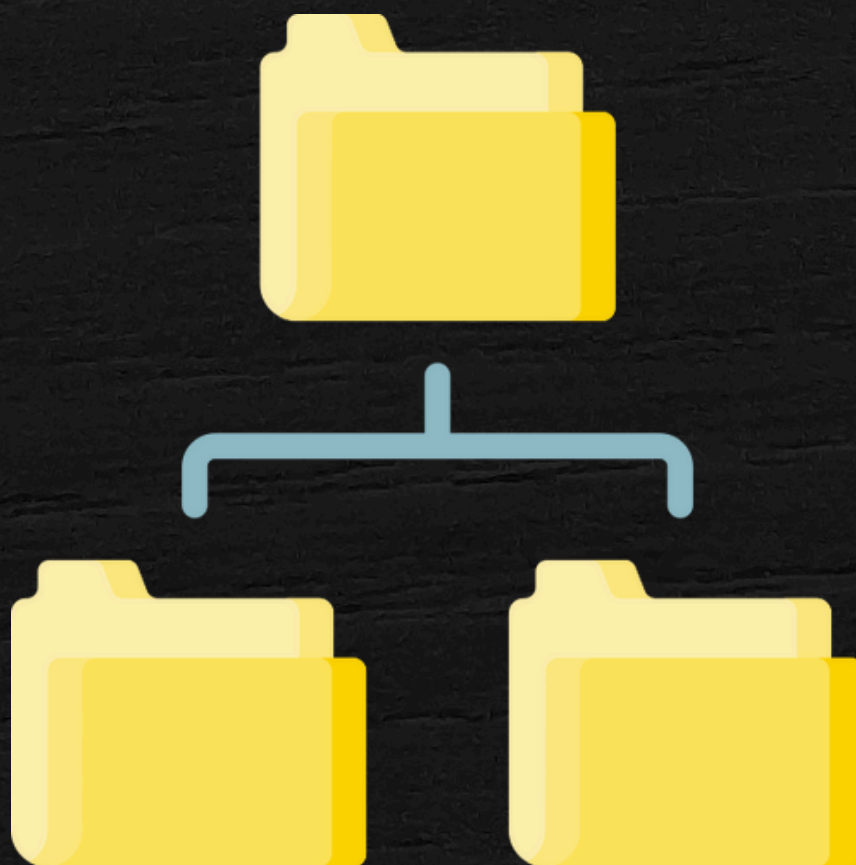


LINUX

ESTRUCTURA DE FICHEROS



[@saulruizplaza](#)

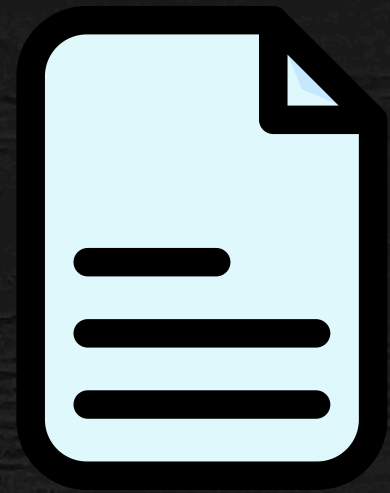
01.



¿QUÉ ES UNA ESTRUCTURA DE FICHEROS?

Una estructura de ficheros es la **organización jerárquica** en la que un sistema operativo almacena y gestiona archivos y directorios. En un sistema operativo basado en Linux, esta estructura empieza desde el directorio raíz (/) y se expande hacia abajo en una jerarquía que contiene directorios y archivos organizados por su función y tipo.

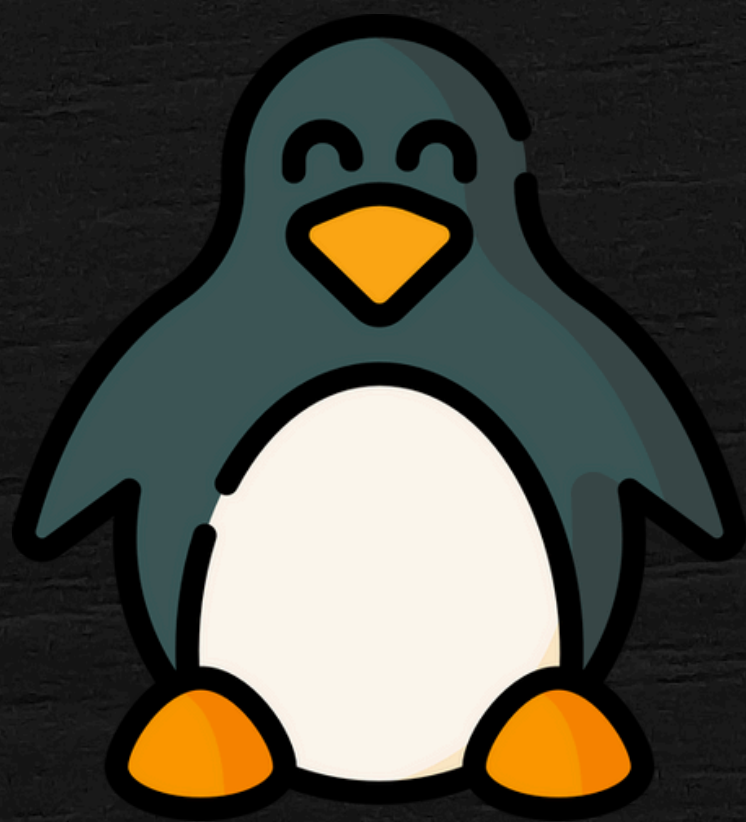
02.



