Cifrado de disco y archivos con software libre

03/05/2024 11:35:43

FAQ Article Print

Category:	- Seguridad, LOPD	**Last update:**	11:39:46 - 06/30/2020
State:	public (all)		

Keywords

Cifrado, Disco duro, Archivos, software libre

Solucion (public)

El cifrado de disco consiste en encriptar la información de todo el disco duro por medio de un proceso matemático de forma que solo pueda decodificarse por medio de una contraseña concreta. Esto evita que cualquiera pueda acceder al contenido de un equipo sin conocer dicha contraseña, pues sólo podrá leer información codificada, lo cual es perfecto para proteger la información de un equipo que ha sido robado. Configurar un volumen de disco cifrado es un proceso muy sencillo que puede llevarse a cabo durante la instalación de la mayoría de distribuciones de GNU/Linux. Durante uno de los pasos de la instalación se pregunta al usuario al respecto del particionado de disco, y se suele incluir una opción para cifrar sus contenidos, como podemos ver en esta imagen de intalación de Debian:

La opción resaltada indica que el volumen de disco estará cifrado, y tras seleccionarla se nos solicitará que elijamos una contraseña para la misma. Una vez finalizada la instalación del sistema, el equipo no podrá iniciarlo si no introducimos antes la contraseña, como se muestra a continuación:

Tras instroducir la contraseña correcta, un mensaje nos informará de que el disco se ha descodificado correctamente y prodecerá con el proceso normal de arranque:

===VeraCrypt===

La configuración de un volumen cifrado también puede realizarse a través de programas libres, como VeraCrypt, que al ser multiplataforma puede utilizarse también en otros sistemas operativos como Windows o Mac.

Al ejecutar el instalador de VeraCrypt se nos presentan (tras los acuerdos de licencia) dos opciones: instalar el programa o simplemente extraerlo, tal y como vemos a continuación:

Esta elección se debe a que VeraCrypt puede utilizarse para cifrar archivos además de discos enteros, y la presencia de un programa de estas características en un equipo alertaría a cualquier intruso de la existencia de archivos cifrados. Así, VeraCrypt es capaz de funcionar con una sencilla extracción, evitando dejar rastros en el sistema y pudiendo ser eliminado con facilidad, de modo que únicamente necesitaríamos extraerlo nuevamente para visionar los archivos cifrados en caso de necesitarlo. Sin embargo, si optamos por cifrar el disco de arranque del sistema es imprescindible realizar una instalación normal, pues sin ella el sistema operativo será incapaz de permitirnos introducir la contraseña, debido a que el programa no se ejecutará en arranque y no podrá, por tanto, comenzar el proceso de descifrado de la unidad. Por fortuna, el propio VeraCrypt nos advierte de ello y nos obliga a instalar debidamente el programa en caso de que intentemos cifrar el disco de arranque.

==Utilización de VeraCrypt==

Una vez descomprimido o instalado podemos ejecutar VeraCrypt, lo que nos llevará a la pantalla principal, donde podremos elegir un disco o un archivo para ser encriptados o descifrados, como puede verse a continuación:

Una vez seleccionado el disco o archivo debemos hacer click en el botón de "Crear Volumen" para acceder a las opciones de encriptado y desencriptado del programa, que se abrirán en una nueva ventana:

Esta ventana nos permite escoger qué tipo de volumen va a cifrarse. La opción seleccionada por defecto, como se ve en la imagen más arriba, se utiliza para crear un disco virtual cifrado en cuyo interior podremos guardar archivos a los que no se podrá acceder sin la debida contraseña. La última opción, como se ve en la siguiente imagen, se utiliza para cifrar un disco de arranque:

Tras seleccionar la opción que nos convenga, el programa nos preguntará si queremos realizar una encriptación estándar u oculta. La opción de crear un volumen oculto nos permite esconder la información importante en forma de datos aparentemente aleatorios diseminados en el interior de un volumen estándar de VeraCrypt. Esto es muy útil, pues si alguien nos obliga a revelar nuestra contraseña, los archivos aún seguirán a salvo en un segundo volumen oculto dentro del primero. En cualquier caso, al elegir esta opción deberemos escoger un volumen preexistente de VeraCrypt dentro del cual crear el volumen oculto (la opción llamada "Direct mode"), o bien crear un volumen oculto nuevo para dicho propósito (la opción llamada "Normal mode"). A continuación abordaremos la creación de un volumen normal de VeraCrypt, tras lo cual se deberán repetir los mismos pasos para el volumen oculto.

