Seguridad Informática

Ingeniería en software

Miguel Ángel López Sánchez

Profe: José Francisco Espinosa Garita

"Encriptación"

G-1 VI cuatrimestre

Fecha de Entrega

16/05/2017

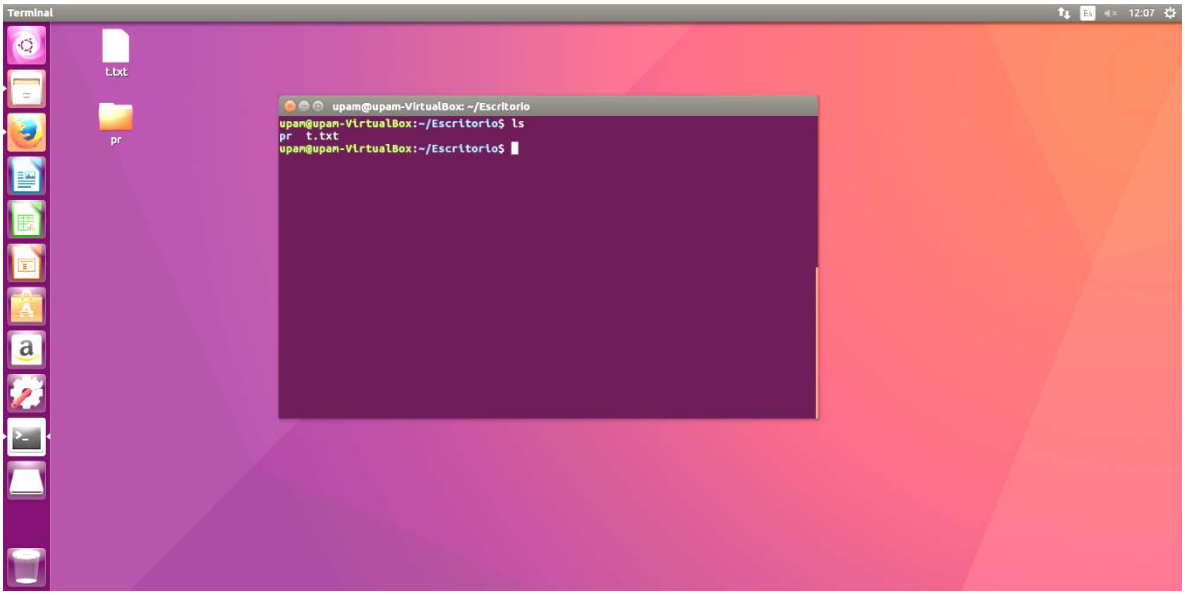
Introducción

Los archivos personales son una parte fundamental de cualquier usuario ya que estos son los únicos que están a nuestra disposición y que no querremos que nadie más vea, pero estos nos están a salvo de hackers maliciosos que se quieran adueñar de estos. Pueden ser tan triviales como música, videos, llegando un poco más allá con fotos personales, cartas, hasta tan importantes como archivos bancarios, información médica, etc.

En esta práctica veremos cómo encriptar estos archivos para que no sean objeto de extorciones ni malos usos de estos. Para ello nos apoyaremos de herramientas de Linux, que es sistema operativo más usado para empresas, por lo tanto, manejando información muy importante.