ELEMENTOS CLAVE DE LA ESTRUCTURA DE FICHEROS

- **Directorios:** Los directorios son contenedores donde se almacenan los archivos.
- **Archivos:** Los archivos son los datos o programas almacenados en el sistema. Pueden ser de distintos tipos, como binarios, texto, configuración, etc.
- **Enlaces simbólicos:** Son accesos directos a otros archivos o directorios en el sistema, que permiten crear una estructura flexible.

DIRECTORIOS DE LINUX



[@saulruizplaza](#)

03.



/ (ROOT)

El **directorio raíz** / es el punto de **inicio** de toda la estructura de ficheros en Linux.

Contiene todos los demás directorios esenciales para el funcionamiento del sistema

¿POR QUÉ ES IMPORTANTE?

Todo el sistema depende de la estructura que comienza en /. Si este directorio no está protegido, un atacante podría comprometer el sistema entero.

04.



/BIN & /SBIN

- **/bin:** Contiene los **binarios esenciales**, programas que se utilizan para las operaciones más básicas del sistema, disponibles para todos los usuarios.
- **/sbin:** Similar a /bin, pero se encuentra en este directorio los binarios esenciales del sistema que solo deben ser utilizados por el **superusuario (root)**.

IMPORTANTE

Controlar el acceso a **/sbin** ya que puede alterar el comportamiento del sistema si no está protegido

[@saulruizplaza](#)

05.



/ETC

- Alberga los archivos de configuración del sistema. Aquí se encuentran configuraciones cruciales como **/etc/passwd** (información de usuarios) y **/etc/shadow** (contraseñas cifradas).

IMPORTANTE

Los atacantes pueden conseguir elevar privilegios si acceden a estos archivos

06.



/HOME

- Contiene los **directorios personales** de cada usuario en el sistema. Aquí se almacenan los archivos, configuraciones y documentos de los usuarios.

BUENAS PRÁCTICAS

1. **Cifra** los directorios de usuario si se almacenan datos sensibles.
2. **Establece** adecuadamente los **permisos** de sus archivos

07.



/VAR

- El directorio `/var` contiene archivos cuyo **contenido cambia con el tiempo**, como logs de eventos del sistema, colas de impresión y bases de datos.

¿POR QUÉ ES IMPORTANTE

Los logs del sistema proporcionan información valiosa para detectar actividades sospechosas o errores del sistema. Considera brindarle un buen espacio en el disco a este directorio.

[@saulruizplaza](#)

08.

/TMP



- Utilizado por aplicaciones y servicios para almacenar **archivos temporales** durante su ejecución.
- Este directorio suele ser limpiado al reiniciar el sistema.

ATENCIÓN

- El directorio `/tmp` puede ser explotado por atacantes que cargan archivos maliciosos o realizan ataques de ejecución desde allí. Así que asegúrese de tener habilitado la opción **noexec** en este directorio

[@saulruizplaza](#)

09.



/USR & /OPT

- **/usr:** Contiene la mayoría de los programas y **archivos compartidos del sistema**. Es uno de los directorios más grandes y se encuentra en casi todos los sistemas Linux.
- **/opt:** Directorio utilizado para almacenar aplicaciones de terceros

10.

/ROOT



- El directorio /root es el **directorio personal del superusuario (root)**. Aquí se almacenan los archivos personales del administrador y configuraciones exclusivas.

ATENCIÓN

- El acceso no autorizado a este directorio proporciona acceso completo al sistema. La seguridad de este directorio es vital para **mantener la integridad del sistema**.
- Una buena práctica sería utilizar **sudo** para tareas administrativas, evitando exponer nuestra contraseña de root por un keylogger

11.



/DEV, /MNT & /MEDIA

- **/dev:** Contiene archivos de **dispositivos físicos**, como discos duros, puertos USB y otros dispositivos de hardware.
- **/mnt y /media:** Se utilizan para **montar dispositivos** adicionales, como unidades USB o discos duros externos.

CUIDADO

- **Deshabilitar la ejecución automática** de dispositivos montados.
- Verificar la integridad de los dispositivos antes de montarlos y asegurarse de que son seguros.

MUCHAS GRACIAS

@saulruizplaza

