

## Uso de correos electrónicos con certificados digitales

---

### Mozilla Thunderbird

Es un cliente de correo electrónico que permite manejar las cuentas y contactos de forma accesible y funcional, unifica cómo trabajar en todos los servicios de correo electrónico y evita tener que acceder a las plataformas Web de los proveedores del servicio de correo electrónico.

Es posible añadir complementos (plugins) para mejorar y personalizar algunas funciones concretas que se desean realizar o perfeccionar, por ejemplo gContactSync para sincronizar los contactos con los de Google u otros proveedores de correo.

**Desarrollador:** Mozilla.org.

**Idioma:** Entre muchos otros, se encuentra en Español.

**Licencia:** Es gratuita, de código abierto y libre distribución.

### Requisitos

- Se encuentra disponible para equipos con sistema operativo Microsoft Windows, Apple OSX y Linux.
- Se precisa disponer de una o varias cuentas de correo electrónico. Estas deben crearse a través de las plataformas Web de los proveedores de estos servicios.

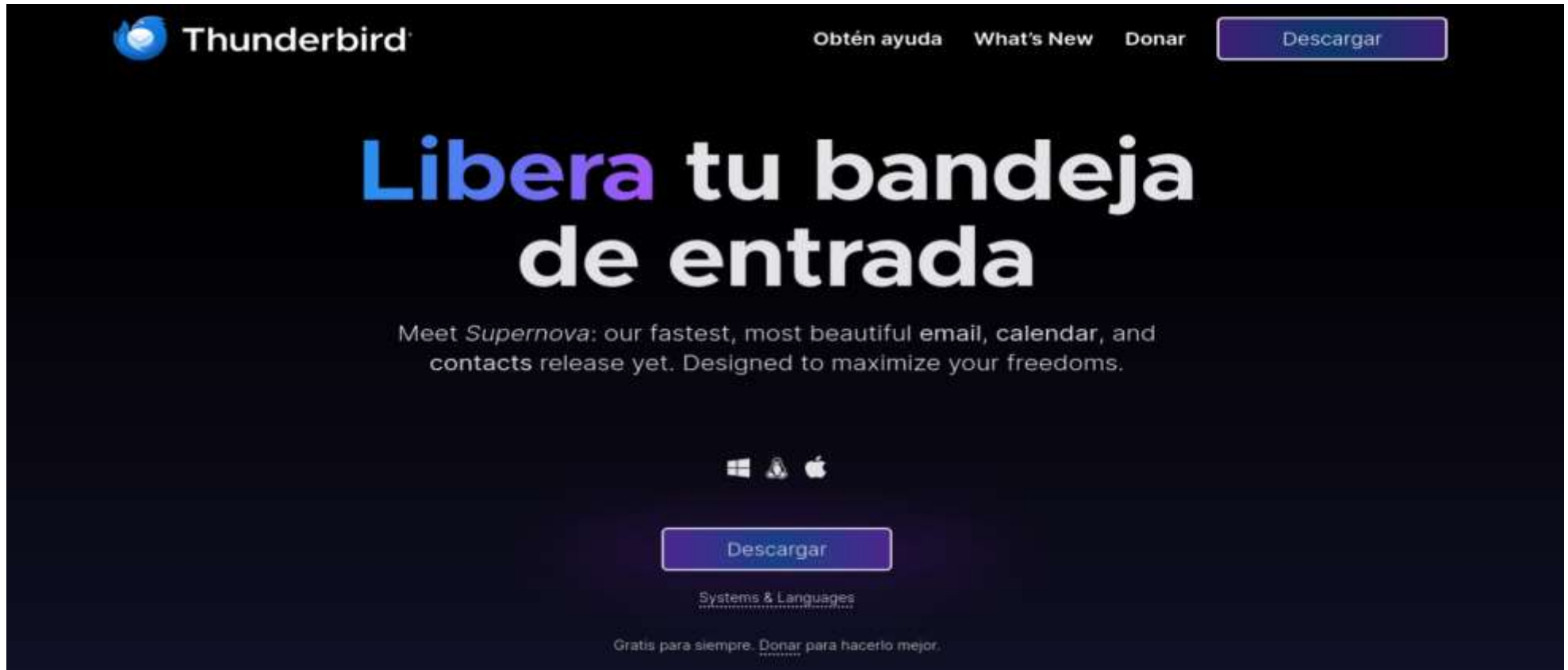
### Accesibilidad

- El procedimiento de instalación es accesible con teclado, ratón y utiliza controles estándar del sistema operativo.
- Se puede utilizar con teclado o combinaciones de teclas.

