|  |  |
| --- | --- |
| Resultado de imagen de grub 2 logo  Protección de grub 2  David Saldaña Castaño | práctica tutorial |

Content

[Motivos para proteger el GRUB. 2](#_Toc507089813)

[Configuración 2](#_Toc507089814)

[BACKUP PREVIO 2](#_Toc507089815)

[Definición de usuarios que pueden editar GRUB. 3](#_Toc507089816)

[Actualización de contraseñas (Seguridad) 4](#_Toc507089817)

[Actualizamos la configuración de Grub. 5](#_Toc507089818)

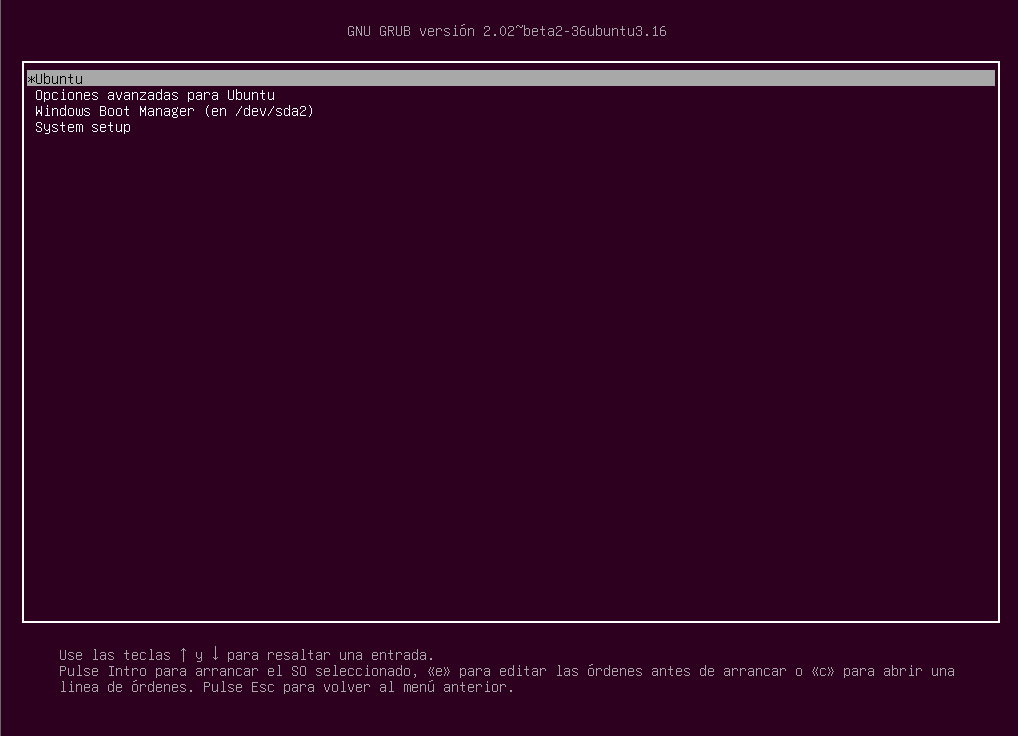
[Medidas adicionales. 5](#_Toc507089819)

# Motivos para proteger el GRUB.

1. Proteger al equipo de posibles atacantes que quieran acceder a nuestro equipo como root.
2. En caso de que el partido sea compartido.
3. En caso de que tengamos que dejar nuestro equipo desatendido o en lugares donde transiten muchas personas.
4. Prevenir que ciertos usuarios puedan usar sistemas operativos inseguros.

# Configuración

Partimos de un sistema DUAL BOOT como vemos en la imagen, con Windows y Ubuntu instalado en el mismo disco.



# BACKUP PREVIO

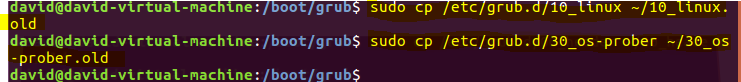
Antes de realizar cambios en los archivos de configuración, vamos a realizar una copia de seguridad en todos y cada uno de ellos creando el mismo directorio pero .old para identificar la configuración antigua.

