Milpa Digital

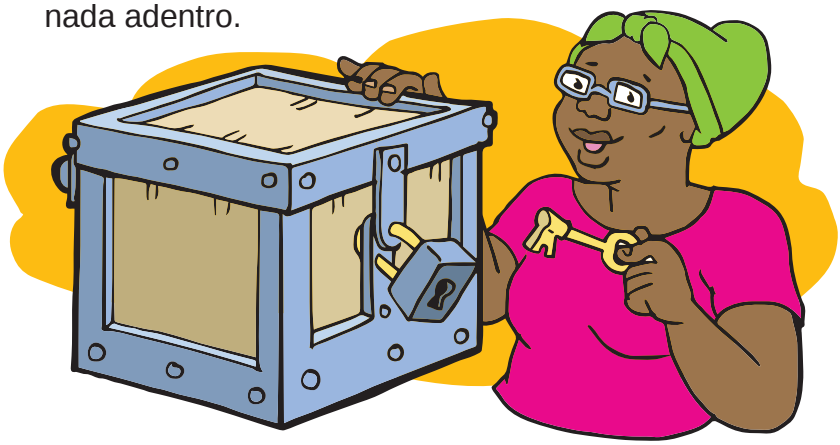
Guardando información de forma segura con VeraCrypt

Cuando guardamos datos sensibles en el disco interno de una computadora, un disco duro externo, o en una memoria externa como un USB, corremos el riesgo de que este soporte caiga en manos de otras personas. Nunca sabemos quién va a terminar revisando nuestros documentos, fotografías o videos, ya sea porque hemos perdido o nos han sustraído la memoria o el disco, o porque alguien con malas intenciones consiguió acceder a ellos mientras no estamos presentes o infectándonos con malware (Milpa 9).

Veracrypt es una herramienta para Windows, MacOS y Linux que nos protege contra este tipo de ataques o accidentes, y lo hace creando **volúmenes cifrados**.

Qué es un volumen cifrado

Podemos pensar en un volumen cifrado como una caja con una llave. La llave es una contraseña fuerte que sólo nosotres conocemos, y para quien no tenga esa llave la caja permanece cerrada, de forma que no se puede ver que archivos y carpetas contiene, ni escribir nada adentro.



Descargar e instalar

Es muy importante descargar el programa sólo de un sitio confiable, y no hacer una búsqueda cualquiera en Google. En este caso, la página de las descargas es: **https://www.veracrypt.fr/en/Downloads.html**

- Elegiremos el **Installer** cuando lo que queremos es cifrar un disco del sistema o crear un volumen cifrado en nuestra propia computadora.
- Elegiremos la **Versión portable** cuando queremos llevar el programa veracrypt en una memoria USB.

Esto puede ser una buena idea si necesitamos usar los archivos que llevamos cifrados en nuestra USB en diferentes computadoras.

Creando un volumen cifrado

Al correr Veracrypt, nos dará varias opciones. Pulsaremos la opción **Crear Volumen**. En el asistente, podemos elegir entre cifrar una partición del sistema, una unidad de disco completa (por ejemplo un USB), o crear un contenedor (algo como una caja, o una carpeta) de archivos cifrado. Ésta última puede ser la opción más sencilla para familiarizarnos con el funcionamiento de Veracrypt, y más adelante podemos elegir cifrar una partición completa cuando estemos más cómodas. Al crear un contenedor, nos preguntará la ubicación donde queremos crearlo, el tamaño máximo del contenedor (por ejemplo, 2GB), y algunas opciones de cifrado (dejaremos las que pone el asistente por defecto). Elegiremos también el formato de ficheros (NTFS), y por último pulsaremos en **Formatear** para terminar de crearlo.

Un **contenedor de archivos cifrado** se verá como un archivo dentro de nuestro disco, pero al descifrarlo desde Veracrypt con nuestra contraseña, se comportará como un Disco nuevo en nuestro sistema, y podemos copiar y mover archivos dentro de él. Desde Veracrypt, podemos descifrarlo introduciendo nuestra contraseña, o volverlo a cerrar.

Suscríbete a ResistenciaDigital en Telegram @CanalResistenciaDigital

Crear un volumen oculto

Una de las opciones cuando creamos un volumen cifrado con Veracrypt es la de crear un volumen oculto. En realidad lo que sucede es que Veracrypt crea dos volúmenes cifrados, **uno dentro de otro**, y lo hace de tal forma que cuando se abre el volumen grande que contiene al que está oculto, no hay forma de saber si dentro hay otro volumen cifrado o no.

Crear un volumen oculto es útil si **por la fuerza tenemos que entregar nuestra contraseña de cifrado** (mediante extorsión, por ejemplo). Si tenemos un volumen oculto podemos dar la contraseña del primer volumen, la gente que mire dentro no tendrá forma de saber que ahí existe otro volumen oculto y por tanto no tenemos que darles esa contraseña.

CódigoSur EDICIONES

Créditos: CódigoSur 2019/2020. MilpaDigital. https://milpadigital.org.