

Bastionado de redes y sistemas

Unidad 1. Actividad 1



5 de octubre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Fases de seguridad de un ordenador 2](#_Toc147421032)

[Fase 1 2](#_Toc147421033)

[Fase 2 3](#_Toc147421034)

[Fase 3 3](#_Toc147421035)

[Fase 4 3](#_Toc147421036)

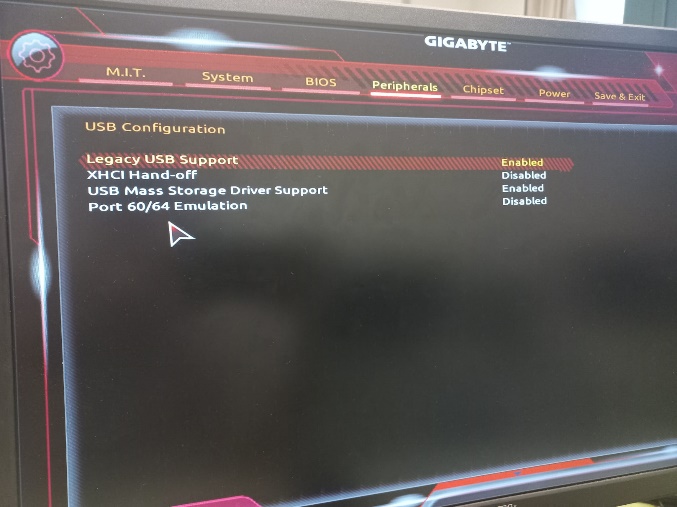
Configuración de Windows y Linux para definir su seguridad.

Seguridad física BIOS / UEFI

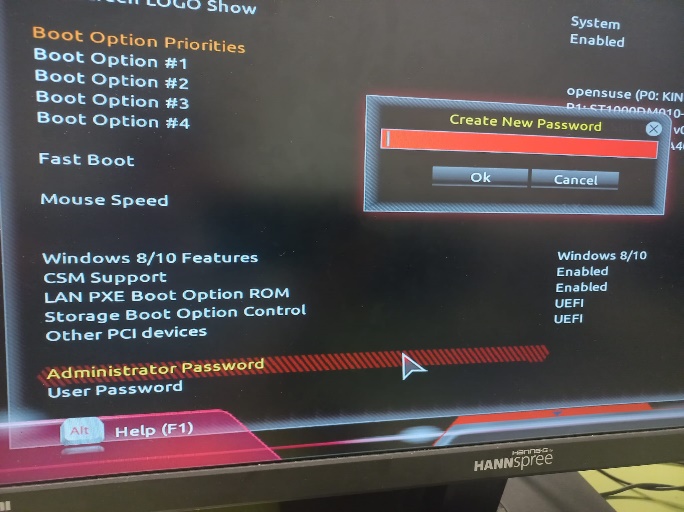
**1 BIOS – poner una contraseña en la BIOS – prohibición de uso USB – Como bloquear el arranque en red.**

Estas imágenes han salido de los ordenadores de clase y la imagen se ha realizado desde mi móvil. La BIOS de estos ordenadores funciona pulsando ‘supr’ al encender el ordenador.

Esta imagen es la que nos muestra en la BIOS como se puede prohibir el uso de USB.



En esta imagen podemos cambiar la contraseña de usuario o administrador.



Desde esta opción podemos desactivar o bloquear la opción de arranque en red.



Sería conveniente que la caja del ordenador este sellada para poder tener mayor seguridad. Ya que si alguien quita la pila que da energía al chip de la BIOS este se desconfigurará.