- Se puede utilizar con puntero de ratón.
- Usa controles estándar del sistema operativo.
- Los lectores de pantalla JAWS y NVDA siguen el desplazamiento del foco por los menús y controles, así como el movimiento del cursor.
- En el lector de pantalla NVDA se puede instalar el complemento MozillaScripts.
- Utiliza el cursor del sistema operativo.
- Usa los colores y tipos de letras del sistema operativo y dispone de opciones para personalizar algunos aspectos.
- Permite conversión a otros formatos.

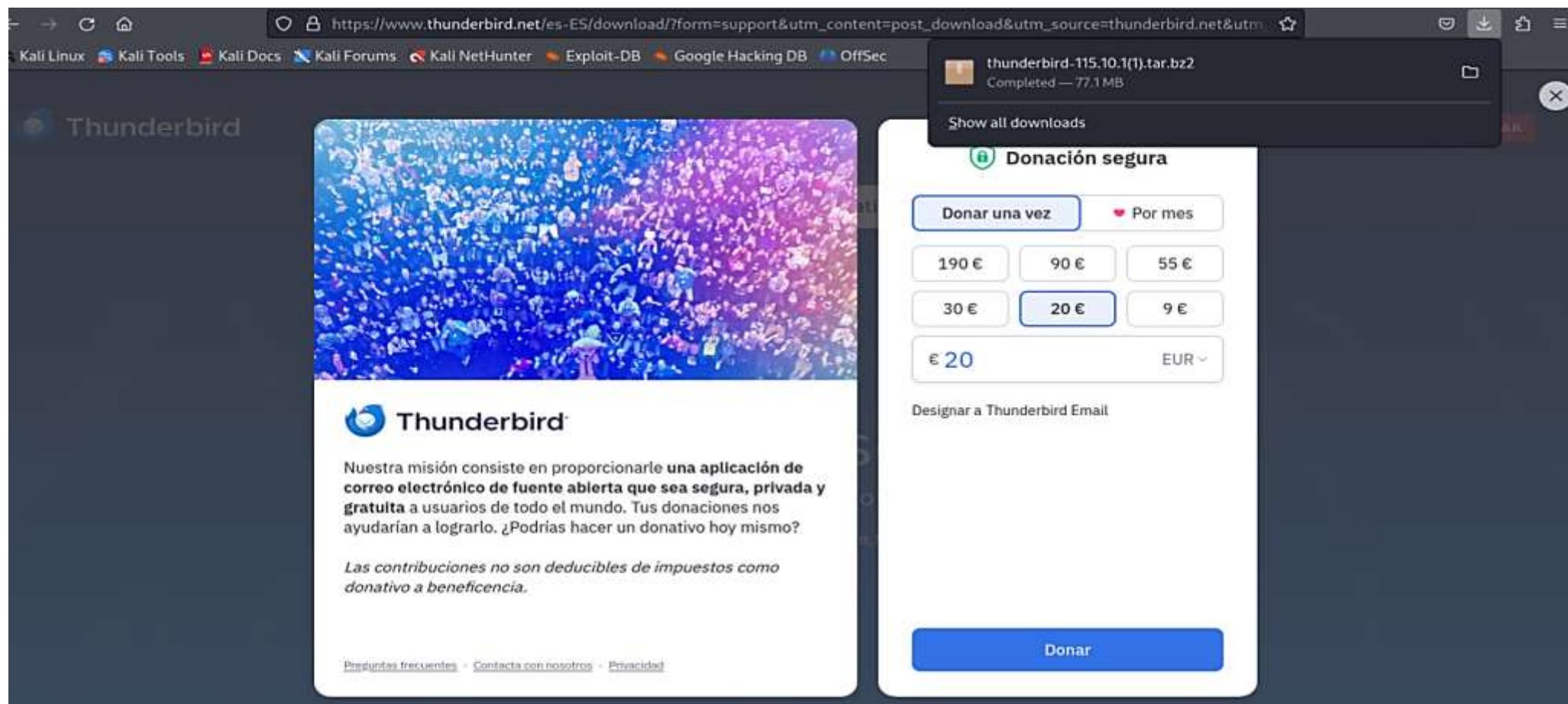
## Instalación en Kali Linux

Vamos a la página oficial de [Thunderbird](#):



