



# Gestión de usuarios y grupos en Ubuntu con CLI

Alfredo Abad

ISO-04-032-UsuariosGruposLinux-CLI.pptx

6-sep-2023

1  
Alfredo Abad



## Comandos básicos

### • *Usuarios:*

- Creación de usuarios: **useradd**
- Modificación de usuarios: **usermod**
- Eliminación de usuarios: **userdel**
- Grupos a los que pertenece un usuario: **groups** <usuario>
- Información sobre la identidad de un usuario: **id** <usuario>
  - Con la opción **-Gn** proporciona información sobre grupos
    - El parámetro **-G** muestra todos los grupos a los que pertenece
    - El parámetro **-n** muestra el nombre en vez del número de grupo

### • *Grupos:*

- Creación de grupos: **groupadd**
- Modificación de grupos: **groupmod**
- Eliminación de grupos: **groupdel**

### • *Relacionar usuarios con grupos:*

- Añadir usuarios a un grupo: **adduser** (también puede usarse para crear usuarios)
- Quitar usuarios de un grupo: **deluser**

2  
Alfredo Abad



## Ejemplo de `groups` e `id -Gn` (averiguando a qué grupos pertenece el usuario `root`)

```
[root@LINUX1 ~]# groups root
root : root bin daemon sys adm disk wheel
```

```
[root@LINUX1 ~]# id -Gn root
root bin daemon sys adm disk wheel
```

3  
Alfredo Abad



## useradd

- **useradd [opciones] nombre-usuario**
- Opciones básicas:
  - 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`
- Después, la contraseña se establece con **passwd usuario**
- Ejemplo:
  - **sudo useradd -g profesores -d /home/pedro -m -s /bin/bash pedro**
  - **sudo passwd pedro** (la contraseña se pide dos veces en secreto)

4  
Alfredo Abad



## usermod y userdel

- **usermod** permite cambiar el nombre del usuario, su carpeta home, su intérprete de comandos, los grupos a los que pertenece y algunos otros parámetros
  - Por ejemplo, cambiar el home de un usuario:
    - `sudo usermod -d /home/carpeta_pedro pedro`
- **userdel** elimina el usuario
  - Con la opción `-r` eliminará también su carpeta home, ejemplo:
    - `sudo userdel -r pedro`
      - Eliminaría el usuario pedro y su carpeta home

5  
Alfredo Abad

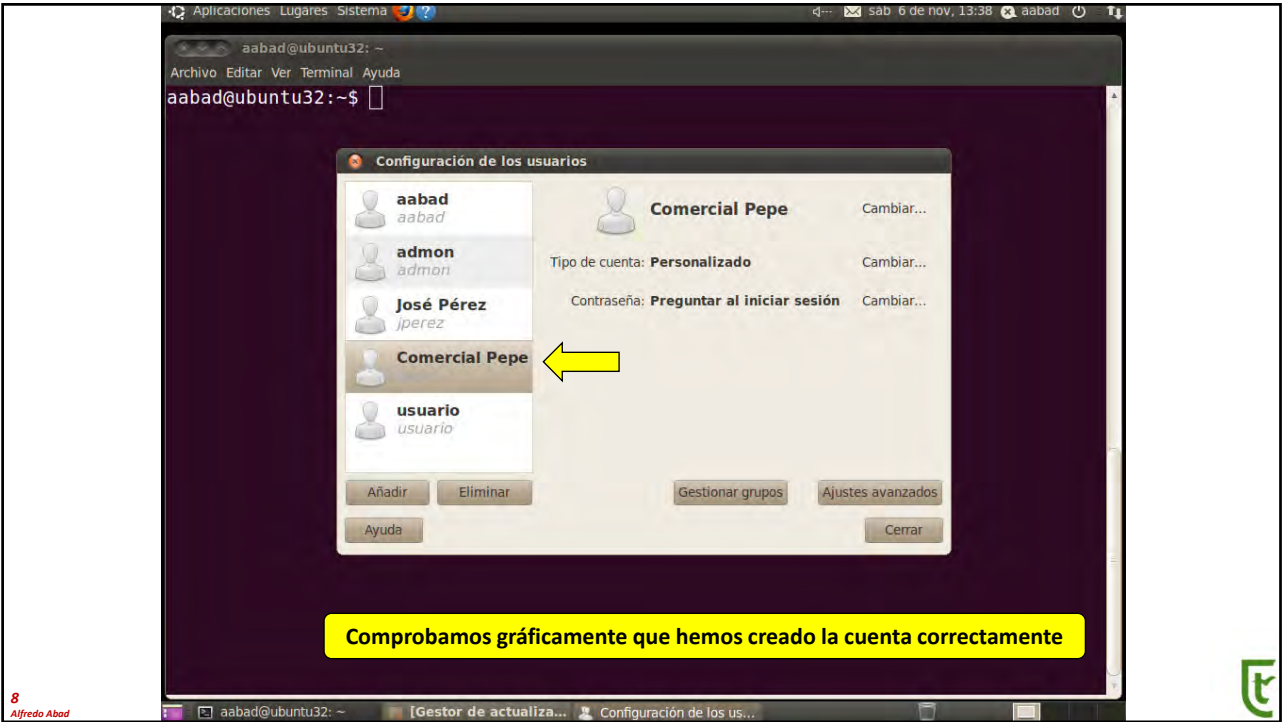
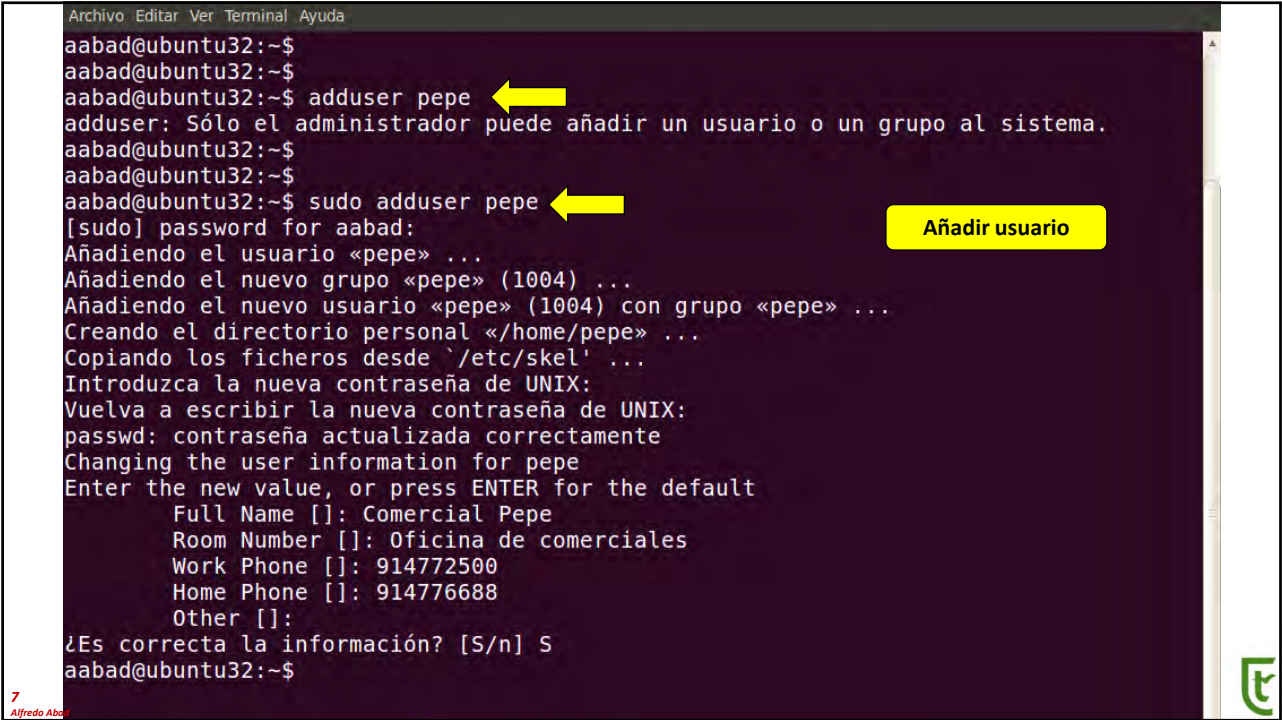


