
Manual de usuario: guía completa

Alejandra Velasco Zárate
José Carlos Yamuni Contreras
José Antonio Juárez Pacheco
Juan Manuel Hernández Solano
04/06/2024

Abstract

Este manual está diseñado para guiar a los usuarios a través del proceso de configuración inicial y las operaciones básicas con GPG (GNU Privacy Guard) en un entorno de terminal. GPG es una herramienta esencial para cifrar y firmar datos, asegurando la privacidad y autenticidad de comunicaciones y archivos. Este manual incluye instrucciones detalladas para instalar GPG en diferentes sistemas operativos, incluyendo Windows, macOS y Linux. También proporciona una guía paso a paso para acceder a la terminal en estos sistemas. Los usuarios aprenderán a generar pares de llaves públicas y privadas, configurando parámetros como nombre, correo electrónico y frase de paso. Además, se explican los comandos necesarios para listar y gestionar las llaves GPG existentes en el sistema, así como los pasos para compartir llaves públicas con otros usuarios y agregar llaves públicas de otros a su propio anillo de llaves. Asimismo, explica detalladamente el uso de la aplicación para firmar y verificar documentos. Demuestra paso a paso todo lo necesario para el funcionamiento correcto de la aplicación. Este manual está diseñado para ser accesible a usuarios de todos los niveles de experiencia, proporcionando comandos específicos y explicaciones claras para cada operación.

Contents

| | | |
|----------|--|----------|
| 1 | Abrir la terminal | 3 |
| 1.1 | Windows | 3 |
| 1.2 | Linux | 3 |
| 1.3 | macOS | 3 |
| 2 | Instalación GPG (GNU Privacy Guard GnuPG) | 4 |
| 2.1 | Windows | 4 |
| 2.2 | Linux | 5 |
| 2.3 | macOS | 5 |
| 3 | Creación de llaves utilizando GnuPG | 6 |

| | | |
|----------|---|-----------|
| 4 | Llaves creadas | 9 |
| 4.1 | Listar todas las llaves en el llavero | 9 |
| 4.2 | Key ID de las llaves | 9 |
| 5 | Abrir aplicación Documento Seguro | 10 |
| 6 | Descripción de la aplicación | 10 |
| 6.1 | Funciones Principales | 10 |
| 6.2 | Firmar Documento | 10 |
| 6.3 | Verificar Documento | 11 |
| 6.4 | Añadir Llave Pública | 11 |
| 6.5 | Eliminar Llave Pública | 11 |
| 7 | Resumen Visual | 12 |
| 8 | Notas Adicionales | 12 |

1 Abrir la terminal

1.1 Windows

Para abrir la terminal en Windows existen varias formas:

- Usando el Menú de inicio:
 1. Haz clic en el botón Inicio o presiona la tecla Windows en tu teclado.
 2. Escribe **cmd** o **Símbolo del sistema** en el cuadro de búsqueda.
 3. Selecciona **Símbolo del sistema** o **Terminal de Windows** en los resultados de búsqueda.
- Usando el Atajo de Teclado:
 1. Presiona las teclas **Windows + X** simultáneamente.
 2. Selecciona **Símbolo del sistema** o **Terminal de Windows** del menú que aparece.
- Terminal de Windows:
 1. Haz clic en el botón Inicio o presiona la tecla Windows.
 2. Busca **Windows** y selecciona **Windows Powershell**.

1.2 Linux

Abrir la terminal en Linux puede variar ligeramente según la distribución que estés utilizando. A continuación, se describen algunos de los métodos más comunes para abrir la terminal en las distribuciones de Linux más populares:

- Usando el Menú de Aplicaciones:
 1. Haz clic en el botón Menú (a menudo un icono con el logo de Ubuntu o un icono de Linux Mint en la esquina inferior izquierda).
 2. Busca y selecciona **Terminal** o **Konsole**.
- Usando el Atajo de Teclado:
 1. Presiona **Ctrl + Alt + T**.

