



IES Luis Vélez de Guevara
Dpto. de Informática

CIFRADO DE CORREO ELECTRÓNICO



Francisco Manuel Gutiérrez Álvarez

Noelia López Rodríguez

Servicio de Red e Internet

FPS Administración de Sistemas Informáticos en Red

IES Luis Vélez de Guevara

Curso 2024/2025

Indice

1. Instalación y Configuración de Thunderbird.....	3
2. Creación e Importación de Par de Claves OpenPGP.....	4
3. Envío de Mensajes Cifrados y Firmados en Thunderbird.....	7
4. Instalación y Configuración de GPG4WIN y Kleopatra.....	9
5. Creación e Importación de Par de Claves en GPG4WIN.....	9
6. Envío de Mensajes Cifrados y Firmados en Kleopatra.....	11
7. Descifrado de Mensajes con Kleopatra.....	12

1. Instalación y Configuración de Thunderbird

1. Instalación:

- Ejecutar los comandos en un entorno Linux:
 - `sudo apt update`
 - `sudo apt install thunderbird`

Solo si tu maquina o sistema operativo no tiene Thunderbird instalado en los sistemas Linux suelen estar instalados predeterminadamente

2. Configuración Inicial:

- Iniciar Thunderbird por primera vez.
- Introducir el nombre, dirección de correo electrónico y contraseña.



The screenshot shows the 'Configuración de cuenta' (Account Configuration) window in Thunderbird. The title bar includes 'Configuración de cuenta' and 'Thunderbird Privacy Notice'. The main heading is 'Configurar su dirección de correo electrónico existente.' (Configure your existing email address). Below this, instructions state: 'Para utilizar su cuenta de correo electrónico actual, introduzca sus credenciales. Thunderbird buscará automáticamente una configuración de servidor recomendada y que funcione.' (To use your current email account, enter your credentials. Thunderbird will automatically search for a recommended server configuration that works). The form contains three input fields: 'Nombre completo' (Full name) with 'Francisco Manuel', 'Dirección de correo electrónico' (Email address) with 'franciscomanuel663.velez@gmail.com', and 'Contraseña' (Password) with masked characters. A checkbox 'Recordar contraseña' (Remember password) is checked. A green success message states: '✓ Configuración encontrada en la base de datos de ISP de Mozilla.' (Configuration found in Mozilla's ISP database). To the right is an illustration of a document icon. At the bottom, it says 'Configuraciones disponibles' (Available configurations).

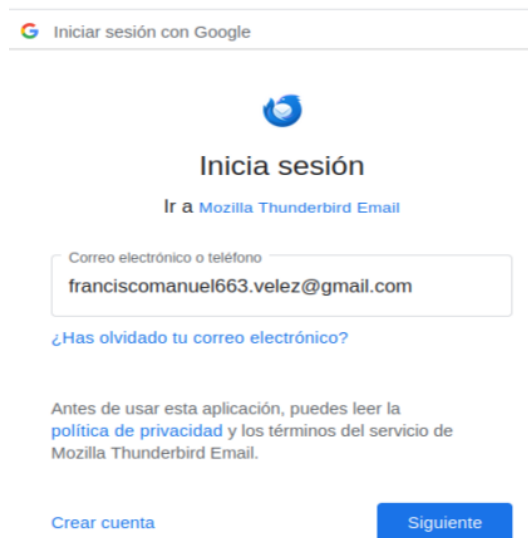
- Elegir el protocolo de correo:
 - **IMAP**: Sincroniza correos con el servidor.
 - **POP3**: Descarga los correos y los elimina del servidor.



The screenshot shows the 'Configuraciones disponibles' (Available configurations) dialog. It has two radio button options. The first option, 'IMAP', is selected and highlighted with a blue border. Its description is 'Mantener sus carpetas y correos electrónicos sincronizados en su servidor' (Keep your folders and emails synchronized on your server). It lists the incoming mail server as 'Entrante IMAP SSL/TLS imap.gmail.com' and the outgoing mail server as 'Saliente SMTP SSL/TLS smtp.gmail.com'. The username is 'Nombre de usuario franciscomanuel663.velez@gmail.com'. The second option, 'POP3', is unselected and has a grey border. Its description is 'Mantener sus carpetas y correos electrónicos en su equipo' (Keep your folders and emails on your computer). At the bottom, there are three buttons: 'Configurar manualmente' (Configure manually), 'Cancelar' (Cancel), and 'Hecho' (Done).