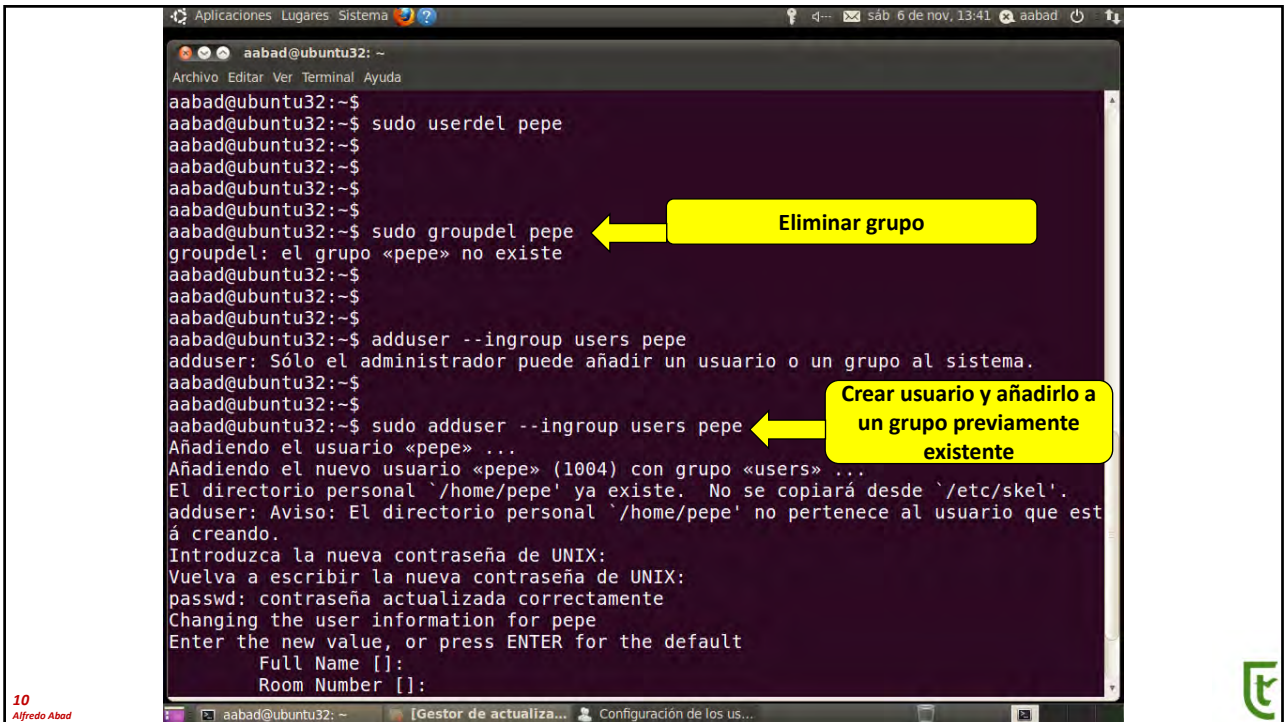
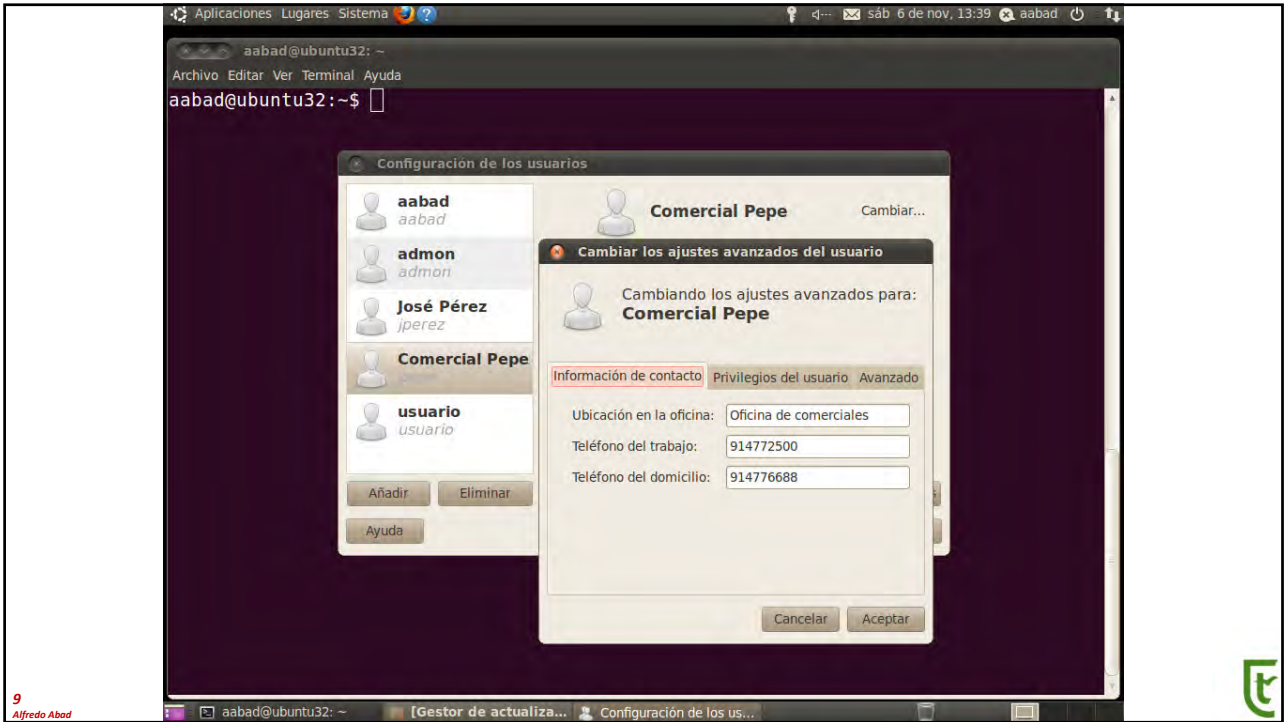
## adduser y deluser

- **adduser** se utiliza para añadir un usuario a un grupo
  - `sudo adduser juan profesores`
    - Añade al usuario juan al grupo profesores
  - Si `adduser` se utiliza sin el nombre del grupo, se crea el usuario juan y un grupo principal para ese usuario con el mismo nombre en el que se incluye
- **deluser** se utiliza para quitar la pertenencia de un usuario a un grupo al que pertenecía
  - `sudo deluser juan profesores`
    - Quita la pertenencia de juan al grupo profesores

