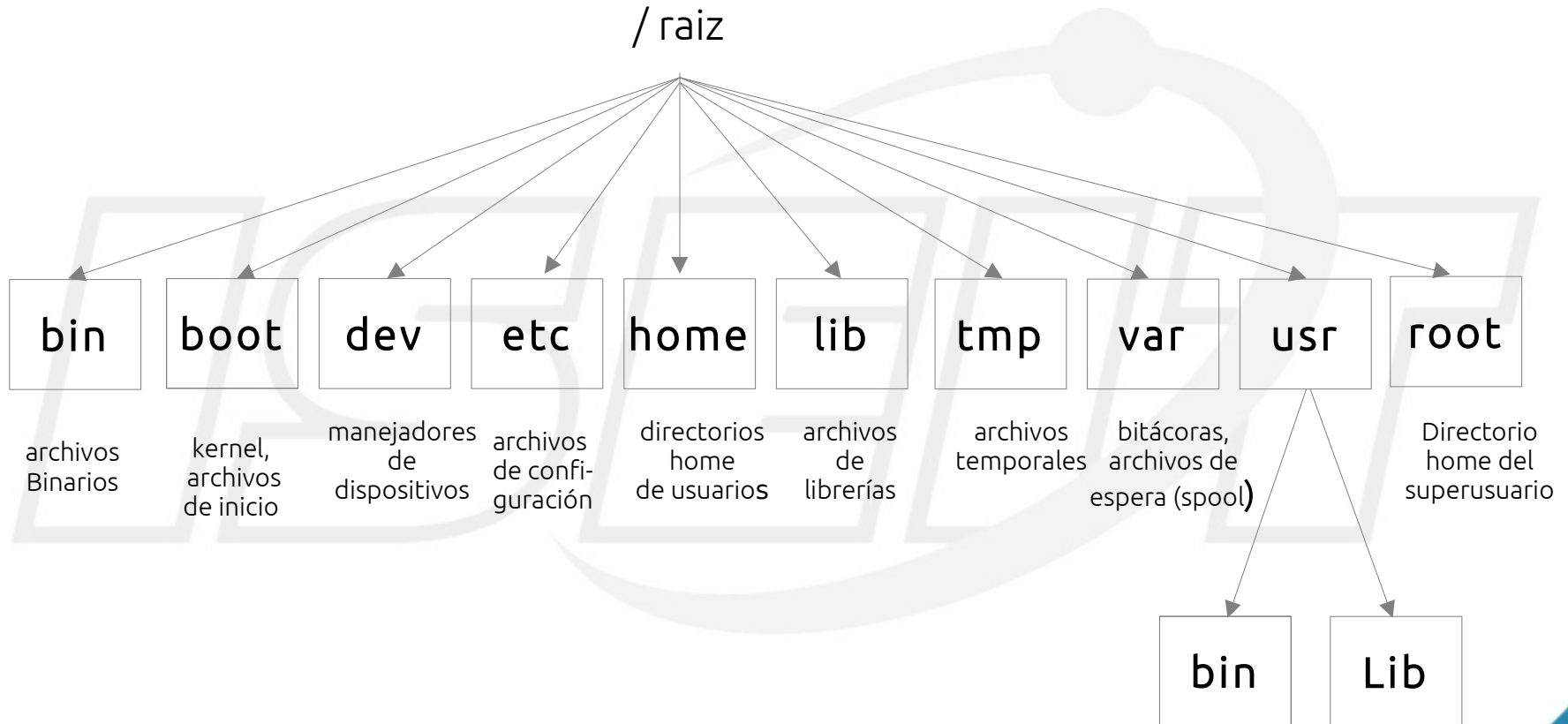


- Sistemas de archivos de Linux
  - Tipos de archivos
  - Directorios estándares
  - Rutas absolutas y relativas
  - Manejo de filesystem
  - Propiedades de los archivos
  - Permisos
  - Comandos para directorios, permisología y pertenencia

- **Directorios:**
  - Manejan información sobre la localización de otros archivos en el sistema, conocidos también como carpetas.
- **Regulares:**
  - Son los que guardan información sobre datos, comandos y otros objetos que pueden ser manipulados por los usuarios.
- **Especiales:**
  - Almacenan información sobre los dispositivos del sistema operativo como por ejemplo las impresoras, terminales, puertos, etc.

El Sistema de Archivos es una estructura jerárquica en árbol invertido.