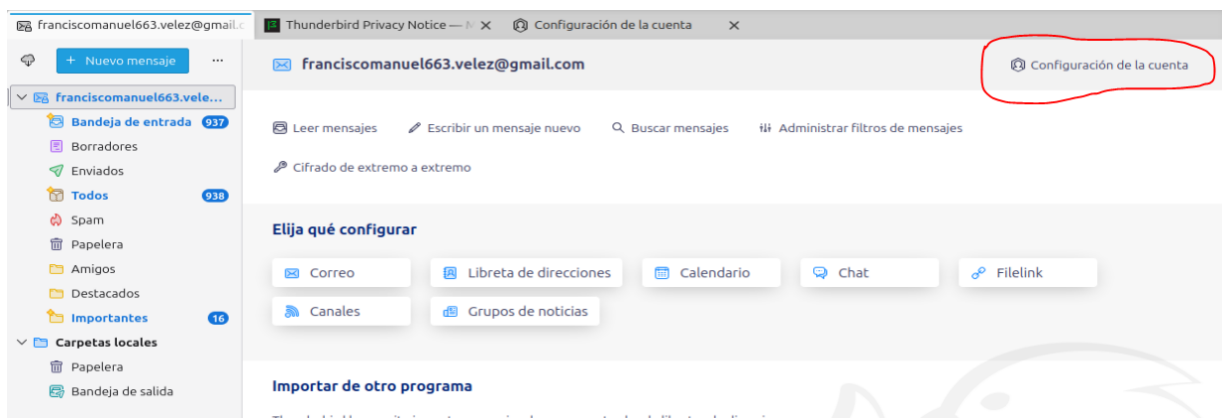
3. Concesión de Permisos:

- Conceder permisos a Thunderbird en caso de usar Gmail.

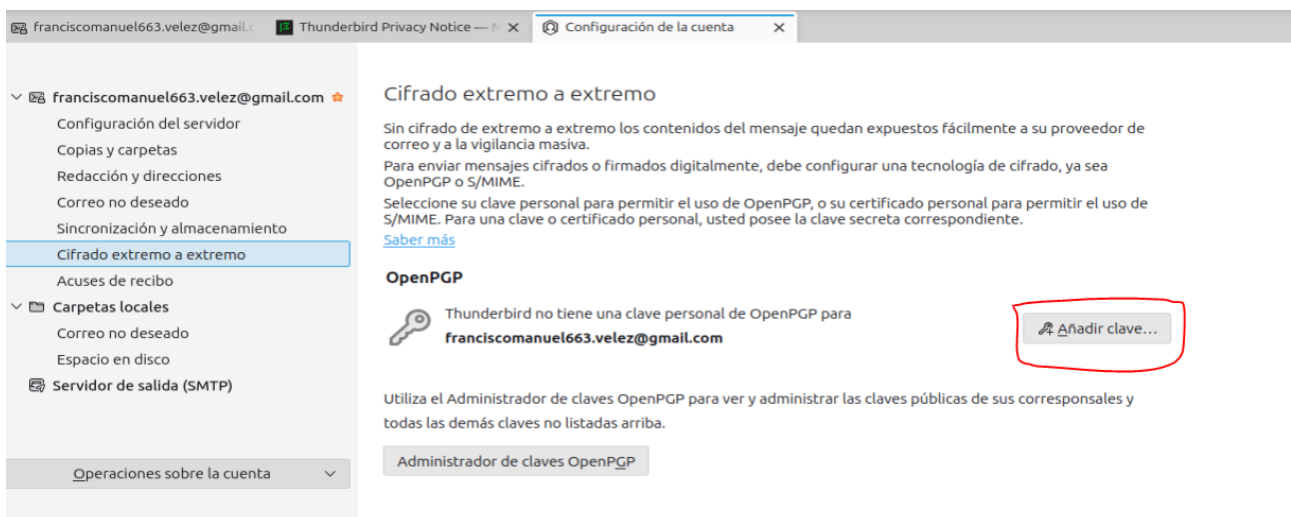


2. Creación e Importación de Par de Claves OpenPGP

1. Acceder al menú de configuración de la cuenta.

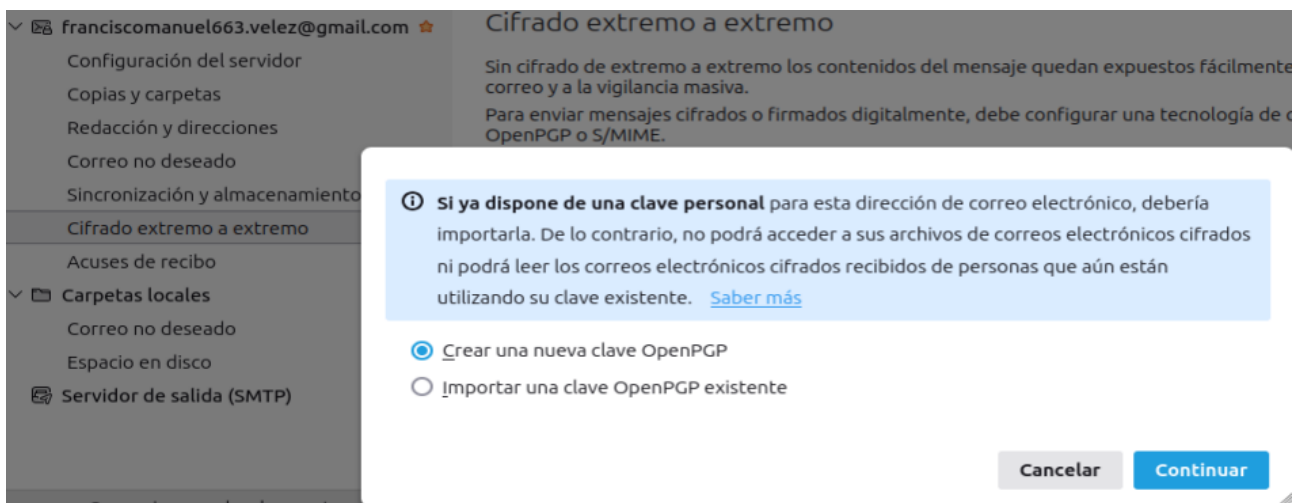


2. Navegar a la sección "Cifrado extremo a extremo" y seleccionar "Añadir clave...".



3. Crear una nueva clave OpenPGP especificando:

- Tipo de clave (RSA o ECC).