6  
Alfredo Abad

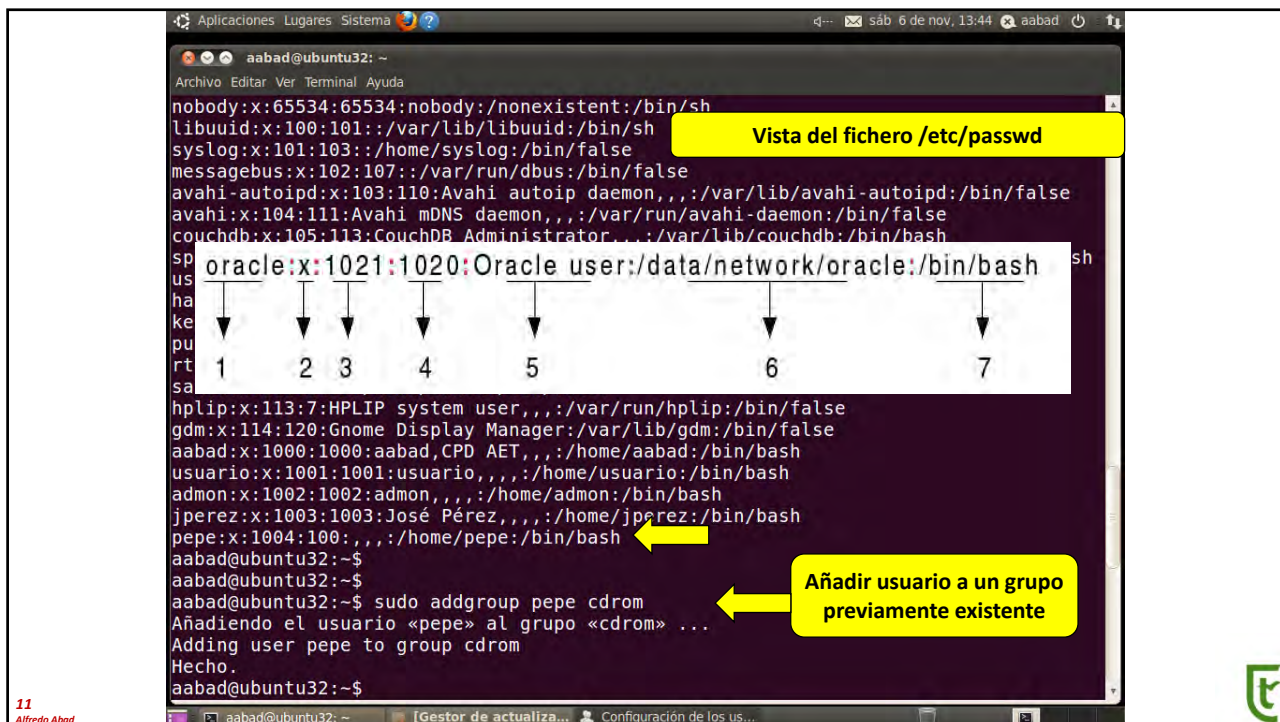




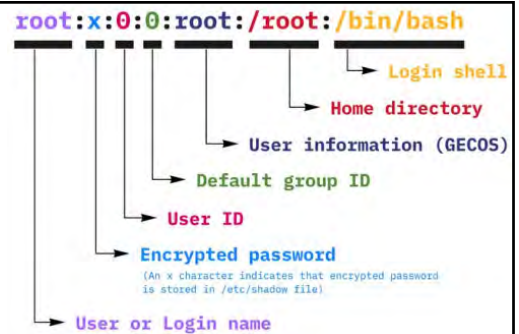


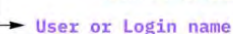
Si eliminas un comando se elimina lo hecho con él.





**/etc/passwd**



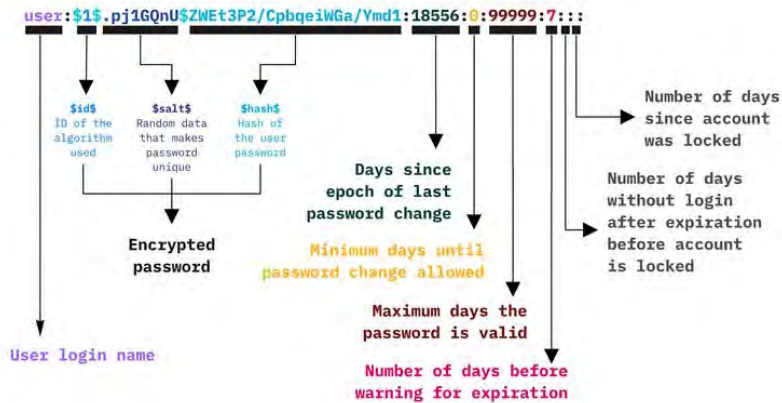
- **Username:** Usado como nombre de usuario (entre 1 y 32 caracteres). 
- **Password:** Una x indica que la contraseña está cifrada y en el fichero `/etc/shadow` como un hash.
- **UID [User ID]:** Número de identificación único de usuario. Los usuarios pueden cambiar muchos parámetros, incluso su name, pero el UID no lo deben cambiar nunca. El UID del root es 0. Las cuentas de servicios y demonios tienen los UID más bajos, mientras que las de usuarios finales comienzan en el valor definido en `UID_MIN` en el fichero `/etc/login.defs`.
- **GID [Group ID]:** Número de identificador único de grupo. Varios usuarios pueden tener el mismo grupo, aunque al crear un usuario se crea un grupo con ese mismo nombre por defecto salvo que se indique lo contrario. Los datos del grupo aparecen en `/etc/group`.
- **GECOS:** Campo de comentarios que incluye información extra sobre el usuario (nombre real, dirección...) Informalmente se le llama información finger.
- **Home directory:** Directorio de inicio del usuario. Los usuarios finales se suelen situar bajo `/home`.
- **Shell:** La shell que utiliza por defecto el usuario (en muchos casos es `/bin/bash`). Si el usuario tiene `/sbin/nologin` o `/usr/bin/false`, significa que no tiene permiso para loguearse en el sistema, lo cual es común en daemons como medida de seguridad.

# Resumen de comandos de gestión de usuarios

useradd /userdel adduser/deluser	crear o borrar un usuario. adduser y deluser - se utilizan con más frecuencia en la práctica que los anteriores por que son mas amigables y ahorran tiempo.
usermod	modificar los campos de /etc/passwd excepto el campo GECOS. Incluye opciones para (des) bloquear un usuario (--lock y --unlock).
chfn	modificar el campo GECOS
chsh	modifica la shell
id	ver info de usuarios y grupos
chage	change age ver y modificar fechas de /etc/shadow



## /etc/shadow



password	un * significa que la cuenta nunca ha tenido password una ! significa cuenta deshabilitada para loguearse mediante password (usermod -l usuario). La contraseña no se borra y al desbloquear el usuario (usermod -u user), se deja el hash como estaba
Lastmod	Tiempo transcurrido desde el último cambio de clave.
Min	Número mínimo de días hasta que se puede volver a cambiar la contraseña.
Max	Número máximo de días hasta que el sistema obliga a cambiar la contraseña del usuario.
Aviso	Número de días previos al Max en los que el usuario es avisado de su obligado cambio de contraseña.
Inactividad	Número de días entre el vencimiento de la contraseña y el bloqueo de la cuenta.
Expiración	Fecha en la que la cuenta se deshabilita. Si se deja en blanco, la cuenta nunca expira.





# Crear un usuario Linux

<https://www.solvetic.com/tutoriales/article/12788-linux-crear-usuario/>

15  
Alfredo Abad



## Gestión de grupos

- Todos los usuarios pertenecen a un único grupo principal o primario, es el que consta como su GID en **/etc/passwd** y opcionalmente pueden pertenecer a otros grupos secundarios o suplementarios que se gestionarían desde **/etc/groups**
- Los grupos permiten conceder permisos a un conjunto de usuarios simultáneamente.
- **/etc/group**
  - Contiene información sobre los grupos del sistema.

www:x:1005:yamada.satou

1 2 3 4

- Campo 1: Nombre del grupo
- Campo 2: Password que permite a un usuario cambiar de grupo. Si está vacío no requiere contraseña, y una x significa que se gestiona mediante el archivo **/etc/gshadow**.
- Campo 3: GID del grupo.
- Campo 4 : usuarios miembros del grupo
- De forma similar, al fichero **/etc/shadow**, existe el fichero **/etc/gshadow**, que almacena los passwords de los grupos encriptados con un hash y también trabaja con los símbolos asterisco \* y exclamación !

