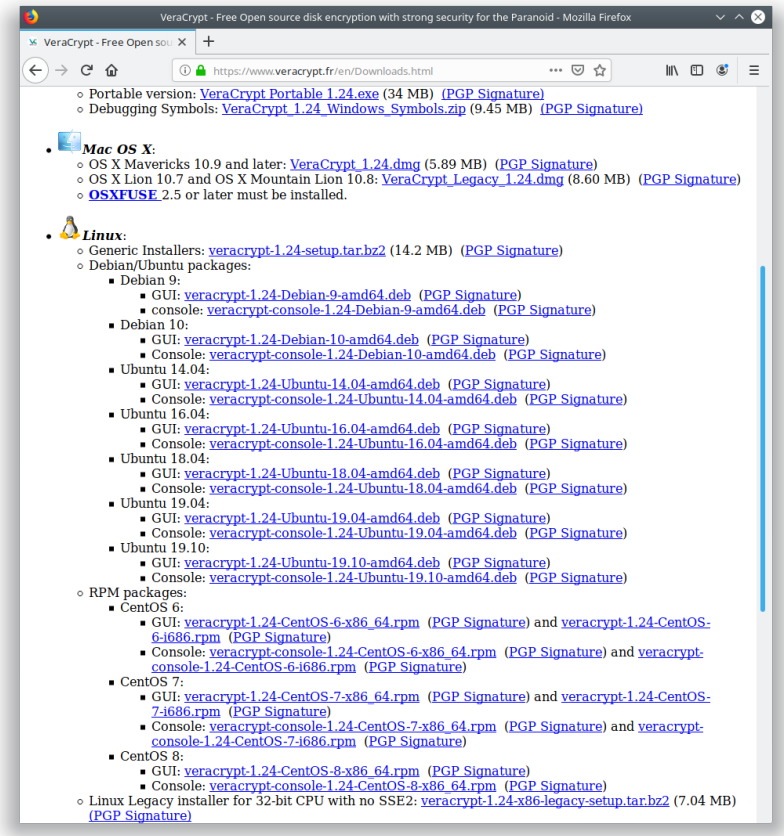
Cifrado de datos y particiones en Windows

TrueCrypt

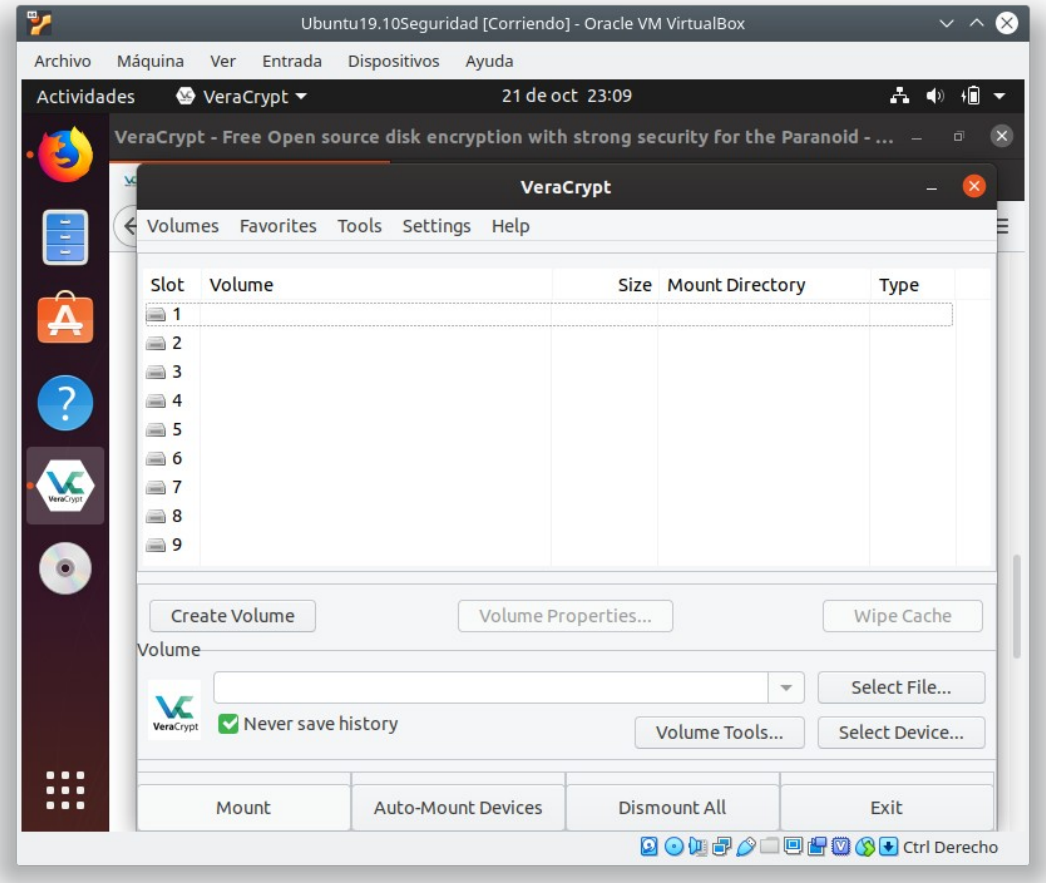
Vamos a probar TrueCrypt como siempre en Linux si es posible como recientemente ha salido la ultima de Ubuntu 19.10. Lo voy a probar y de paso realizo las practicas con ella. Mientras instalaba me he fijado en que existe:

Solo lo digo por documentar un poco mas las practicas.
El primer enlace no encotre nada referente en Linux asi que seguire en VeraCrypt, que tiene hasta el paquete .deb con la ultima version de Ubuntu.



