Cifrado en Linux: Manual Paso a Paso

El cifrado de archivos es una práctica esencial para proteger la información sensible de accesos no autorizados. En el entorno Linux, la herramienta estándar y más recomendada para esta tarea es **GnuPG (GNU Privacy Guard)**, una implementación libre del estándar OpenPGP.

Este manual le guiará a través de los pasos necesarios para instalar GnuPG y utilizarlo para cifrar y descifrar archivos de forma segura.

---

1. Herramienta Principal: GnuPG (gpg)

GnuPG (a menudo llamado `gpg`) permite cifrar y firmar datos utilizando dos métodos principales:

1. **Cifrado Simétrico (por contraseña):** Utiliza una única contraseña para cifrar y descifrar el archivo. Es ideal para proteger archivos personales o para transferencias rápidas donde la clave se comparte de forma segura.
2. **Cifrado Asimétrico (por clave pública/privada):** Utiliza un par de claves. Se cifra con la **clave pública** del destinatario, y solo puede descifrarse con su correspondiente **clave privada**. Es el método más seguro para compartir archivos con terceros.

---

2. Instalación de GnuPG

En la mayoría de las distribuciones modernas de Linux, GnuPG ya viene preinstalado. Si no es el caso, puede instalarlo fácilmente usando el gestor de paquetes de su distribución.

Distribución	Comando de Instalación
Debian/Ubuntu	`sudo apt update && sudo apt install gnupg`
Fedora/CentOS/RHEL	`sudo dnf install gnupg`
Arch Linux	`sudo pacman -S gnupg`

Para verificar que la herramienta está instalada, ejecute:

```
gpg --version
```

---

3. Cifrado Simétrico (con Contraseña)

Este es el método más sencillo y rápido para proteger un archivo con una contraseña.

Paso a Paso

1. **Cifrar el archivo:** Utilice la opción `-c` (symmetric encryption).

   `bash gpg -c nombre_del_archivo.txt`

2. **Introducir Contraseña:** El sistema le pedirá que introduzca y confirme una contraseña. **Asegúrese de que sea una contraseña fuerte y que pueda recordar.**

   `Cifrado simétrico. Introduzca la frase de paso: Repita la frase de paso:`

3. **Resultado:** Se creará un nuevo archivo cifrado con la extensión `.gpg` (o `.asc` si se usa la opción `--armor` para texto plano). El archivo original (`nombre_del_archivo.txt`) se mantiene intacto.

   Archivo cifrado: `nombre_del_archivo.txt.gpg`

Ejemplo Práctico

Cifrar un archivo llamado `informe_secreto.pdf`:

```
gpg -c informe_secreto.pdf
```

Descifrado

Para recuperar el archivo original, utilice la opción `-d` (decrypt) o simplemente el comando `gpg` sin opciones, indicando el nombre del archivo cifrado.

1. **Descifrar el archivo:**

   `bash gpg informe_secreto.pdf.gpg`

2. **Introducir Contraseña:** El sistema le pedirá la contraseña que usó para cifrarlo.

   `Necesaria frase de paso. Introduzca la frase de paso:`

3. **Resultado:** El archivo descifrado se guardará con el nombre original (`informe_secreto.pdf`).

---

4. Cifrado Asimétrico (con Claves)

Este método es más avanzado y requiere generar un par de claves (pública y privada). Es ideal para compartir archivos con personas que también usan GnuPG.

A. Generar su Par de Claves (Solo la primera vez)

1. **Iniciar la generación:**

   `bash gpg --full-generate-key`

2. **Seguir las instrucciones:** El sistema le guiará a través de la selección del tipo de clave, tamaño y tiempo de expiración. Finalmente, le pedirá su nombre, dirección de correo electrónico y una **frase de paso** para proteger su clave privada.

B. Cifrar para un Destinatario

Para cifrar un archivo para otra persona, necesita su **clave pública**. Asumiremos que ya ha importado la clave pública de su destinatario (por ejemplo, `juan@ejemplo.com`).

1. **Cifrar el archivo:** Utilice la opción `-r` (recipient) y especifique el identificador del destinatario (nombre, correo o ID de clave).

   ```bash
   gpg -e -r "juan@ejemplo.com" archivo_a_enviar.zip
   ```

2. **Resultado:** Se genera el archivo cifrado (`archivo_a_enviar.zip.gpg`) que solo Juan podrá descifrar con su clave privada.

C. Descifrar un Archivo Recibido

Si recibe un archivo cifrado para usted, el proceso es similar al simétrico, pero GnuPG utilizará automáticamente su clave privada.

1. **Descifrar el archivo:**

   ```bash
   gpg archivo_cifrado_de_tercero.tar.gz.gpg
   ```

2. **Introducir Frase de Paso:** El sistema le pedirá la frase de paso que protege su **clave privada** (la que creó en el paso A).

3. **Resultado:** El archivo se descifra y se guarda con su nombre original.
