C. GESTION DE CONTRASEÑAS

1. Cambiar la propia contraseña.

El usuario puede cambiar su contraseña en cualquier momento ejecutando el comando `passwd`. El comando `passwd` pide la contraseña actual y la nueva dos veces para comprobar que se introduce correctamente.

```
$ passwd
Changing password for usuario1.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

Recordar que el binario de este comando debe tener el bit set-UID activado para que la nueva contraseña pueda ser almacenada en `/etc/shadow`.

2. Cambiar la contraseña de otro usuario.

Solo es posible hacerlo el usuario root o cualquier otro usuario que este incluido en /etc/sudoers, es decir pueda ejecutar sudo.

```
$ sudo passwd usuario1
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
```

3. Bloquear y desbloquear la contraseña

Es posible que en un momento determinado al administrador le interese bloquear la contraseña de un usuario para que no entre en el sistema. Para ello se puede utilizar el comando `passwd` de la forma siguiente:

```
$ sudo passwd -l usuario1
passwd: información de caducidad de la contraseña cambiada
```

El mensaje que recibirá el usuario es que se le ha denegado el permiso.

Si se quiere desbloquear la cuenta ejecutar la orden siguiente:

```
$ sudo passwd -u usuario1
passwd: información de caducidad de la contraseña cambiada
```

A partir de ahora el usuario1 puede acceder al sistema.

4. Forzar el cambio de contraseña para un usuario.

A menudo al realizar el registro en determinados sitios web se asigna al usuario una contraseña que es temporal y se le fuerza a que cambie esta contraseña cuando se conecte por primera vez. Para ello hay que ejecutar el siguiente comando:

```
$ sudo passwd -e usuario1
passwd: información de caducidad de la contraseña cambiada
```

Cuando se conecte el usuario1 con la contraseña temporal tendrá que cambiarla. Una vez cambiada hay que volver a logearse con la nueva contraseña.

5. Configurar el tiempo de expiración de la contraseña.

Existen dos métodos para realizar esta acción

1. Configurar el mínimo número de días hasta que el usuario pueda cambiar su contraseña
2. Configurar el máximo de días que se puede estar sin cambiar la contraseña y, pasados esos días la contraseña hay que cambiarla.

En el primer caso deberan pasar al menos XX días para que el usuario pueda cambiar su contraseña. Por ejemplo:

```
$ sudo passwd -n 10 usuario1
passwd: información de caducidad de la contraseña cambiada.
```

Si ahora el usuario1 ejecuta `passwd` y no han transcurrido esos días no puede cambiar su contraseña.

```
$ passwd
Cambiando la contraseña de usuario1.
Contraseña actual de :
Debe esperar más tiempo para cambiar la contraseña
passwd: Error de manipulación del testigo de autenticación
passwd: no se ha cambiado la contraseña
```

En el segundo caso, para fijar el máximo de días que se puede estar sin cambiar la contraseña, y, pasados esos días se debe cambiar, hay que ejecutar el comando siguiente:

```
$ sudo passwd -x 100 usuario1
passwd: información de caducidad de la contraseña cambiada.
```

6. Comprobar el estado de una contraseña.

Para comprobar el estado de la contraseña de un usuario hay que ejecutar el comando siguiente:

```
$ sudo passwd -S usuario1
usuario1 P 03/03/2022 90 120 7 -1
```

Donde:

- usuario1: login del usuario consultado.
- P, L, NP: indican si la contraseña esta funcionando, está bloqueda o no tiene contraseña, respectivamente.
- 03/03/2022: fecha del último cambio
- 90: periodo mínimo de cambio
- 120: periodo máximo de cambio
- 7: periodo de aviso
- -1: inactividad de la contraseña