**Configuración inicial:**

**Generar un par de claves:**

gpg --full-generate-key

Sigue las instrucciones para seleccionar el tipo de clave y la longitud. También se te pedirá ingresar tu nombre, dirección de correo electrónico y una frase de contraseña.

**Listar claves:**

gpg --list-keys

**Exportar clave pública:**

gpg --armor --export tu-correo@example.com > clave\_publica.asc

**Exportar clave privada:**

gpg --armor --export-secret-keys tu-correo@example.com > clave\_privada.asc

**Importar una clave:**

gpg --import clave\_privada.asc

**Uso básico:**

**Cifrado asimetrico:**

gpg –encrypt archivo.txt

**Cifrado simetrico:**

Gpg –c texto.txt

**Cifrado ascii:**

Gpg –c –a texto.txt

**Descifrar un archivo:**

gpg --decrypt archivo.txt.gpg

**Firmar un archivo:**

gpg --sign archivo.txt

**Verificar la firma:**

gpg --verify archivo.txt.gpg

**Importar una clave pública:**

gpg --import clave\_publica.asc

**Listar claves secretas:**

gpg --list-secret-keys

**Comandos adicionales:**

**Editar una clave:**

gpg --edit-key tu-correo@example.com

**Revocar una clave:**

gpg --gen-revoke tu-correo@example.com > revocacion.asc

**Cambiar la frase de contraseña:**

gpg --edit-key tu-correo@example.com