# Seguridad a nivel de datos

# Fase 2

Sistema de arranque – GRUB2 decide qué sistema operativo quieres arrancar (necesitas una partición)

\*Mirar los apuntes del año pasado\*

# Fase 3

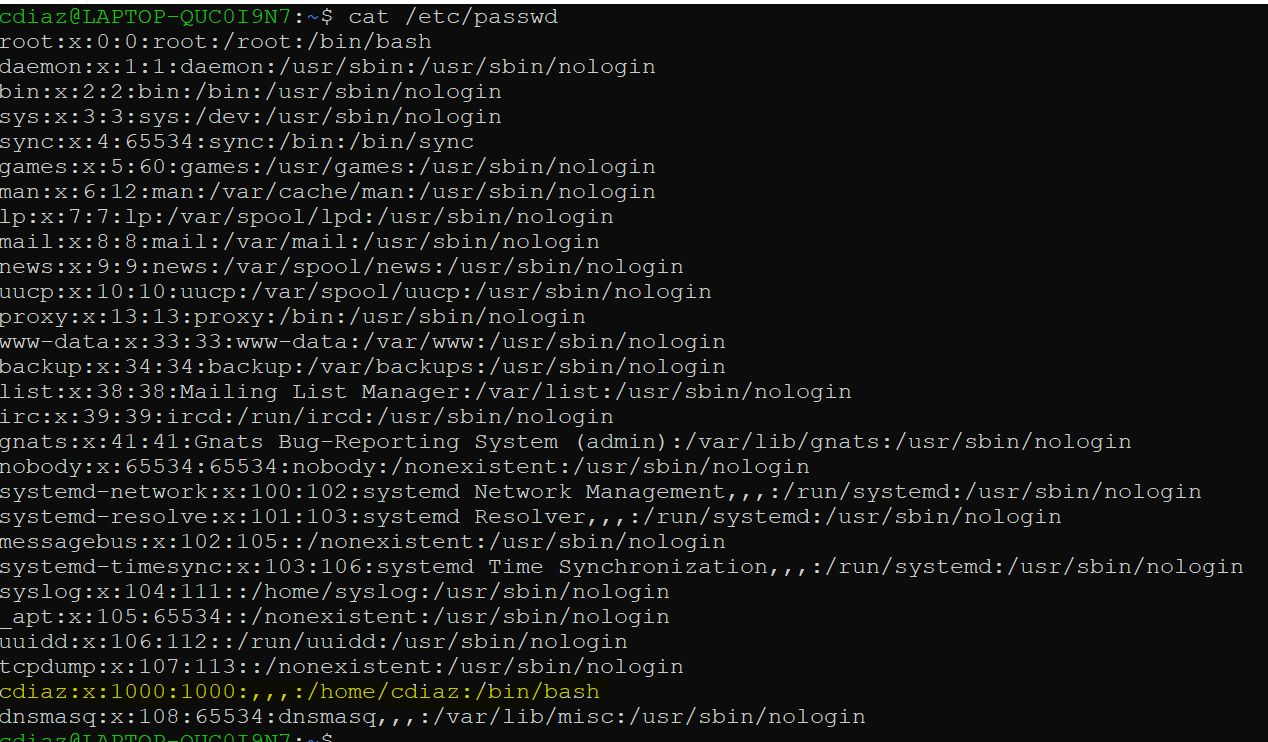
Usuario y contraseña

En Windows se puede ver que al instalarlo te crea más usuarios por defecto.

**Riesgo** que nuestro usuario este como administrado

**Medida** Podemos hacer que nuestro usuario no pueda cambiar la contraseña.

En Linux poniendo el comando cat /etc/passwd te mostrara los usuarios que tienes creado



