



ESCUELA POLITÉCNICA NACIONAL  
ESCUELA DE FORMACIÓN DE TECNÓLOGOS

GUIA DE PRÁCTICAS LABORATORIO

No. Práctica: 6

CARRERA: ASI

ASIGNATURA: Sistemas Operativos 1

CÓDIGO: TSI213

FECHA: (16/06/16)

**1. PROPÓSITO DE LA PRÁCTICA: (exponga los Resultados de Aprendizaje esperados)**

Administración de usuarios y grupos Linux

**2. OBJETIVO GENERAL:**

Administrar usuarios y grupos del sistema operativo Linux

**3. OBJETIVOS ESPECÍFICOS:**

- Crear usuarios del sistema
- Crear grupos del sistema
- Añadir usuarios a grupos
- Iniciar sesión como otros usuarios
- Obtener privilegios de root para el usuario actual
- Otorgar privilegios de root a otros usuarios

**4. INSTRUCCIONES:**

4.1 Lea y comprenda las instrucciones en el documento adjunto sobre los comandos utilizados para administrar los usuarios y grupos Linux.

4.2 Realice las actividades propuestas en el documento.



ESCUELA POLITÉCNICA NACIONAL  
ESCUELA DE FORMACIÓN DE TECNÓLOGOS

**GUIA DE PRÁCTICAS DE LABORATORIO**

**5. DESCRIPCIÓN DE ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:**

Siga las instrucciones en el documento adjunto.

**6. BIBLIOGRAFIA REFERENCIAL:**

- [http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m1/gestion\\_de\\_usuarios\\_y\\_grupos\\_en\\_linux.html](http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m1/gestion_de_usuarios_y_grupos_en_linux.html)
- [https://help.ubuntu.com/community/RootSudo#Allowing\\_other\\_users\\_to\\_run\\_sudo](https://help.ubuntu.com/community/RootSudo#Allowing_other_users_to_run_sudo)
- <http://manpages.ubuntu.com/manpages/trusty/es/man8/adduser.8.html>
- <https://help.ubuntu.com/lts/serverguide/user-management.html>

---

**FIRMA DEL DOCENTE:**



## PRÁCTICA DE LABORATORIO 6

### ANEXO

#### USUARIOS Y GRUPOS DE USUARIOS EN LINUX

El sistema Unix es un sistema operativo multiusuario. Linux está basado en el sistema Unix. Para que múltiples usuarios puedan hacer uso del sistema de una forma segura y ordenada, es necesario que el sistema disponga de mecanismos de administración y seguridad para proteger los datos de cada usuario, así como para proteger y asegurar el correcto funcionamiento del sistema.

#### Cuentas de usuario

Para poder utilizar el sistema operativo Unix es necesario disponer de una cuenta de usuario que se compone de **nombre de usuario (login)** y de **contraseña (password)**. Las cuentas de usuario son creadas por el administrador que en Unix es un usuario especial llamado **root** (ver más abajo). Los usuarios deberán pertenecer al menos a un grupo de usuarios ya que obligatoriamente deben tener asignado un grupo principal o grupo primario.

Cuando un usuario entra en un sistema Unix, debe identificarse indicando su **nombre de usuario** y su **contraseña**. Si se equivoca al introducir su nombre o su contraseña, el sistema le denegará el acceso y no podrá entrar.

#### Inicio de sesión en Linux

Una vez se haya identificado de forma satisfactoria, el usuario podrá utilizar el sistema y ejecutar todas las aplicaciones que le sean permitidas, así como leer, modificar o borrar aquellos archivos sobre los cuales tenga permiso.

Las cuentas de usuario no solo ofrecen al usuario un nombre y una contraseña, también le proporciona una **ruta para almacenar sus documentos y su perfil**, generalmente dentro de la carpeta /home/nombre-usuario y comúnmente denominada **carpeta home del usuario**, y un **intérprete de comandos (shell)** que le permitirá ejecutar aplicaciones.

