**LA BIBLIA DE LINUX**

Todas las distribuciones de Linux (Debian, Ubuntu, Kali Linux…) Provienen de un kernel llamado GNU/Linux.

Distribuciones cronológicas: <https://upload.wikimedia.org/wikipedia/commons/1/1b/Linux_Distribution_Timeline.svg>

Distribuciones principales de GNU/Linux para Ciberseguridad:

* Ciberseguridad para principiantes:
  + Kali Linux: Basado en Debian, con muchas (demasiadas) herramientas. Está bien para principiantes. Se usa para seguridad ofensiva o defensiva. Sobre todo para pentesting.
  + Kali Purple: Basado en Debian, sobre todo para seguridad defensiva (Blue team).
  + Parrot: Debian. La diferencia con Kali es el entorno del escritorio, pero se parecen bastante.
  + BlackBuntu: Basado en Ubuntu (Ubuntu se basa en Debian).
* Ciberseguridad para anonimato y privacidad:
  + Tails: Para anonimato y privacidad.
* Ciberseguridad para informática forense:
  + Sift WorkStation.
  + Caine.

## **Estructura de Ficheros de Linux:**

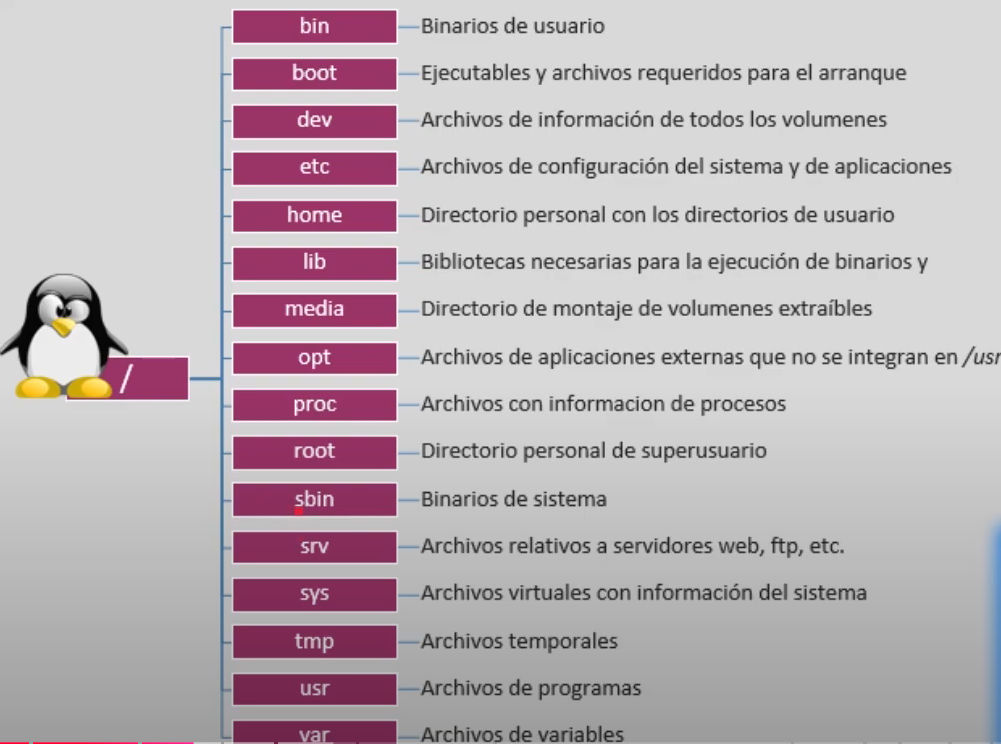
*INODOS, BLOQUES Y SUPER BLOQUES*

* **INODOS:** los Inodos contienen metadatos de todos los ficheros y directorios. Todos los ficheros y directorios van a tener asociados su Inodo y es de esta forma que el SO va a referenciarlos, mediante su Inodo, no mediante su nombre.
* **Bloques:** Es una unidad de almacenamiento donde se guardan los datos de los ficheros. Aquí relacionamos Ficheros con Inodos.
* **Super Bloques:** Contiene información crucial sobre el sistema de ficheros.

*DIRECTORIOS*

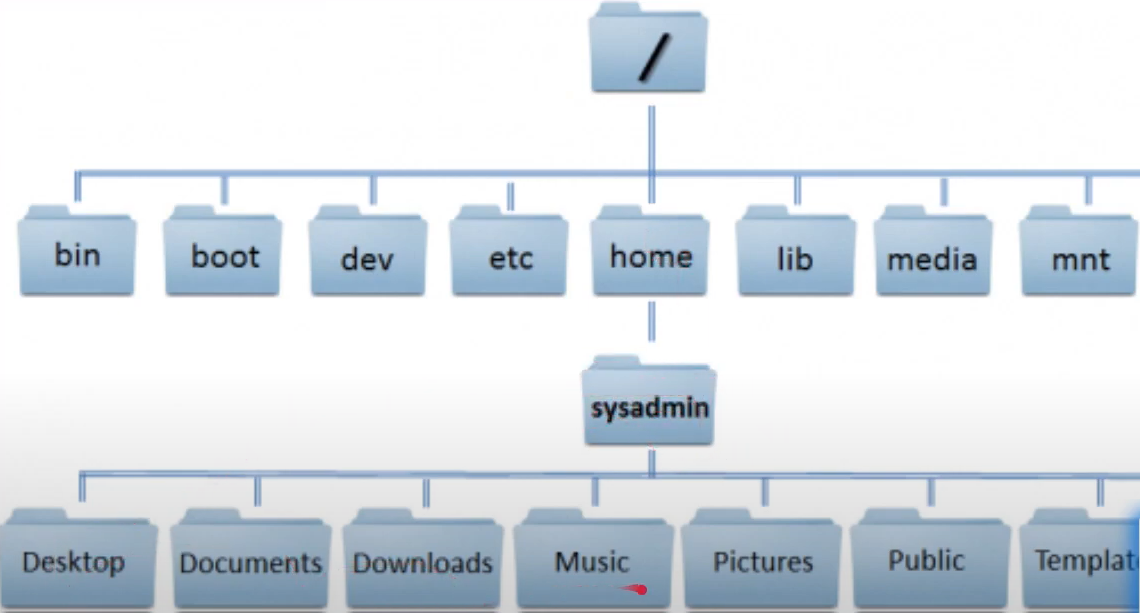
La raíz es la base de todo, esta se representa con /. De esta derivan todos los directorios.

