```
# CREAR CLAVES:
gpg --gen-key

si queremos que salgan todas las opciones usa: gpg --full-generate-key

 En el proceso nos pedira crear una *contraseña para la hora de descifrar
 mensajes que nos envien con nuestra pub, (debe de ser muy fuerte)


pub = clave principal
sub = clave subordinanda


# LISTAR CLAVES:
gpg --list-keys
gpg --list-public-keys
gpg --list-secret-keys
# VER UUID :
gpg --list-secret-keys --keyid-format=long

# EXPORTAR CLAVE PRIVADA:
gpg -a --export-secret-key "Nombre" > PRIV-key

# EXPORTAR CLAVE PUBLICA: (la nuestra)
gpg -a --export -o clave.pub

# IMPORTAR CLAVE PUBLICA: (de un tercero)
gpg --import clave.pub


# CIFRAR MENSAJES (con cualquier clave ya sea nuestra de otra persona)
gpg -er "Clave-Publica" mensaje-que-ciframos

# DESCIFRAR MENSAJES (receptor descifra el mensaje)
gpg -d mensaj > NombreQueQuieras
Pedirá la *contraseña


# ELIMINAR UNA CLAVE PÚBLICA
gpg --delete-key "Nombre de Usuario"

# ELIMINAR CLAVE SECRETA
gpg --delete-secret-key "Nombre de Usuario"


# --- FIRMAS --- # (el que recibe el mensaje puede verificar quien lo envió)

# FIRMAR Y CIFRAR: (--sign = -s)
gpg --sign mensaje (encripta y firma con nuestra clave)

# FIRMAR "SIN" CIFRAR (texto plano)
gpg --clear-sign mensaje

# VERIFICACION DE FIRMA: (para los dos casos anteriores)
gpg --verify mensaje
```

```
###
# FIRMA EN ARCHIVO SEPARADO (se enviarían 2: mensaje y firma.sig)
gpg --detach-sig archivo (puede ser cifrado o no)

# VERIFICACION DE FIRMA:
gpg --verify firma.sig mensaje

# VERIFICAR FICHERO DESCARGADO Y SU ASC CORRESPONDIENTE:
gpg --verify correspondiente.asc fichero-descargado-x86_64.AppImage

# --- EDITAR CLAVES --- #

 gpg --edit-key "user"

 Una vez dentro comandos:

 passwd    ==> cambiar passwd
 trust     ==> nivel de confianza en la clave (para que no pregunte siempre)
 expire    ==> Cambiar fecha de caducidad (ver instrucciones abajo)
 quit      ==> Salir
 save      ==> Guardar y salir

# --- CAMBIAR FECHA DE CADUCIDAD --- #

El primer paso será editar la llave con el comando: gpg --edit-key "Nombre Clave"


Se lista la clave pública con ID 85268F85 (identificada con pub al
comienzo de la línea)
y la subclave 13B69DCC (identificada con sub al comienzo de la línea),
que es la que uso para cifrar.

Con el anterior comando, entraremos en una CLI de gpg.
Clave pública y subclave tienen fechas de expiración independientes.
Lo primero será seleccionar la clave pública con la ejecución:
> key 0

Renovamos fecha de caducidad con comando  "expire" y ampliamos la fecha de
caducidad utilizando la unidad que deseemos. (0 no caduca nunca)
> expire

Sin salir de la consola de gpg, cambiamos el selector a la clave 1
> key 1

#  --- BORRAR SUBCLAVE --- #

El --edit-keymenú interactivo de GnuPG funciona de manera diferente.
No selecciona una subclave por key [subkey-id], pero key [key-index],
 en su caso, sería key 2
 (la segunda subclave desde arriba, la clave principal no cuenta).

 sec  rsa4096/11111111
          created: 2016-12-12  expires: 2017-12-12  usage: SC
          confiance : ultime        validity: ultimate
ssb  rsa4096/22222222
          created: 2016-12-12  expires: 2017-12-12  usage: E
```

```
ssb  rsa4096/33333333     ============================> 2ª
          created: 2016-12-12  expires: never       usage:
ssb  rsa4096/44444444
          créé : 2016-12-12  expires: 2017-12-12  usage: S
[  ultimate ] (1). me <me@example.com>

 Después de seleccionar una o más teclas (*), ejecute delkeypara eliminar
 las subclaves seleccionadas. ¡No te olvides save!
```