16  
Alfredo Abad





## Resumen de comandos de gestión de grupos

<b>groupadd</b>	añade un nuevo grupo
<b>groupdel</b>	borra un grupo
<b>groupmod</b>	modifica la información de /etc/groups
<b>gpasswd</b>	modifica el password del grupo, reflejado en /etc/gshadow
<b>usermod</b>	modifica pertenencia a grupos de un usuario

17  
Alfredo Abad



## Comandos de gestión de grupos (I)

- Añadir un usuario existente a un grupo (-G mayúscula):
  - **sudo usermod -a -G examplegroup exampleusername**
- Añadir un nuevo grupo al sistema
  - **sudo groupadd mynewgroup**
- Cambiar el grupo primario de un usuario (-g minúscula)
  - **usermod -g groupname username**
- Ver los grupos a los que pertenece un usuario: **groups / id**

```
chris@ubuntu: ~  
chris@ubuntu:~$ groups  
chris adm cdrom sudo dip plugdev lpadmin sambashare  
chris@ubuntu:~$ id  
uid=1000(chris) gid=1000(chris) groups=1000(chris),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)  
chris@ubuntu:~$
```

18  
Alfredo Abad



## Comandos de gestión de grupos (y II)

- Crear un usuario y a la vez asignarle a un grupo (luego habrá que asignarle una contraseña con passwd):

- `useradd -G examplegroup exampleusername`
- `sudo passwd exampleusername`

```
chris@ubuntu: ~  
chris@ubuntu:~$ sudo useradd -G ftp jsmith  
chris@ubuntu:~$ sudo passwd jsmith  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
chris@ubuntu:~$
```

- Añadir un usuario a múltiples grupos:
  - `usermod -a -G group1,group2,group3 exampleusername`
- Visualizar todos los grupos de un Sistema:
  - `getent group`

```
chris@ubuntu: ~  
chris@ubuntu:~$ getent group  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:syslog,chris  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mail:x:8:
```

19

Alfredo Abad

## Ficheros /etc/passwd /etc/shadow y /etc/group en GNU/Linux

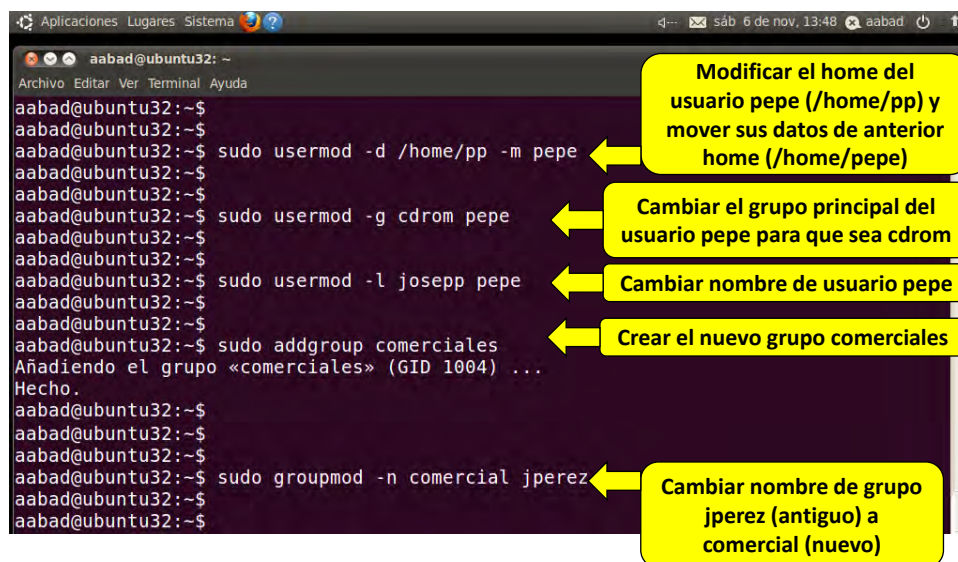
Estudiar el siguiente documento:

ISO-04-032-UsuariosGruposLinux-CLI\_Blog elhacker.NET\_Ficheros \_etc\_passwd  
\_etc\_shadow y \_etc\_group en GNU\_Linux.pdf

20

Alfredo Abad





```
aabad@ubuntu32: ~  
Archivo Editar Ver Terminal Ayuda  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$ sudo usermod -d /home/pp -m pepe  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$ sudo usermod -g cdrom pepe  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$ sudo usermod -l josepp pepe  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$ sudo addgroup comerciales  
Añadiendo el grupo «comerciales» (GID 1004) ...  
Hecho.  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$ sudo groupmod -n comercial jperez  
aabad@ubuntu32:~$  
aabad@ubuntu32:~$
```

Modificar el home del usuario pepe (/home/pp) y mover sus datos de anterior home (/home/pepe)

Cambiar el grupo principal del usuario pepe para que sea cdrom

Cambiar nombre de usuario pepe

Crear el nuevo grupo comerciales

Cambiar nombre de grupo jperez (antiguo) a comercial (nuevo)

21

Alfredo Abad



## Ficheros relacionados con la gestión de usuarios y grupos

- **/etc/passwd**
  - Contiene información sobre cada usuario: ID, grupo principal, descripción, directorio de inicio, shell, etc.
- **/etc/shadow**
  - Contiene las contraseñas encriptadas de los usuarios cuando se emplean shadow passwords
- **/etc/group**
  - Contiene los miembros de cada grupo, excepto para el grupo principal, que aparece en /etc/passwd
- **/etc/skel/**
  - Directorio que contiene la plantilla de perfil para los nuevos usuarios

22

Alfredo Abad



## Algunos grupos especiales

- Grupos especiales asociados a dispositivos (para la gestión de derechos o privilegios)
  - cdrom
    - Afecta a los dispositivos de tipo CD (p.ej.: /dev/hdc)
  - floppy
    - Afecta a unidades de disquete (p.ej.: /dev/fd0)
  - dialout
    - Puertos serie, módems, etc
  - audio
    - Dispositivos de audio
- Para dar acceso a un usuario a los servicios de estos dispositivos basta con añadir al usuario al grupo correspondiente

23  
Alfredo Abad



## Crear una cuenta de sistema (cuenta de servicio)

- Una cuenta de sistema (propia de un servicio) no suele necesitar el directorio HOME
  - Ni necesita una contraseña, puesto que es una cuenta que no iniciará una sesión interactiva
  - Las cuentas de servicio se utilizan para proporcionar permisos (o derechos o privilegios) a los procesos en el seno de los cuales se ejecuta el servicio
- Se puede crear con el siguiente comando:
  - **# adduser --system --no-create-home USERNAME**

24  
Alfredo Abad



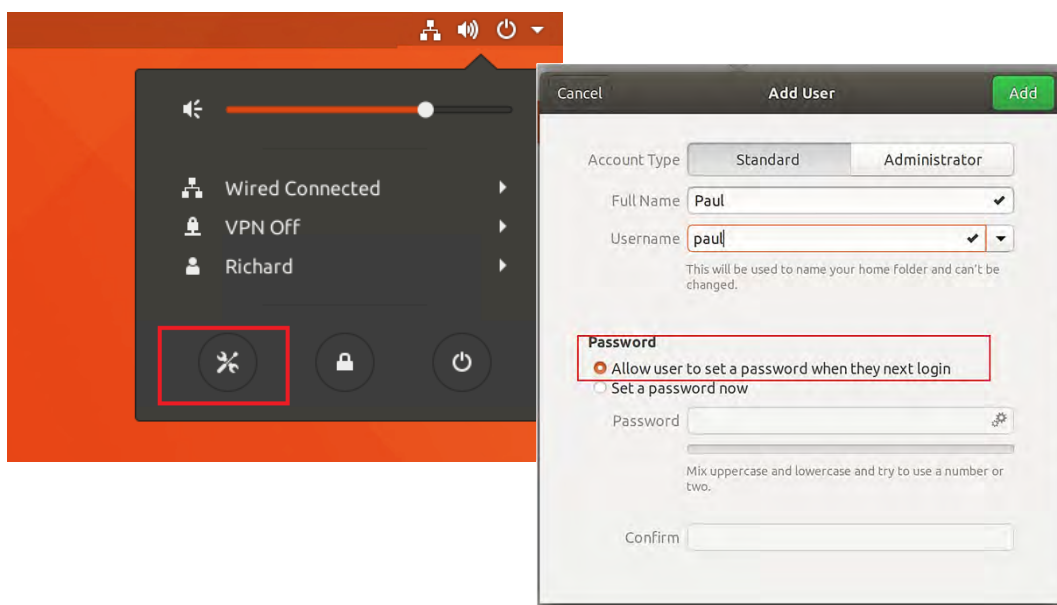
## Forzar a que un usuario cambie su contraseña en el siguiente inicio de sesión

- Cuando expira una contraseña, automáticamente se pide su cambio:
  - **sudo passwd --expire USUARIO**
- También puede usar el comando **chage** con la opción **-d** o **-lastday**, que establece el número de días desde el 1 de enero de 1970 cuando se modificó por última vez la contraseña
  - Cuando se establece a 0, se hace expirar la contraseña
  - **sudo chage --lastday 0 USUARIO**

