

Alumno: Diego Lordén Celeiro

Asignatura: DISEÑO Y ADMINISTRACIÓN DE SISTEMAS Y REDES

Documento: Practica 3.

Portada

Índice

[1. Introducción 3](#_Toc187086869)

[2. Herramientas Utilizadas 4](#_Toc187086870)

[3. Gestión de Usuarios 6](#_Toc187086871)

[3.1 Creación de Usuarios 6](#_Toc187086872)

[3.2 Modificación de Usuarios 8](#_Toc187086873)

[3.3 Eliminación de Usuarios 10](#_Toc187086874)

[4. Gestión de Grupos 11](#_Toc187086875)

[4.1 Creación y Modificación de Grupos 11](#_Toc187086876)

[4.2 Eliminación de Grupos 12](#_Toc187086877)

[5. Recuperación de Contraseñas 12](#_Toc187086878)

[5.1 Arranque desde un Sistema Alternativo 12](#_Toc187086879)

[5.2 Modificación del Archivo /etc/shadow 13](#_Toc187086880)

[5.3 Validación 14](#_Toc187086881)

[5.4 Alternativa: Uso de passwd 14](#_Toc187086882)

[6. Consideraciones de Seguridad 15](#_Toc187086883)

[7. Conclusión 16](#_Toc187086884)

[8 Bibliografía 17](#_Toc187086885)

# 1. Introducción

En los sistemas operativos Linux, la gestión de usuarios y grupos es una tarea fundamental para garantizar el control y la seguridad de los recursos del sistema. Esta práctica tiene como objetivo principal proporcionar una guía detallada para crear, modificar y eliminar usuarios y grupos, además de abordar la recuperación de contraseñas en situaciones comunes. Se busca que el estudiante comprenda cómo administrar estos aspectos mediante comandos y archivos críticos, preparándolo para enfrentar problemas reales en un entorno profesional.



**Propósito**

El propósito de esta práctica es capacitar al estudiante para:

* Gestionar usuarios y grupos de manera eficiente.
* Configurar atributos específicos para usuarios, como fechas de expiración y shells personalizados.
* Recuperar contraseñas utilizando métodos seguros.