# Fase 4

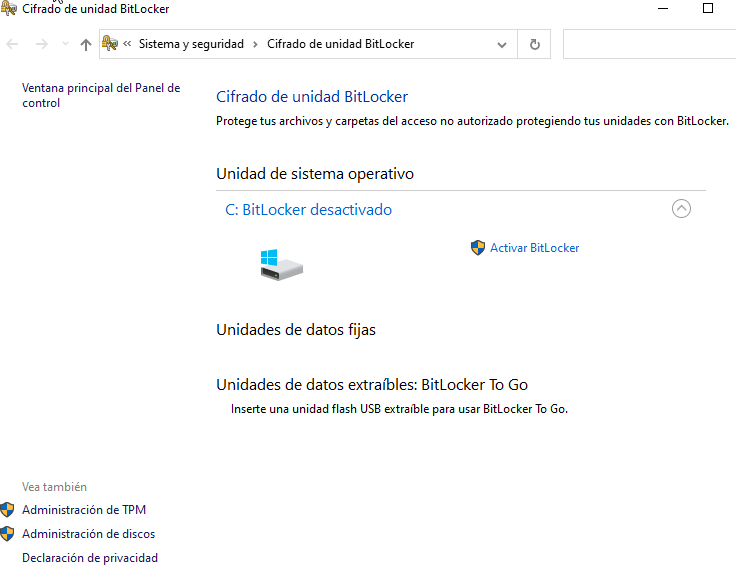
Datos – encriptación

Datos podemos dividirlo en particiones: Windows que lo dividimos en Bitlocker y TrueGrypt (investigar sirve para recuperar datos)

**Bitlocker**

BitLocker es una característica de cifrado de disco completo incluida en ciertas versiones del sistema operativo Windows. Está diseñado para proteger los datos almacenados en el disco duro de una computadora u otros dispositivos de almacenamiento mediante la encriptación de todo el disco, lo que lo hace ilegible sin la clave de cifrado o la contraseña correcta.

En Windows 10 Pro ya esta Bitlocker instalado, simplemente tenemos que activarlo:



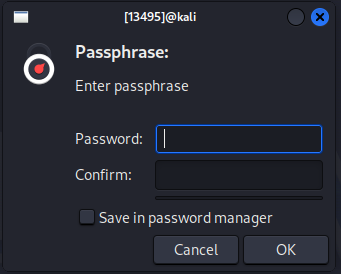
**GPG**

En Linux podemos utilizar gpg

Nos creamos un archivo con el comando touch borrar.txt, despues comprobamos que hemos creado el archivo:

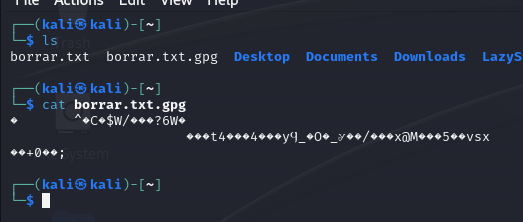


Nos pedirá una clave que debe de ser un poco complicada para que sea aceptada.



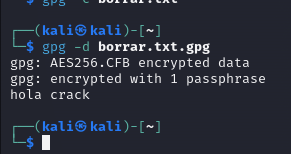
La contraseña es kali123!

Para comprobar que funciona volvemos a mirar el directorio y vemos que nos sale un .gpg, despues intentamos mirar que hay dentro del fichero:



Como vemos es imposible que veamos lo que hay dentro del fichero.

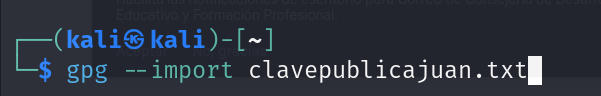
Para poder desencriptar el fichero tenemos que usar el comando gpg -d :



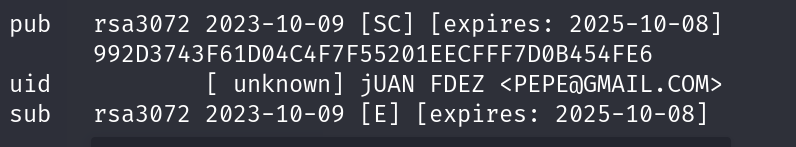
Como vemos aquí está el mensaje que está dentro del archivo.

Ahora vamos descargarnos las claves publicas de algunos compañeros y vamos a elegir uno que nos envíe su archivo gpg y otro que no.