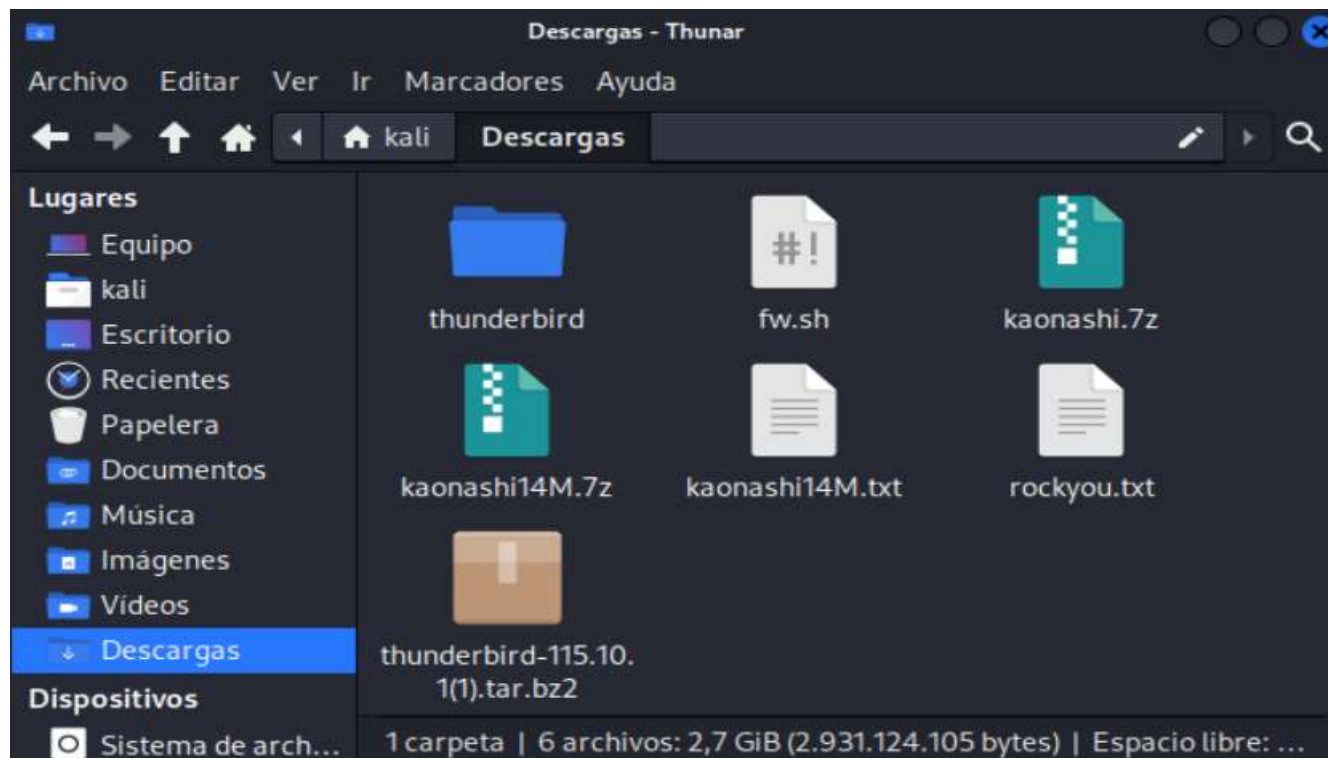
Pulsamos en Descargar:





El paquete de instalación se descarga en la carpeta **Descargas**.