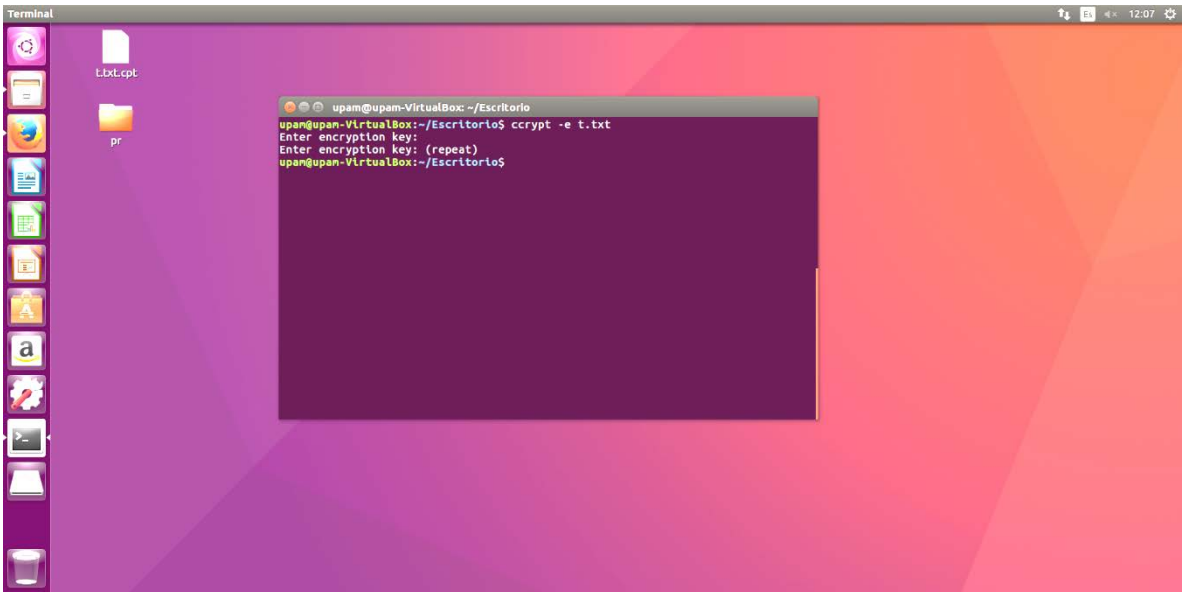
Desarrollo

Lo primero que debemos saber es qué documentos querremos encriptar. Para esta práctica crearemos 1 archivo de texto y una carpeta para encriptar.



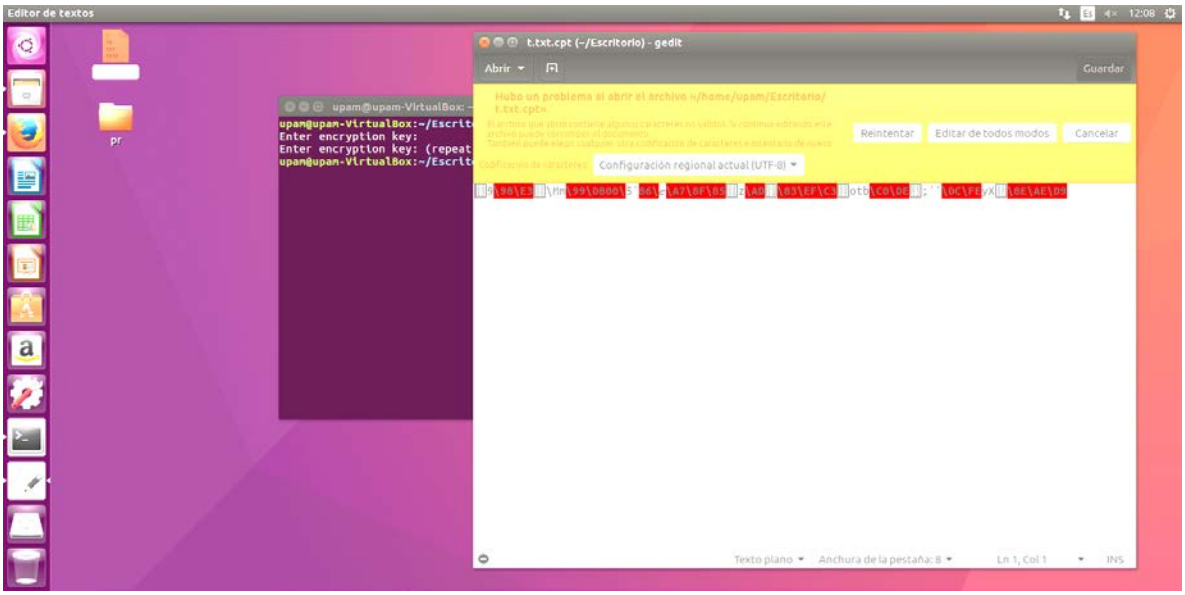
Después debemos usar la herramienta “ccrypto” de Linux, (Si no viene preinstalada podemos obtenerla con el comando “apt-get install ccrypto”).

