1. **Introducción**
   En sistemas Linux, la gestión de usuarios y permisos es un aspecto esencial para garantizar la seguridad y el funcionamiento adecuado del sistema. En este tutorial, vamos a cubrir conceptos básicos y avanzados relacionados con los usuarios, grupos y la administración de permisos en Linux.

   a. **¿Qué es un usuario?**
      Un **usuario** en Linux es una cuenta asociada a una persona o entidad que interactúa con el sistema. Cada usuario tiene su propio espacio de trabajo, configuraciones y privilegios. Los usuarios permiten personalizar la experiencia del sistema y gestionar recursos de manera aislada.

   b. **Diferencias entre usuario y root**

- **Usuario**:
  - Un usuario tiene permisos limitados.
  - Los usuarios pueden realizar tareas específicas dependiendo de los permisos asignados a sus cuentas.
  - La mayoría de las tareas cotidianas como crear archivos, ejecutar programas y navegar por directorios, se realizan bajo una cuenta de usuario normal.
- **Root**:
  - **Root** es el superusuario o administrador del sistema.
  - Tiene permisos ilimitados en el sistema y puede realizar cualquier acción, como modificar archivos del sistema, cambiar configuraciones de seguridad o añadir/eliminar usuarios.
  - **Root** es una cuenta crítica y peligrosa si se usa incorrectamente, por lo que generalmente se recomienda utilizarla solo cuando sea necesario.

   c. **Importancia del usuario en Linux**
      Los usuarios son esenciales en Linux porque permiten la segregación de tareas y la administración eficiente del sistema. Cada usuario puede tener su propio espacio de trabajo (como archivos y configuraciones) y permisos controlados para acceder a recursos compartidos. Además, asignar usuarios con permisos específicos ayuda a mantener la seguridad del sistema al limitar el acceso a recursos sensibles.

2. **Comandos básicos**
   a. ***Whoami***
      Muestra el nombre del usuario actualmente conectado.
   b. ***id***
      El comando `id` muestra información sobre el usuario actual, como el UID (User ID), el GID (Group ID) y los grupos a los que pertenece.
   c. ***adduser***
      Permite crear una nueva cuenta de usuario en el sistema.
   d. ***usermod***
      -Se utiliza para modificar las propiedades de un usuario.
      -Cambia el nombre del usuario.
      -Cambia el grupo primario de un usuario.

3. **Grupos**
    a. **¿Qué es un grupo?**
    En Linux, un **grupo** es un conjunto de usuarios que comparten ciertos permisos y privilegios. Los grupos permiten administrar y aplicar permisos de manera colectiva, de modo que los usuarios del mismo grupo pueden acceder y modificar los mismos recursos.
    b. ***group***
    Muestra información sobre los grupos del sistema.
    c. ***groupadd***
    Crea un nuevo grupo en el sistema.
    d. ***groupdel***
    Elimina un grupo del sistema.
    e. ***usermod -aG***
    Agrega un usuario a un grupo.
    f. ***id***
    Muestra los grupos a los que pertenece un usuario.
4. **Permisos y privilegios**
    a. **rwx**
    -r: Lectura
    -w: Escritura
    -x: Ejecución
    b. ***chmod***
    Permite cambiar los permisos de un archivo o directorio.
    c. ***chown***
    Cambia el propietario de un archivo o directorio.
    d. ***chgroup***
    Cambia el grupo asociado con un archivo o directorio.
    e. **Uso del sudo**

El comando sudo permite ejecutar comandos con privilegios de superusuario. Es una manera de ejecutar tareas administrativas sin iniciar sesión como root, lo que mejora la seguridad.

Uso básico:
Para ejecutar un comando con privilegios elevados:

5. **Configuración avanzada**

El comando chage se utiliza para cambiar las configuraciones de caducidad de la cuenta de usuario, como la fecha de expiración de la contraseña o el bloqueo de la cuenta.

    a. ***chage***
        - **Bloquear una cuenta de usuario**: Para bloquear la cuenta de un usuario y evitar que inicie sesión.

        - **Deshabilitar una cuenta de usuario**: Para deshabilitar temporalmente una cuenta sin eliminarla.

6. Casos prácticos