.	ime Tool	s	Wipe Select Select I	Cache t File Device	



### Una vez localizado marcaremos Open

	tolder		≣ ▼ 🗖
	*	Name	Date modified
Libraries		My Volume	12/30/2014 11:28 1
Git	1		
A Music			
Pictures			
Subversion	E		
📑 Videos			
🜉 Computer			
🏭 Local Disk (C:)			
👝 Local Disk (D:)			

#### Y montaremos el volumen marcando Mount:

olumes	System	Favorites	Tools	Settings	Help				Homep	bag
Drive	Volume					Size	Encryption alg	gorithm	Туре	-
- K:										
M:										
-N:										
-0:										
-P:										
-Q:										
- K.										
-T:										
- T:										
T:	Create Volun	ne		Volume	Properties			Wipe	Cache	,
T:	Create Volur	ne		Volume 1	Properties			Wipe	Cache	,
T:	Create Volun	ne		Volume 1	Properties			Wipe	Cache	, 
T:	Create Volur	ne ata Wy Volun	ne	Volume I	Properties			Wipe	Cache	)
T:	F:\D	ne ata Wy Volun ever save his	ne	Volume 1	Properties			Wipe (	Cache File	
T:	F:\D	ne ata'My Volun ever save his	ne tory	Volume 1	Properties	ume Tool	• [ s]	Wipe ( Select Select D	Cache : File Device	
Volume	F:\D	ne ata Wy Volun ever save his	ne tory	Volume I	<sup>o</sup> roperties Volu	ume Tool	• [ s	Wipe Select Select D	Cache File	
Volume	F:\D Ve	ne ata\My Volun ever save his	ne tory	Volume I	Properties	ume Tool	• [ s ] [	Wipe Not Select D	Cache File	



Al seleccionar Mount se nos pedirá la contraseña de protección y con ello ya tendremos nuestra **unidad montada y lista para usar.** 

Password:		ОК
PKCS-5 PRF:	Autodetection   TrueCrypt Mode	Cancel
	Use PIM	
	Cache passwords and keyfiles in memory	
	Display password	
	Else keyfiles	Mount Options.

Si miramos en nuestro equipo veremos el volumen creado como cualquier otra unidad de nuestro equipo.

)rganize 👻 🛛 Pr	opert	ties System properties	>>
Documents	^	Name	Туре
Git		👝 Local Disk (F:)	Local Disk
J Music		👝 Big (H:)	Local Disk
Pictures	=	👝 Iomega HDD (L:)	Local Disk
Subversion		👝 Local Disk (M:)	Local Disk
Videos		Devices with Remov	able Storage
		DVD RW Drive (G:)	CD Drive
N Lagel Diele ((			



## Para dejar de usarla basta con seleccionar Dismount

olumes	System	Favorites	Tools	Settings	Help				Homep	oage
Drive	Volume					Size	Encryption	algorithm	Туре	-
J:										
— K:										=
M:	F:\Data\My	Volume				249 MB	AES		Normal	1
-N:										
-0:										
-P:										-
`Q:										
-R:										
- S:										
S:										
S:										
S:	reate Volum	ne		Volume	Propertie	s]		Wine	Cache	
S: T:	reate Volur	ne		Volume F	Propertie	5		Wipe	Cache	
S: T:	reate Volur	ne		Volume F	Propertie	5		Wipe	Cache	•
S: T:	reate Volur	ne ata\My Volun	ne	Volume F	Propertie	5		Wipe	Cache	
S: T:	F:\D	ne ata Wy Volun	ne	Volume F	Propertie	S	- I	Wipe	Cache	
S: T: Volume	F:\D F:\D Ne	ne ata\My Volun ever save hist	ne tory	Volume F	Propertie	s	• ( S	Wipe Select	Cache t File Device	
Volume	F:\D	ne ata Wy Volun ever save hist	ne tory	Volume F	Propertie	s	• ( S	Wipe Select Select D	Cache t File Device	
S: T: Volume	F:\D F:\D V	ne ata\My Volun ever save hist	ne tory	Volume I	Propertie	s	s	Wipe Select Select D	Cache t File Device	

## REFERENCIAS

- VERACRYPT (FREE OPEN-SOURCE ON -THE-FLY ENCRYTION).- USER'S GUIDE, versión
   1.16.- Released by IDRIX on October 7, 2015 (veracrypt.codeplex.com)
- CIFRADO\_TrueCrypt.pdf. Tutorial SICUZ