Abrimos la carpeta **Descargas** y pulsando el botón derecho del ratón sobre el archivo descargado seleccionamos **Extraer aquí**. Se crea la carpeta **Thunderbird**:



Abrimos la terminal y movemos la carpeta **Thunderbird** al directorio **/opt**:

```
sudo mv thunderbird /opt/
```

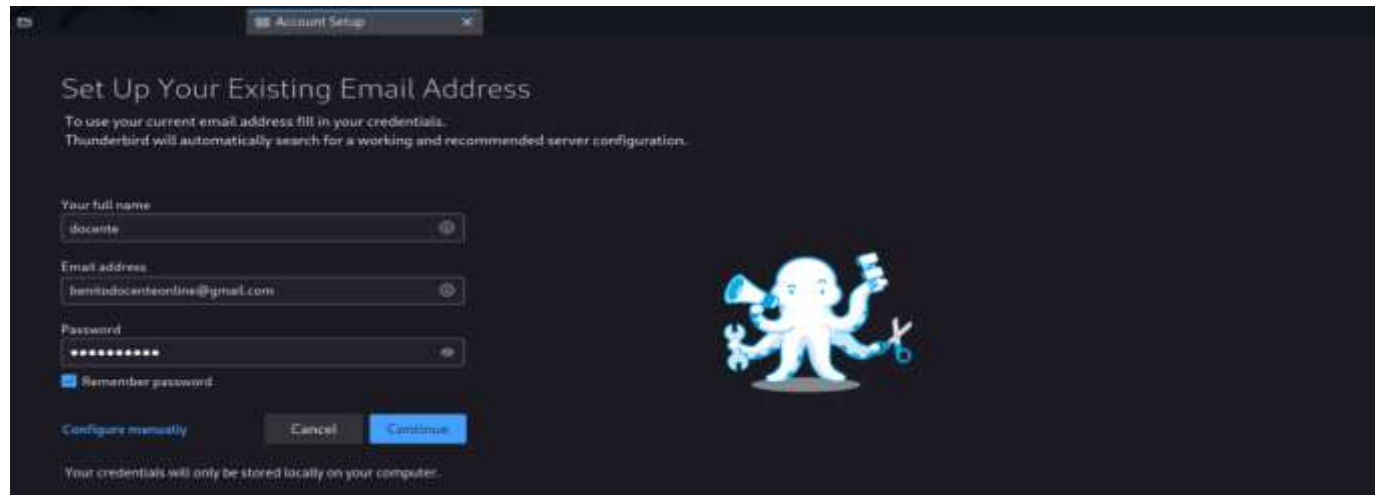
Creamos un enlace simbólico a **Thunderbird**:

```
sudo ln -s /opt/thunderbird/thunderbird /usr/bin/thunderbird
```

Para usar **Thunderbird** lo indicamos desde la terminal:

```
Thunderbird
```

Para su configuración, nos solicita un **Nombre, cuenta de correo y contraseña**. Lo escribimos y pulsamos **Continuar**:



La aplicación busca la configuración de la cuenta en su base de datos, dejamos seleccionada la opción **IMAP** y pulsamos **Done**:

Account Setup

Your full name  
docente

Email address  
benitodocenteonline@gmail.com

Password  
•••••

☒ Remember password

✓ Configuration found in Mozilla ISP database.