Estos son los directorios más importantes:



* Bin: Contiene los programas que se pueden ejecutar por TODOS los usuarios.
* Boot: Aquí se almacenan los archivos para el arranque del sistema.
* Sbin: Ejecutables esenciales para el arranque del sistema y su recuperación.
* Dev: Archivos de información que hacen el puente entre el hardware y el software.
* Etc: Archivos de configuración del sistema y aplicaciones.
  + /etc/passwd: Aquí se guardan datos de los usuarios del sistema. Nombre de usuario, Id, Id del grupo, información del usuario, Home…
  + /etc/group: Contiene información sobre los grupos del sistema.
  + /etc/shadow: Almacena las contraseñas de los usuarios de manera encriptada.
  + /etc/fstab: aquí se definen como y donde se montan los sistemas de archivos. Principalmente contiene información sobre las particiones.
  + /etc/network/interface: Aquí definimos la configuración de red para las interfaces de red. Funciona en la mayoría de distribuciones, excepto en las muy recientes.
  + /etc/hostname: Contiene el nombre del host del sistema.
  + /etc/resolv.conf: Aquí se definen los servidores DNS.
* Home: Directorio personal donde tenemos el directorio de cada usuario y de este descienden el escritorio, documentos, descargas… Cada usuario va a tener su directorio Home.

Adicionalmente, en este directorio vamos a tener directorios ocultos que empiezan por un punto, y dependiendo de la shell que uses vas a tener uno llamado .bashrc, zshrc…. Son importantes mencionarlos porque vamos a poder modificar o definir los alias, setear variables de entorno y realizar configuraciones permanentes.



* Media: Sirve para gestionar cuando enchufamos USB’s o cualquier hardware externo.
* Root: Es el Home del Administrador.
* Tmp: Archivos temporales que se eliminan cada vez que se apaga el equipo.
* Var: en este directorio es importante destacar que podemos ver los logs del sistema.
* Usr: Contiene los ficheros y directorios compartidos con todos los usuarios.
  + /Usr/bin/: Aquí encontramos los ejecutables.
  + /Usr/lib/: Aquí encontraremos las librerías.

Caben destacar dos directorios especiales que no se almacenan en los discos duros. Son sistemas de archivos virtuales mantenidos por el kernel del SO. Estos directorios sirven de interfaz entre el kernel y el espacio de usuario. En ellos podemos realizar configuraciones del sistema en tiempo real. Interactúas directamente con el Kernel en lugar de leer los datos del disco duro.

* /proc/: Nos muestra información sobre los procesos en ejecución, sobre el hardware del sistema e información básica del sistema.
* /sys/: Estructura de directorios que representa el Hardware del sistema. Este es bastante importante.

*ENLACES DUROS Y BLANDOS*

* **Enlace duro:**  Si por ejemplo tenemos un archivo llamado pepe.txt en dos directorios distintos. Un enlace duro es el que relaciona este archivo por su Inodo. Esto quiere decir que son el mismo archivo, puesto que tienen el mismo Inodo. Si se modifica uno, el otro también es modificado.
* **Enlace blando:** Este sería lo que en Windows es hacer una copia. Tenemos dos archivos llamados pepe.txt en dos directorios distintos y en esta ocasión si se modifica uno el otro no se modifica.

*PERMISOS*

* **Lectura (W):** Permisos de escritura.
* **Escritura (R):** Permisos de lectura.
* **Otro (o):** Engloba el resto de usuarios que no son el propietario.

*SHELL Y TIPOS*

El Shell es un intérprete de comandos, que interpreta un comando a lenguaje máquina.

* Sh: Es la Shell más básica y viene por defecto en la mayoría de distribuciones.
* Bash: Surgió de Sh, es como Sh con proteínas. Esta la vas a encontrar en la mayoría de distribuciones de forma predeterminada. También puede usarse como lenguaje de programación.
* ZsH: Recoge características de otras Shells. Es una mejora de Bash.
* Hay muchas shells, pero estas son unas de las más importantes.

En la Shell, si tenemos el símbolo $ estamos como usuario normal, si el símbolo es # estamos como administrador.

Nota: Los ejemplos los vamos a realizar con Kali Linux y en bash.