Cuando el usuario ejecuta una aplicación (proceso), el sistema carga la aplicación en memoria y la ejecuta. Los procesos en ejecución pertenecen a algún usuario. El sistema asigna a los procesos el usuario que los ejecuta. Ejemplo, si el usuario "pepe" ejecuta la aplicación "konqueror", en la lista de procesos del sistema aparecerá un nuevo proceso llamado "konqueror" cuyo propietario es "pepe". **Obligatoriamente, todos los procesos del sistema pertenecen a algún usuario.** Ejecutando el comando 'ps aux' podemos ver todos los procesos en ejecución. Si ejecutamos el comando 'top' lo veremos a tiempo real.



```
root@cnice-desktop: ~
Archivo Editar Ver Terminal Solapas Ayuda
top - 15:05:37 up 2:54, 2 users, load average: 0.14, 0.12, 0.09
Tasks: 73 total, 1 running, 72 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.7% us, 1.0% sy, 0.0% ni, 96.7% id, 0.0% wa, 1.7% hi, 0.0% si
Mem: 191416k total, 178696k used, 12720k free, 19784k buffers
Swap: 232900k total, 6064k used, 226836k free, 79724k cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
4133 root 15 0 32904 9576 6380 S 1.0 5.0 0:55.20 Xorg
9157 root 15 0 74656 13m 10m S 0.7 7.4 0:01.36 nautilus
9799 root 15 0 40524 14m 9476 S 0.3 7.9 0:00.41 gnome-terminal
 1 root 16 0 1564 528 460 S 0.0 0.3 0:01.11 init
 2 root 34 19 0 0 0 S 0.0 0.0 0:00.00 ksoftirqd/0
 3 root RT 0 0 0 0 S 0.0 0.0 0:00.00 watchdog/0
 4 root 10 -5 0 0 0 S 0.0 0.0 0:01.82 events/0
 5 root 11 -5 0 0 0 S 0.0 0.0 0:00.04 khelper
 6 root 10 -5 0 0 0 S 0.0 0.0 0:00.00 kthread
 8 root 10 -5 0 0 0 S 0.0 0.0 0:00.32 kblockd/0
 9 root 20 -5 0 0 0 S 0.0 0.0 0:00.00 kacpid
97 root 15 0 0 0 0 S 0.0 0.0 0:00.03 pdflush
98 root 15 0 0 0 0 S 0.0 0.0 0:00.01 pdflush
100 root 18 -5 0 0 0 S 0.0 0.0 0:00.00 aio/0
 99 root 15 0 0 0 0 S 0.0 0.0 0:00.11 kswapd0
 687 root 10 -5 0 0 0 S 0.0 0.0 0:00.00 kseriod
1784 root 10 -5 0 0 0 S 0.0 0.0 0:00.00 khubd
```

Mostrando procesos con top. La segunda columna indica el propietario

Cuando se crea un nuevo archivo, el propietario del archivo será el **usuario** que lo ha creado y el grupo del archivo será el **grupo principal** de dicho usuario. Ejemplo, si "pepe" cuyo grupo principal es "profes" crea un nuevo archivo llamado examen.txt, el propietario de examen.txt será "pepe" y el grupo propietario será "profes", o lo que es lo mismo, el archivo pertenecerá al usuario pepe y al grupo profes. **Obligatoriamente, todos los archivos del sistema pertenecen a algún usuario y a algún grupo.**

```
root@cnice-desktop: ~
Archivo Editar Ver Terminal Solapas Ayuda
pepe@cnice-desktop:~$ ls -l
total 4
-rw-r--r-- 1 pepe profes 11 2007-07-04 14:55 examen.txt
pepe@cnice-desktop:~$
```

El archivo examen.txt pertenece al usuario pepe y al grupo profes

La cuenta de usuario le permite acceder al sistema tanto de forma presencial (sentado delante del ordenador) como de forma remota accediendo desde otro equipo por la red. Los permisos que tiene el usuario cuando utiliza el sistema presencialmente son los mismos que tiene cuando lo hace



ESCUELA POLITÉCNICA NACIONAL  
ESCUELA DE FORMACIÓN DE TECNÓLOGOS  
CAMPUS POLITÉCNICO “ING. JOSÉ RUBÉN ORELLANA”



remotamente. Lo habitual es utilizar el sistema de forma remota ya que al ser Unix un sistema multiusuario, la única forma de que varios usuarios lo utilicen de forma simultánea es remotamente.