25  
Alfredo Abad



## Gráficamente



26  
Alfredo Abad





## Habilitar y deshabilitar la cuenta root

- Habilitar la cuenta root (basta con asignarle una contraseña)
  - **sudo passwd root**
  - (Nos pedirá la clave de sudo y dos veces la contraseña que deseemos asignar a root)
- Deshabilitar la cuenta root (una de los siguientes tres comandos)
  - **sudo passwd -l root**
  - **sudo usermod -p '!' root**
  - **sudo - root passwd**

27  
Alfredo Abad



## Listar Usuarios Ubuntu

<https://www.solvetic.com/tutoriales/article/12894-listar-usuarios-ubuntu/>

28  
Alfredo Abad



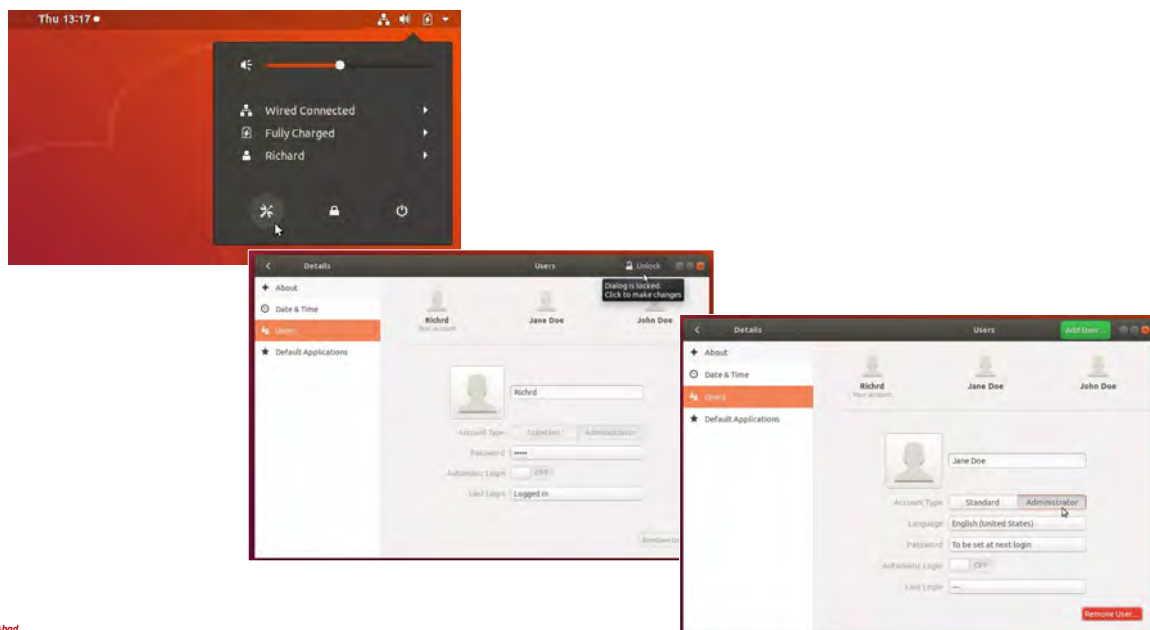


# Convertir un usuario normal en administrador en Ubuntu

29  
Alfredo Abad



## Método gráfico



30  
Alfredo Abad



## Método de línea de comandos

- Añadimos al usuario al grupo sudo
  - `sudo usermod -aG sudo usuario`
- Una vez hecho el cambio podemos validar (o reiniciar sesión):
  - `su - usuario`
- Ejecución de whoami (para comprobar que el cambio se ha realizado)
  - `sudo whoami`
    - root

31  
Alfredo Abad



## Gestión de la caducidad de la contraseña

32  
Alfredo Abad



## Parámetros chage más usados (I)

- **-d o --lastday ULTIMO\_DIA**: Opciones del comando Chage que permite especificar el último cambio de contraseña que realiza un usuario usando el formato de fecha "YYYY-MM-DD".
- Un ejemplo de ello sería:
  - `chage -d 2023-07-19 <nombre_usuario>`
  - `chage --lastday 2023-07-19 <nombre_usuario>`
- Aquí se establecería la fecha del último cambio de contraseña del usuario que pongamos a 19-07-2023 así que el sistema tomará en cuenta que el usuario cambió la contraseña en esa fecha.
- Si quieres eliminar la fecha del último cambio de contraseña podrías usar esta sintaxis configurando entonces que la contraseña no se ha cambiado desde la creación de la cuenta de usuario:
  - `chage -d 0 <nombre_usuario>`

33  
Alfredo Abad



## Parámetros chage más usados (II)

- **-E o --expiredate EXPIRE\_DATE**: permite configurar la fecha o el número de días desde el 1 de enero de 1970 a los cuales ya no se podrá acceder a la cuenta del usuario mencionado.
  - Establece una fecha de vencimiento de una cuenta de usuario como vemos en este ejemplo.
  - Tras la fecha que configuremos, el usuario no podrá acceder a su cuenta.
  - `sudo chage --expiredate 2023-09-01 <nombre_usuario>`
  - `sudo chage -E 2023-09-01 <nombre_usuario>`
- **-I o --inactive INACTIVA**: nos permite asignar el número de días de inactividad desde el momento en que una contraseña haya caducado antes de que la cuenta sea bloqueada automáticamente.
  - En el siguiente ejemplo veremos que será 30 el número de días de inactividad tras los cuales el usuario no podrá acceder a su cuenta y se desactivará.
  - `sudo chage -I 30 <nombre_usuario>`
  - `sudo chage --inactive 30 <nombre_usuario>`

34  
Alfredo Abad



## Parámetros chage más usados (y III)

- **-l o --list:** despliega la información de antigüedad de la cuenta dando información sobre cambios de contraseña:
  - `sudo chage --list <nombre_usuario>`
  - `sudo chage -l <nombre_usuario>`
- **-W o --warndays:** permite asignar la cantidad de días de advertencia para avisar antes de que sea necesario un cambio de contraseña a la cuenta.
  - `sudo chage --warndays 8 <nombre_usuario>`
  - `sudo chage -W 8 <nombre_usuario>`

35  
Alfredo Abad



## Ver el estado de la cuenta: chage -l (usuario)

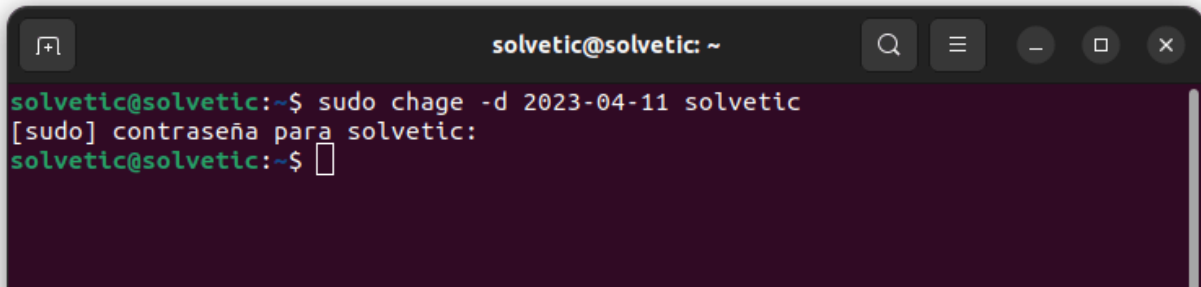
```
solvetic@solvetic: ~  
solvetic@solvetic:~$ chage -l solvetic  
Último cambio de contraseña           : abr 16, 2023  
La contraseña caduca                   : nunca  
Contraseña inactiva                   : nunca  
La cuenta caduca                       : nunca  
Número de días mínimo entre cambio de contraseña : 0  
Número de días máximo entre cambio de contraseña : 99999  
Número de días de aviso antes de que caduque la contraseña : 7  
solvetic@solvetic:~$
```