1.3 macOS

Abrir la terminal en macOS es un proceso sencillo y se puede hacer de varias maneras.

- Usando Spotlight:
 1. Haz clic en el ícono de Spotlight (una lupa) en la esquina superior derecha de la barra de menú, o presiona **Cmd + Space** en tu teclado.
 2. Escribe **Terminal** en el cuadro de búsqueda.
 3. Selecciona **Terminal** en los resultados de búsqueda.
- Usando el Finder:
 1. Abre el Finder haciendo clic en el ícono del Finder en el Dock.

2. Ve a **Aplicaciones** en la barra lateral.
 3. Desplázate hacia abajo y abre la carpeta **Utilidades**.
 4. Haz doble clic en **Terminal**.
- Usando Launchpad:
 1. Haz clic en el ícono de **Launchpad** en el Dock (se ve como un ícono de cohete).
 2. Busca **Terminal** usando el campo de búsqueda en la parte superior.
 3. Haz clic en el ícono de **Terminal** para abrirlo.

2 Instalación GPG (GNU Privacy Guard GnuPG)

2.1 Windows

Instalar GPG (GNU Privacy Guard) en Windows es un proceso sencillo. Aquí tienes una guía paso a paso para hacerlo:

1. Descargar el Instalador de GPG para Windows:
 - (a) Abre tu navegador web y dirígete al sitio oficial de GPG: <https://gpg4win.org/>
 - (b) Haz clic en el botón Download para descargar la última versión de Gpg4win.
2. Ejecutar el Instalador:
 - (a) Una vez que la descarga esté completa, abre el archivo ejecutable (**.exe**).
 - (b) Si se te solicita, permite que el instalador realice cambios en tu dispositivo (haz clic en **Sí** en la ventana de Control de cuentas de usuario).
3. Configurar la Instalación:
 - (a) Selecciona tu idioma preferido y haz clic en Aceptar.
 - (b) En la pantalla de bienvenida, haz clic en Siguiente.
 - (c) En la pantalla de selección de componentes, puedes dejar los valores predeterminados, que suelen incluir GnuPG, Kleopatra, y GpgOL. Estos componentes son suficientes para la mayoría de los usuarios. Haz clic en Siguiente.
 - (d) Selecciona el directorio de instalación (puedes dejar la ubicación predeterminada) y haz clic en Siguiente.
4. Completar la Instalación:
 - (a) Haz clic en Instalar para comenzar el proceso de instalación.
 - (b) Una vez que la instalación se haya completado, haz clic en Siguiente.
 - (c) Haz clic en Finalizar para cerrar el instalador.
5. Verificar la Instalación:

- (a) Abre la aplicación Kleopatra, que se instala junto con Gpg4win. Kleopatra es una interfaz gráfica que facilita la gestión de llaves GPG.
- (b) En Kleopatra, puedes crear nuevas llaves, importar llaves existentes, y gestionar tus pares de llaves.
- (c) Otra opción es verificarlo en tu terminal. Abre la terminal (si no sabes como ve a la sección 1) y escribe: `gpg --version`.

2.2 Linux

Instalar GPG (GNU Privacy Guard) en Linux es bastante sencillo, ya que está disponible en los repositorios de la mayoría de las distribuciones. Aquí te muestro cómo hacerlo en algunas de las distribuciones de Linux más populares:

- Ubuntu/Debian:
Para instalar GPG en sistemas basados en Debian, como Ubuntu, puedes utilizar el siguiente comando en la terminal.


```
sudo apt update
sudo apt install gnupg
```
- Fedora:
En Fedora, puedes instalar GPG utilizando el comando `dnf`.


```
sudo dnf install gnupg
```
- openSUSE:
En openSUSE, puedes instalar GPG utilizando el comando `zypper`.


```
sudo zypper install gnupg
```
- Arch Linux:
En Arch Linux, puedes instalar GPG utilizando `pacman`.


```
sudo pacman -S gnupg
```

Después de instalar GPG, puedes verificar que la instalación se haya realizado correctamente ejecutando en la terminal:

```
gpg --version
```

2.3 macOS

Para instalar GPG (GNU Privacy Guard) en macOS, puedes seguir estos pasos:

- Usando GPG Suite:
 1. Instala Homebrew: Si no tienes Homebrew instalado, primero abre la Terminal y ejecuta el siguiente comando para instalarlo.