- Tiempo de vigencia.

Generar clave OpenPGP

Identidad Francisco Manuel <franciscomanuel663.velez@gmail.com> - franciscomanuel663.velez

Caducidad de la clave
Establezca la fecha de vencimiento de la clave recién generada. Puede cambiar esta fecha para ampliar el tiempo de caducidad si fuera necesario.

☒ La clave caduca en 3 años

☐ La clave no caduca

Configuración avanzada
Gestionar la configuración avanzada de su clave OpenPGP.

Tipo de clave: RSA

Tamaño de clave: 3072

Retroceder **Cancelar** **Generar clave**


i La generación de la clave puede tardar varios minutos en completarse. No salga de la aplicación mientras la generación de la clave esté en proceso. Navegar activamente o realizar operaciones que hagan un uso intensivo de disco repondrá el 'grupo de aleatoriedad' y acelerará el proceso. Se le avisará cuando la generación de la clave se haya completado.

¿Generar la clave pública y secreta para Francisco Manuel "franciscomanuel663.velez@gmail.com"?

Cancelar **Confirmar**

4. Publicar la clave y compartirla con otros usuarios mediante la opción "Publicar".

OpenPGP

 Thunderbird encontró 1 clave personal de OpenPGP asociada con **franciscomanuel663.velez@gmail.com** [Añadir clave...](#)

✓ Su configuración actual usa ID de clave **0x64A4190C94252276** [Saber más](#)

✓ ¡Clave OpenPGP creada correctamente!

☐ Ninguno

No usar OpenPGP para esta identidad.

☒ **0x64A4190C94252276**

Caduca el: 14/1/2028

Publicar la clave pública en un servidor de claves permite que otros la descubran

[Publicar](#)

Utiliza el Administrador de claves OpenPGP para ver y administrar las claves públicas de sus correspondientes y todas las demás claves no listadas arriba.

[Administrador de claves OpenPGP](#)

5. Para importar una clave, usar la opción "Administrador de claves PGP" > "Descubrir claves en línea".


 **franciscomanuel663.velez@gmail.com**

✓ Su configuración actual usa ID de clave **0x64A4190C94252276** [Saber más](#)

Administrador de claves OpenPGP

Archivo Editar Ver Servidor de claves Generar

- Importar clave(s) pública(s) desde archivo
- Importar clave(s) secreta(s) desde archivo
- Importar revocación(es) desde archivo
- Exportar clave(s) pública(s) a archivo
- Enviar clave(s) pública(s) por correo electrónico
- Copia de seguridad de las claves secretas en un archivo
- Guardar el certificado de revocación en un archivo
- Recargar caché de claves
- Cerrar

 Thunderbird encontró 1 clave personal de OpenPGP asociada con **franciscomanuel663.velez@gmail.com**

✓ Su configuración actual usa ID de clave **0x64A4190C94252276** [Saber más](#)

Administrador de claves OpenPGP

Archivo Editar Ver Servidor de claves Generar

Buscar claves

[Descubrir claves en línea](#)

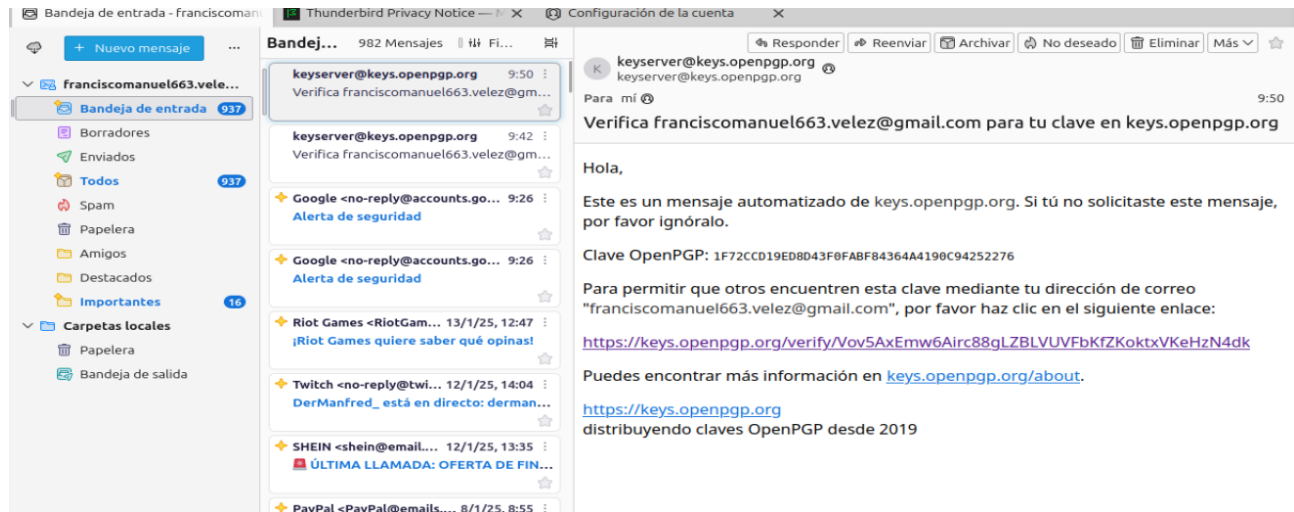
[Publicar](#)

Nombre	ID de clave	Creado	Caduc...
Francisco Manuel <franciscomanuel663.velez@gmail.co...	0x64A4190...	14/1/2...	14/1/2...