Cifrado de datos y particiones en Windows

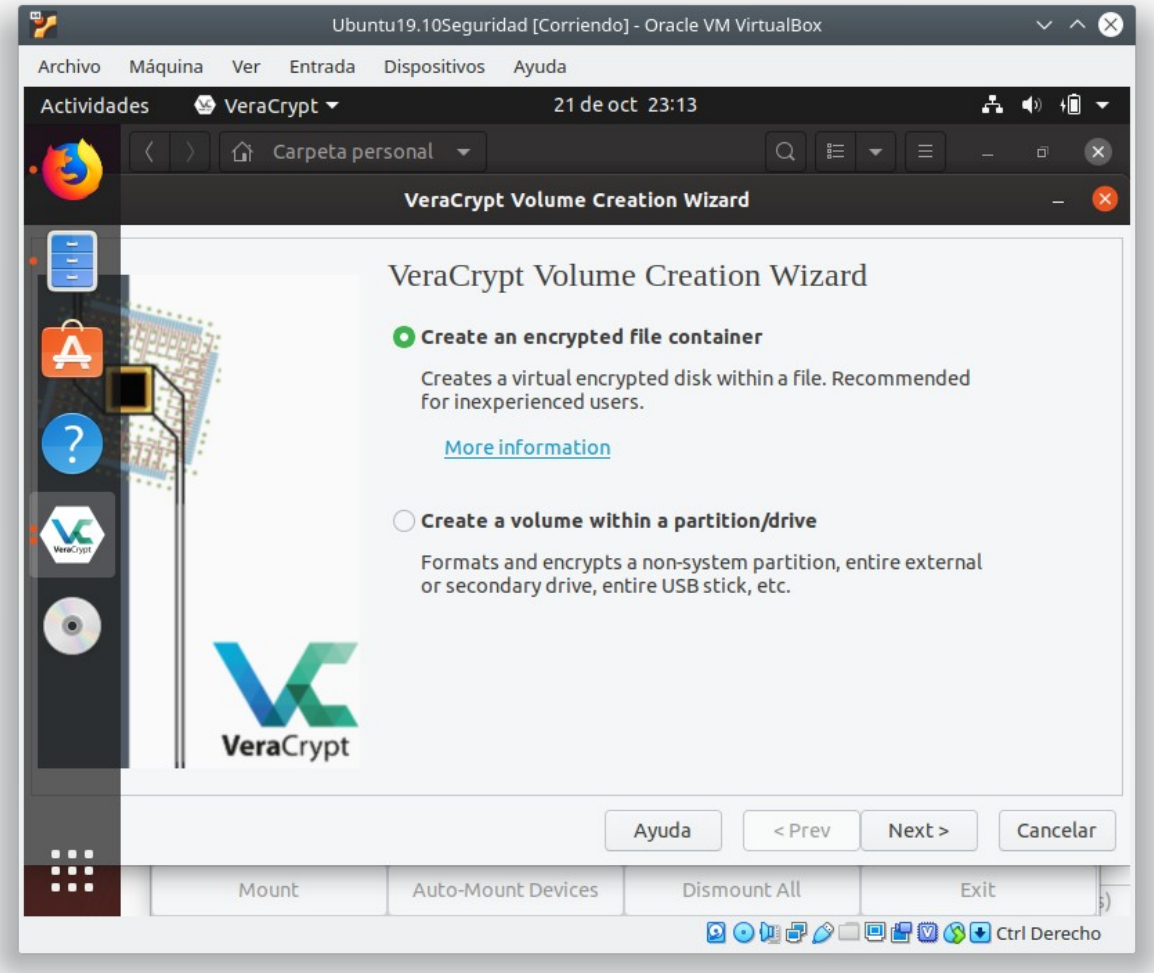
La instalación no la voy añadir seguiré una vez lo tenga instalado y aquí esta.



Como se puede apreciar es muy similar al de la practica.

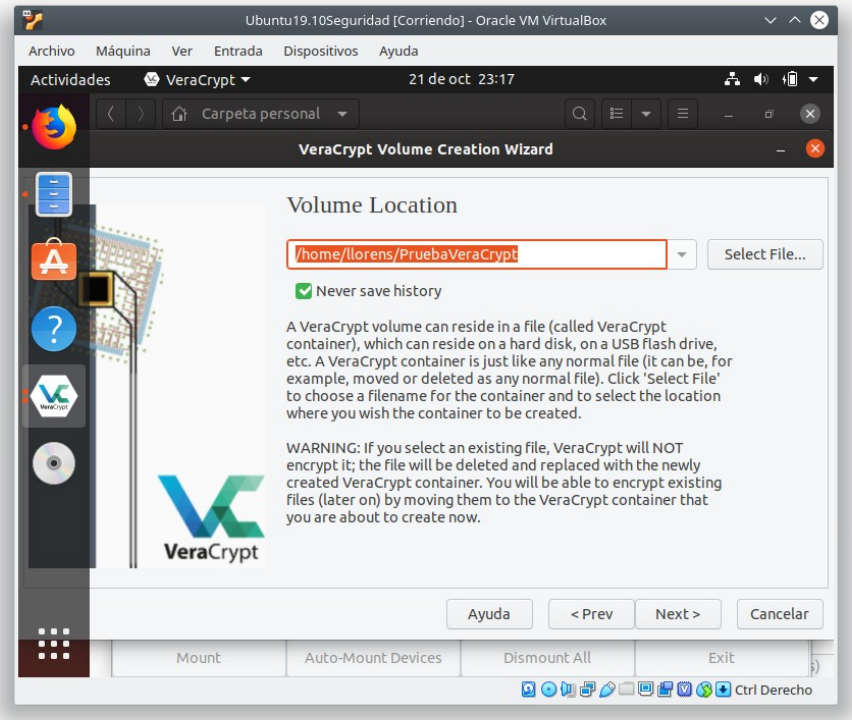
Cifrado de datos y particiones en Windows

Primeramente nos pregunta si quieres crear un archivo contenedor o un partición entera tipo discoduro externo o memoria usb. En este caso seleccionare la primera opción.