Available configurations

☒ **IMAP**  
Keep your folders and emails synced on your server

☐ POP3  
Keep your folders and emails on your computer

Incoming **IMAP** **SSL/TLS**  
imap.gmail.com

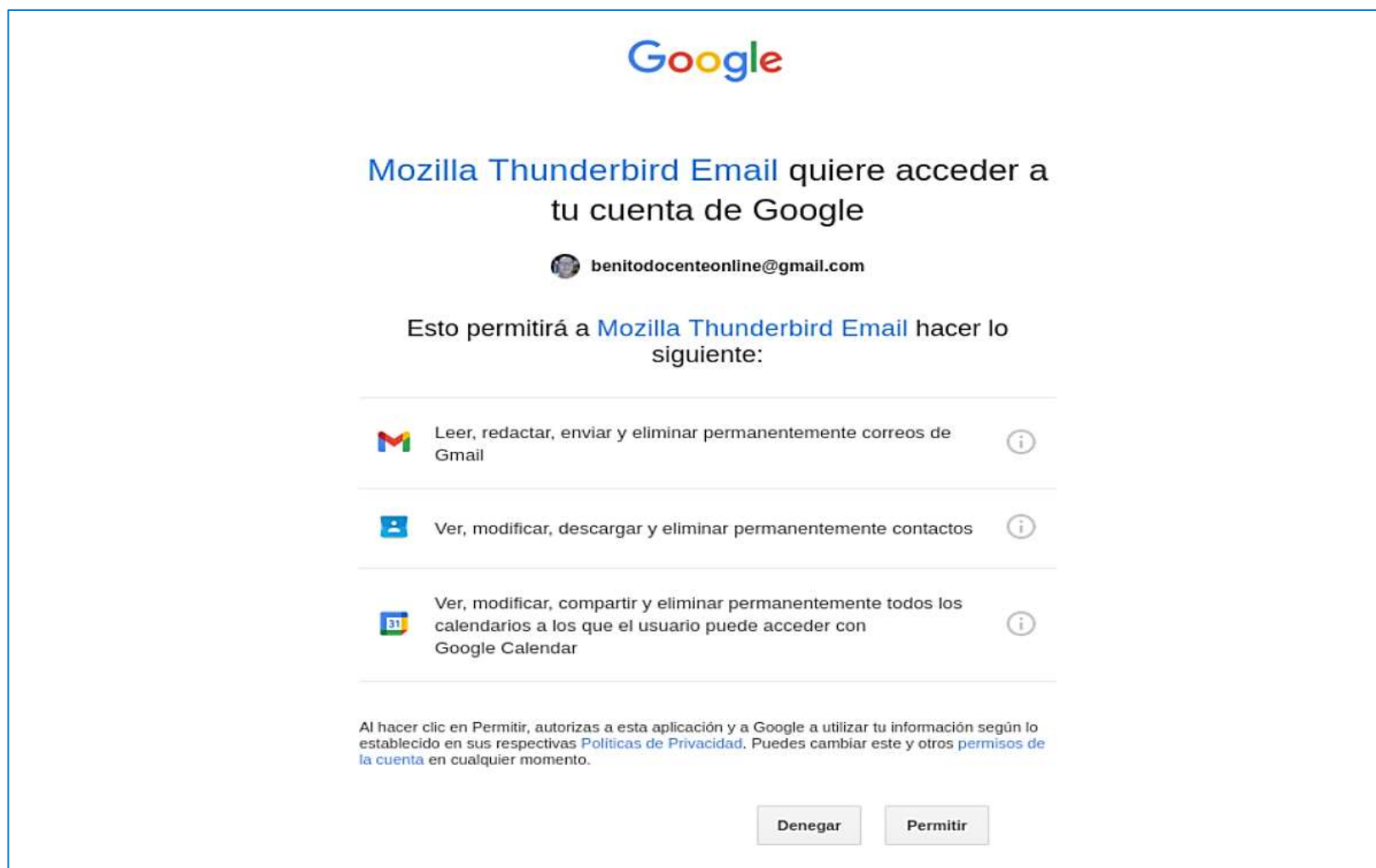
Outgoing **SMTP** **SSL/TLS**  
smtp.gmail.com

Username  
benitodocenteonline@gmail.com

[Setup documentation](#) - [Support forum](#) - [Privacy policy](#)