Primero encriptare el archivo t.txt con el comando: “ccrypto -e t.txt”



Nos pedirá una contraseña para cuando querramos desencriptarlo.

Observamos que el archivo cambio de extensión y si lo quisiéramos abrir nos mostraría el texto encriptado.

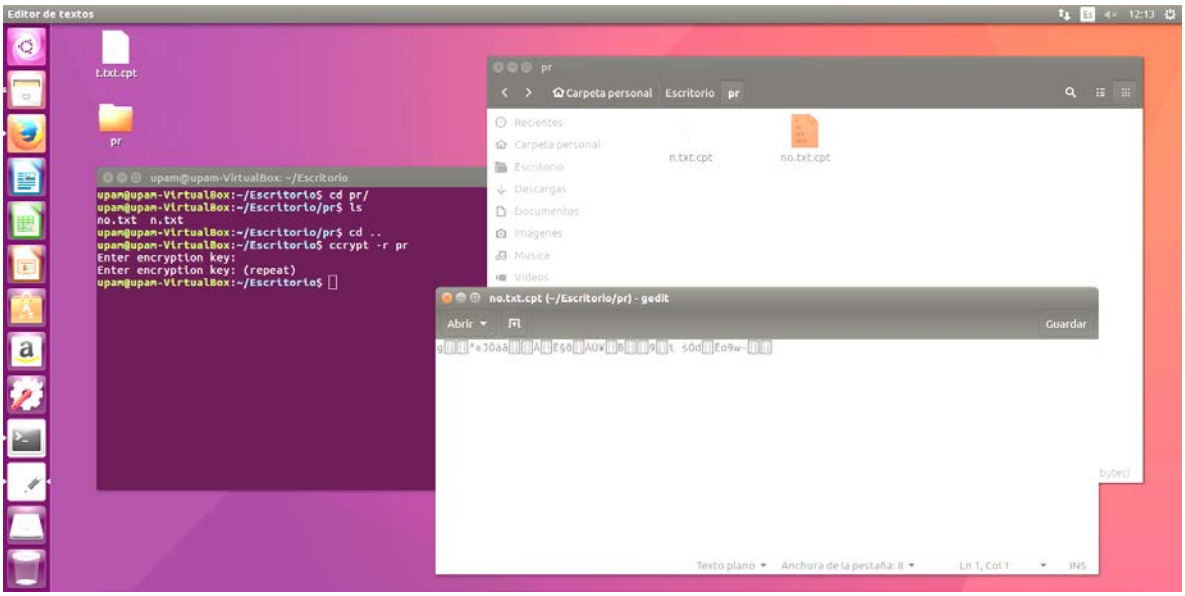


Para desencriptarlo usamos el comando: “ccrypto -d t.txt”