El sistema Unix codifica los usuarios con un número diferente a cada uno que es el **identificador de usuario (uid = User Identifier)**. Internamente el sistema trabaja con el uid, no con el nombre del usuario. Normalmente a los usuarios que creamos se les asignan uids desde 1000 en adelante. Los números uid menores que 100 se reservan para usuarios especiales del sistema.

En Unix, por defecto, la información de los usuarios de un sistema se guarda en el archivo **/etc/passwd**. Es un archivo de texto que puede visualizarse con cualquier editor. Cada línea del archivo /etc/passwd almacena los parámetros de un usuario. Solo puede modificarlo el administrador (root). A continuación mostramos el archivo passwd:

```
root@cnice-desktop: ~
Archivo Editar Ver Terminal Solapas Ayuda
root@cnice-desktop:~# more /etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
dhcp:x:101:101::/nonexistent:/bin/false
syslog:x:102:102::/home/syslog:/bin/false
klog:x:103:103::/home/klog:/bin/false
cupsys:x:100:106::/home/cupsys:/bin/false
messagebus:x:104:107::/var/run/dbus:/bin/false
haldaemon:x:108:108:Hardware abstraction layer,,,:/var/run/hal:/bin/false
hplip:x:105:7:HPLIP system user,,,:/var/run/hplip:/bin/false
gdm:x:106:111:Gnome Display Manager:/var/lib/gdm:/bin/false
cnice:x:1000:1000:cnice,,,:/home/cnice:/bin/bash
pepe:x:1001:1001:/home/pepe:/bin/bash
root@cnice-desktop:~#
```

#### Volcado del archivo /etc/passwd

Las contraseñas de cada usuario se guardan encriptadas con un sistema de codificación irreversible, en el archivo **/etc/shadow** que también es un archivo de texto.



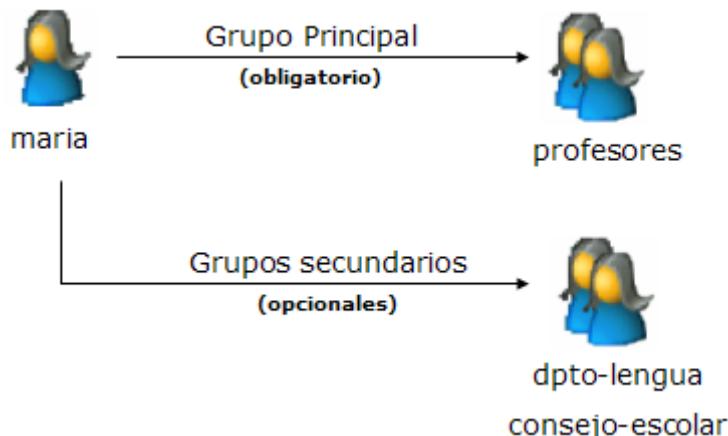
```
root@cnice-desktop: ~
Archivo Editar Ver Terminal Solapas Ayuda
root@cnice-desktop:~# more /etc/shadow
root:$1$bxCRdz6o$nZjer82zVOH1dnjx9t6Bp.:13686:0:99999:7:::
daemon:*:13686:0:99999:7:::
bin:*:13686:0:99999:7:::
sys:*:13686:0:99999:7:::
sync:*:13686:0:99999:7:::
games:*:13686:0:99999:7:::
man:*:13686:0:99999:7:::
lp:*:13686:0:99999:7:::
mail:*:13686:0:99999:7:::
news:*:13686:0:99999:7:::
uucp:*:13686:0:99999:7:::
proxy:*:13686:0:99999:7:::
www-data:*:13686:0:99999:7:::
backup:*:13686:0:99999:7:::
list:*:13686:0:99999:7:::
irc:*:13686:0:99999:7:::
gnats:*:13686:0:99999:7:::
nobody:*:13686:0:99999:7:::
dhcp!:13686:0:99999:7:::
syslog!:13686:0:99999:7:::
klog!:13686:0:99999:7:::
cupsys!:13686:0:99999:7:::
messagebus!:13686:0:99999:7:::
haldaemon!:13686:0:99999:7:::
hplip!:13686:0:99999:7:::
gdm!:13686:0:99999:7:::
cnice:$1$BSQ/myOT$C8o0ya.JDU7KF79u7tG/i1:13686:0:99999:7:::
pepe:$1$uG6zQclD$uKcgbPhheADAu59iBFmg/:13698:0:99999:7:::
root@cnice-desktop:~#
```