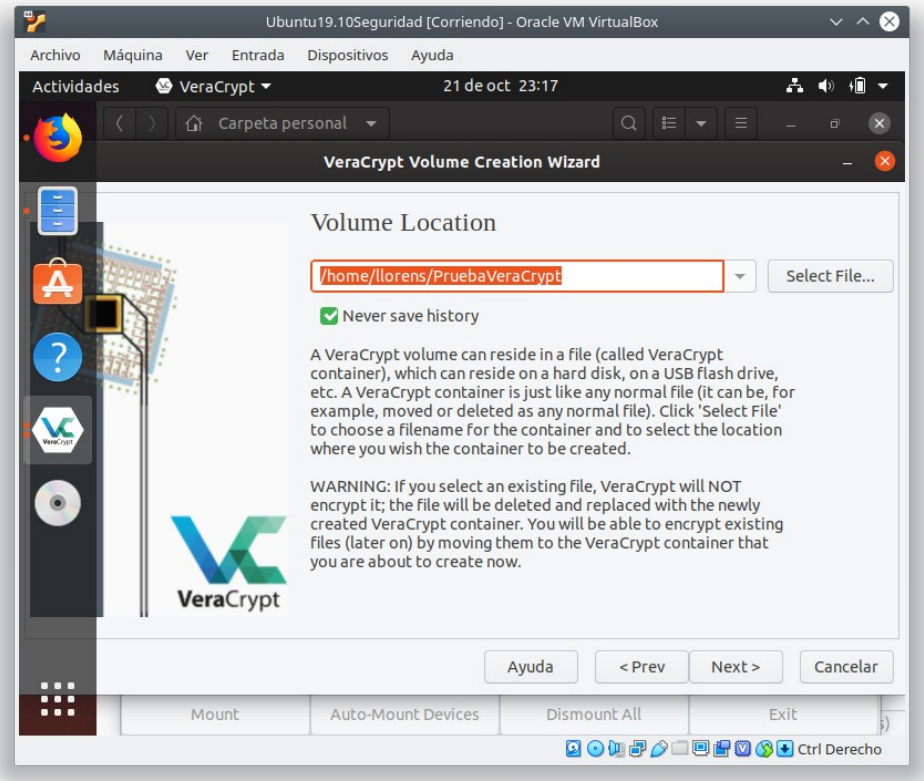


Cifrado de datos y particiones en Windows

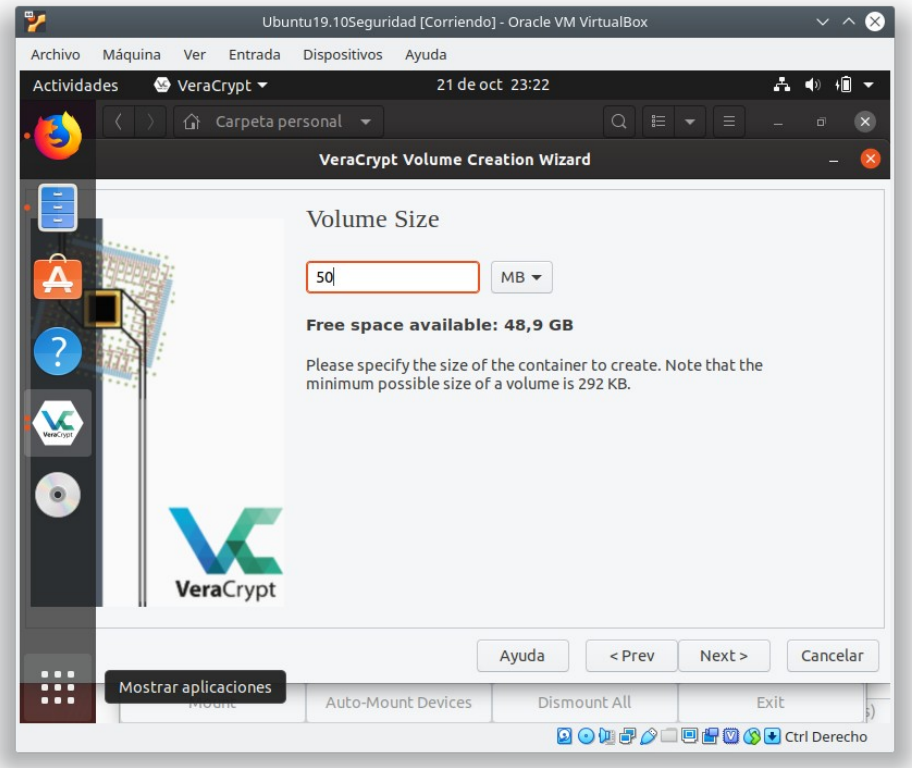
Seleccionamos la ubicación en este caso en mi home



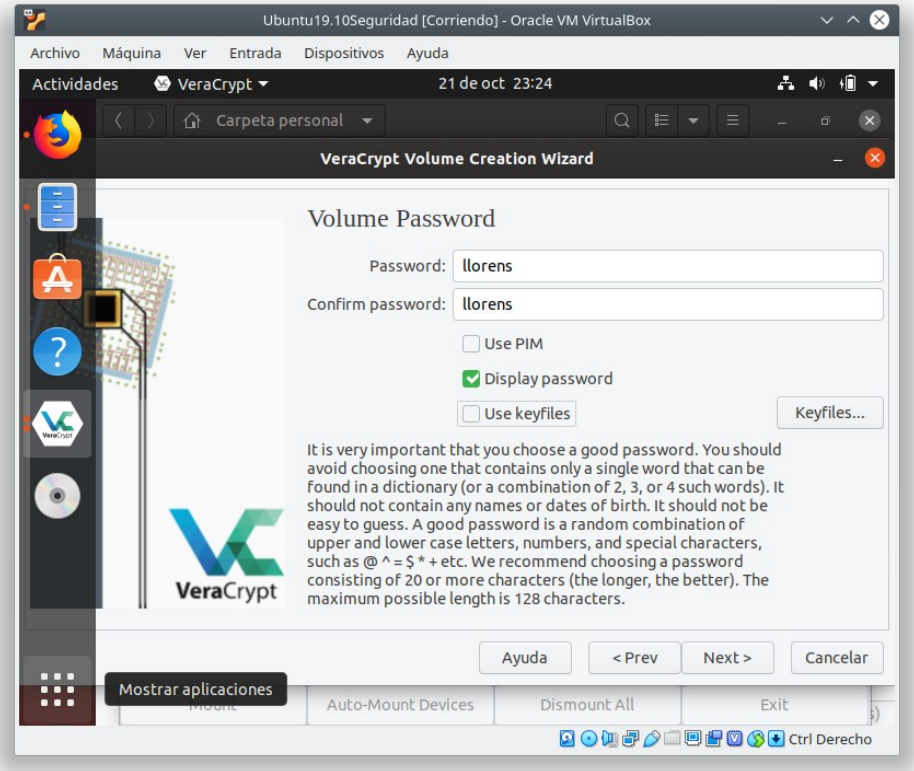
Seguidamente nos aparece los tipos de encriptacion que estan disponibles con una breve descripción, benchmark, etc.



Después elegiremos el tamaño del volumen que queremos crear.