Podemos crear la carpeta con **mkdir nombrecarpeta**, o directamente enviar el contenido del fichero del directorio principal al de backup con:

**Sudo cp ruta origen ~/ruta destino**

Los ficheros a configurar son:

* **/etc/grub.d/10\_linux**
* **/etc/grub.d/30\_os-prober**
* **/boot/grub/grub.cfg**
* **/etc/grub.d/00\_header**

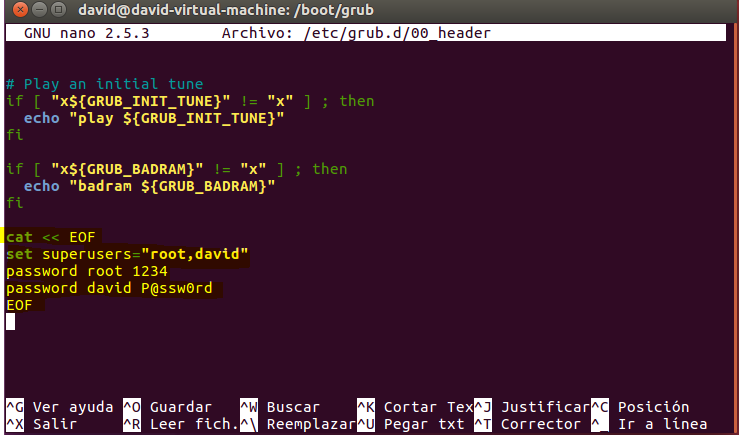






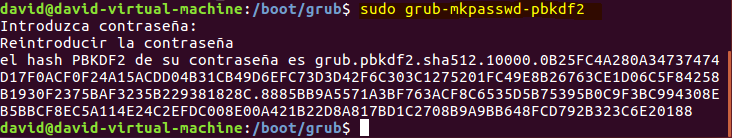
# Definición de usuarios que pueden editar GRUB.

Definimos los usuarios que podrán modificar el root con sus contraseñas en el fichero 00\_header dentro de **/etc/grub.d**

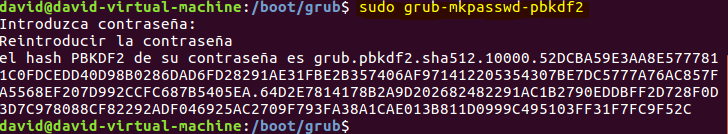


Ciframos las contraseñas de los usuarios para proteger nuestro equipo.

Utilizamos el comando **sudo grub-mkpasswd-pbkdf2** y nos creará el hash de la contraseña david

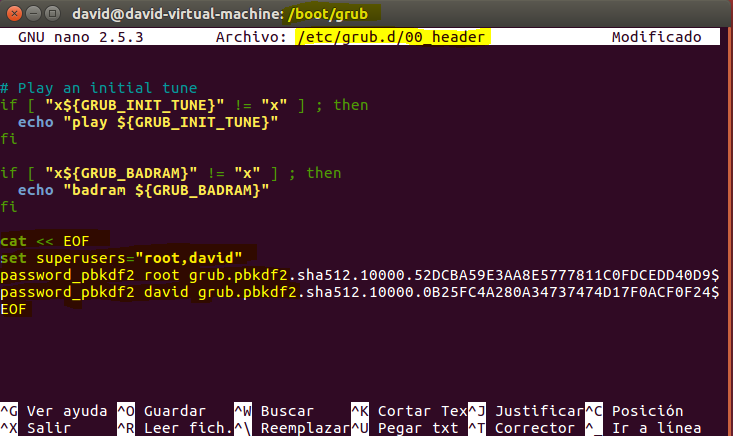


Hacemos lo mismo para la otra contraseña (root) y nos creará un hash diferente.



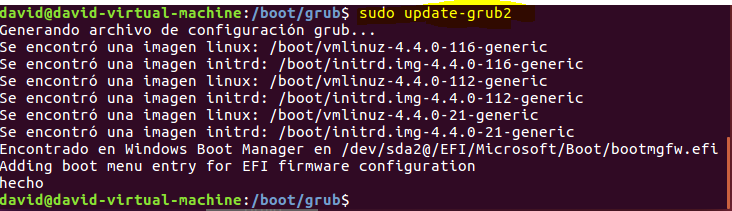
# Actualización de contraseñas (Seguridad)

Actualizamos las contraseñas en el archivo **/etc/grub-d/00\_header** sustituyendo las contraseñas por el hash



# Actualizamos la configuración de Grub.

Ejecutando el siguiente comando: **sudo update-grub2**



Dado este paso, si tenemos una versión igual o superior de GRUB, el grub está completamente protegido contra el acceso a la línea de comandos contra la edición de las entradas y contra la ejecución de las entradas del GRUB.

# Medidas adicionales.

Además de proteger GRUB, debemos seguir otras **medidas adicionales** como:

1. **Cifrar las particiones del disco duro.**
2. **Configurar la BIOS/UEFI para que no se pueda arrancar desde un LiveUSB.**
3. **Proteger la BIOS/UEFI con contraseña.**
4. **Limitar el acceso físico.**