3. Envío de Mensajes Cifrados y Firmados en Thunderbird

1. Crear un nuevo mensaje y seleccionar la opción **Cifrar** antes de enviarlo.

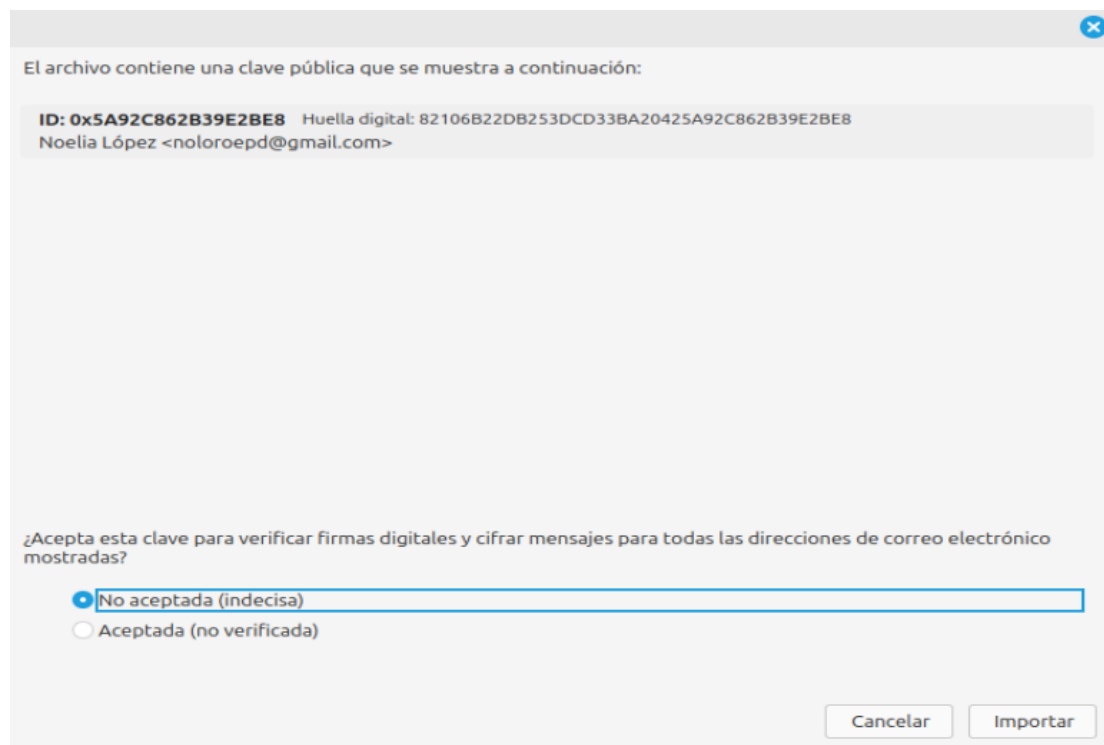
Para ello tenemos que activar nuestra clave pública, tenemos que darle a publicar y nos enviará un correo donde accedemos a un mensaje y activamos el cifrado