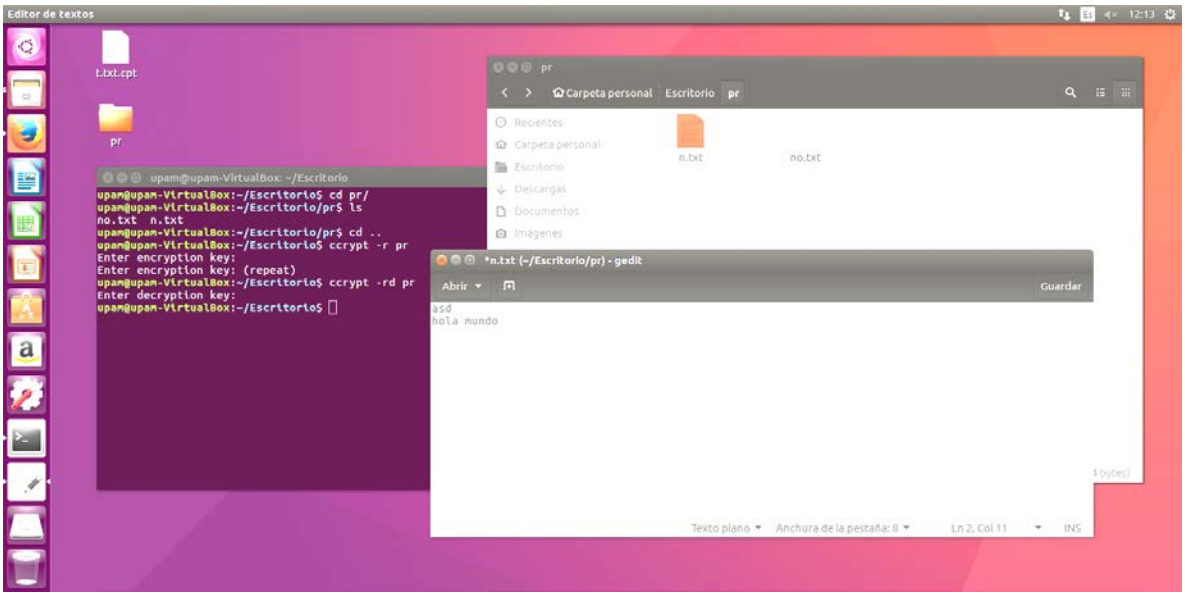
Ahora encriptaremos la carpeta con el comando pr: “ccrypto -r pr”.

La carpeta sigue igual, pero con este método lo que se consigue es encriptar de forma recursiva todos los elementos de cualquier carpeta.

Para el mismo caso, nos pedirá una contraseña para la seguridad.



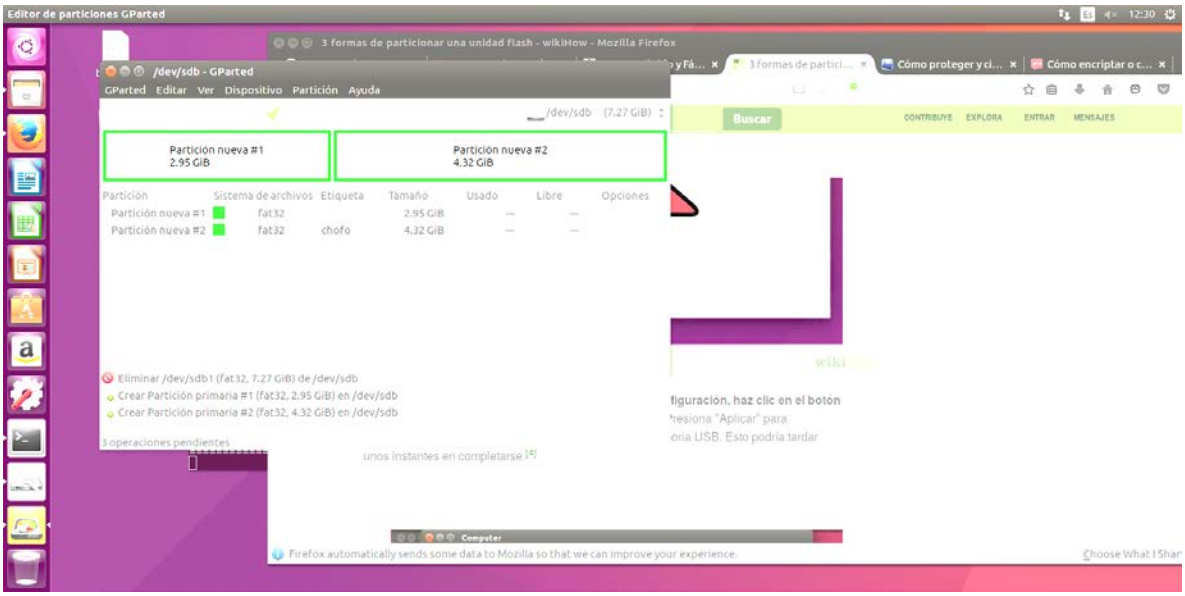
Para desencriptarlo usamos el comando: “ccrypto -rd pr”