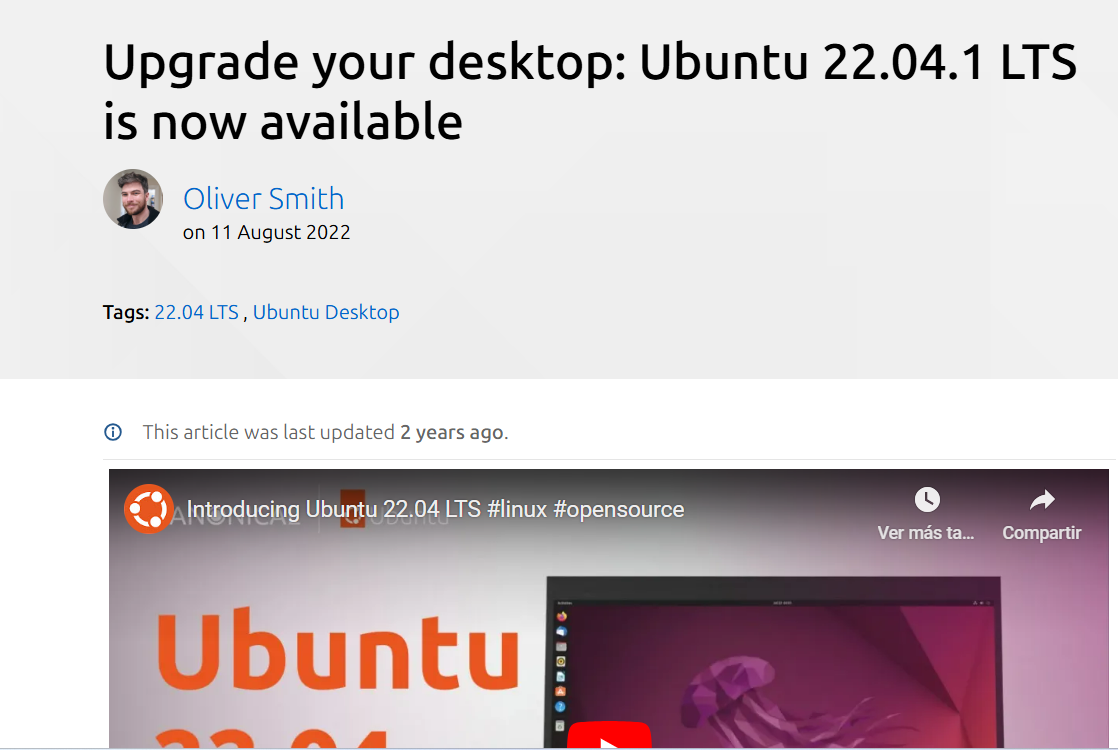
**Objetivos específicos**

* Explorar los comandos principales para la administración de usuarios y grupos.
* Modificar archivos del sistema como /etc/passwd y /etc/shadow.
* Resolver problemas comunes relacionados con el acceso y la seguridad del sistema.
* Comprender las implicaciones de seguridad al modificar configuraciones de usuarios y grupos.

# 2. Herramientas Utilizadas

**Sistema Operativo**

* **Distribución Linux**: Ubuntu 22.04 LTS
  + Elegida por su popularidad y facilidad de uso en entornos educativos y profesionales.



**Entorno de Virtualización**

* **VirtualBox**: Gestor de máquinas virtuales.
  + Proporciona un entorno controlado para realizar pruebas sin afectar el sistema anfitrión.



**Comandos Principales**

* useradd, usermod, userdel para la gestión de usuarios.
* groupadd, groupmod, groupdel para la gestión de grupos.
* passwd para la gestión de contraseñas.
* cat, grep, nano y vim para la verificación y edición de archivos de configuración.

**Archivos Importantes**

* **/etc/passwd**: Contiene información de los usuarios registrados.
* **/etc/shadow**: Almacena las contraseñas cifradas.
* **/etc/group**: Gestiona la información de grupos.

# 3. Gestión de Usuarios

## 3.1 Creación de Usuarios

**Comando useradd**

El comando useradd permite crear usuarios con configuraciones específicas. Ejemplo:



* **-m**: Crea un directorio de inicio para el usuario.
* **-s**: Especifica el shell predeterminado.

**Personalización de Usuarios**

* **Usuario con fecha de expiración**:

sudo useradd -e 2024-12-31 -m usuario2

su

Esto crea un usuario que no podrá iniciar sesión después de la fecha especificada.

* **Usuario con shell no estándar**:

sudo useradd -m -s /bin/zsh usuario3



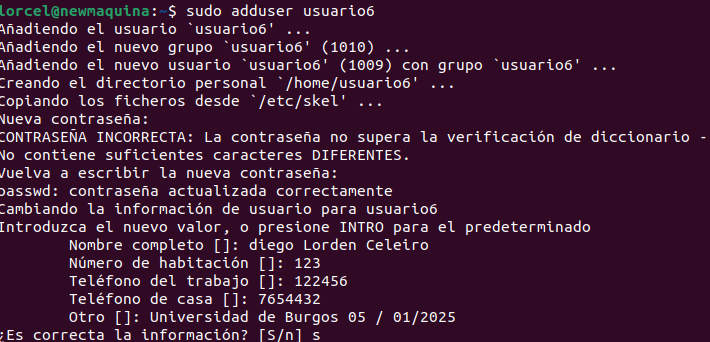
Este usuario utilizará el shell Zsh en lugar del predeterminado Bash.

**Diferencias con adduser**

El comando adduser simplifica la creación de usuarios solicitando información adicional durante el proceso. Por ejemplo:

sudo adduser usuario6

* Solicita datos como contraseña, nombre completo y otros atributos opcionales como (número de habitación, número de teléfono etc…).



**Verificación**

* Comprobar la información del usuario en /etc/passwd:

cat /etc/passwd | grep usuario6



* Validar si el directorio de inicio y los permisos han sido creados correctamente.

## 3.2 Modificación de Usuarios

**Comando usermod**

El comando usermod permite cambiar atributos de un usuario existente. Ejemplos:

**1.Cambiar el shell:**

sudo usermod -s /bin/zsh usuario6



* + Explicación: El parámetro -s permite definir el shell que el usuario utilizará al iniciar sesión. En este caso, se cambia de Bash (el predeterminado) a Zsh, un shell avanzado con características mejoradas como autocompletado y personalización.
  + Verificación: Puedes validar el cambio en el archivo /etc/passwd, donde se verá reflejado el nuevo shell asignado al usuario.

