

CASO PRÁCTICO 1

- **TÍTULO**
GESTIÓN DE USUARIOS Y GRUPOS

- **SITUACIÓN**

Se necesita organizar el acceso a los recursos de un sistema Linux para garantizar su seguridad. Para ello debemos crear los usuarios y grupos precisos, y asignarles los permisos correspondientes.

- **INSTRUCCIONES:**

1. Crea en un sistema Linux dos grupos: contabilidad y administración.

```
root@debian1:~# addgroup contabilidad
Añadiendo el grupo `contabilidad' (GID 1001) ...
Hecho.
root@debian1:~# addgroup administracion
Añadiendo el grupo `administracion' (GID 1002) ...
Hecho.
root@debian1:~#
```

Se entra en root con su - y se ejecuta el comando addgroup con los respectivos comandos.

2. Crea cuatro usuarios y asigna dos de ellos a cada grupo de los creados anteriormente.

```
root@debian1:~# adduser antonio
Añadiendo el usuario `antonio' ...
Añadiendo el nuevo grupo `antonio' (1003) ...
Añadiendo el nuevo usuario `antonio' (1001) con grupo `antonio' ...
Creando el directorio personal `/home/antonio' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
Las contraseñas no coinciden.
passwd: Error de manipulación del testigo de autenticación
passwd: no se ha cambiado la contraseña
¿Intentar de nuevo? [s/N] s
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para antonio
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
Nombre completo []: antonio
Número de habitación []: 1
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] s
```

Se ha creado el usuario con adduser y se ha puesto su respectiva contraseña segura tal y como se indica en la unidad así como en los otros 3 usuarios.

```

root@debian1:~# usermod -a -G contabilidad maria
root@debian1:~# usermod -a -G contabilidad jose
root@debian1:~# usermod -a -G administracion antonio
root@debian1:~# usermod -a -G administracion pepe
root@debian1:~# groups pepe
pepe : pepe administracion
root@debian1:~# groups antonio
antonio : antonio administracion
root@debian1:~# groups jose
jose : jose contabilidad
root@debian1:~# groups maria
maria : maria contabilidad

```

Como se ve en la diapositiva se han añadido los usuarios a sus respectivos grupos y se ha comprobado con el comando groups.

3. Si no lo has hecho inicialmente, revisa y cambia la contraseña de los usuarios anteriores de forma que cumplan lo estudiado en la unidad. Ya se pusieron sus contraseñas seguras desde un principio, con su mayúscula, carácter especial y número.
4. Asigna los permisos necesarios para que los usuarios que no pertenezcan al grupo de administración puedan borrar ficheros.

```
drwxr-xrwx 7 root amdinistracion 4096 ene 3 20:49 home
```

Se ha cambiado el propietario de la carpeta home (ya que no se especifica cual es) a administración para que, el usuario tenga todos los permisos (root), el grupo administración que no pueda borrar y los otros que puedan hacer todo. Los comandos utilizados son: chown para la carpeta y chmod para los permisos. Si quiere que todos tengan todos los permisos seria 777 en vez de 757 o que solo puedan borrar y no leer ni ejecutar los otros seria, 772, pero como se ha entendido que los otros podrán hacer todo y el grupo todo menos borrar pues ha sido 757, pero aquí están las otras posibles soluciones.

Conclusión: Linux es muy lioso y se puede liar bastante fácil, a parte que ni en la teoría ni en internet ponía algo similar y he tenido que buscar fuentes externas, ya que en la teoría solo aparecía chmod y a la hora de buscar en internet como hacerlo con un grupo o usuario específico no venía nada.