36  
Alfredo Abad





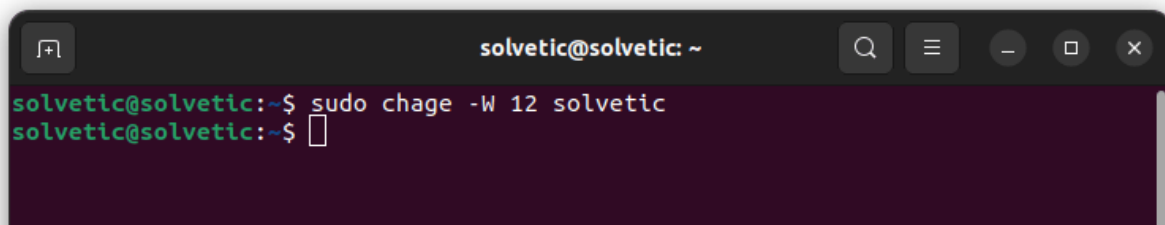
Para establecer la fecha o el número de días de cambio de la contraseña ejecutamos:  
**sudo chage -d (fecha) (usuario)**



```
solvetic@solvetic: ~  
solvetic@solvetic:~$ sudo chage -d 2023-04-11 solvetic  
[sudo] contraseña para solvetic:  
solvetic@solvetic:~$
```

37  
Alfredo Abad

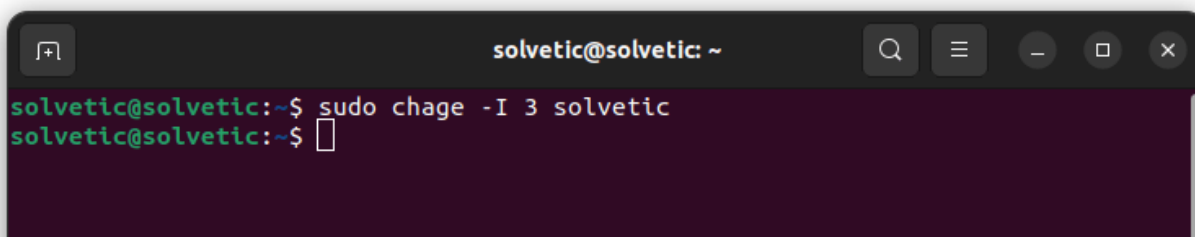
Al bloquearse la cuenta después de no uso se deberá hablar con el administrador del sistema para su reactivación.  
Para establecer la cantidad de días de advertencia antes del cambio de contraseña ejecuta:  
**sudo chage -W #días (usuario)**



```
solvetic@solvetic: ~  
solvetic@solvetic:~$ sudo chage -W 12 solvetic  
solvetic@solvetic:~$
```

38  
Alfredo Abad

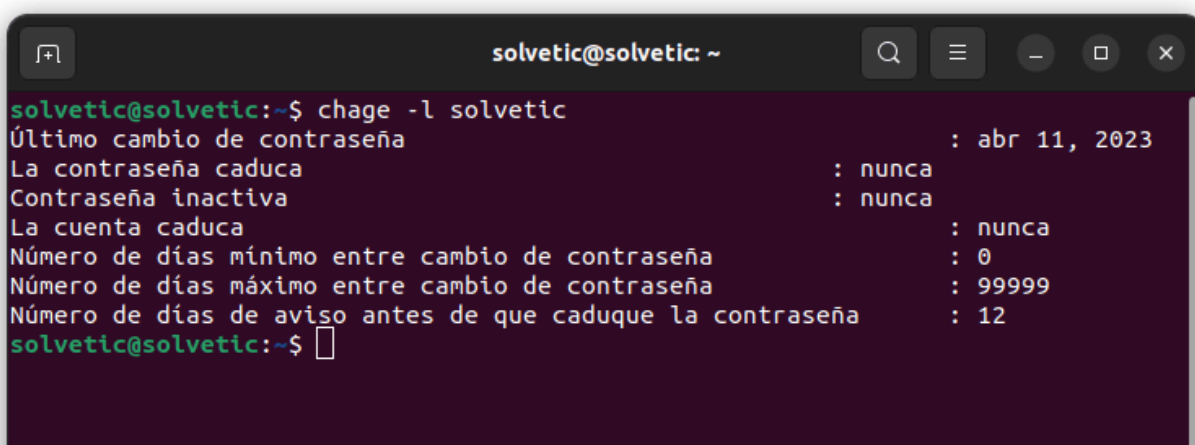
Para definir el número de días de inactividad una vez caduque la contraseña ejecutamos:  
**sudo chage -I #días (usuario)**



```
solvetic@solvetic: ~  
solvetic@solvetic:~$ sudo chage -I 3 solvetic  
solvetic@solvetic:~$
```

39  
Alfredo Abad

Confirma todos los cambios realizados:  
**chage -l (usuario)**



```
solvetic@solvetic: ~  
solvetic@solvetic:~$ chage -l solvetic  
Último cambio de contraseña           : abr 11, 2023  
La contraseña caduca                   : nunca  
Contraseña inactiva                   : nunca  
La cuenta caduca                       : nunca  
Número de días mínimo entre cambio de contraseña : 0  
Número de días máximo entre cambio de contraseña : 99999  
Número de días de aviso antes de que caduque la contraseña : 12  
solvetic@solvetic:~$
```

40  
Alfredo Abad



## ¿Cómo gestionar la complejidad de la contraseña en Linux? (para diversas distribuciones)

Estudiar la siguiente página web:

<https://blog.hostdime.com.co/mejorar-la-seguridad-de-contrasenas-en-linux/>

41  
Alfredo Abad



## ¿Cómo deshabilitar la cuenta de un usuario?

42  
Alfredo Abad



Cuando el administrador de sistemas quiere evitar que se utilice cierta cuenta de usuario, es buena idea deshabilitar el usuario en vez de eliminarlo, de esta forma conseguimos, si fuera necesario, poder reestablecer la cuenta de usuario en muy poco tiempo manteniendo todos los permisos.

Veamos distintas formas para deshabilitar un usuario en Linux:

### 1) Linux, deshabilitar usuario con `usermod`:

Para deshabilitar usuario:

```
usermod -L usuario
```

**L=lock**

**U=Unlock**

Para habilitar usuario:

```
usermod -U usuario
```

43  
Alfredo Abad



Veamos un laboratorio completo para entender su funcionamiento:

```
#Creamos el usuario sysadmit
```

```
useradd sysadmit
```

```
#Asignamos password al usuario sysadmit
```

```
passwd sysadmit
```

```
#Conectamos vía SSH al propio host, como el usuario sysadmit
```

```
#Conecta OK.
```

```
ssh sysadmit@localhost
```

```
#Salimos de la conexión SSH, ejecutando: exit
```

```
#Deshabilitamos el usuario
```

```
usermod -L sysadmit
```

44  
Alfredo Abad



```
#Volvemos a conectar vía SSH al propio host, como el usuario
sysadmit
#Nos contestará: Permission denied, please try again.

ssh sysadmit@localhost

#Habilitamos el usuario sysadmit

usermod -U sysadmit

#Conectamos vía SSH al propio host, como el usuario sysadmit
#Conecta OK.

ssh sysadmit@localhost
```

45  
Alfredo Abad



## 2) Linux, deshabilitar usuario con passwd:

Otra opción es utilizar el comando `passwd`.

El comando `passwd` es utilizado para cambiar la contraseña de un usuario, sin embargo disponemos de los parámetros: `-l` (lock) y `-u` (unlock) para deshabilitar o habilitar la cuenta.

Para deshabilitar usuario:

```
passwd -l usuario
```

Para habilitar usuario:

```
passwd -u usuario
```

46  
Alfredo Abad





**Linux, ver si un usuario está deshabilitado.**

Tanto si utilizamos el comando `usermod` o el comando `passwd` para deshabilitar una cuenta, el resultado quedará plasmado en el fichero `/etc/shadow`

El fichero `/etc/shadow` contiene las contraseñas cifradas de cada usuario.