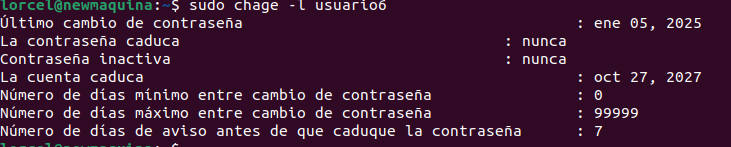


**2.Asignar fecha de expiración:**

sudo usermod -e 2027-10-27 usuario6



* + Explicación: La opción -e permite establecer una fecha de expiración para el usuario, especificada en formato AAAA-MM-DD. Después de esta fecha, el usuario no podrá iniciar sesión hasta que el administrador elimine o extienda la fecha de expiración.
  + Verificación: Usa el comando chage -l usuario1 para comprobar la fecha de expiración configurada.



**3. Agregar a un grupo secundario:**

sudo usermod -aG sudo usuario6



* + Explicación: El parámetro -aG agrega al usuario a un grupo secundario, manteniendo sus pertenencias actuales. En este caso, se añade al grupo sudo, otorgándole privilegios administrativos.
  + Verificación: Con el comando groups usuario1, puedes confirmar la pertenencia del usuario al grupo sudo.

****

## 3.3 Eliminación de Usuarios

**Comando userdel**

Elimina usuarios y, opcionalmente, sus archivos personales:

sudo userdel -r usuario6



* **-r**: Elimina el directorio de inicio y los archivos asociados al usuario.

**Precauciones**

* Verificar que el usuario no esté en sesión antes de eliminarlo.
* Revisar dependencias en archivos del sistema como /etc/group.
* Realizar un respaldo del directorio de inicio si contiene datos importantes.

# 4. Gestión de Grupos

## 4.1 Creación y Modificación de Grupos

**Crear un Grupo**

sudo groupadd grupo1



**Modificar un Grupo**

* Cambiar el nombre de un grupo:

sudo groupmod -n grupo\_Diego grupo1



**Agregar Usuarios a Grupos**

* Creamos un usuario nuevo con el comando que usamos antes el :

sudo usermod –m –s /bin/bash usuario 7



* Agregar un usuario a un grupo existente:

sudo usermod -aG grupo\_Diego usuario7



* Verificar la pertenencia a grupos con:

groups usuario7



## 4.2 Eliminación de Grupos

**Comando groupdel**

sudo groupdel grupo1



* Precaución: Asegúrese de que el grupo no esté asociado a usuarios activos.

Comprobación miramos con el groups que no hay ningún grupo ya asociado a ese usuario, porque el usuario sigue estando solo se borra el grupo.



# 5. Recuperación de Contraseñas

## 5.1 Arranque desde un Sistema Alternativo

En caso de que un usuario pierda el acceso a su cuenta debido a una contraseña olvidada o problemas de autenticación, el arranque desde un sistema operativo alternativo es una solución común. Este método implica utilizar una distribución en modo Live, como Ubuntu Live o Slax, para acceder al sistema afectado sin necesidad de autenticación.

**Pasos:**

1. **Crear un medio de arranque**: Descargar una imagen ISO de la distribución de Linux deseada y crear un USB de arranque con herramientas como Rufus o Etcher.
2. **Iniciar el sistema**: Configurar el BIOS o UEFI para arrancar desde el USB.
3. **Montar la partición afectada**: Donde corresponde a la partición donde se encuentra instalado el sistema afectado.

## 5.2 Modificación del Archivo /etc/shadow

El archivo /etc/shadow almacena las contraseñas cifradas de los usuarios. Para restablecer o eliminar una contraseña, es necesario editar este archivo. A continuación, se detallan los pasos:

**Métodos de Recuperación**

1. **Eliminar el hash de la contraseña**: Borrar el contenido entre los dos primeros : para eliminar la contraseña y permitir el acceso sin contraseña temporalmente:
2. **Sustituir el hash por uno conocido**: Generar un nuevo hash para una contraseña conocida utilizando openssl:

openssl passwd -6 nueva\_contraseña



Sustituir el hash generado en el archivo /etc/shadow.