- bin Archivos binarios, Comandos Generales de uso común.
- sbin Archivos Binarios, Comandos para el Administrador.
- boot Imágenes del Kernel que se cargan en el booteo.
- etc Archivos de Configuración del Sistema.
- dev Archivos especiales de Dispositivos.
- lib Librerías del Sistema usadas por los programas.
- Home Directorios Home de los usuarios ordinarios.
- root Directorio Home del Administrador del sistema.
- usr Archivos de usuarios para Aplicaciones compartidas.
- opt Aplicaciones de terceros (opcional)
- tmp Archivos temporales que se generan en el sistema.
- mnt Punto de Montaje para Dispositivos externos (cdrom, floppy).
- var Archivos variables de Colas y bitácoras de registro.

- Ver el directorio Actual de Trabajo: `pwd`
- Cambiar (sin el *directorio* va al home directory) : `cd directorio`
- Listar el contenido Actual: `ls directorio`
- Crear un directorio nuevo: `mkdir directorio`
- Borrar Directorios vacios: `rmdir directorio`
- Copiar hacia otro directorio: `cp directorio-fuente directorio-destino`
- Mover o renombrar: `mv directorio-fuente directorio-destino`

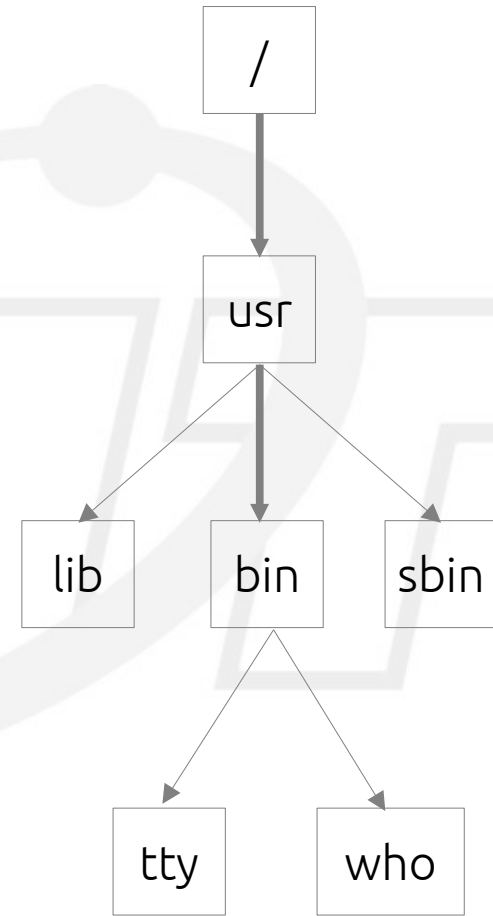
- Una ruta (pathname) absoluta describe el camino al archivo o directorio empezando desde el directorio raíz (/)

/usr/bin/tty

- Una ruta relativa describe el camino al archivo o directorio desde el directorio actual

bin/tty

- El directorio actual es el punto de referencia si la ruta no empieza con una /.
- El . y .. son directorios especiales para referenciar el actual y el anterior.



- Los **Filesystems** o **Sistemas de Archivos** son estructuras compuestas por archivos regulares, directorios y dispositivos que pueden ser manejados por los siguientes comandos:
  - **mount** (permite ver y montar sistemas de archivos)
    - ejem. `mount -t vfat /dev/fd0 /mnt/floppy`
  - **umount** (permite desmontar un filesystem montado)
    - ejem: `umount /mnt/floppy`
  - **df** (permite ver el espacio usado y disponible en los filesystems montados)

Nota: Ver los archivos `/etc/fstab` y `/etc/mtab`.



- Cada archivo es propiedad de un único usuario
- Cada archivo también pertenece a un único grupo
- Los mismos principios de propiedad se aplican a los directorios

```
$ ls -al
drwxr-xr-x  2  jenw  users  ...  .
drwxr-xr-x  6  root  root   ...  ..
-rw-r--r--  1  jenw  users  ...  .profile
$
```

usuario

grupo



- Los permisos son para:
  - Usuario o Dueño del archivo. (u)
  - Grupo al cual Pertenece el archivo. (g)
  - Otros o el resto del mundo. (o)
- Los tipos de permisos son:
  - Lectura (r).
  - Modificación (w)
  - Ejecución (x)
  - Ninguno (-)

usuario  
**rwx**

grupo  
**rwx**

otros  
**rwx**

## Cambio de Permisología en modo Simbólico:

- Cambie los permisos de acceso con  
**chmod** *usuario* [=+*-*] *permisos archivos...*
  - = reemplaza los permisos
  - + agrega los permisos
  - remover los permisos
- Los usuarios pueden pertenecer a uno o más grupos:
  - u usuario
  - g grupo
  - o otros
  - a todos los tipos de usuarios (opción colectiva, como *ugo*)
- Los permisos pueden ser uno o más de los siguientes:
  - r leer
  - w escribir
  - x ejecutar