#### Volcado del archivo /etc/shadow

### Grupos de usuarios

Para poder administrar los permisos de los usuarios de una forma más flexible, el sistema Unix permite la organización de usuarios en grupos y establecer permisos a los grupos. Ejemplo, si en un centro educativo el grupo "profesores" tiene acceso a ciertas carpetas, cuando demos de alta un profesor nuevo, tan solo tendremos que añadirle al grupo "profesores" para que pueda acceder a todas esas carpetas. Es lo que se denomina administración de permisos por grupos.

Todos los usuarios pertenecen al menos a un grupo que es el **grupo principal del usuario**, también llamado grupo primario del usuario, pero pueden pertenecer a más grupos. En caso de que pertenezcan a más grupos, éstos serán **grupos secundarios**.



**Todo usuario debe pertenecer a un grupo principal obligatoriamente**

Los grupos pueden contener varios usuarios. Los grupos de usuarios solo pueden contener usuarios, nunca podrán contener a otros grupos.

El sistema Unix codifica los grupos de usuarios con un número diferente a cada uno que es el **identificador de grupo (gid = Group IDentifier)**. Internamente el sistema trabaja con el gid, no con el nombre del grupo. Normalmente a los grupos que creamos se les asignan gids desde 1000 en adelante. Los números gid menores que 100 se reservan para grupos especiales del sistema.

En Unix por defecto, la información de los grupos de un sistema se guarda en el archivo **/etc/group**. Es un archivo de texto que puede visualizarse con cualquier editor. Cada línea del archivo /etc/group almacena los parámetros del grupo y los usuarios que contiene. Solo puede modificarlo el administrador (root). Las contraseñas de los grupos se guardan encriptadas con un sistema de codificación irreversible, en el archivo **/etc/gshadow** que también es un archivo de texto.

## Usuario root

El usuario root, a veces llamado superusuario, es el usuario administrador del sistema. Está identificado con el número de usuario cero (uid=0) y tiene permisos sobre todo el sistema sin ningún tipo de restricción. El usuario root puede acceder a cualquier archivo, ejecutar, instalar y desinstalar cualquier aplicación, modificar los archivos de configuración del sistema y administrar usuarios. Si dispones de la contraseña de root tendrás control total sobre todo el sistema.

Los desarrolladores de Ubuntu decidieron deshabilitar por defecto la cuenta de administración del root en todas las instalaciones de Ubuntu. Esto no significa que la cuenta se haya eliminado que no pueda ser accedida, simplemente se le ha otorgado una contraseña que no coincide con ningún valor encriptado. Por lo tanto, no puede iniciar sesión por sí mismo.

