HFC

INTRODUCIÓN A UNIX

DANNA MÁRQUEZ
FERNANDO ROMERO

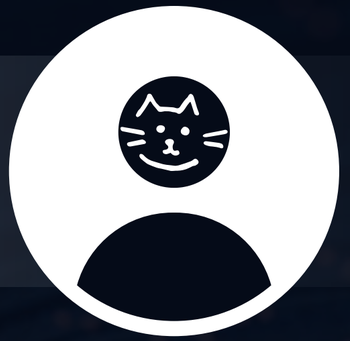
EJERCICIO

USUARIOS Y GRUPOS

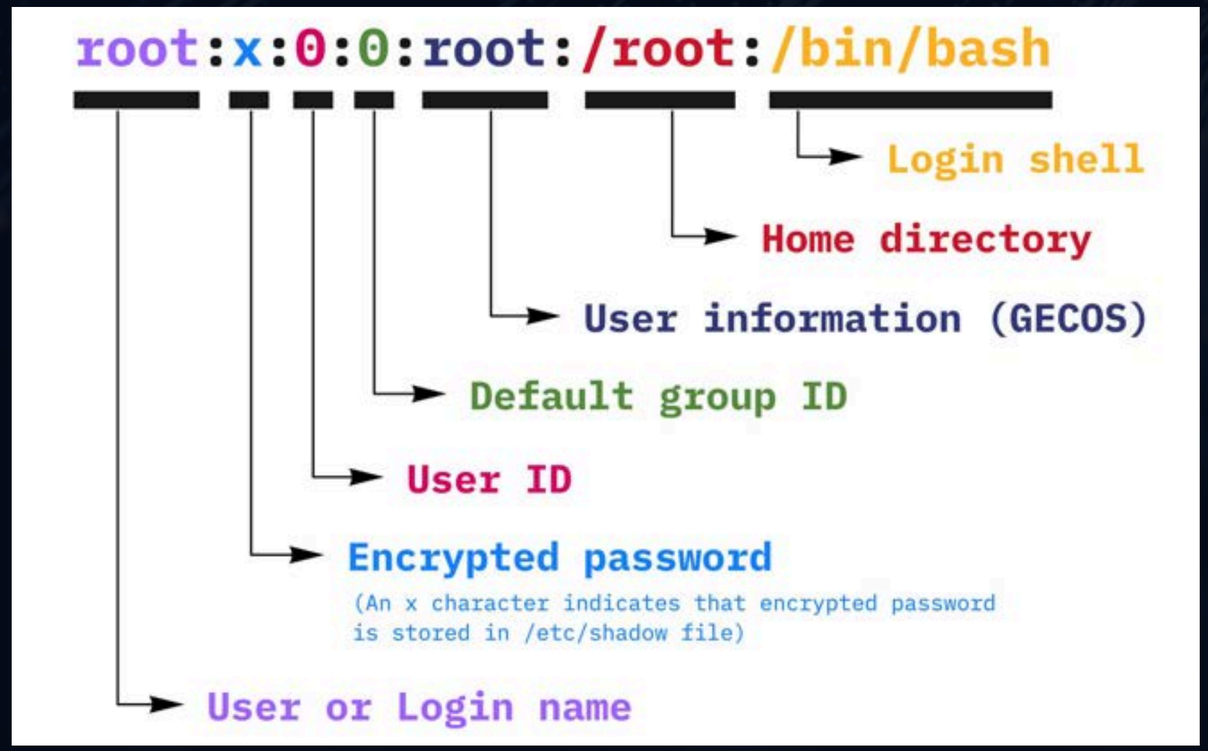
Los usuarios y grupos son **fundamentales** para la administración, la seguridad y la organización del sistema. Aportan valiosas características como lo son:

- **Administrar permisos**: Un grupo puede tener permisos específicos sobre archivos y directorios.
- **Organizar usuarios**: Usuarios con roles similares pueden agruparse
- **Principio de Mínimos Privilegios (PoLP)**: Limitar permisos al mínimo necesario.
- **Protección contra escalamiento de privilegios**: Evitar que usuarios obtengan permisos elevados.

USUARIOS

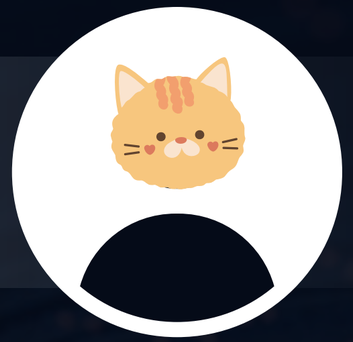


- **/etc/passwd**: Archivo que almacena información de los usuarios.