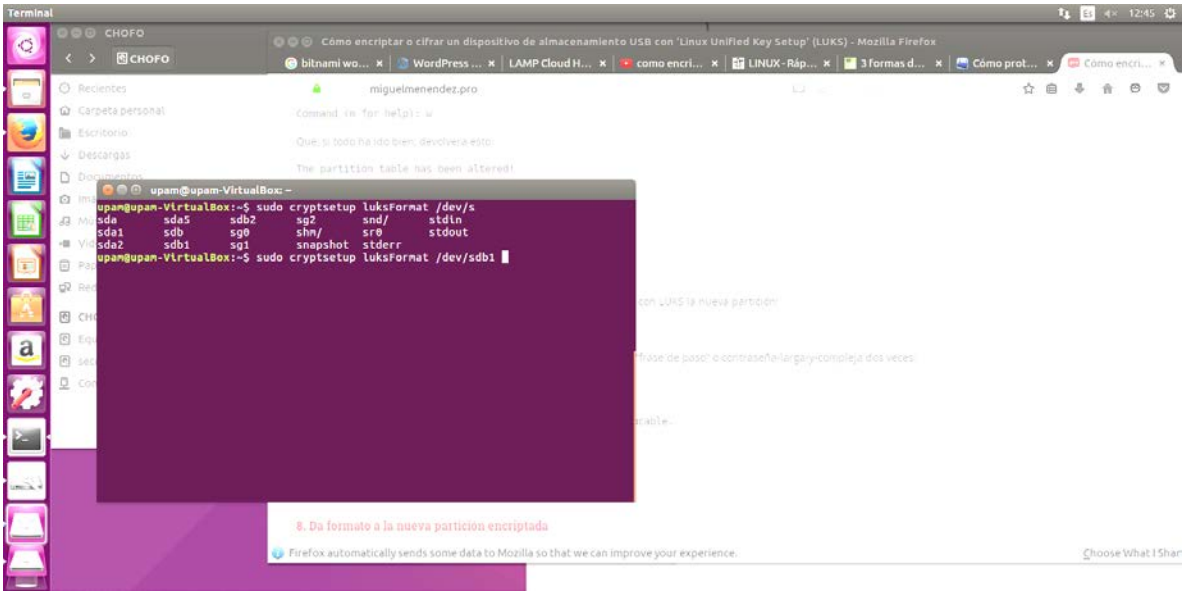
También puede surgir la necesidad de querer proteger un dispositivo drive. Esto sucede a menudo cuando es necesario transportar información valiosa y secreta de un equipo a otro, y se corre el riesgo de perderse o ser robado el USB.

Para ello nos apoyaremos de la herramienta “cryptosetup”, y en esta práctica en particular particionaremos una memoria USB de 8 GB para encriptar solo una partición.

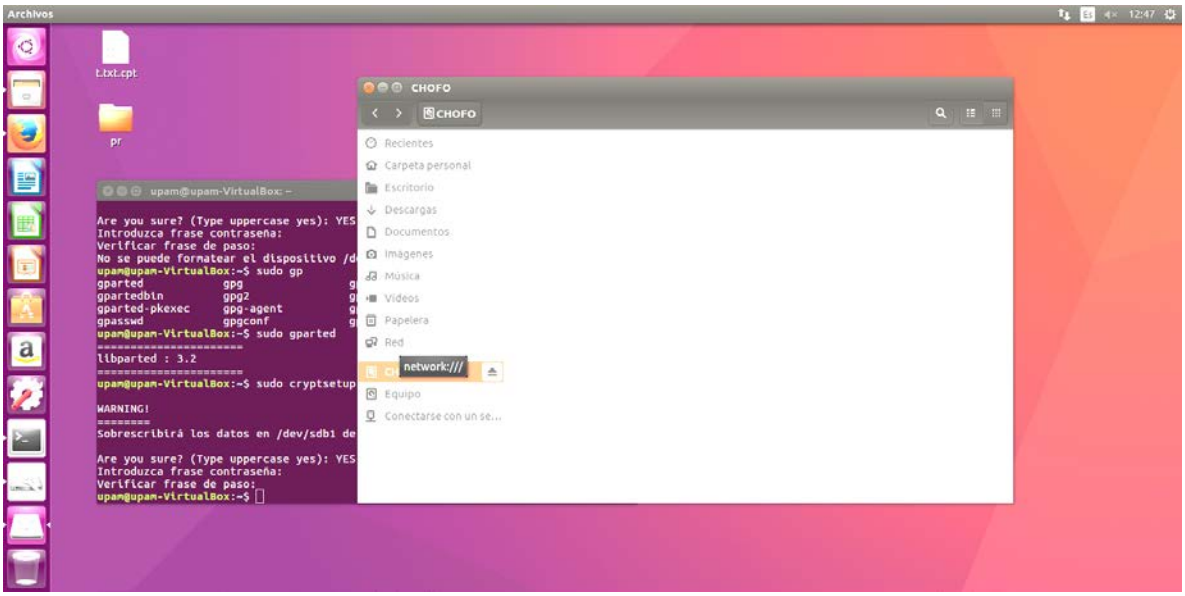
Lo primero que debemos hacer es particionar la memoria en 2 partes.