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install)"
```
 2. Sigue las instrucciones en pantalla para completar la instalación.
 3. Una vez que tengas Homebrew instalado, ejecuta el siguiente comando en la Terminal para instalar GPG:

```
brew install gnupg
```

- Usando MacPorts: Otra alternativa es utilizar MacPorts, una herramienta para instalar software en macOS.
 1. Si no tienes MacPorts instalado, primero visita la página de instalación de MacPorts y sigue las instrucciones para instalarlo.
 2. Después de haberlo instalado, abre la Terminal y ejecuta `sudo port selfupdate`.
 3. Luego, instala GPG con:
`sudo port install gnupg`
- Descarga e instalación manual: Si prefieres una instalación manual, también puedes descargar los binarios directamente desde el sitio web de GnuPG.
 1. Ve al sitio web de **GnuPG**.
 2. Selecciona la versión para macOS y descarga el archivo adecuado para macOS.
 3. Abre el archivo descargado y sigue las instrucciones de instalación.

Para asegurarte de que GPG se ha instalado correctamente, puedes verificar la versión instalada ejecutando:

```
gpg --version
```

3 Creación de llaves utilizando GnuPG

Una vez que GPG está instalado, el proceso de creación de llaves es el mismo en todos los sistemas operativos. Pasos:

1. Abrir la Terminal o la Línea de Comandos (Veáse la sección 1 si no sabe hacerlo).
2. Para generar llaves ejecute el siguiente comando en la terminal:
`gpg --full-generate-key`.
3. Te aparecerán las siguientes opciones:
 - (1) RSA and RSA
 - (2) DSA and Elgamal
 - (3) DSA (sign only)
 - (4) RSA (sign only)
 - (9) ECC (sign and encrypt) *default*
 - (10) ECC (sólo firmar)
 - (14) Existing key from card
4. Para uso de firmar y verificar firmas se pueden utilizar las opciones (3), (4), (10). Para fines de instruir se creará una llave (4) RSA (sign only). Selecciona la opción 4,3 o 10.

```
Símbolo del sistema - gpg --f x + v
Microsoft Windows [Versión 10.0.22631.3447]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\ >gpg --full-generate-key
gpg (GnuPG) 2.4.5; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
(1) RSA and RSA
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(9) ECC (sign and encrypt) *default*
(10) ECC (sólo firmar)
(14) Existing key from card
Su elección: |
```

Figure 1: Opciones de llaves

5. Aparecerá una mensaje preguntando de qué tamaño quiere la llave, nuestra recomendación es introducir la longitud recomendada (es la que aparece entre paréntesis).

```
Símbolo del sistema - gpg --f x + v
Microsoft Windows [Versión 10.0.22631.3447]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\ >gpg --full-generate-key
gpg (GnuPG) 2.4.5; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
(1) RSA and RSA
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(9) ECC (sign and encrypt) *default*
(10) ECC (sólo firmar)
(14) Existing key from card
Su elección: 4
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (3072) 3072|
```

Figure 2: Longitud de llaves

6. A continuación especifique el periodo de tiempo de validez de la llave, siguiendo las siguientes especificaciones:
- 0 si quiere que la llave nunca caduque.
 - X donde X es el número de días.
 - Xw donde w indica semanas y X el número de semanas.
 - Xm donde m indica meses y X el número de meses.
 - Xy donde y indica años y X el número de años.
7. Le pedirá verificar el periodo de tiempo, escriba s si está seguro de lo contrario escriba n .