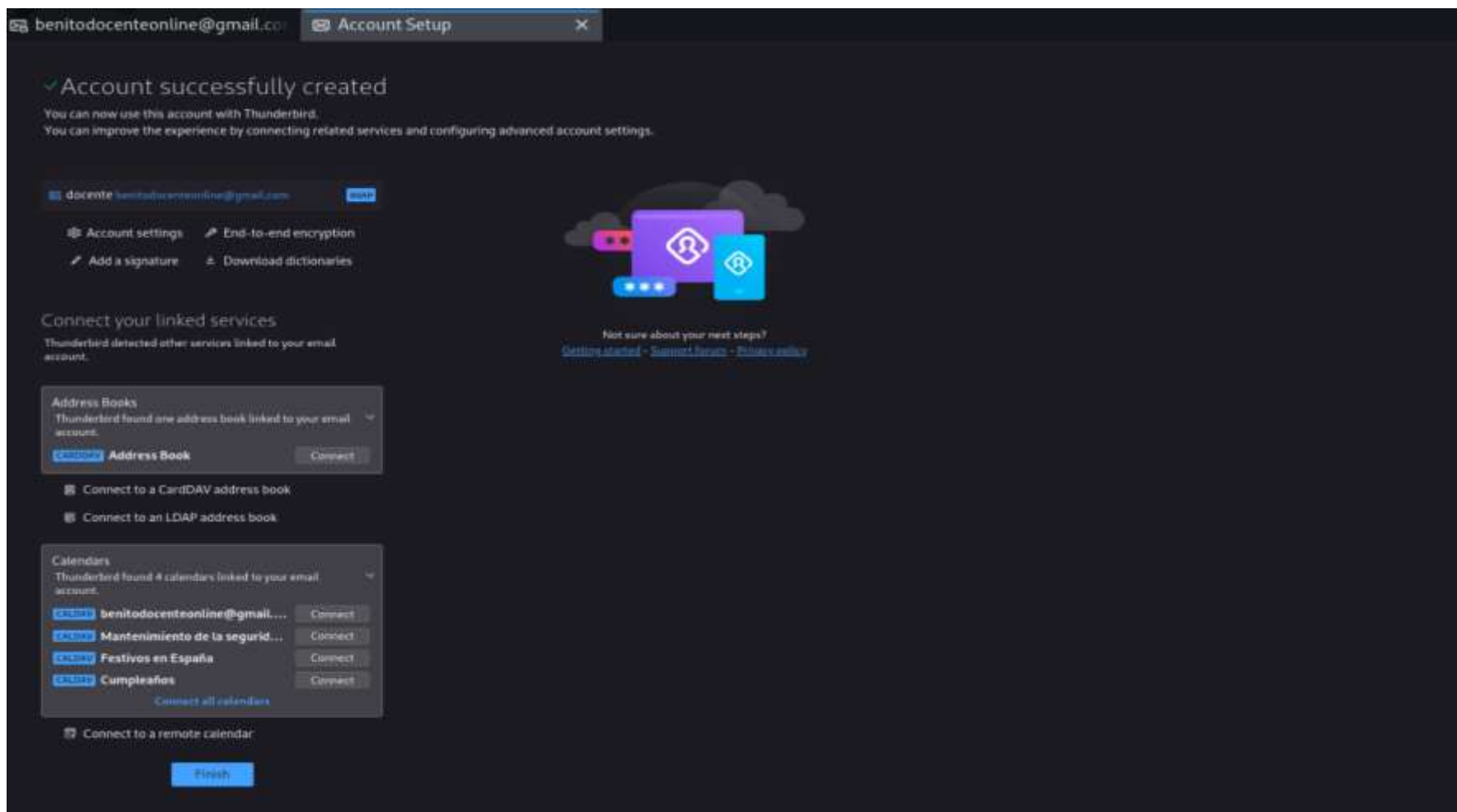
[Configure manually](#) [Cancel](#) [Done](#)

La aplicación se conecta con el servidor de correo y termina la configuración de la cuenta. Según el tipo de cuenta de correo y el tipo de verificación que tengas, se validará el uso del cliente de correo **Thunderbird**:

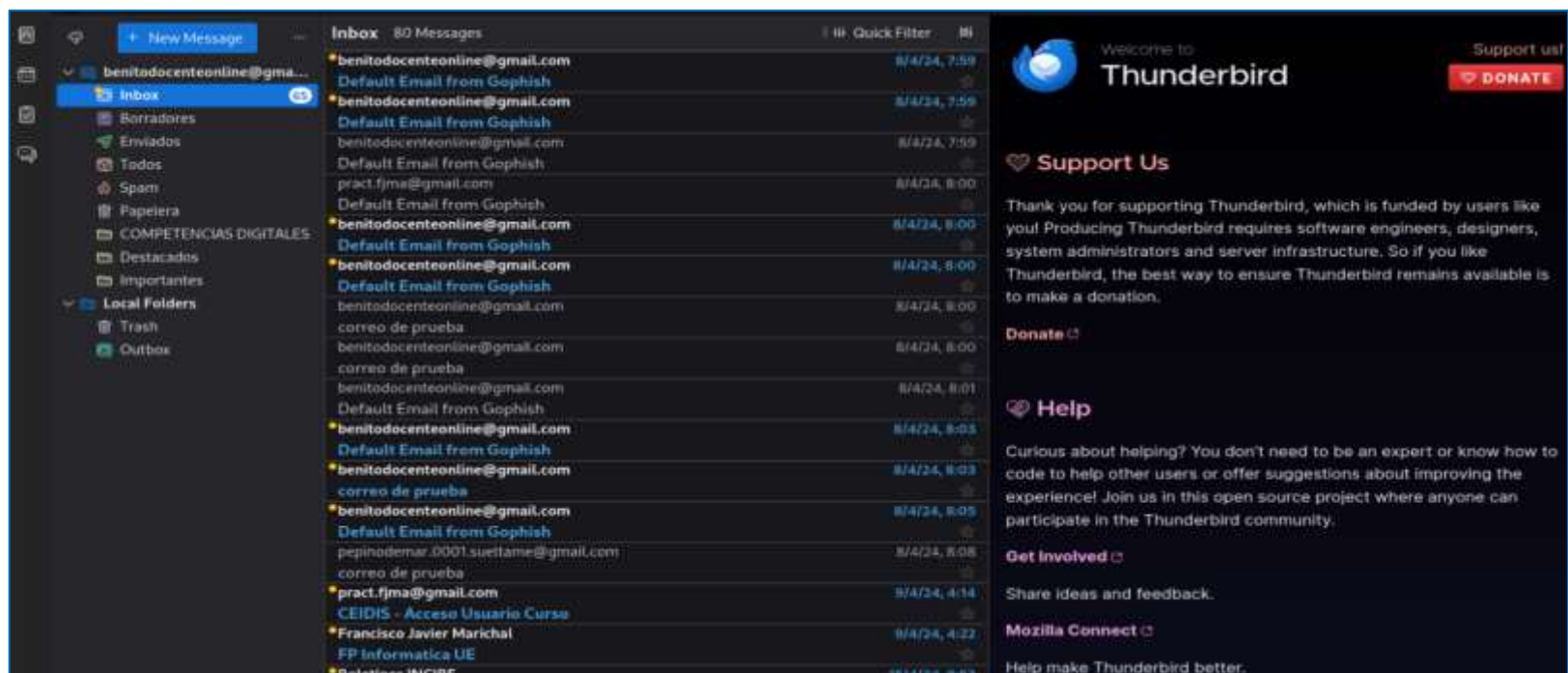




Pulsamos **Finalizar**:



Thunderbird se sincroniza con el servidor:





## Generación de par de claves:

Abrimos la aplicación **Kleopatra** y pulsamos sobre **Nuevo par de claves**:



Introducimos un nombre y la dirección de correo electrónico para el certificado:

 Crear certificado OpenPGP — Kleopatra 

Introduzca un nombre y/o una dirección de correo electrónico para el certificado.

---

**Nombre**

benitodocente

**Dirección de correo electrónico**

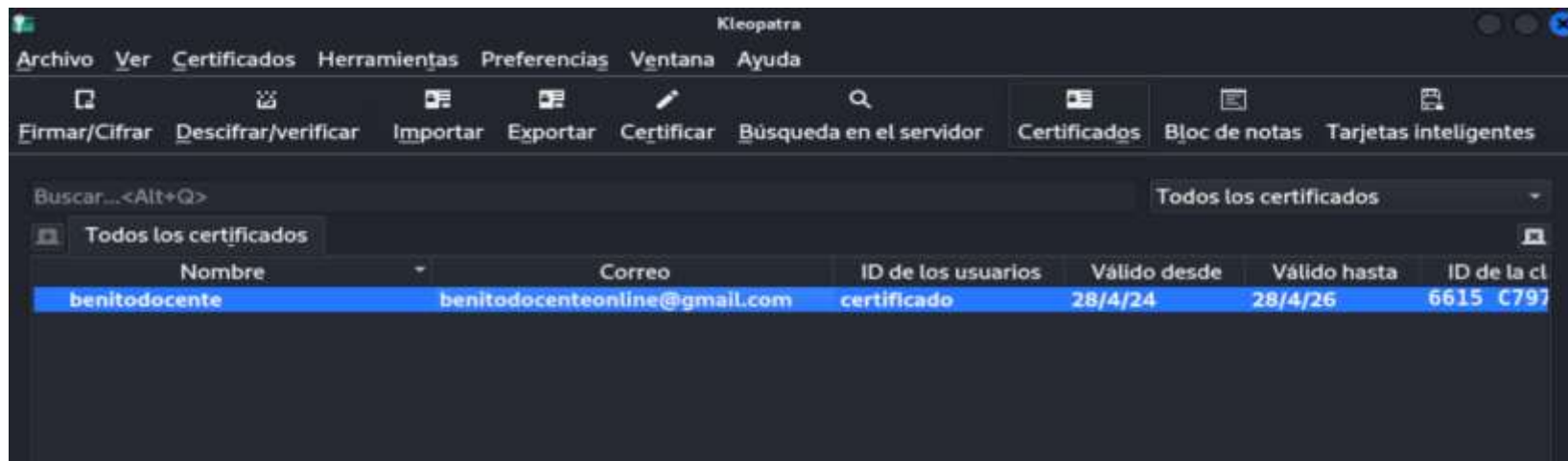
benitodocenteonline@gmail.com

☐ **Proteger la clave generada con una frase de contraseña.**

[\\_Configuración avanzada...](#)