La siguiente ventana nos pedirá escoger la localización del volumen. Este paso es importante, pues el archivo creado contendrá la información cifrada y puede llegar a resultar muy evidente. Por este motivo, es conveniente aprovechar los nombres de determinados archivos de sistema, si bien hay que tener cuidado de

colocarlos en lugares donde no puedan ser malinterpretados o reemplazados por el ordenador en su funcionamiento habitual (el propio VeraCrypt nos advertirá de que utilizar determinadas extensiones de archivos ejecutables puede causar problemas de este tipo). Un ejemplo de esta forma de camuflaje es la utilización de core.dump como nombre en sistemas GNU/Linux (pues es un volcado de memoria de un proceso que fracasa, normalmente utilizado para su análisis posterior) o hiberfil.sys para sistemas Windows (pues este es el nombre de los archivos generados para el proceso de hibernación).

Elegido el nombre del archivo, se nos dará a escoger el tipo de cifrado. Existen muchas opciones basadas en diversos procesos matemáticos (algunos de ellos encadenados en cascada), pero la opción por defecto, AES, es la que nos proporcionará un mejor rendimiento debido a que puede ser descodificada nativamente por la mayoría de máquinas modernas.

El siguiente paso consitirá en asignar el tamaño del volumen, que puede ir desde pocos Kib hasta vario TB. Para ser consistente con el camuflaje del archivo, en Windows debería tener exactamente el tamaño de la memoria RAM del equipo, mientras que en Linux no debería exeder el orden de los GB. Una vez superado este paso, se nos pedirá que seleccionemos una contraseña para el volumen. Además de utilizar letras, VeraCrypt nos da la opción de escoger uno o más archivos para que sean utilizados de contraseña (sea en lugar o además de la contraseña escrita), pudiéndolos seleccionar en la ventana emergente que aprece tras verificar la opción de "Use keyfiles" y dar click en el botón correspondiente.

Esta opción tiene la ventaja de que no tenemos que recordar una contraseña, sino únicamente los archivos que deben utilizarse para desbloquear el volumen, lo cual puede resultar muy conveniente si se utilizan archivos comunes (como una foto que está disponible en nuestra nube, o el archivo readme de una versión concreta de un programa fácilmente accesible). Los archivos incluso pueden ser renombrados sin que haya inconveniente alguno, pero deben estar todos presentes y no deben sufrir ningún cambio interno. Incluso la modificación de un único píxel en una imagen gigantesca hará que el archivo deje de funcionar como llave, por lo que es mejor, como ya se ha indicado, que este esté disponible en varias localizaciones para evitar que una corrupción accidental de datos nos impida el acceso a nuestra información.

Elegida la contraseña, la siguiente ventana nos dará la opción de definir nuestro sistema de archivos y nos pedirá que realicemos movimientos aleatorios con el ratón hasta que se llene una barra verde, proporcionando así números aleatorios (obtenidos a través de la transformación matemática de los movimientos) para fortalecer el proceso de encriptación. Al hacer click en siguiente se inciará la escritura del volumen, que puede llevar un tiempo e incluso presentar la apariencia de que el programa se ha bloqueado. Sin embargo, con un poco de paciencia terminará por finalizar el proceso y podremos repetir los pasos para el volumen oculto o finalizar el proceso, si este ya ha sido configurado.

=Acceder a un volumen cifrado=

Para acceder a un volumen cifrado de VeraCrypt solo tenemos que seleccionar el archivo en cuestión, tal y como hicimos en el primar paso, seleccionar una unidad disponible en la lista que aparece en la parte de arriba de la ventana y hacer click en la opción de montar:

El programa nos pedirá la contraseña para descifrar el volumen y, una vez introducida y/o cargados los archivos pertinentes, la unidad quedará montada como un disco duro virtual, accesible desde nuestro navegador de archivos, en cuyo interior podremos guardar todos los datos que queramos encriptar. Una vez hecho esto, sólo hace falta hacer click en la opción de "Dismount All" para que el archivo desaparezca de la lista de unidades activas en nuestro equipo; en su interior se habrá cifrado cualquier archivo que hayamos introducido y podremos acceder nuevamente a él montando nuevamente la unidad como acabamos de hacer.

Podéis adquirir VeraCrypt en el siguiente enlace:

[1]https://sourceforge.net/projects/veracrypt/

[1] https://sourceforge.net/projects/veracrypt/