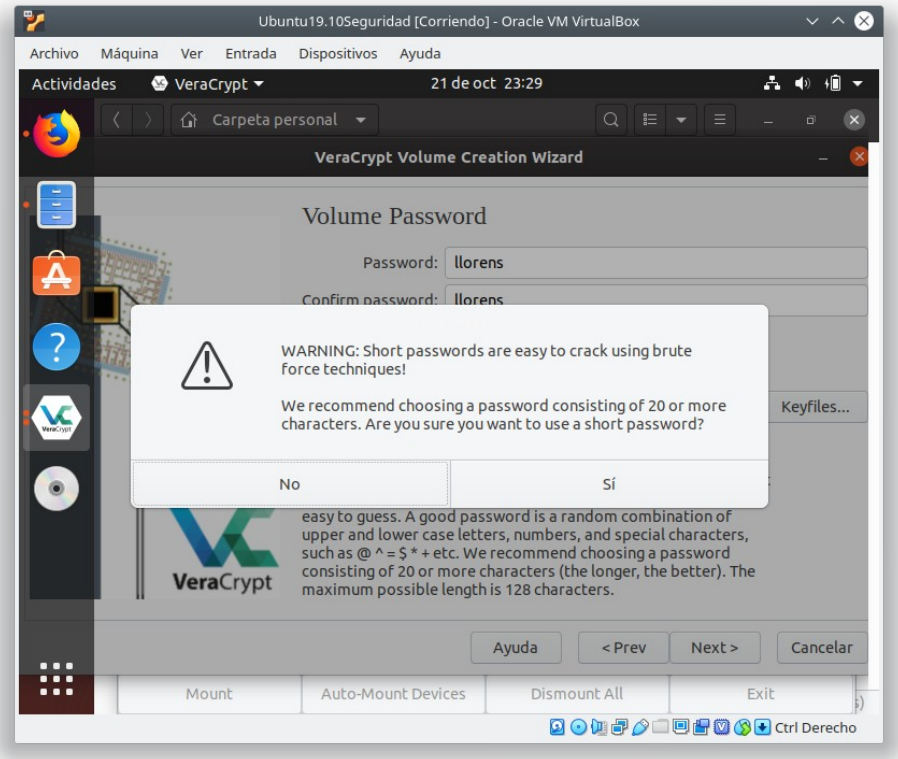


Introducimos la contraseña

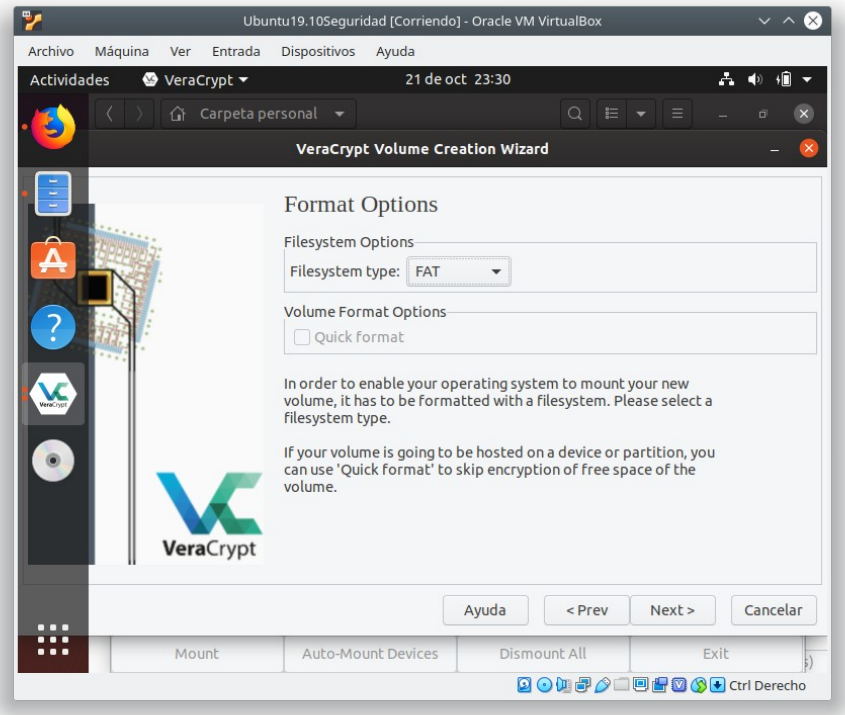


Cifrado de datos y particiones en Windows

Al ser una contraseña muy fácil te recomienda unos cuantos consejos para que sea mas dificil de descifrar con fuerza bruta.

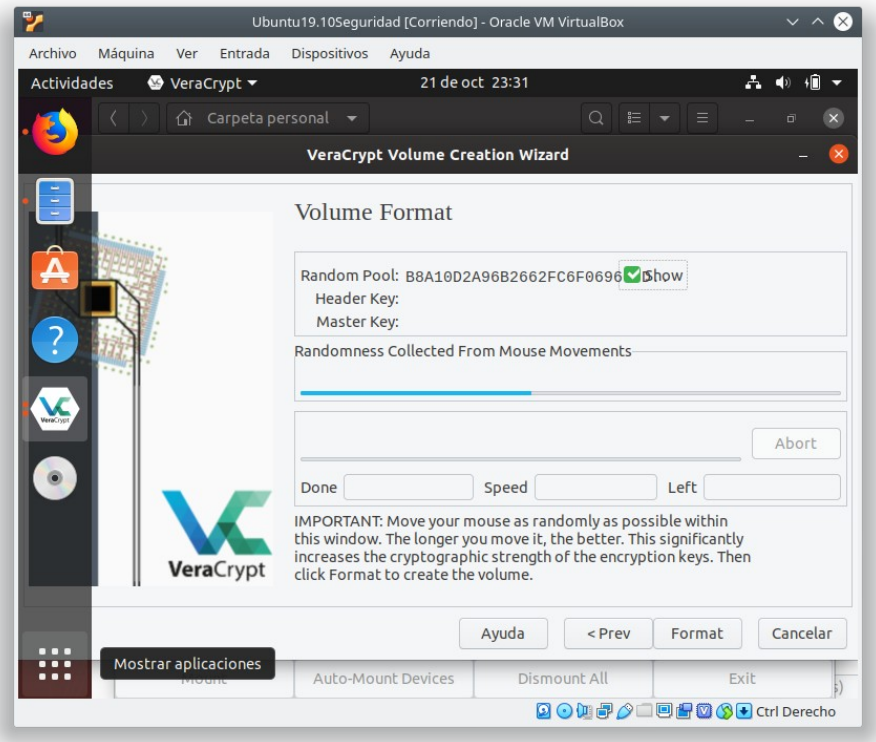


Seleccionamos que formato tendrá la unidad o volumen.

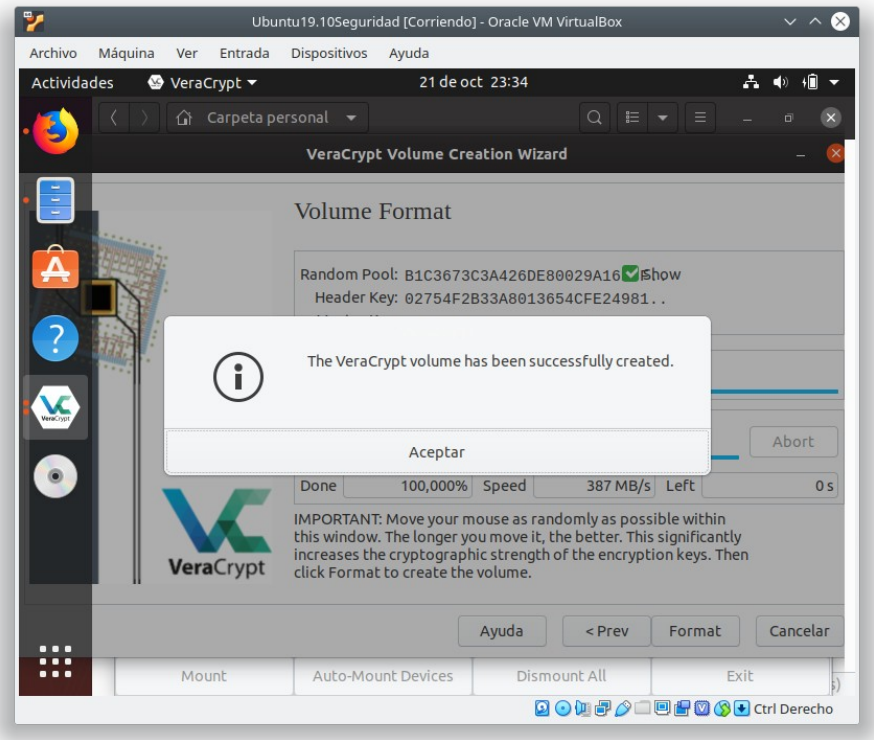


Cifrado de datos y particiones en Windows

Después de mover el ratón para recolectar el movimiento y seguir algún patrón después de rellenar la barra le pulsamos a formatear.

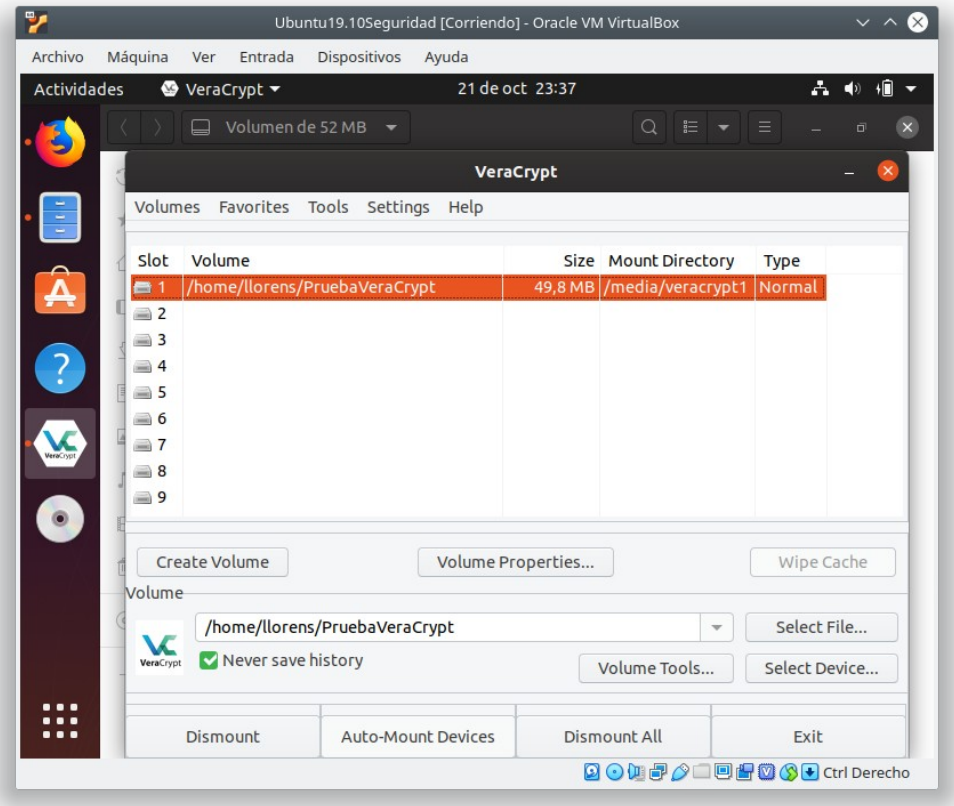


La tendremos lista.

