¿Qué es GPG?

GNU Privacy Guard (GnuPG o GPG) es una herramienta de cifrado y firmas digitales que implementa el estándar OpenPGP. GnuGPG permite encriptar y firmar tanto datos como comunicaciones (emails por ejemplo). Cuenta con un sistema de gestión de claves versátil, junto con módulos de acceso para todo tipo de directorios de claves públicas. También conocido como GPG, es una herramienta de línea de comandos con funciones para una fácil integración con otras aplicaciones.

GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. Las claves públicas pueden ser compartidas con otros usuarios de muchas maneras, un ejemplo de ello es depositándolas en los servidores de claves.

NOTA: NUNCA COMPARTA SU CLAVE PRIVADA, GUÁRDELA A BUEN RECAUDO Y SÓLO REMITA O PUBLIQUE EN UN SERVIDOR DE CLAVES LA PÚBLICA.

GPG para usuarios linux

Todas las distribuciones linux incorporan la aplicación por defecto.

Generar una par de claves (pública y privada)

```
gpg --gen-key
```

Se debe contestar a una serie de preguntas en orden para generar la clave pública y privada:

- Key type. RSA-RSA por defecto.
- Expiration time: Tiempo de validez de la clave.
- User data (Real name, email, comment) . Estos datos son usados para identificar la clave en servidores de claves públicas y/o cuando se le envían a otros usuarios
- Password: Contraseña para proteger la clave privada.

Exportar la clave publica

```
gpg --armor --output myname_public_key.asc --export 'Name Surname'
```

Importar una clave publica

```
gpg --import johndoe.asc
```

Listar las claves públicas importadas con el siguiente comando:

```
gpg --list-keys
```

Encriptar archivos con una clave pública importada

```
gpg --encrypt --recipient 'Name Surname' file.txt
```

Desencriptar archivos con la clave privada (si es de nuestra propiedad)

```
gpg --output file.txt --decrypt file.txt.gpg
```

Otros links utiles sobre gpg

- <https://www.madboa.com/geek/gpg-quickstart/>