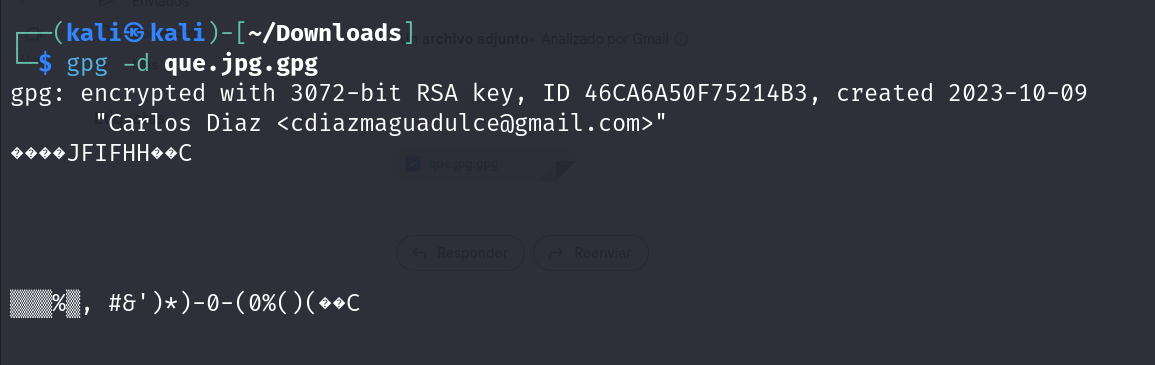
En mi caso me he descargado la clave pública de Juan Manuel. Lo primero que hacemos es añadir la clave a nuestro anillo:



Comprobamos que lo tenemos:



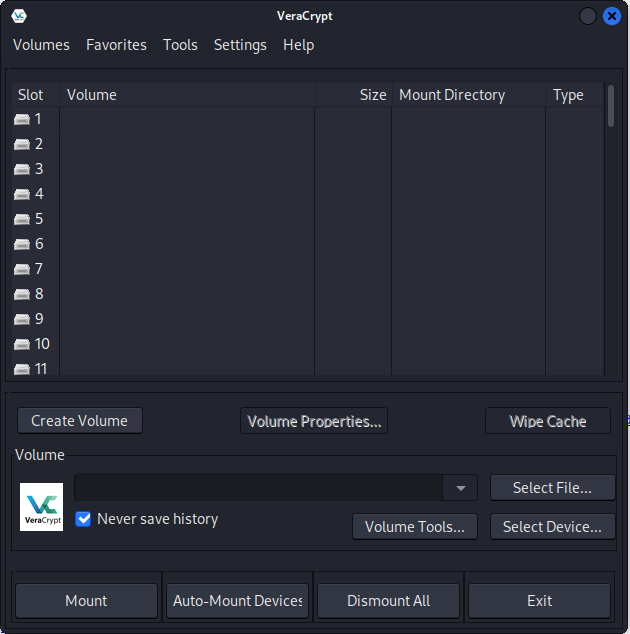
Ahora usamos el comando gpg -d :



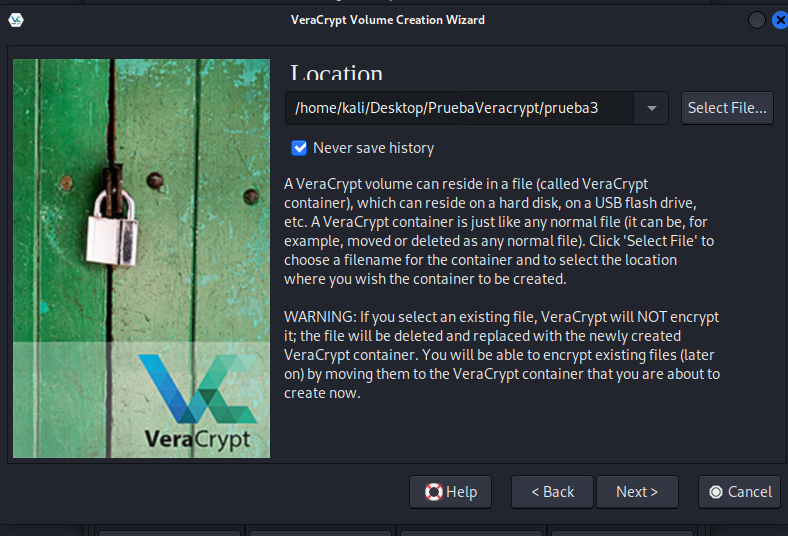
Como vemos ya está desencriptado (no se ve ningún mensaje porque es una foto).