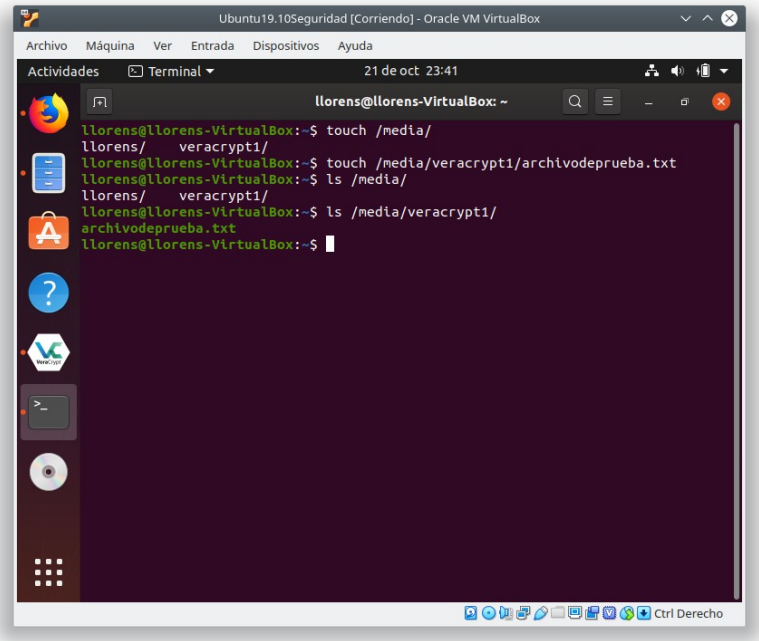


Cifrado de datos y particiones en Windows

Una vez realizado probaremos de montarlo



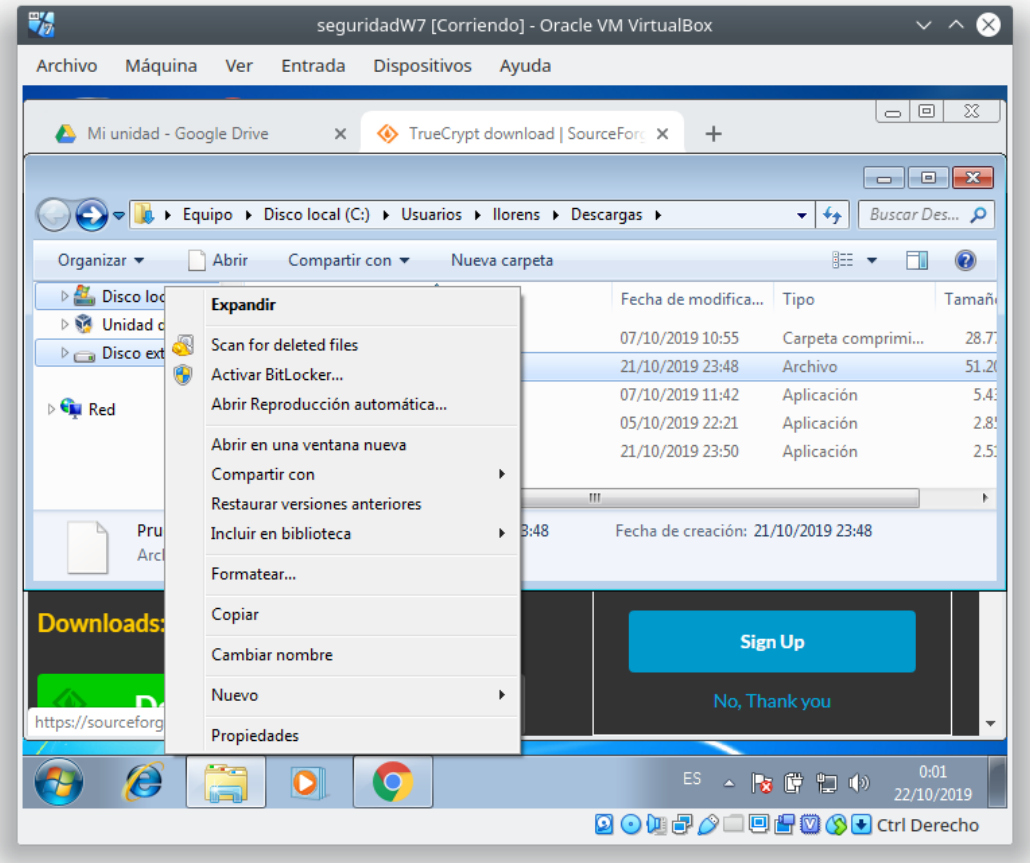
Y una vez montado se comportara como una unidad mas. Pese a estar en mi /home /llorens estará montado en /media/ veracrypt1. Como ejemplo pongamos un archivo con touch



Cifrado de datos y particiones en Windows

BitLocker

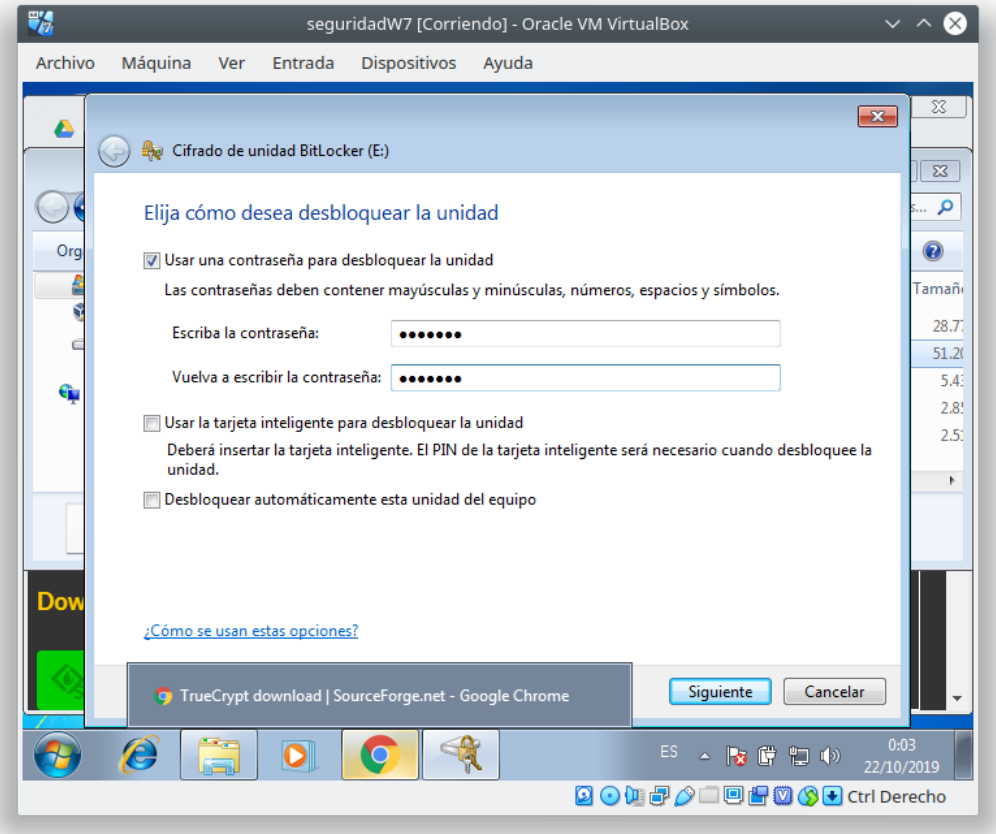
Para esta practica vamos a encriptar un discoduro externo de 50 Gb que incorpora la maquina de Windows.