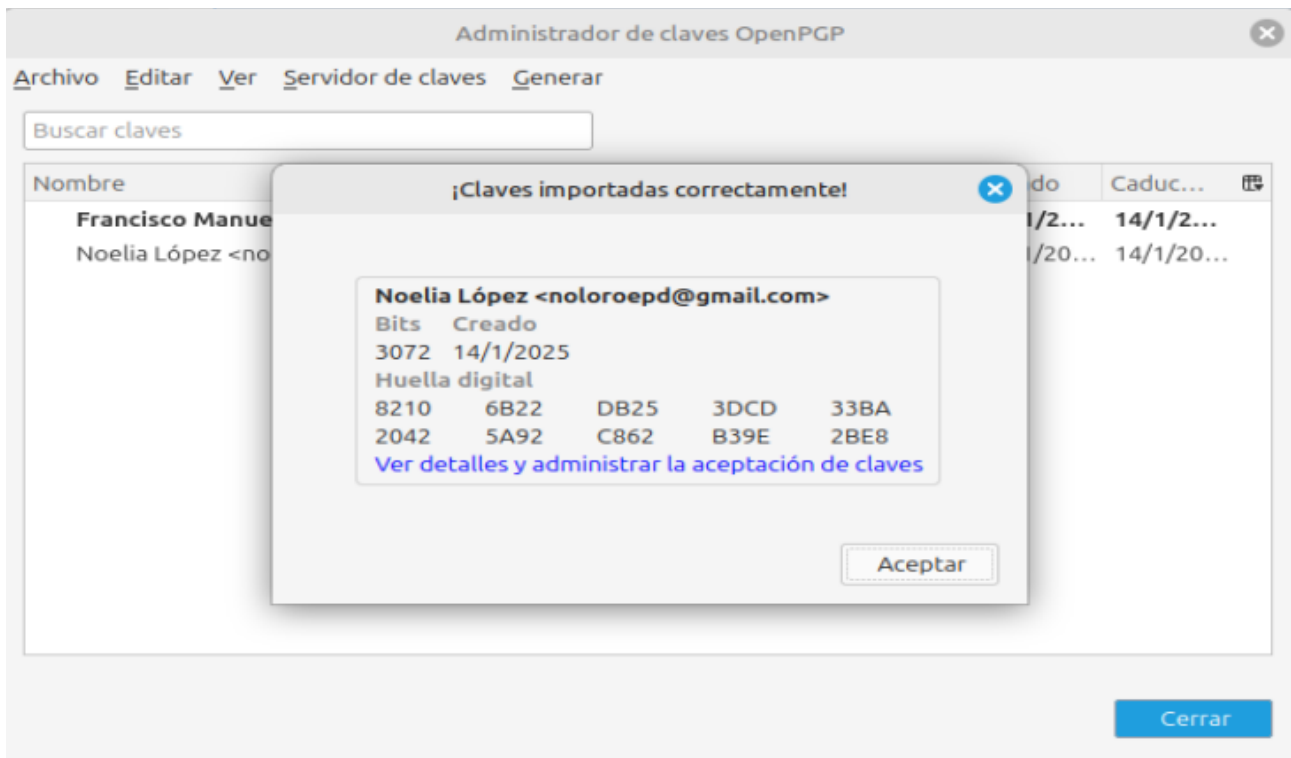


keys.openpgp.org

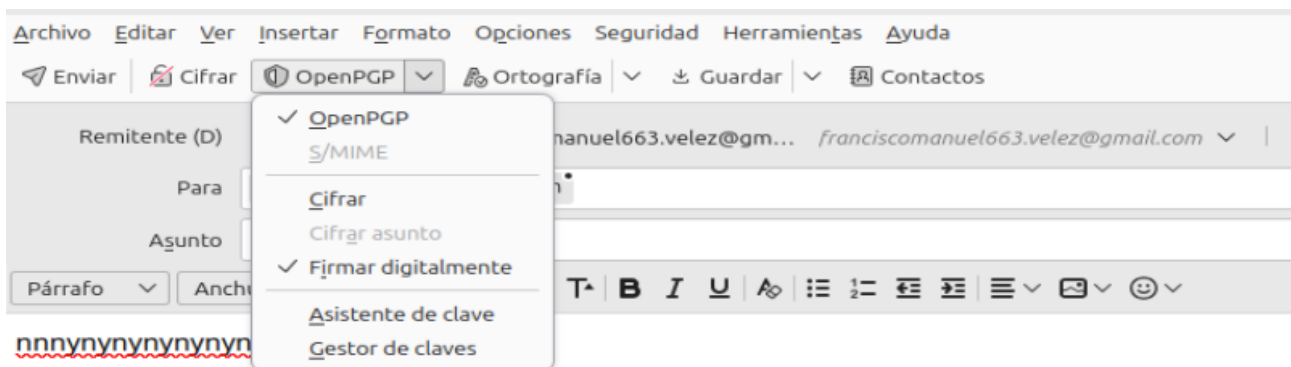
Tu clave 1F72CCD19ED8D43F0FABF84364A4190C94252276 ahora está publicada con la identidad franciscomanuel663.velez@gmail.com.