Si por ejemplo, ejecutamos:

```
cat /etc/shadow|grep sysadmit
```

Veremos la contraseña cifrada el usuario `sysadmit`

La diferencia entre una cuenta deshabilitada y otra habilitada es:

Si la cuenta está deshabilitada, la cadena de la contraseña empieza por el carácter: `!`

Ejemplo:

```
[root@LINUX1 ~]# cat /etc/shadow|grep sysadmit
sysadmit:$6$VYURxYg7$MFqrlyskXd.UyfR2fkS3HQsTBKutFX9tgsgbY5

[root@LINUX1 ~]# usermod -L sysadmit

[root@LINUX1 ~]# cat /etc/shadow|grep sysadmit
sysadmit:!!$6$VYURxYg7$MFqrlyskXd.UyfR2fkS3HQsTBKutFX9tgsgbY
```

47  
Alfredo Abad



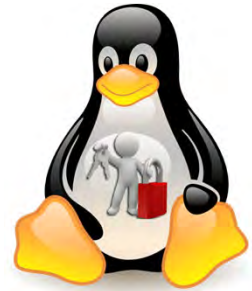
## Permitir que root inicie sesión gráfica en Ubuntu con GNOME

Por defecto, la cuenta `root` está deshabilitada. Se habilitará al asignarle una contraseña, pero para ser utilizada desde la GUI es necesario realizar unos ajustes porque GNOME impide que `root`, aun estando habilitado, consuma la interfaz gráfica:

<https://itsfoss.com/ubuntu-login-root/>

48  
Alfredo Abad





# Ajuste de permisos de directorios de usuarios de nueva creación con adduser

49  
Alfredo Abad



## Descripción del problema

- Por defecto, cada nueva cuenta de usuario que cree en un sistema Linux, el directorio de inicio de la cuenta se abre automáticamente a todos los demás usuarios en el sistema
  - La carpeta de inicio del usuario y todo el contenido se vuelve accesible y legible por todos
- En algunos entornos, esto puede no interesar y habrá que asegurarse de que todos los usuarios creados en un sistema Linux disponen de directorios de inicio protegidos desde el momento de su creación
- Algo a tener en cuenta es que aunque todos los usuarios pueden ver contenido en otros directorios principales, no podrán editar ese contenido
  - Solo pueden ver pero no editar
  - Pero aún así, sigue siendo un problema de seguridad

50  
Alfredo Abad



## adduser y /etc/adduser.conf

- Cada vez que ejecuta el comando **adduser**, los valores predeterminados para el usuario se extraen del archivo **/etc/adduser.conf**
- Todas las configuraciones de configuración en ese archivo se aplican a todas las cuentas nuevas
- Si se desea evitar que los usuarios vean las carpetas de inicio, se puede editar ese archivo de configuración y realizar los cambios allí
- Por lo tanto, para evitar permisos legibles por todo el mundo para todos los usuarios nuevos creados en sistemas Linux, deben ejecutarse los siguientes comandos para abrir el archivo predeterminado adduser.conf:
  - **sudo nano /etc/adduser.conf**

51  
Alfredo Abad



```
sudo nano /etc/adduser.conf
```

Then change the line that reads:

```
</>  
# If DIR_MODE is set, directories will be created with the specified  
# mode. Otherwise the default mode 0755 will be used.  
DIR_MODE=0755
```

and change it to the line below

```
</>  
# If DIR_MODE is set, directories will be created with the specified  
# mode. Otherwise the default mode 0755 will be used.  
DIR_MODE=0750
```

Save the file and you're done...

52  
Alfredo Abad



## La ejecución de adduser ahora quedará así:

```
</>
sudo adduser johndoe
Adding user `johndoe' ...
Adding new group `johndoe' (1001) ...
Adding new user `johndoe' (1001) with group `johndoe' ...
Creating home directory `/home/johndoe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for johndoe
Enter the new value, or press ENTER for the default
    Full Name []: John Doe
    Room Number []: 101
    Work Phone []: 123-133-1244
    Home Phone []: 123-133-1244
    Other []:
Is the information correct? [Y/n] Y
```

Only the admin or an account with sudo permissions enabled will be able to view content in other home directories...

53  
Alfredo Abad



## Resumen de algunos ficheros que intervienen

- **/etc/passwd**
  - Contains one line for each user account.
- **/etc/shadow**
  - Contains the password information in encrypted format for the system's accounts and optional account aging information.
- **/etc/group**
  - Defines the groups on the system.
- **/etc/default/useradd**
  - This file contains a value for the default group, if none is specified by the useradd command.
- **/etc/login.defs**
  - This file defines the site-specific configuration for the shadow password suite stored in /etc/shadow file.

54  
Alfredo Abad



# Scripts de configuración en inicio de sistema y de sesión

55  
Alfredo Abad



## Scripts predeterminados

- Existen cuatro ficheros de texto ejecutables y personalizables predeterminados que el sistema operativo ejecuta de forma automática cuando se dan ciertas condiciones.
  - Estos scripts, una especie de guiones que contienen órdenes y estructuras son interpretados por el Shell.
- Podemos modificarlos con cualquier editor de texto e incluir cualquier orden de la línea de comandos que se ejecutará en el momento que lo haga el script
- **Importante:** En caso de que un fichero de configuración general entre en conflicto con uno específico hay que tener en cuenta que primero se procesa el general y a continuación el específico
- (Ver ejemplo en diapo siguiente)

56  
Alfredo Abad





```

.bashrc
73  esac
74
75  # enable color support of ls and also add handy aliases
76  if [ -x /usr/bin/dircolors ]; then
77      test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval "$(dircolors -b)"
78      alias ls='ls --color=auto'
79      #alias dir='dir --color=auto'
80      #alias vdir='vdir --color=auto'
81
82      alias grep='grep --color=auto'
83      alias fgrep='fgrep --color=auto'
84      alias egrep='egrep --color=auto'
85  fi
86
87  # colored GCC warnings and errors
88  #export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'
89
90  # some more ls aliases
91  alias ll='ls -alF'
92  alias la='ls -A'
93  alias l='ls -CF'

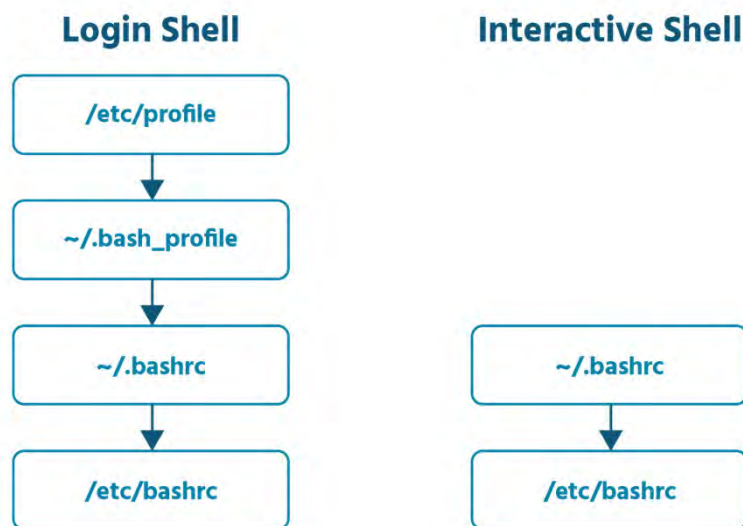
```

57  
Alfredo Abad

## Nombre y función de los cuatro ficheros

- **~/.bashrc**
  - Es un fichero oculto que se encuentra en el home de cada usuario, que es de su propiedad y que puede modificar.
  - **Se ejecuta cada vez que su propietario abre un terminal bash**
  - Se usa para personalizar configuraciones de un usuario específico: crear alias, cambiar el prompt, definir funciones nuevas, etc.
- **/etc/bash.bashrc (o /etc/bashrc)**
  - Es un fichero de configuración general propiedad del root que solo el root puede modificar.
  - **Se ejecuta cada vez que cualquier usuario abre un terminal bash**
  - Se usa para personalizar la configuración de todos los usuarios
- **~/.profile (o ~/bash\_profile)**
  - Es un fichero oculto que se encuentra en el home de cada usuario, que es de su propiedad y que puede modificar.
  - **Se ejecuta cada vez que su propietario inicia sesión**
  - Se usa para personalizar configuraciones de un usuario específico.
- **/etc/profile**
  - Es un fichero de configuración general propiedad del root que solo el root puede modificar.
  - **Se ejecuta cada vez que cualquier usuario inicia sesión**
  - Se usa para personalizar la configuración de todos los usuarios.