Tan sencillo como pulsar sobre la unidad el botón derecho y seleccionar Activar Bitlocker.

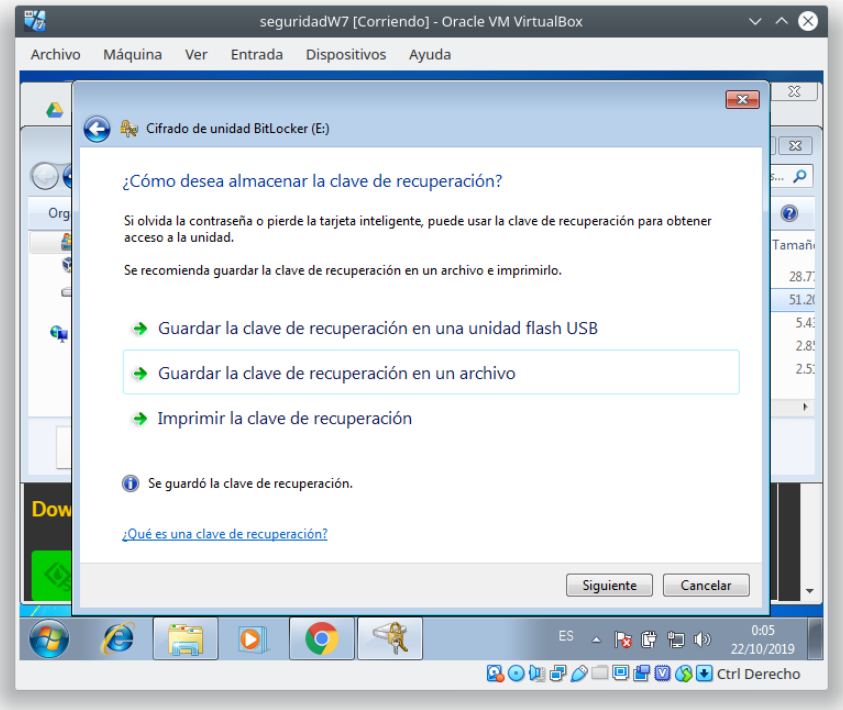
Cifrado de datos y particiones en Windows

Nos solicitara una contraseña

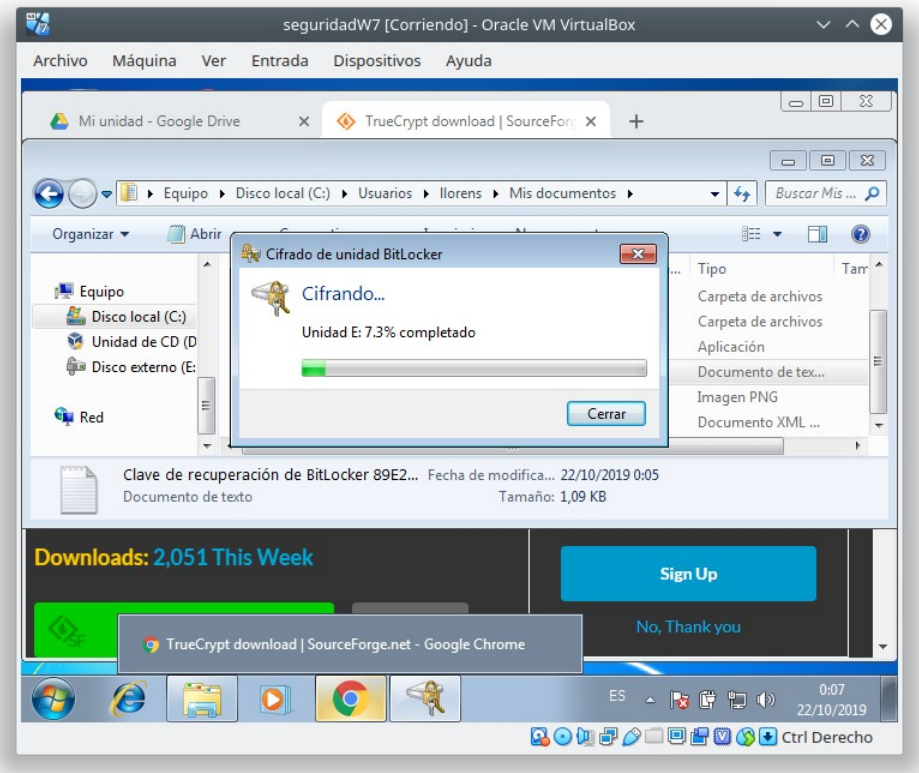


Cifrado de datos y particiones en Windows

Seguidamente nos pregunta donde deseas alamacenar la clave de recuperacion. Lo he guardado en un documento.