**Precaución**

Siempre realizar una copia de seguridad del archivo antes de editarlo:

sudo cp /etc/shadow /etc/shadow.bak



## 5.3 Validación

Una vez realizados los cambios:

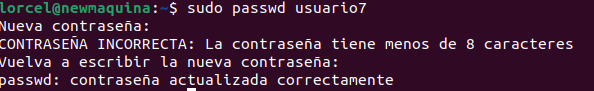
1. Desmontar la partición:
2. Reiniciar el sistema desde su partición habitual.
3. Probar el acceso con la nueva configuración de la contraseña.

Si los cambios no surten efecto, verificar los permisos y la integridad del archivo /etc/shadow.

## 5.4 Alternativa: Uso de passwd

Si el acceso root está disponible, el comando passwd permite restablecer contraseñas directamente:

sudo passwd usuario7



Esto solicita una nueva contraseña y actualiza automáticamente el archivo /etc/shadow.

Ahora comprobamos el hash de la contraseña con un cat en la carpeta correspondiente del usuario7.



# 6. Consideraciones de Seguridad

**Buenas Prácticas**

1. **Contraseñas Seguras**: Las contraseñas deben ser largas, contener caracteres alfanuméricos y símbolos, y evitar información fácilmente adivinable como nombres o fechas significativas.
2. **Rotación Regular de Contraseñas**: Configurar políticas para exigir el cambio periódico de contraseñas mediante herramientas como chage.
3. **Autenticación Multifactorial (MFA)**: Implementar mecanismos adicionales, como autenticadores móviles, para mejorar la seguridad en sistemas críticos.
4. **Auditorías de Seguridad**: Realizar revisiones periódicas de los usuarios y permisos asignados para identificar configuraciones obsoletas o inseguras.
5. **Cifrado y Backups**: Asegurarse de que los archivos de configuración y contraseñas estén encriptados y respaldados en ubicaciones seguras.

**Riesgos**

1. **Errores en la Modificación de Archivos Críticos**: La edición incorrecta de /etc/passwd o /etc/shadow puede hacer que el sistema sea inoperable. Siempre realizar copias de seguridad antes de realizar cambios.
2. **Accesos No Autorizados**: La configuración de permisos incorrectos puede permitir a usuarios no autorizados acceder a datos sensibles.
3. **Ataques de Fuerza Bruta**: Configurar límites de intentos de inicio de sesión para evitar ataques automatizados mediante herramientas como fail2ban
4. **Falta de Políticas de Caducidad**: Usuarios sin fechas de expiración pueden quedar activos indefinidamente, representando un riesgo de seguridad.

# 7. Conclusión

Esta práctica proporciona una comprensión profunda y aplicada de cómo gestionar usuarios y grupos en un entorno Linux. Se cubrieron aspectos fundamentales como la creación, modificación y eliminación de usuarios y grupos, así como tareas avanzadas como la recuperación de contraseñas en sistemas bloqueados.

Los conocimientos adquiridos sobre comandos clave como useradd, usermod y passwd permiten personalizar configuraciones y solucionar problemas comunes en sistemas reales. La interacción directa con archivos críticos como /etc/passwd y /etc/shadow enfatiza la importancia de mantener la integridad y seguridad de los sistemas.

Además, la incorporación de consideraciones de seguridad asegura que los administradores de sistemas puedan implementar políticas robustas para proteger los entornos que gestionan. Estas habilidades no solo son esenciales en el ámbito educativo, sino que también tienen una aplicación directa en roles profesionales relacionados con la administración y seguridad de sistemas operativos Linux.

En resumen, esta práctica fomenta un enfoque integral para gestionar usuarios, proteger datos sensibles y garantizar la estabilidad de los sistemas Linux.

# 8 Bibliografía

**Understanding the /etc/shadow File -**

<https://www.cyberciti.biz/faq/understanding-etcshadow-file/>

**Linux Command Line Basics**

<https://linuxcommand.org/>

**Ubuntu Official Documentation**

<https://help.ubuntu.com/>

**Recupera la contraseña de root para acceder a Linux**

<https://www.softzone.es/linux/tutoriales/recuperar-contrasena-root-linux/>

**Restablecer y cambiar contraseñas en Linux fácilmente**

<https://keepcoding.io/blog/cambiar-contrasenas-en-linux/>

**Creación y gestión de grupos en Linux IBM**

[**https://www.ibm.com/docs/es/ibm-mq/9.4?topic=windows-creating-managing-groups-linux**](https://www.ibm.com/docs/es/ibm-mq/9.4?topic=windows-creating-managing-groups-linux)