```

Por favor, especifique el período de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
La clave nunca caduca
¿Es correcto? (s/n) s

```

Figure 3: Periodo de validez de la llave

8. GnuPG debe construir un ID de usuario para identificar la llave, por esta razón le pedirá:

- Nombre completo de la persona que crea la llave.
- Correo de la persona que crea la llave.
- Un comentario para identificarlo (sugerencia: poner su usuario de Sigue Al Congreso como comentario).

9. Después de ingresar toda la información le pedirá confirmación de datos, en caso de ser todo correcto escriba V.

```

GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Sigue Al Congreso
Dirección de correo electrónico: siguealcongreso@gmail.com
Comentario: Usuario
Ha seleccionado este ID de usuario:
"Sigue Al Congreso (Usuario) <siguealcongreso@gmail.com>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.

```

Figure 4: Configuración de la llave

10. Una vez teniendo la llave configurada le aparecerá una pestaña pequeña para introducir la contraseña que estará ligada a la misma.

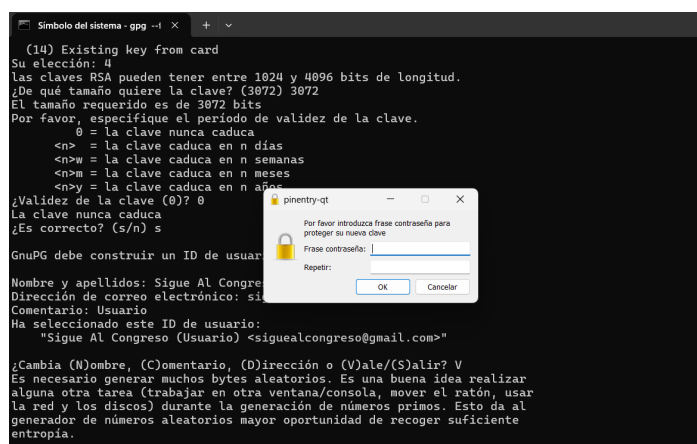


Figure 5: Contraseña de la llave

! →

IMPORTANTE: no perder esta contraseña porque es la que le pedirán cada vez que quiera firmar un documento o hacer cualquier acción con esta llave).

11. Finalmente, una vez introducida su llave después de unos segundos deberá aparecerle un mensaje en el cual se confirma la creación correcta de la llave.

4 Llaves creadas

4.1 Listar todas las llaves en el llavero

Para ver las llaves que se tienen en su llavero, basta con ejecutar el siguiente comando en la terminal:

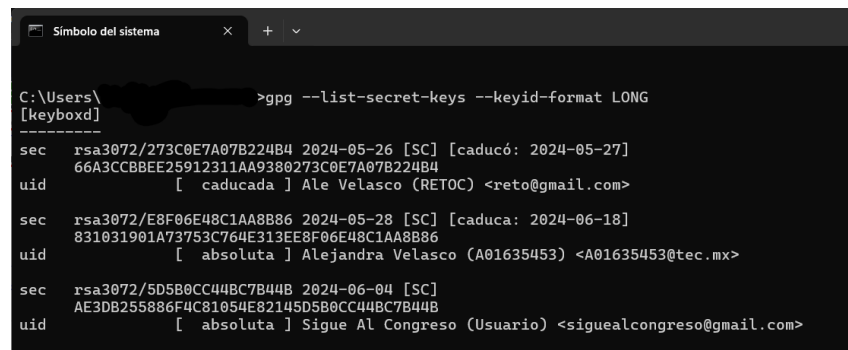
```
gpg --list-keys
```

4.2 Key ID de las llaves

Para conocer las key ID públicas y privadas de las llaves, abra la terminal y ejecute el siguiente comando:

```
gpg --list-secret-keys --keyid-format LONG
```

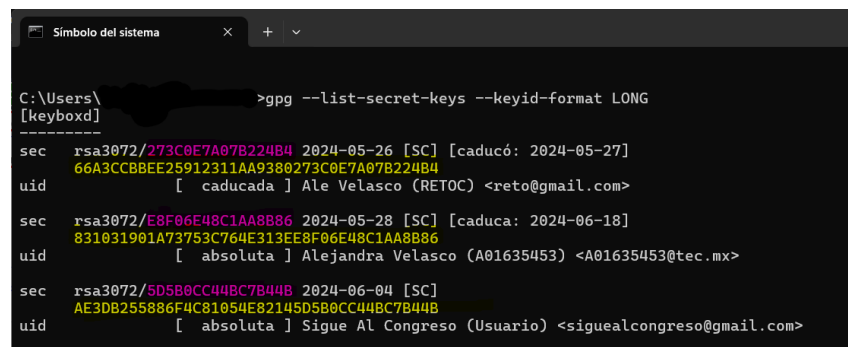
La terminal imprimirá algo así:



```
Símbolo del sistema  x  +  v
C:\Users\[keyboxd] >gpg --list-secret-keys --keyid-format LONG
-----
sec  rsa3072/273C0E7A07B224B4 2024-05-26 [SC] [caducó: 2024-05-27]
uid  66A3CCBEE25912311AA9380273C0E7A07B224B4
uid  [ caducada ] Ale Velasco (RETOC) <reto@gmail.com>
sec  rsa3072/E8F06E48C1AA8B86 2024-05-28 [SC] [caduca: 2024-06-18]
uid  831031901A73753C764E313EE8F06E48C1AA8B86
uid  [ absoluta ] Alejandra Velasco (A01635453) <A01635453@tec.mx>
sec  rsa3072/5D5B0CC44BC7B44B 2024-06-04 [SC]
uid  AE3DB255886F4C81054E82145D5B0CC44BC7B44B
uid  [ absoluta ] Sigue Al Congreso (Usuario) <siguealcongreso@gmail.com>
```

Figure 6: ID de las llaves

Para saber cuál es la **key ID pública** y cuál es la **key ID privada** de las llaves observe la siguiente figura:



```
Símbolo del sistema  x  +  v
C:\Users\[keyboxd] >gpg --list-secret-keys --keyid-format LONG
-----
sec  rsa3072/273C0E7A07B224B4 2024-05-26 [SC] [caducó: 2024-05-27]
uid  66A3CCBEE25912311AA9380273C0E7A07B224B4
uid  [ caducada ] Ale Velasco (RETOC) <reto@gmail.com>
sec  rsa3072/E8F06E48C1AA8B86 2024-05-28 [SC] [caduca: 2024-06-18]
uid  831031901A73753C764E313EE8F06E48C1AA8B86
uid  [ absoluta ] Alejandra Velasco (A01635453) <A01635453@tec.mx>
sec  rsa3072/5D5B0CC44BC7B44B 2024-06-04 [SC]
uid  AE3DB255886F4C81054E82145D5B0CC44BC7B44B
uid  [ absoluta ] Sigue Al Congreso (Usuario) <siguealcongreso@gmail.com>
```

Figure 7: Key ID pública y privada

La combinación alfanumérica que está en *amarillo* corresponde a la **key ID pública** de cada llave y la combinación alfanumérica que está en

morado es la **key ID privada** de cada llave.
! → IMPORTANTE: No compartir el key ID privado.

5 Abrir aplicación Documento Seguro

Antes de abrir la aplicación hay un paso que se debe realizar una sola vez. Ya hecho una vez, puede ignorar esta instrucción. Para abrir la aplicación necesitas tener varios paquetes instalados en tu computadora, entonces se necesita abrir la terminal en la carpeta donde está la aplicación y todos sus documentos y ejecutar:

```
pip install -r requirements.txt
```

Ya teniendo todos los paquetes puede abrir la aplicación sin ningún problema.

Abra la terminal en la carpeta donde está la aplicación, para ejecutarla con Streamlit escriba el siguiente comando y presionando Enter:

```
streamlit run app.py
```

La app se abrirá automáticamente en el navegador.

6 Descripción de la aplicación

6.1 Funciones Principales

La aplicación tiene cuatro funciones principales que puedes seleccionar desde la barra lateral:

1. Firmar Documento
2. Verificar Documento
3. Añadir Llave Pública
4. Eliminar Llave Pública

A continuación, te explicamos cómo funciona cada una.

6.2 Firmar Documento

Esta función te permite firmar digitalmente un documento, garantizando que el contenido no ha sido alterado desde su firma.

1. Selecciona **Firmar documento** en la barra lateral.
2. Ingresa tu **key_id** de tu llave privada en el campo correspondiente (Para saber cuál es su **key_id** de tu llave privada véase la sección 4.2).
3. Sube el archivo que deseas firmar utilizando el botón de carga de archivos.
4. Haz clic en **Firmar**.
5. Si todo es correcto, podrás descargar el documento firmado y guardarlo donde tu quieras.

6.3 Verificar Documento

Esta función te permite verificar la firma de un documento firmado digitalmente, asegurando que el documento es auténtico y no ha sido modificado.

1. Selecciona **Verificar documento** en la barra lateral.
2. Ingresa el usuario del propietario de la llave pública en el campo correspondiente.
3. Sube el archivo firmado que deseas verificar.
4. Haz clic en **Verificar documento**.
5. La aplicación te indicará si la firma es auténtica o no.

6.4 Añadir Llave Pública

Los documentos que firmarás con tu llave privada vienen ligados a una llave pública. Para que otras personas puedan verificar tu firma y así validar el documento, necesitará tu llave pública, por lo que tendrás de dar de alta. Esta función te permite añadir una nueva llave pública a la base de datos de la aplicación, una vez creada tu llave con la que firmarás tus documentos es necesario que registres tu llave, con hacerlo una vez es suficiente.

1. Selecciona **Añadir llave pública** en la barra lateral.
2. Ingresa el comentario (usuario) asociado a la llave.
3. Ingresa el `key_id` público asociado a la llave (Para saber el `key_id` público véase 4.2).
4. Ingresa el correo electrónico asociado a la llave.
5. Haz clic en **Añadir**.
6. La aplicación te informará si la llave pública fue añadida correctamente.

! → IMPORTANTE: Si no registras tu llave pública las personas no podrán verificar tus documentos firmados. Registrar tus llaves se debe hacer solo una vez.

6.5 Eliminar Llave Pública

Esta función te permite eliminar una llave pública de la base de datos, esta función es solo por si hubo una equivocación al momento de dar de alta alguna llave en la aplicación.

1. Selecciona **Eliminar llave pública** en la barra lateral.
2. Ingresa el comentario (usuario) asociado a la llave que deseas eliminar.
3. Ingresa el correo electrónico asociado a la llave que deseas eliminar.
4. Haz clic en **Eliminar**.
5. La aplicación te informará si la llave pública fue eliminada correctamente.

7 Resumen Visual

Al abrir la aplicación, verás una barra lateral con las opciones mencionadas. Selecciona la función que deseas utilizar y sigue las instrucciones proporcionadas en la interfaz.

8 Notas Adicionales

- **Confidencialidad y Seguridad:** La aplicación utiliza tecnología de cifrado robusta compatible con estándares de seguridad globales.
- **Fácil de Usar:** La interfaz es intuitiva y no requiere conocimientos técnicos avanzados.
- **Requisitos:** Asegúrate de tener las llaves y la información necesaria para firmar y verificar los documentos.

Soporte y Contacto

Si tienes alguna pregunta adicional o necesitas soporte técnico, no dudes en contactar al equipo de soporte de **Documento Seguro**. Estamos aquí para ayudarte a proteger y asegurar tus documentos.

Alejandra Velasco Zárate - A01635453@tec.mx
José Antonio Juárez Pacheca - A00578621@tec.mx
José Carlos Yamuni Contreras - A01740285@tec.mx
Juan Manuel Hernández Solano - A00572208@tec.mx
Junio 2024