Por este motivo, se recomienda a los usuarios hacer uso de la herramienta sudo para llevar a cabo tareas de administración del sistema. Sudo permite a los usuarios autorizados elevar temporalmente sus privilegios utilizando su propia contraseña en lugar de que tengan que conocer la contraseña del root. Esto permite que todas las acciones de los usuarios dentro del sistema puedan ser monitoreadas. Si por algún motivo se desea habilitar la cuenta del root, se le debe otorgar una contraseña.

```
sudo passwd
```

Sudo pedirá la contraseña del usuario y luego que se ingrese la nueva contraseña para el usuario root:

```
[sudo] password for username: (enter your own password)
Enter new UNIX password: (enter a new password for root)
Retype new UNIX password: (repeat new password for root)
passwd: password updated successfully
```



Para deshabilitar la contraseña de la cuenta del root, se debe ejecutar el siguiente comando:

```
sudo passwd -l root
```

Para deshabilitar la cuenta del root, se utiliza el siguiente comando:

```
usermod --expiredate 1
```

Para conocer más sobre sudo:

```
man sudo
```

Por defecto, el usuario inicial creado por el instalador de Ubuntu, es un miembro de grupo sudo, el cual es añadido al fichero /etc/sudoers como un usuario sudo autorizado. Si se quiere otorgar a otro usuario privilegios de root, simplemente se debe añadir a ese usuario al grupo sudo.

## Administración de usuarios y grupos

La administración de usuarios y grupos solamente puede realizarlas el usuario root utilizando los comandos de gestión de usuarios. Las tareas y los comandos para realizarlas son:

- Creación de usuarios / useradd
- Modificación de usuarios / usermod
- Eliminación de usuarios / userdel
- Creación de grupos / groupadd
- Modificación de grupos / groupmod
- Eliminación de grupos / groupdel
- Añadir usuarios a un grupo / adduser
- Quitar usuarios de un grupo / deluser

## Creación de usuarios

El comando **useradd** permite añadir un usuario indicando como parámetros la información particular para crear el usuario en la misma línea de comandos. La sintaxis es:

//Crear usuario

```
useradd [opciones] nombre-usuario
```

Entre las opciones más destacables tenemos:

- **-g: Grupo principal** que queremos tenga el usuario (debe existir previamente)
- **-d: Carpeta home** del usuario. Suele ser /home/nombre-usuario
- **-m: Crear** carpeta home si es que no existe.



- -s: Intérprete de comandos (shell) del usuario. Suele ser /bin/bash

Ejemplo, si deseamos crear un usuario llamado 'pedro' cuyo grupo principal sea 'profesores', cuya carpeta home sea /home/pedro y su intérprete de comandos sea /bin/bash, ejecutaremos el siguiente comando:

// Crear un usuario

```
sudo useradd -g profesores -d /home/pedro -m -s /bin/bash pedro
```

De esta manera habremos creado al usuario pedro y su carpeta home. Si no utilizamos la opción -m, no se creará la carpeta home del usuario; en tal caso tendríamos que crearla manualmente. Tan solo nos quedará establecer su contraseña con el comando passwd:

// Establecer la contraseña del usuario

```
sudo passwd pedro
```

Entonces el sistema nos preguntará dos veces la contraseña que queremos asignar a pedro.

El comando useradd permite crear muchos usuarios automáticamente mediante archivos de comandos (scripts).

Se recomienda que el nombre de usuario sea en minúsculas y además de letras también puede contener números y algún signo como guiones normales y guiones bajos. Debemos recordar que unix distingue entre mayúsculas y minúsculas, es decir, Pepe es distinto de pepe.

## Modificación de usuarios

Se utiliza el comando **usermod** y permite cambiar el nombre del usuario, su carpeta home, su intérprete de comandos, los grupos a los que pertenece y algunos otros parámetros.

// Cambiar el home de un usuario

```
sudo usermod -d /home/carpeta_pedro pedro
```

## Eliminación de usuarios

Se realiza con el comando **userdel** seguido del nombre del usuario. Con la opción -r eliminará también su carpeta home, ejemplo:

// Eliminación de un usuario

```
sudo userdel -r pedro
```

Eliminaría el usuario pedro y su carpeta home.