Ambos usuarios que se comparten la clave pública tienen que hacer estos pasos

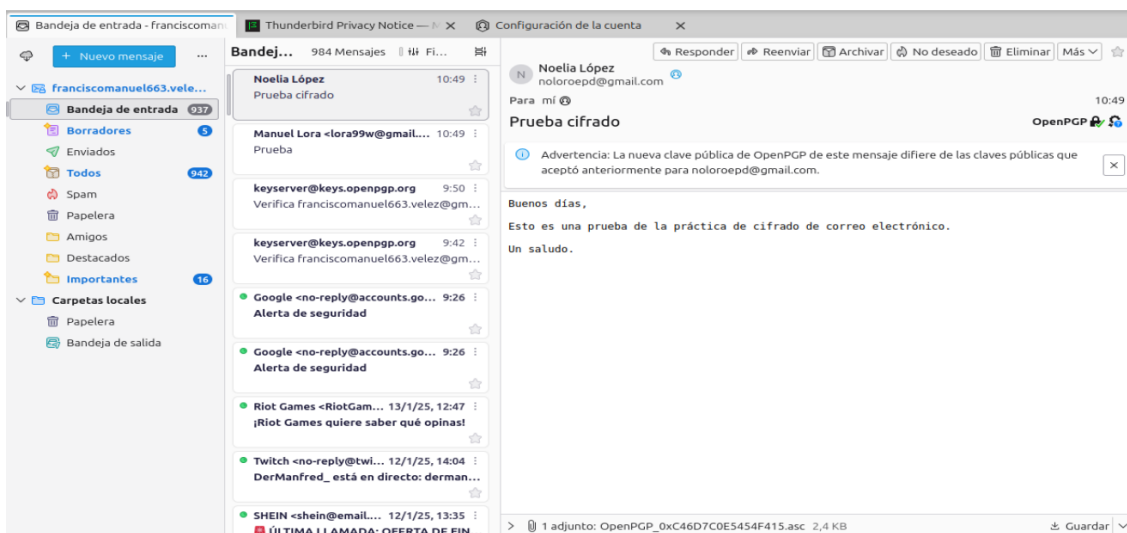




2. Para firmar un mensaje, seleccionar "OpenPGP" > "Firmar digitalmente".



3. Verificar que el destinatario recibe el mensaje cifrado y/o firmado correctamente.

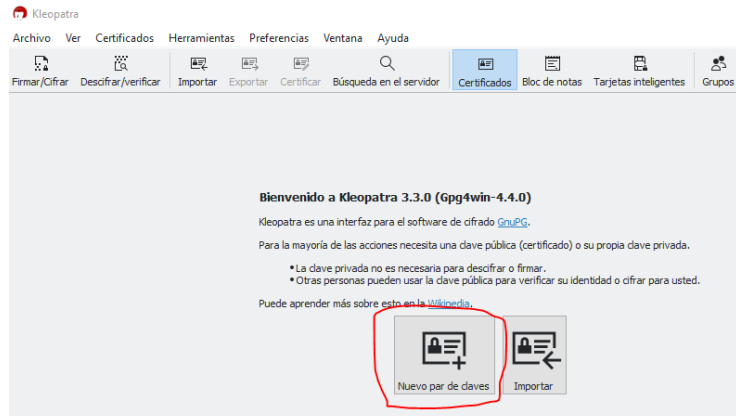


4. Instalación y Configuración de GPG4WIN y Kleopatra

1. Descargar el instalador desde <https://www.gpg4win.org/>.
2. Durante la instalación, incluir la herramienta **Kleopatra**.

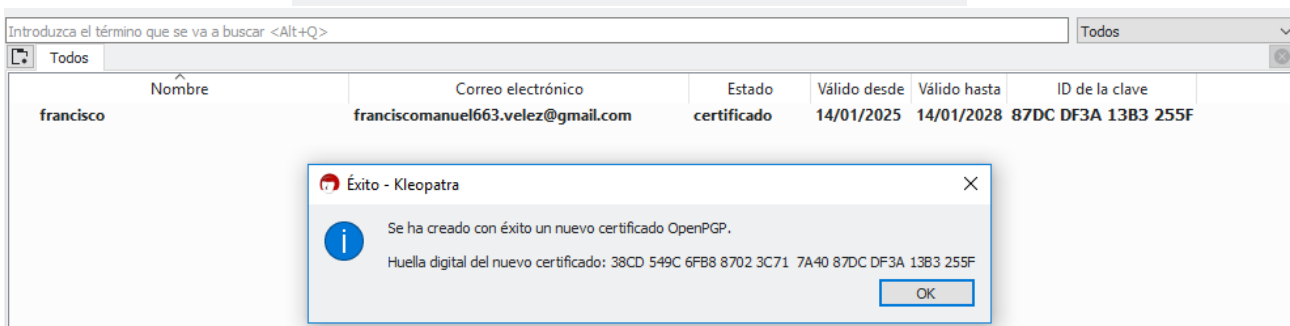
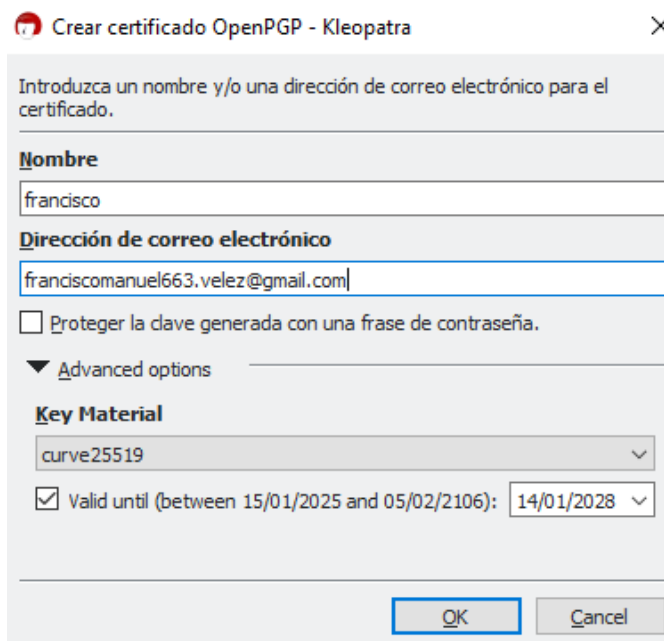
5. Creación e Importación de Par de Claves en GPG4WIN