- Nombre de usuario
- Indica el estado de la contraseña (**x** si está activa y almacenada, **!** si el usuario está bloqueado y **!!** si el usuario no posee contraseña)
- UID
- GID
- Comentario
- Directorio hogar
- Shell

USUARIOS



- **/etc/shadow**

Este archivo almacena las contraseñas cifradas y datos de seguridad del usuario.
Solo root puede leerlo.

```
dalix:$6$abc123$Hc9H...T5g4:19230:0:99999:7:::
        usuario:contraseña:último_cambio:min:max:aviso:expira:reservado
```

HASHES

Un **algoritmo o función hash** recibe una entrada de cualquier longitud, la procesa o **digiere** y retorna una cadena de la misma longitud.

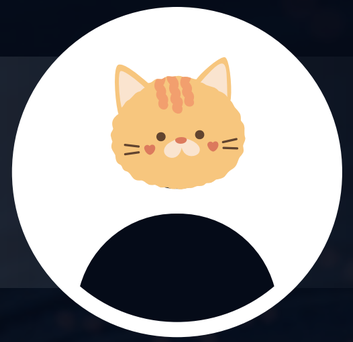
¡Cuál es la utilidad? Ayudan a verificar la integridad un archivo, y ofrecen un método no-retornable de “almacenar” nuestras contraseñas.

Hoy en día, para aún más seguridad se le agrega “sales”, es decir, un contenido aleatorio, antes de digerirlos.

HASHES

algsal$hash

USUARIOS

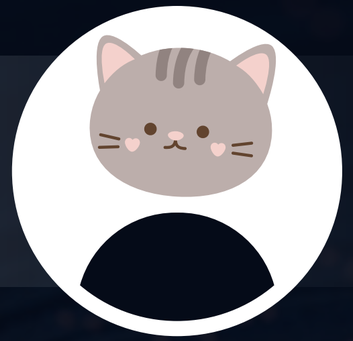


dalix:6abc123$Hc9H...T5g4:19230:0:99999:7:::

usuario:contraseña:último_cambio:min:max:aviso:inactividad:expir:reservado

- Nombre de usuario
- Contraseña **hasheada** del usuario en formato **UNIX**
- Último cambio de contraseña en formato epoch
- Periodo mínimo de espera para poder cambiar la contraseña
- Tiempo de expiración de la contraseña (99999 implica que no expira)
- Tiempo de anticipación que se da al usuario para cambiar la contraseña
- Máximos dias de inactividad tras expirar la contraseña antes de deshabilitar la cuenta (Típicamente vacío)
- Fecha de expiración en formato epoch (Vacío)
- Campo reservado e ignorado

USUARIOS

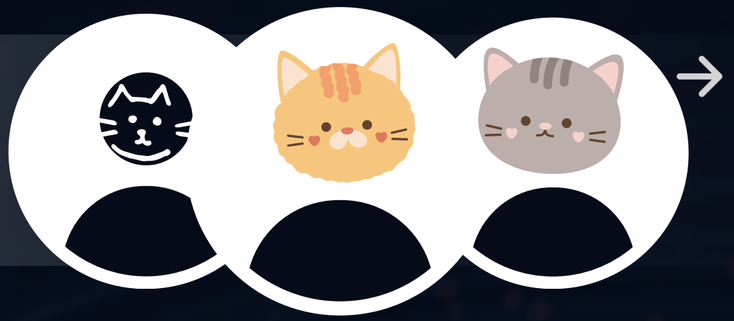


- useradd: Crea un nuevo usuario
  - sudo useradd -m -s /bin/bash dalix

- usermod: Permite modificar usuarios existentes, permitiendo cambiar su nombre, directorio personal, shell, grupos y más.
  - sudo usermod -l dalix danna

- userdel: Elimina usuario:
  - sudo userdel -r juan

GRUPOS



Es una entidad que agrupa a varios usuarios para gestionar permisos de acceso a archivos, directorios y recursos del sistema de manera eficiente.