## Creación de grupos

El comando **groupadd** permite añadir un grupo indicando como parámetro el nombre del grupo. Ejemplo, si deseamos crear un grupo llamado 'alumnos' ejecutaremos:



// Añadir un grupo

```
sudo groupadd alumnos
```

## Modificación de grupos

El comando **groupmod** permite modificar el nombre de un grupo o el gid del mismo. La sintaxis es:  
`sudo groupmod [-g nuevo-gid] [-n nuevo-nombre] nombre-grupo`, ejemplo:

// Cambiar el gid del grupo profesores

```
sudo groupmod -g 2000 profesores
```

## Eliminación de grupos

Se realiza con el comando **groupdel** seguido del nombre del grupo, ejemplo:

// Eliminación de un grupo

```
sudo groupdel profesores
```

Eliminaría el grupo profesores. Si algún usuario tuviera dicho grupo como grupo primario, el comando **groupdel** no eliminará el grupo.

## Añadir usuarios a un grupo

Se utiliza el comando **adduser** seguido del nombre del usuario y del nombre del grupo al que queremos añadirle, ejemplo:

// Añadir a 'juan' al grupo 'profesores'

```
sudo adduser juan profesores
```

## Quitar usuarios de un grupo

Se utiliza el comando **deluser** seguido del nombre del usuario y del nombre del grupo del que queremos quitarle, ejemplo:

// Quitar a 'juan' del grupo 'profesores'

```
sudo deluser juan profesores
```

Para más información de todos estos comandos se puede consultar la ayuda del manual ejecutando **man** seguido del nombre del comando.

```
man adduser
```



## Herramienta gráfica de administración de usuarios

Ubuntu dispone de una herramienta gráfica de administración de usuarios que es '**users-admin**'. Para ejecutarla podemos abrir una consola de root y ejecutar users-admin o si hemos iniciado sesión como root, podemos pulsar Alt+F2 y ejecutar users-admin.



## Herramienta users-admin para administración de usuarios y grupos

Se trata de una herramienta bastante intuitiva que dispone de una pestaña para administrar usuarios y otra para administrar grupos.

### Permitiendo iniciar sesión como otro usuario

**No se recomienda el uso de los siguientes comandos para acceder como root debido a que pueden causar problemas al eliminar accidentalmente archivos del sistema o problemas similares.**

El siguiente comando permite iniciar sesión como otro usuario del sistema:

```
sudo -i -u <username>
```

Por ejemplo, para convertirse en el usuario amanda.

```
sudo -i -u amanda
```

La contraseña que se pide es su propia contraseña no la de amanda.



## Preguntas:

1. ¿Se pueden descifrar las contraseñas almacenadas en el archivo /etc/shadow?
2. ¿En Linux, cada usuario tiene que tener su nombre de usuario y contraseña?
3. ¿Qué comando se debe ejecutar para otorgar privilegios de root a un usuario del sistema?
4. ¿Cuál es la diferencia entre los comandos adduser y useradd?
5. ¿Cuál es la diferencia entre los comando sudo y su?
6. ¿Qué hacen los comandos sudo -i y sudo su? ¿Cuál es la diferencia entre estos dos?

## Referencias

- [http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m1/gestion\\_de\\_usuarios\\_y\\_grupos\\_en\\_linux.html](http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m1/gestion_de_usuarios_y_grupos_en_linux.html)
- [https://help.ubuntu.com/community/RootSudo#Allowing\\_other\\_users\\_to\\_run\\_sudo](https://help.ubuntu.com/community/RootSudo#Allowing_other_users_to_run_sudo)
- <http://manpages.ubuntu.com/manpages/trusty/es/man8/adduser.8.html>
- <https://help.ubuntu.com/12.04/serverguide/user-management.html>