1. Abrir Kleopatra y seleccionar "Archivo" > "Nuevo par de claves OpenPGP...".

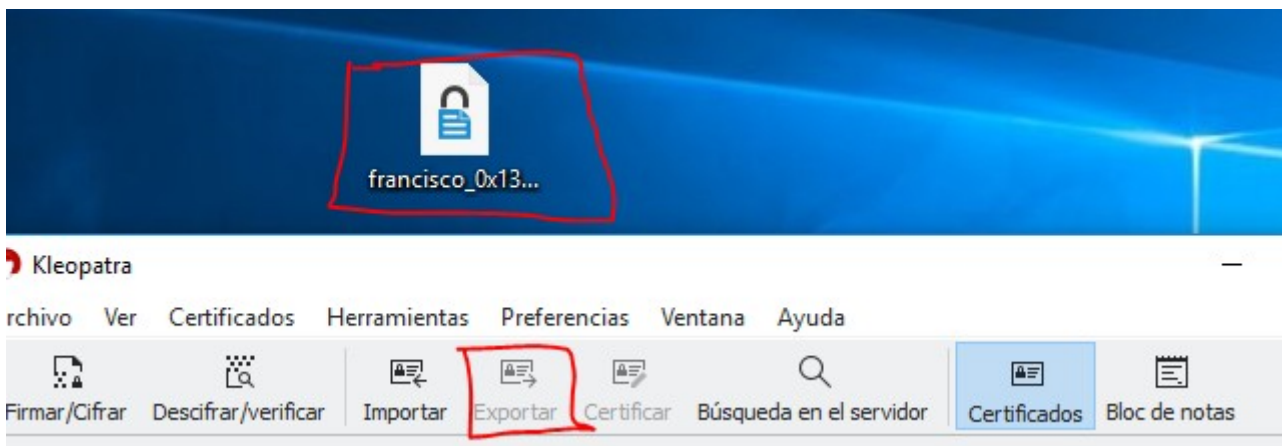


2. Especificar:

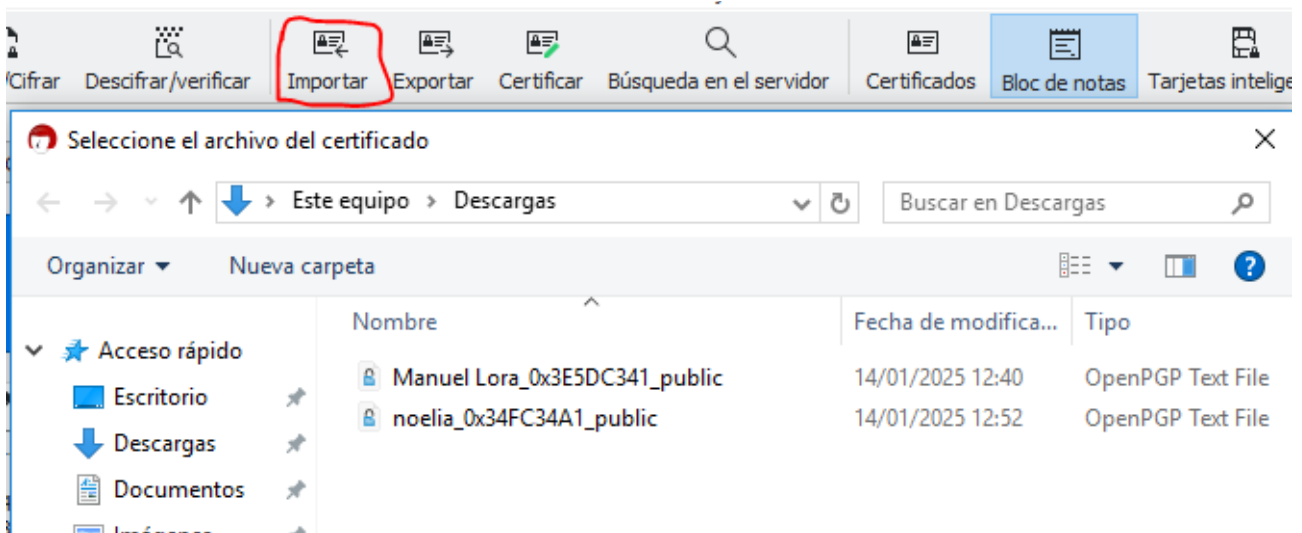
- Dirección de correo electrónico asociada.
- Tipo de cifrado y vigencia.



3. Exportar la clave seleccionando "Exportar". Se generará un archivo con extensión .asc.



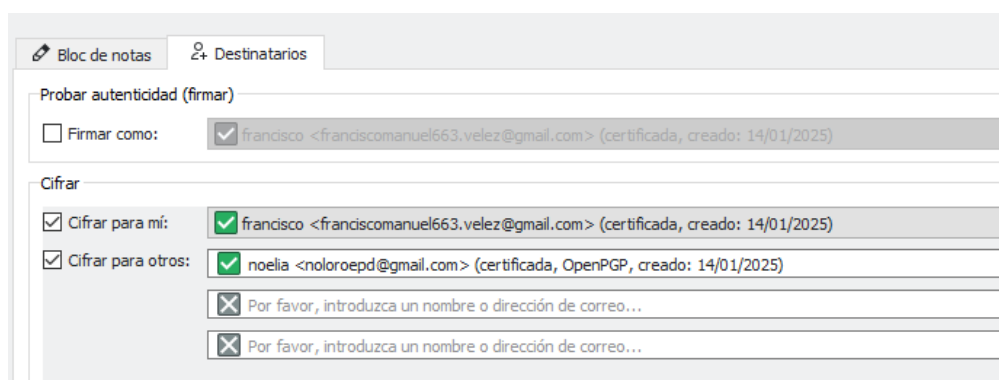
4. Importar claves de otros usuarios seleccionando "Importar" y el archivo correspondiente.