## Cambio de Permisología en modo Octal:

- Use números octales para representar con bits los permisos:

usuario	grupo	otros	<i>Tipo de usuario</i>
rwX	rwX	rwX	<i>Protección requerida</i>
421	421	421	<i>Valores octales</i>
7	7	7	<i>La suma resulta en...</i>

- Sume los bits del número octal que correspondan a los permisos que se asignarán:

rw-	r--	---	<i>Protección requerida</i>
420	400	000	<i>Valor octal: 640</i>
6	4	0	

```
$ chmod 755 archivos... - asigna los permisos a rwxr-xr-x
$ chmod 644 archivos... - asigna los permisos a rw-r--r--
$ chmod 600 archivos... - asigna los permisos a rw-----
```

## Cambio de Pertenencia:

- Cambiar el usuario propietario:

**chown [-R] *usuario archivos...***

- Cambiar el grupo:

**chgrp [-R] *grupo archivos...***

- Cambiar al propietario y al grupo:

**chown [-R] *usuario:grupo archivos...***

```
# chown jenw /home/jenw/archivo1
```

```
# chgrp users /home/jenw/archivo1
```

```
# chown jenw:users /home/jenw/archivo1
```

Los permisos especiales son:

- SUID
- SGID
- Sticky bit

## SUID

Cuando se activa el permiso **setuid** de un archivo ejecutable ocasiona que al correr cualquier usuario dicho archivo lo haga no con sus privilegios, sino con los privilegios del usuario propietario de dicho archivo.

## SGID

Si se activa el permiso **setgid** de un programa éste se ejecuta con los privilegios asociados al grupo propietario del archivo y no con los del grupo del usuario que lo ejecuta.

## Sticky bit

Cuando se crea un directorio, tanto el usuario propietario del mismo como los miembros de su grupo, tienen permisos de lectura y escritura sobre el directorio.

Cuando se activa el **sticky bit** en un directorio se limitan las posibilidades de borrado de archivos de los usuarios con permiso de escritura en el mismo: **para borrar un archivo en el directorio hay que ser el propietario del archivo o el propietario del directorio**. En cualquier otro caso, aunque se pertenezca a un grupo con permiso de escritura en el directorio, no es posible eliminar los archivos.

Esta opción sólo afecta al directorio en el que se ha activado y no a sus subdirectorios.

Para activar estos permisos hay que agregar otro número en el esquema de permisología de los archivos

SUID  
4

SGID  
2

STICKY  
1

Este cuarto número, se coloca como primer dígito en el conjunto numérico que representa la permisología del archivo. Su valor puede variar desde el 1 hasta el 7, dependiendo de la suma que resulte según los permisos especiales que se desean asignar al archivo.



Valor	Permiso Especial	Descripción
1	--- --- --t	sticky bit
2	--- --s ---	sgid
3	--- --s --t	sticky bit + sgid
4	--s --- ---	suid
5	--s --- --t	suid + sticky bit
6	--s --s ---	suid + sgid
7	--s --s --t	suid + sgid + sticky bit

- En linux existen los archivos tipos directorios, regulares y los especiales que podemos referenciar por rutas absolutas o relativas.
- La Estructura del Sistema de Archivos en linux es jerárquica en forma de árbol invertida y pueden ser montados o desmontados con los comandos mount y umount.
- Los comandos básicos para el manejo de directorios son el pwd, cd, ls, mkdir, rmdir, cp y mv.
- Los archivos en linux tienen propiedades de pertenencia y permisología.
- Los comandos para el manejo de la permisología y pertenencia son el chmod, chown y chgrp.
- Los archivos con el bit SUID o SGID habilitado se ejecutan con los privilegios del usuario o grupo propietario y no del usuario que ejecuta el archivo.