Grupo Primario

- Es el grupo principal asignado a un usuario cuando se crea, se define en el archivo /etc/passwd

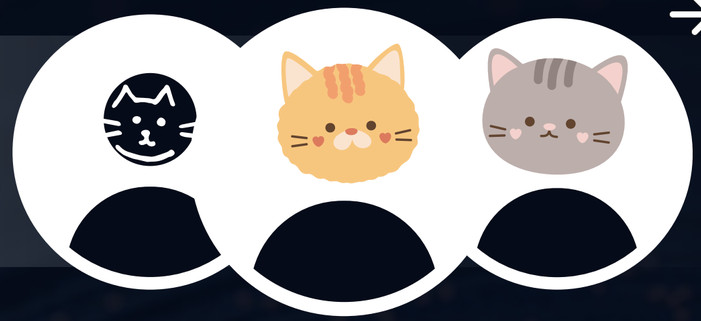
Grupos Secundarios (o Suplementarios)

- Grupos adicionales a los que un usuario puede pertenecer.
- Permiten compartir acceso con otros usuarios sin cambiar su grupo primario.
- Se definen en el archivo /etc/group.

/etc/group: `grupo:x:GID:usuarios`

x → Indica que la contraseña del grupo (si existe) está almacenada en /etc/gshadow.
GID (Group ID) → Número único que identifica al grupo.
Usuarios → Lista de usuarios que pertenecen a este grupo (separados por comas).

GRUPOS



- groupadd: Crea un nuevo grupo en el sistema.
  - sudo groupadd hfc
- groupmod: Permite cambiar el nombre o GID de un grupo.
  - sudo groupmod -n nuevogrupo grupo
- groupdel: Elimina un grupo del sistema.
  - sudo groupdel hfc
- id: Muestra la información de un usuario y sus grupos.
  - uid=1001(juan) gid=1001(juan) grupos=1001(juan),27(sudo),1002(developers)

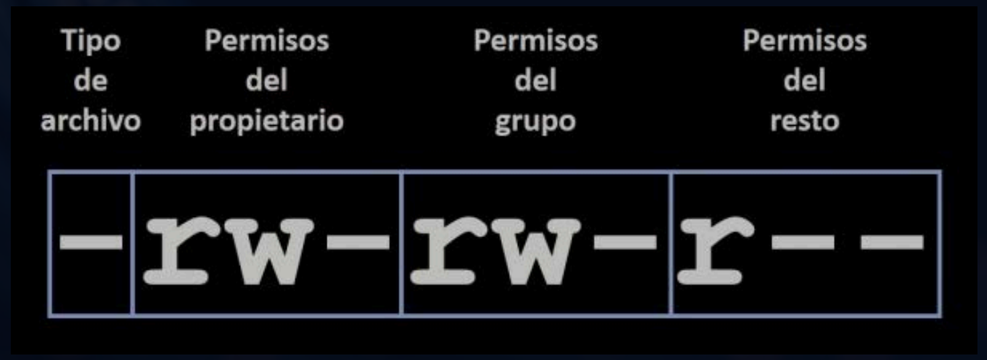
PERMISOS

Permiso	Simbolo	N0	Descripción
Lectura	r	4	Ver el contenido del archivo.
Escritura	w	2	Modificar el contenido del archivo.
Ejecución	x	1	Ejecutar el archivo si es un programa o script.

- chown: Permite cambiar el propietario (usuario) y/o grupo de un archivo o directorio.
  - sudo chown juan archivo.txt
  - sudo chown maria:developers archivo.txt

- chgrp: Permite cambiar el grupo de un archivo o directorio.
  - sudo chgrp contabilidad informe.pdf

- chmod: Permite modificar los permisos de lectura, escritura y ejecución de un archivo o directorio.
- Ejemplo:
  - rw-r--r--
  - chmod u+x script.sh == chmod 744 script.sh
  - rwxr--r--



Los permisos se pueden aplicar recursivamente:
chmod -R 755 directorio/

NOTACIÓN SIMBOLICA

[quién] [operador] [permisos]

Usuarios

- u → Usuario dueño del archivo (user)
- g → Grupo del archivo (group)
- o → Otros (usuarios que no son el dueño ni están en el grupo) (others)
- a → Todos (equivalente a ugo)