6. Envío de Mensajes Cifrados y Firmados en Kleopatra

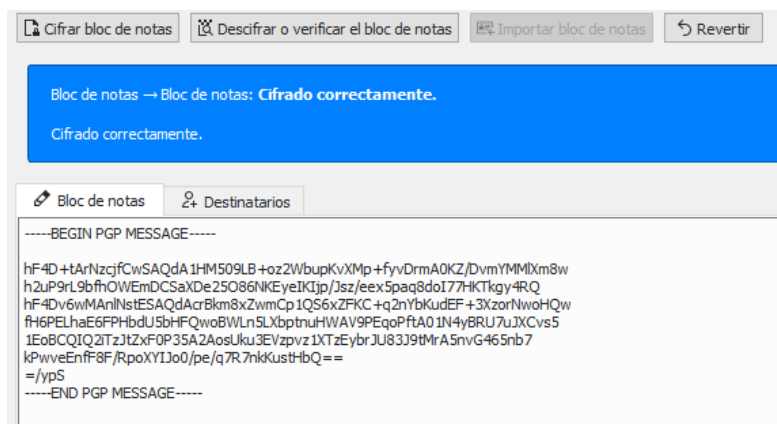
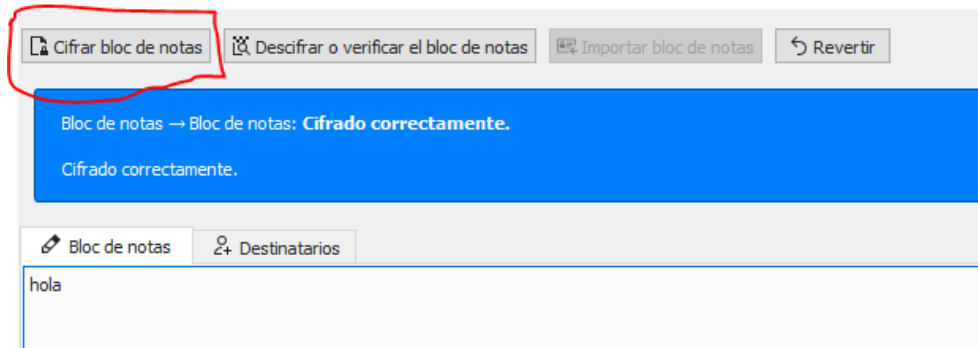
1. Para un archivo:

- Seleccionar "Firmar/Cifrar".
- Elegir destinatarios y confirmar.



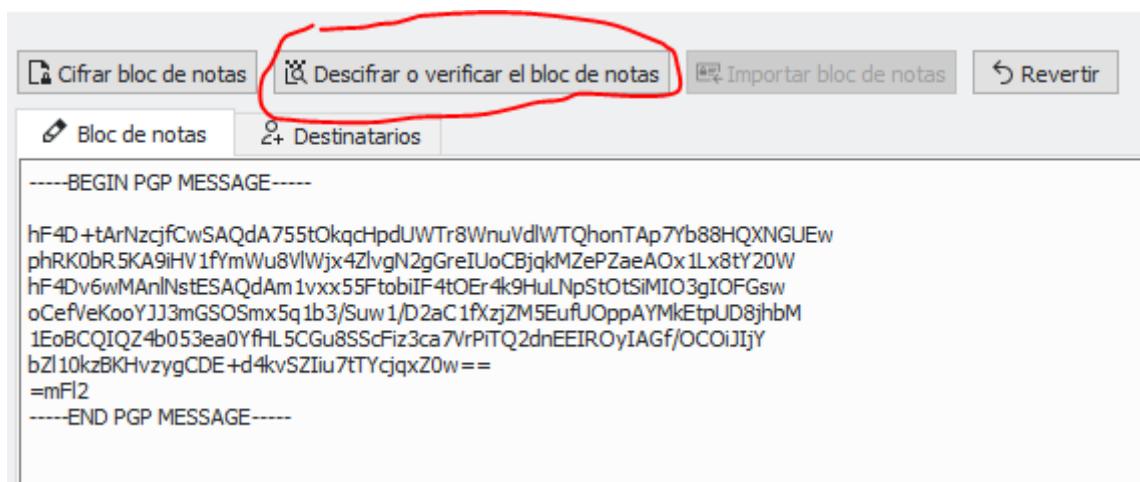
2. Para texto:

- Usar el "Bloc de Notas".
- Escribir el mensaje, seleccionar "Firmar o cifrar" y especificar destinatarios.
- Copiar y enviar el texto cifrado.



7. Descifrado de Mensajes con Kleopatra

1. Copiar el mensaje cifrado al "Bloc de Notas".
2. Seleccionar "Descifrar/verificar".



3. Verificar que el mensaje descifrado corresponde al remitente esperado.

Cifrar bloc de notas

Descifrar o verificar el bloc de notas

Importar bloc de notas

Revertir

Bloc de notas → Bloc de notas: **Descifrado correctamente.**

Nota: No puede estar seguro de quién ha cifrado este mensaje, ya que no está firmado.
Destinatarios:

- noelia <noloroepd@gmail.com> (certificado, OpenPGP, creado: 14/01/2025)
- francisco <franciscomanuel663.velez@gmail.com> (certificado, OpenPGP, creado: 14/01/2025)

Bloc de notas

Destinatarios

hola