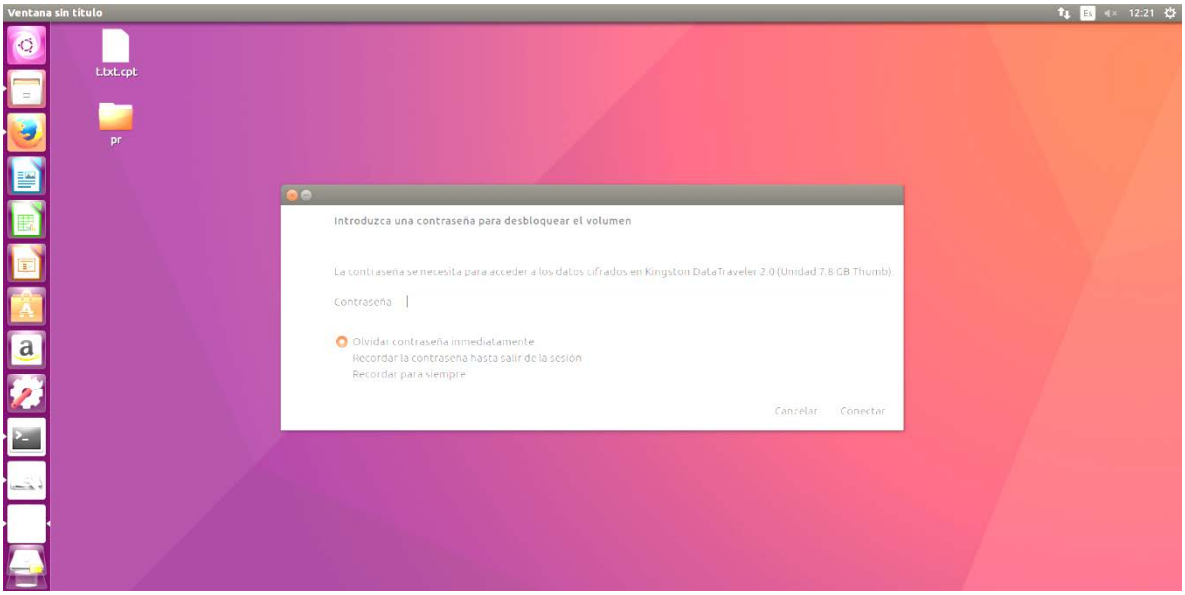


Ahora nos vamos a la terminal y determinamos la partición a encriptar con el comando: “cryptosetup luksformat /dev/<nombre de la partición>”.



De igual manera nos pedirá una contraseña, en nuestro caso será “123” porque solo es una práctica. Así cuando insertemos el pendrive en otro equipo nos aparezca una partición libre y otra con petición de contraseña.





Conclusión

El proteger archivos personales es de suma importancia, mas sobre todo si estos involucran a demás personas y dinero, ya que ciertos hackers maliciosos pueden voltear nuestro mundo de cabeza.

El ataque de robo de archivos personales es más común de lo que se aparenta, y por lo general nos damos cuenta demasiado tarde. Por esto es nuestro deber estar un paso adelante en la seguridad de cualquier archivo y acceso a nuestro equipo.