## Precedencia de ejecución de scripts en Ubuntu para /bin/bash



59

Alfredo Abad



## Notas sobre la precedencia de ficheros (procede de AI de Bing)

- El orden de precedencia de los ficheros de inicio de usuario en Linux depende del tipo de shell que se utilice. Por lo general, existen dos tipos de shell: las Bourne-compatible (como bash o sh) y las C-compatible (como csh o tcsh). Cada tipo de shell tiene sus propios ficheros de inicio que se ejecutan al iniciar sesión o al abrir una terminal.
- Para las **shells Bourne-compatible**, el orden de precedencia es el siguiente<sup>2</sup>:
  - `/etc/profile`: se ejecuta para todos los usuarios al iniciar sesión.
  - `~/.bash_profile`: se ejecuta para el usuario actual al iniciar sesión (solo si existe).
  - `~/.bash_login`: se ejecuta para el usuario actual al iniciar sesión (solo si no existe `~/.bash_profile`).
  - `~/.profile`: se ejecuta para el usuario actual al iniciar sesión (solo si no existen `~/.bash_profile` ni `~/.bash_login`).
  - `/etc/bash.bashrc`: se ejecuta para todos los usuarios al abrir una terminal interactiva.
  - `~/.bashrc`: se ejecuta para el usuario actual al abrir una terminal interactiva.
- Para las **shells C-compatible**, el orden de precedencia es el siguiente:
  - `/etc/csh.cshrc`: se ejecuta para todos los usuarios al iniciar sesión o al abrir una terminal interactiva.
  - `/etc/csh.login`: se ejecuta para todos los usuarios al iniciar sesión.
  - `~/.tcshrc`: se ejecuta para el usuario actual al iniciar sesión o al abrir una terminal interactiva (solo si existe y la shell es tcsh).
  - `~/.cshrc`: se ejecuta para el usuario actual al iniciar sesión o al abrir una terminal interactiva (solo si no existe `~/.tcshrc` o la shell es csh).
  - `~/.login`: se ejecuta para el usuario actual al iniciar sesión.

60

Alfredo Abad



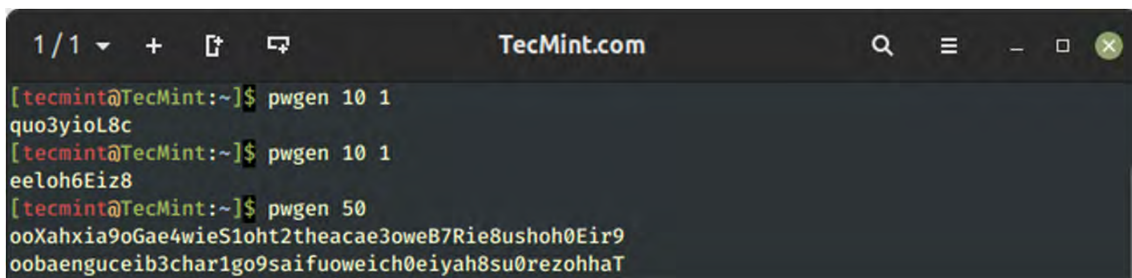
# Creación de contraseñas complejas en Linux

61  
Alfredo Abad



## pwgen

- `sudo apt install pwgen`
- Sintaxis de uso:
  - `pwgen [opciones] [longitud_clave] [numero_de_claves]`
- Opciones: diapo siguiente



```
1 / 1 + [f] [m] TecMint.com [Q] [≡] [-] [□] [X]
[tecmint@TecMint:~]$ pwgen 10 1
quo3yioL8c
[tecmint@TecMint:~]$ pwgen 10 1
eeloh6Eiz8
[tecmint@TecMint:~]$ pwgen 50
ooXahxia9oGae4wieS1oht2theacae3oweB7Rie8ushoh0Eir9
oobaenguceib3char1go9saifuoweich0eiyah8su0rezohhaT
```

62  
Alfredo Abad



## Opciones de pwgen

- -0, --no-numerals Don't include numbers in the generated passwords.
- -1 Print the generated passwords one per line.
- -A, --no-capitalize Don't bother to include any capital letters in the generated passwords.
- -a, --alt-phonics This option doesn't do anything special; it is present only for backwards compatibility.
- -B, --ambiguous Don't use characters that could be confused by the user when printed, such as 'l' and '1', or '0' or 'O'. This reduces the number of possible passwords significantly, and as such reduces the quality of the passwords. It may be useful for users who have bad vision, but in general use of this option is not recommended.
- -c, --capitalize Include at least one capital letter in the password. This is the default if the standard output is a tty device.
- -C Print the generated passwords in columns. This is the default if the standard output is a tty device.
- -N, --num-passwords=num Generate num passwords. This defaults to a screenful if passwords are printed by columns, and one password.
- -n, --numerals Include at least one number in the password. This is the default if the standard output is a tty device.
- -H, --sha1=/path/to/file[#seed] Will use the sha1's hash of given file and the optional seed to create password. It will allow you to compute the same password later, if you remember the file, seed, and pwgen's options used. ie: pwgen -H ~/your\_favorite.mp3#your@email.com gives a list of possibles passwords for your pop3 account, and you can ask this list again and again.
  - WARNING: The passwords generated using this option are not very random. If you use this option, make sure the attacker can not obtain a copy of the file. Also, note that the name of the file may be easily available from the ~/.history or ~/.bash\_history file.
- -h, --help Print a help message.
- -s, --secure Generate completely random, hard-to-memorize passwords. These should only be used for machine passwords, since otherwise it's almost guaranteed that users will simply write the password on a piece of paper taped to the monitor...
- -v, --no-vowels Generate random passwords that do not contain vowels or numbers that might be mistaken for vowels. It provides less secure passwords to allow system administrators to not have to worry with random passwords accidentally contain offensive substrings.
- -y, --symbols Include at least one special character in the password.

63  
Alfredo Abad



## También se encuentra disponible en forma de plugin para Firefox

**FxPassword Generator**

**Password Options:**

- include Numbers: ☒
- include capital letters: ☒
- no ambiguous characters: ☒
- include special character: ☒
- no vowels: ☐
- password length: 6

**generate**

**New Password:**

ka4Ak;

[embed this in your website](#) [by subclosure.com](#)

64  
Alfredo Abad



## makepasswd

- **sudo apt install makepasswd**
- Sintaxis de uso:
  - **makepasswd --char 20 --count 7**

A terminal window titled 'TecMint.com' showing the execution of the 'makepasswd' command. The prompt is '[tecmint@TecMint:~]\$'. The first command is 'makepasswd', which outputs 'e4jHJIgr0D'. The second command is 'makepasswd --char 50', which outputs 'YcNwyGbeWY3JP3aiXuGCV Ae0VbI1Vr4Wjti5dRBhYUw5J4AQmy'. The third command is 'makepasswd --char 20 --count 7', which outputs a 20-character password 'wcn5rXt7ApcXvMfsDvDg' followed by a newline and a 7-character password '5VSECmf5eapFGTIsI0EP'. The terminal window has a dark background and a green border. The TecMint logo is visible in the bottom right corner.

```
1/1 + [ ] [x] TecMint.com
[tecmint@TecMint:~]$
[tecmint@TecMint:~]$ makepasswd
e4jHJIgr0D
[tecmint@TecMint:~]$
[tecmint@TecMint:~]$ makepasswd --char 50
YcNwyGbeWY3JP3aiXuGCV Ae0VbI1Vr4Wjti5dRBhYUw5J4AQmy
[tecmint@TecMint:~]$
[tecmint@TecMint:~]$ makepasswd --char 20 --count 7
wcn5rXt7ApcXvMfsDvDg
5VSECmf5eapFGTIsI0EP
pc4Ia7T55TrFWymoQVyN
rjNgNbBPR7D8djzoye2C
jV9u0w47Ij7Yem0ooVMW
RtgUNQfE0BMQHyMh2F4N
YGwf4FKGi1qcMzVyrj5a
[tecmint@TecMint:~]$
```

65  
Alfredo Abad