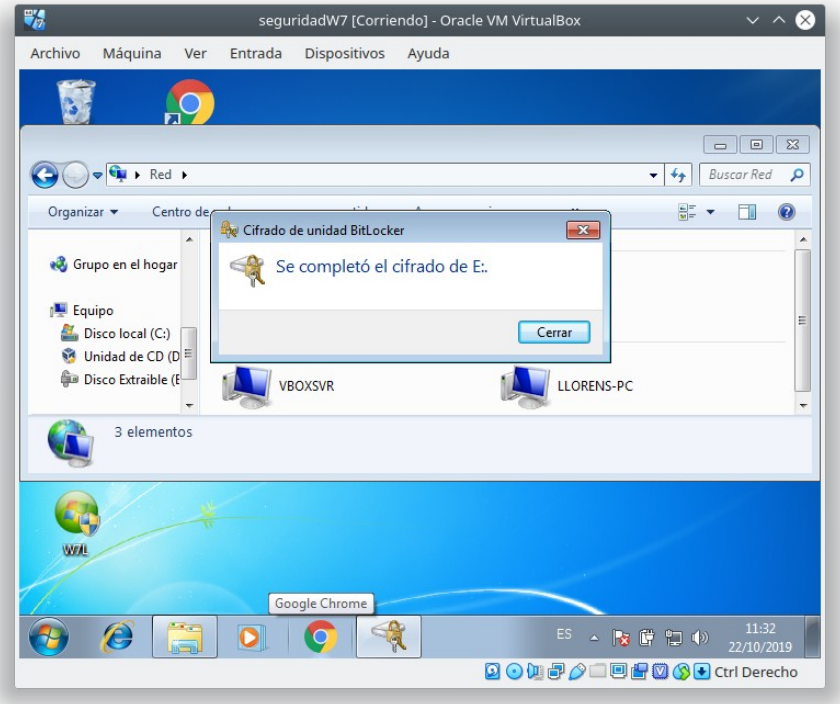


Empieza el cifrado



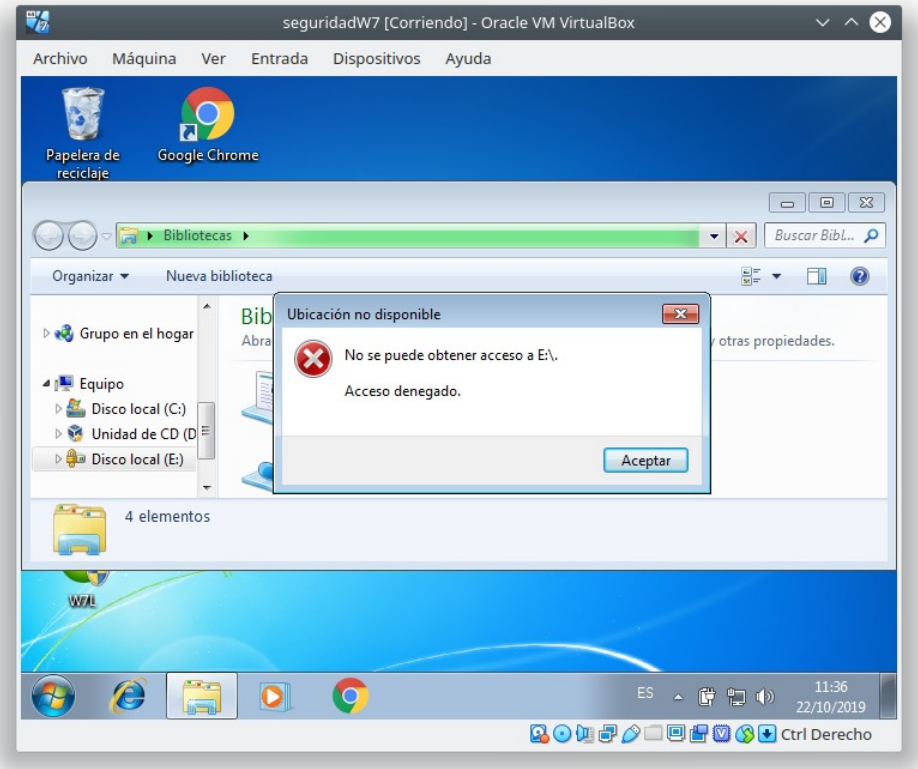
Cifrado de datos y particiones en Windows

Hasta que finalice.



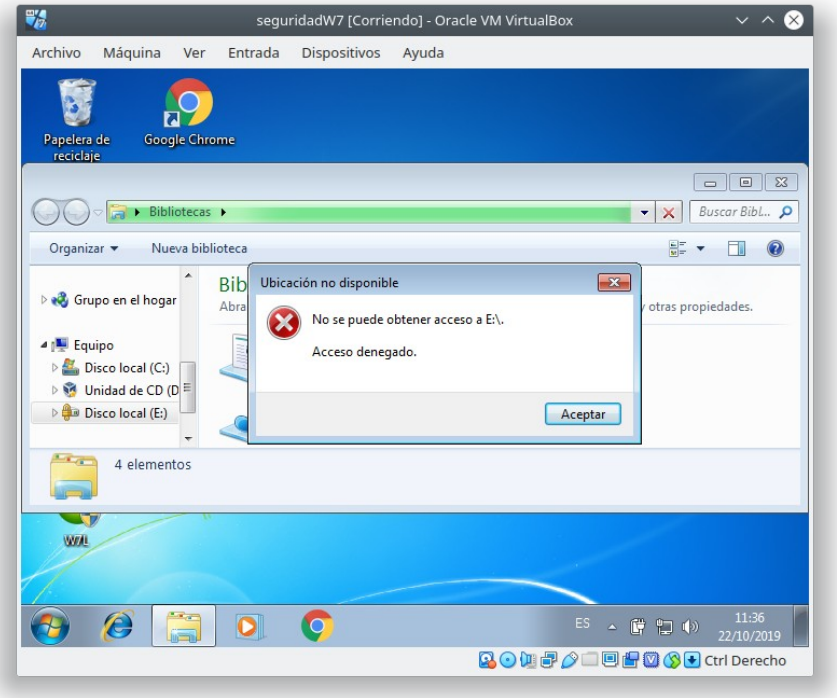
Cifrado de datos y particiones en Windows

Ahora cada vez que reiniciemos no nos permite acceder a esta unidad si no lo configuramos previamente.