**Veracrypt**

Lo primero que hay que hacer es descargar Veracrypt. (Dejo un enlace de la guía que he usado para instalarlo <https://www.solvetic.com/tutoriales/article/8440-como-instalar-veracrypt-en-kali-linux/> ):



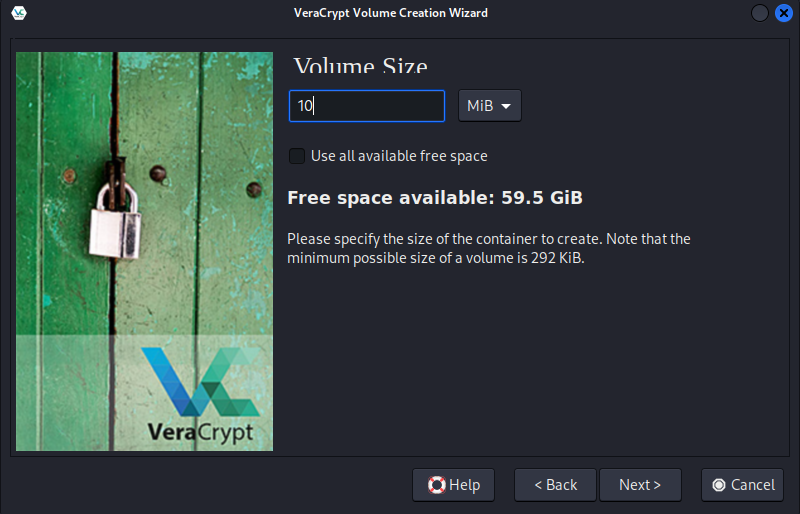
Lo primero que vamos a hacer es crear un volumen. Y vamos a seleccionar donde lo queremos tener:



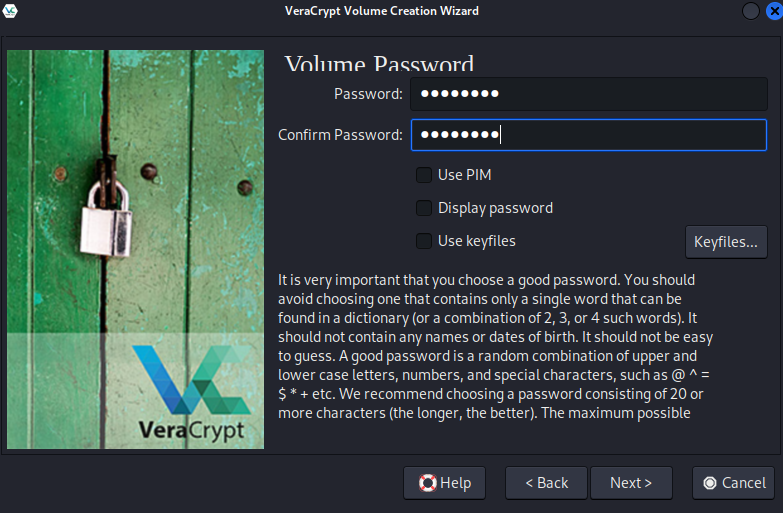
Ahora podemos elegir el tipo de algoritmo de encriptación que queremos



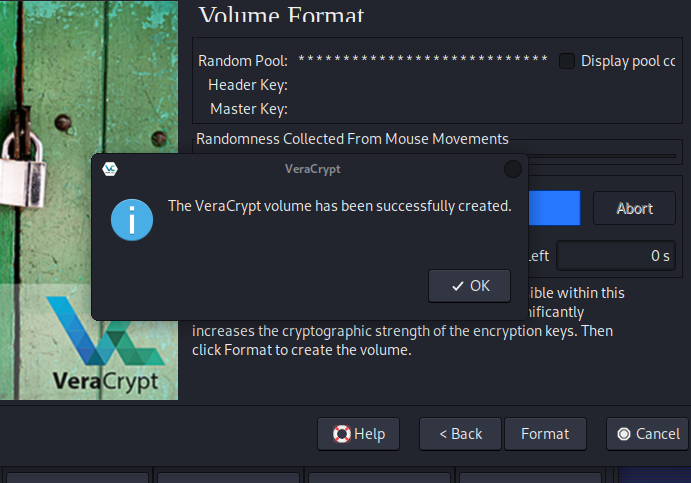
Ahora se elige el tamaño del volumen que queremos:



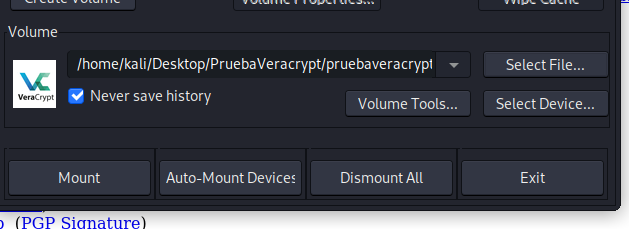
Por último se elige la contraseña (en mi caso he puesto kali123!):



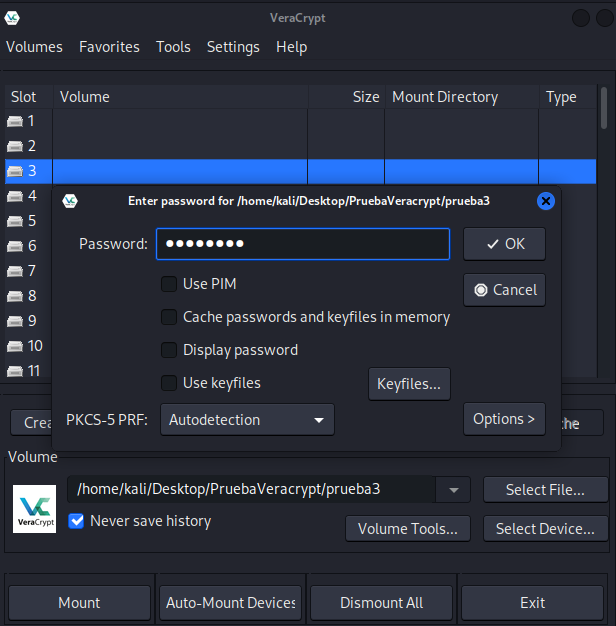
Y ahora nos saldría un mensaje confirmando que ha sido creado con éxito:



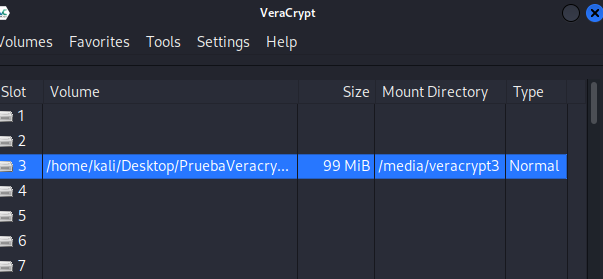
Ahora vamos a seleccionar el archivo de prueba que nos hemos creado:



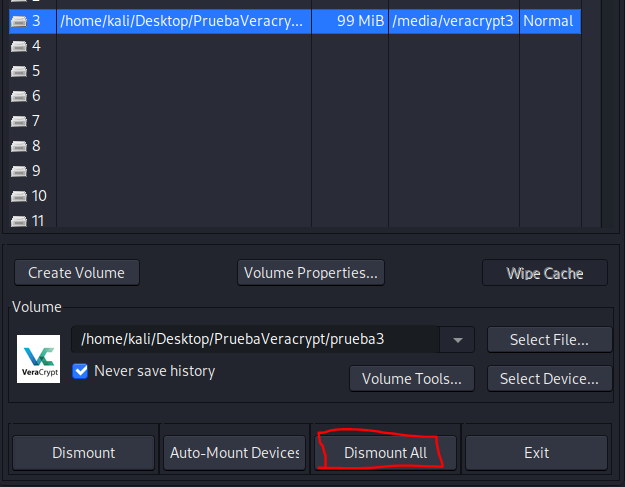
Ahora nos pide la contraseña previe que le hemos puesto:



Como vemos ya me sale mi volumen creado.



Ahora simplemente para desmontarlo podemos pulsar en Dismount all:



Grub---poner instalación y que se puede poner contraseña

# Seguridad a nivel de aplicación