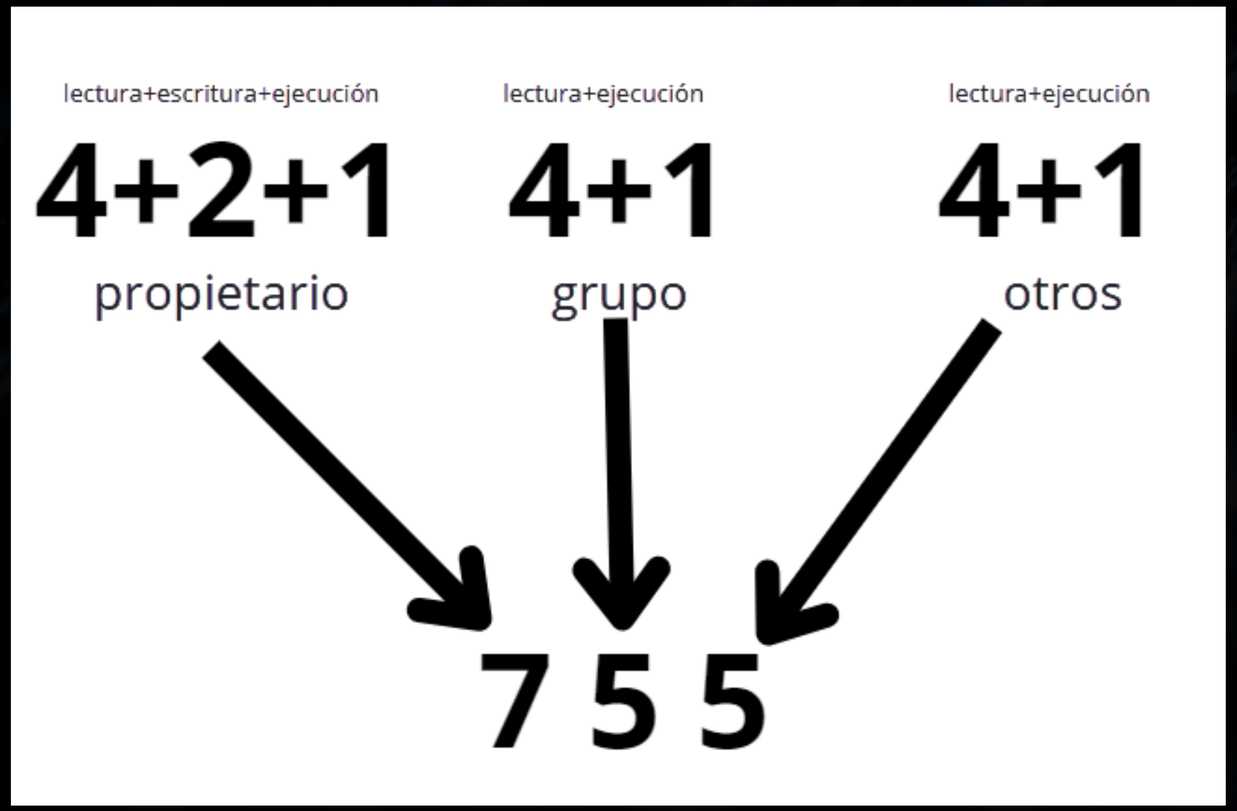
Operadores

- + → Agrega permisos
- - → Quita permisos
- = → Establece exactamente estos permisos (borrando los anteriores)

Tipos de Permisos

- r → Lectura (read)
- w → Escritura (write)
- x → Ejecución (execute)

NOTACIÓN DECIMAL



Lectura 4
Escritura 2
Ejecución 1

EJERCICIO

--x-w--r--	
--x-w--r--	
rw--wxr-x	
rwxr-x----	

SUID Y SGID

SUID (Set User ID) y **SGID (Set Group ID)** permiten que un archivo o programa se ejecute con los privilegios del propietario o grupo, en lugar de los del usuario que lo ejecuta

SUID

Hace que un programa se ejecute con los permisos del propietario en lugar del usuario que lo ejecuta.

SGID

Hace que un archivo o programa se ejecute con los permisos de su grupo en lugar del usuario que lo ejecuta.

sudo permite ejecutar comandos como otro usuario (normalmente root), mientras que SUID/SGID permiten que archivos específicos se ejecuten con privilegios elevados sin necesidad de sudo.
Un programa con SUID root puede ser riesgoso porque se ejecuta como root sin pedir contraseña.

Los bits SGID y SUID pueden cambiar cómo se ejecutan los archivos

- SUID (chmod u+s archivo): El archivo se ejecuta con los permisos de su propietario en lugar del usuario que lo ejecuta.
- SGID (chmod g+s directorio): Los archivos creados dentro del directorio heredan su grupo

CONTINUARÁ...