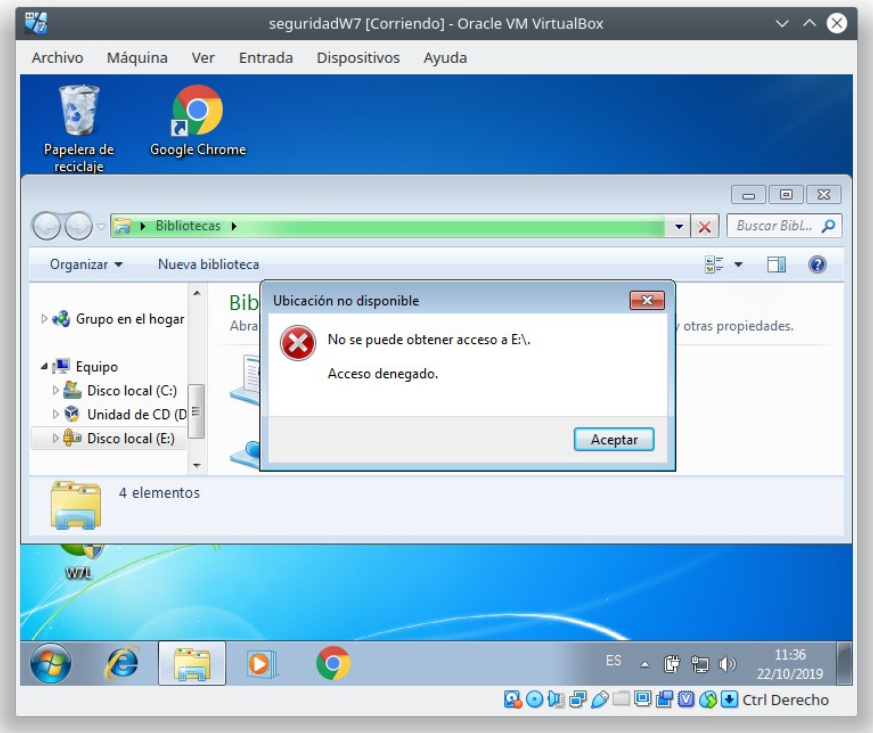


Cifrado de datos y particiones en Windows

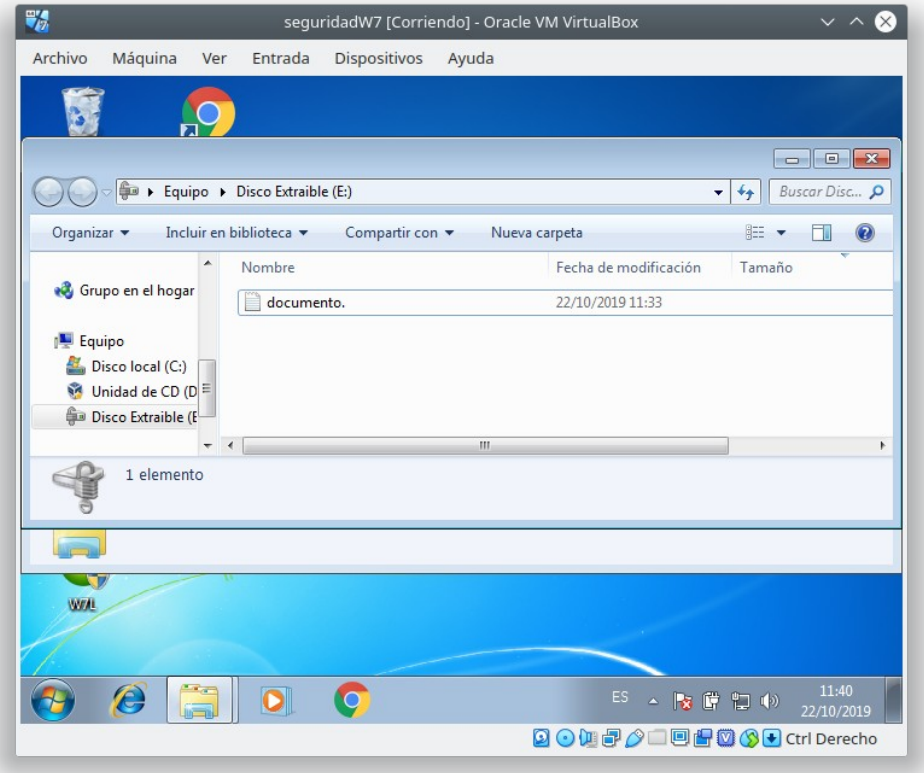
Pulsamos boton derecho sobre la unidad y seleccionamos “Desbloquear unidad”



Nos solicita la contraseña y si deseamos que esta se desbloquee automaticamente cada vez que inicies el sistema.



Y ya la tendremos otra vez operativa.



Consejos para donde se podría utilizar un cifrado de datos.
-Tu imaginate que tenemos un almacenamiento ilimitado en una cuenta de Google Drive. Y al ser corporativo no sabes si algún administrador o tercera persona tiene acceso a esta información . Pues la encriptacion en un método infalible para que no te detecten lo que estas almacenando. Podrías alojar infinidad de documentos e información teniéndolo a buen recaudo con algunos métodos anteriores. Seguro no hay nada, pero ya nos aseguramos de que por lo menos no saben lo que has guardado ahí.

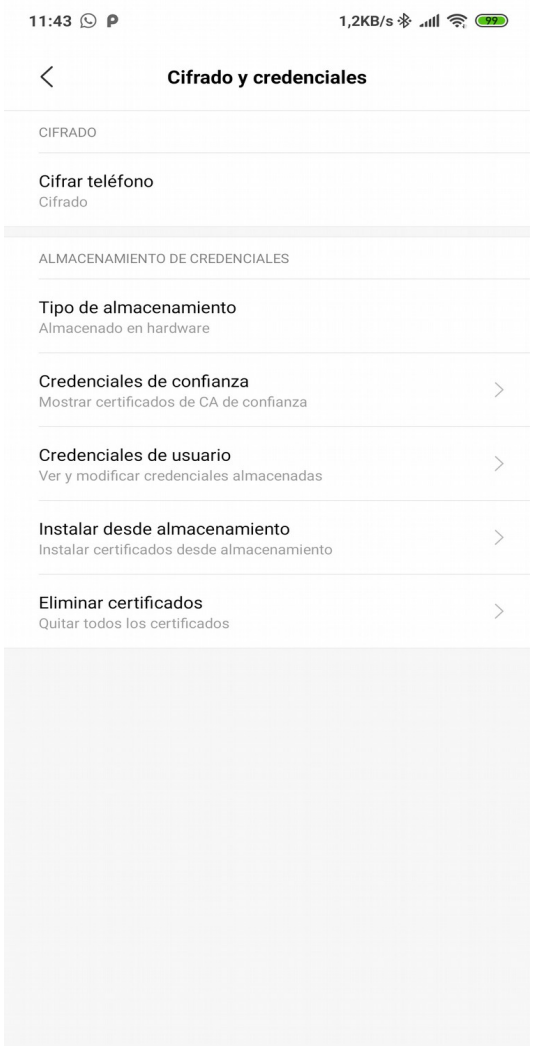
- Una memoria USB
Actualmente ya se están quedando un poco en desuso ya que los servicios cloud como Google Drive, Dropbox, Mega, etc. Te permite tener en cualquier pc o dispositivo con Internet tener acceso a lo que tengas almacenado.
Pero bueno, decides tener o pasar un pen USB a un amigo y esta información es importante que contiene información y datos personales, fotos, etc. Una buena costumbre seria encriptar la información y así en caso de perdida nos nos preocuparíamos de que cayese en terceras manos.

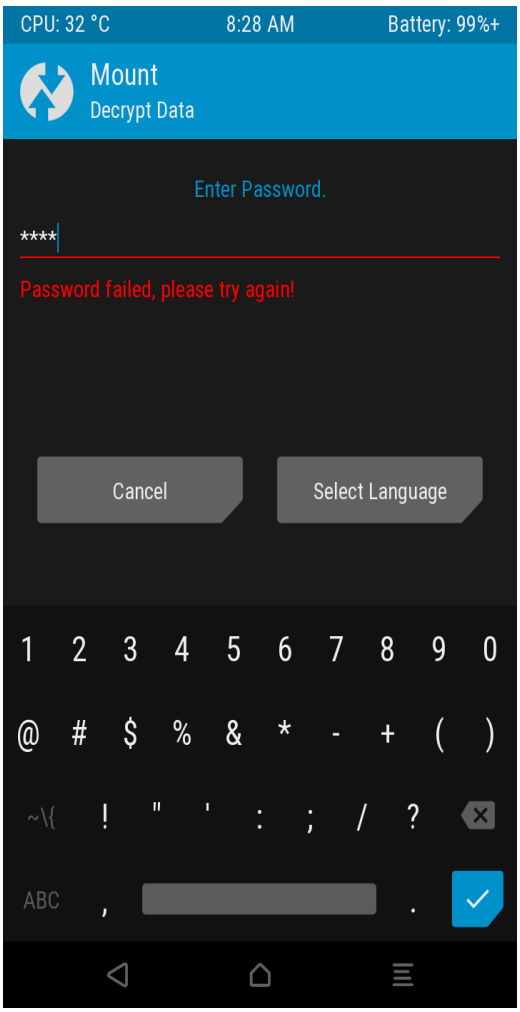
Cifrado de datos y particiones en Windows

-Dispositivos móviles

En equipos portátiles se aconseja su encriptación y en móviles Android desde hace unas versiones que se encripta toda la memoria

Aporto capturas.





Cifrado de datos y particiones en Windows

La primera es desde el sistema y la segunda aunque no es seguro desbloquear el bootloader del móvil, es necesario para poder ser root. Como se aprecia el recovery personalizado requiere siempre una contraseña por que el almacenamiento esta encriptado si no los datos aparecen como la tercera captura totalmente irreconocibles.