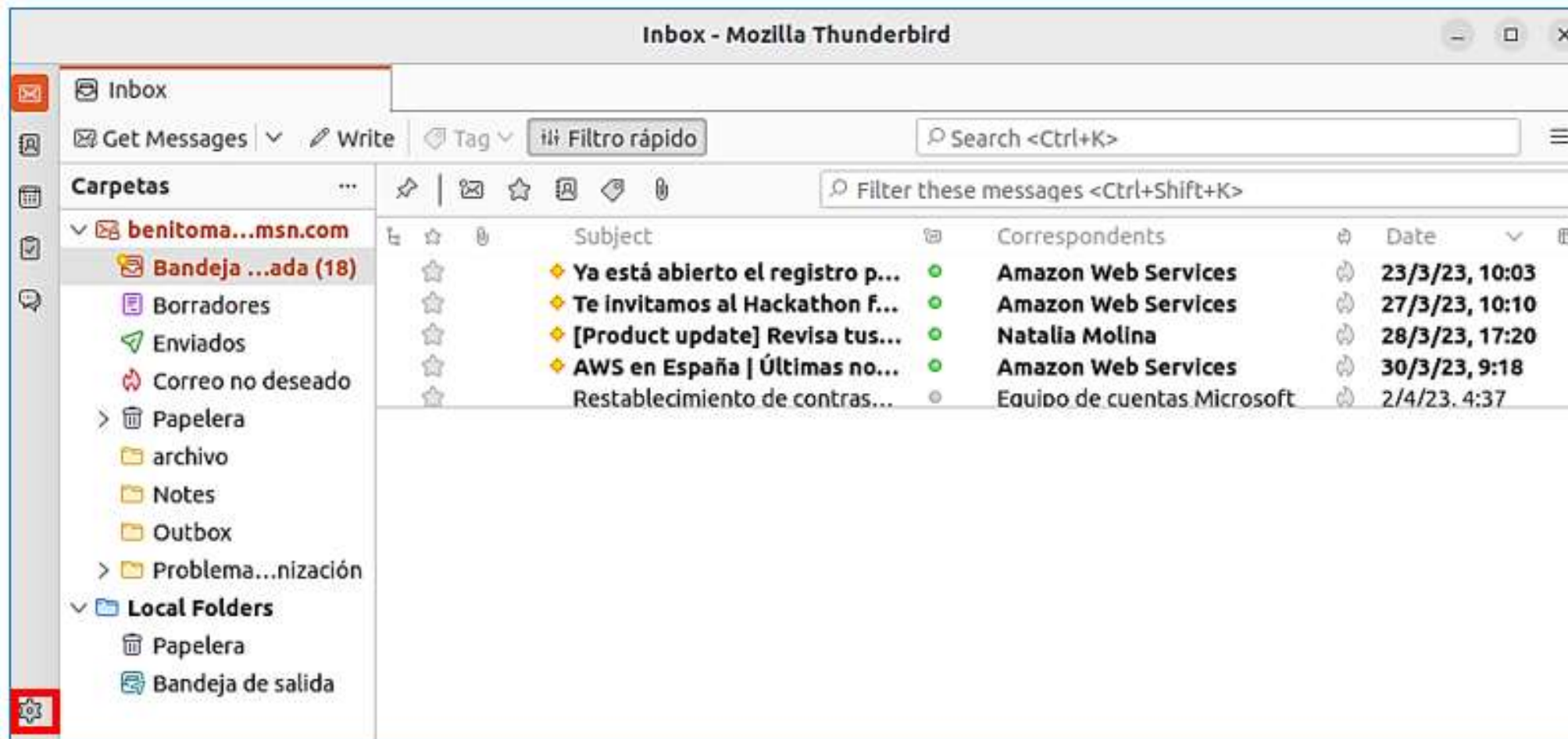
[\\_Aceptar](#) [Cancel\\_](#)

Se crea el nuevo certificado:



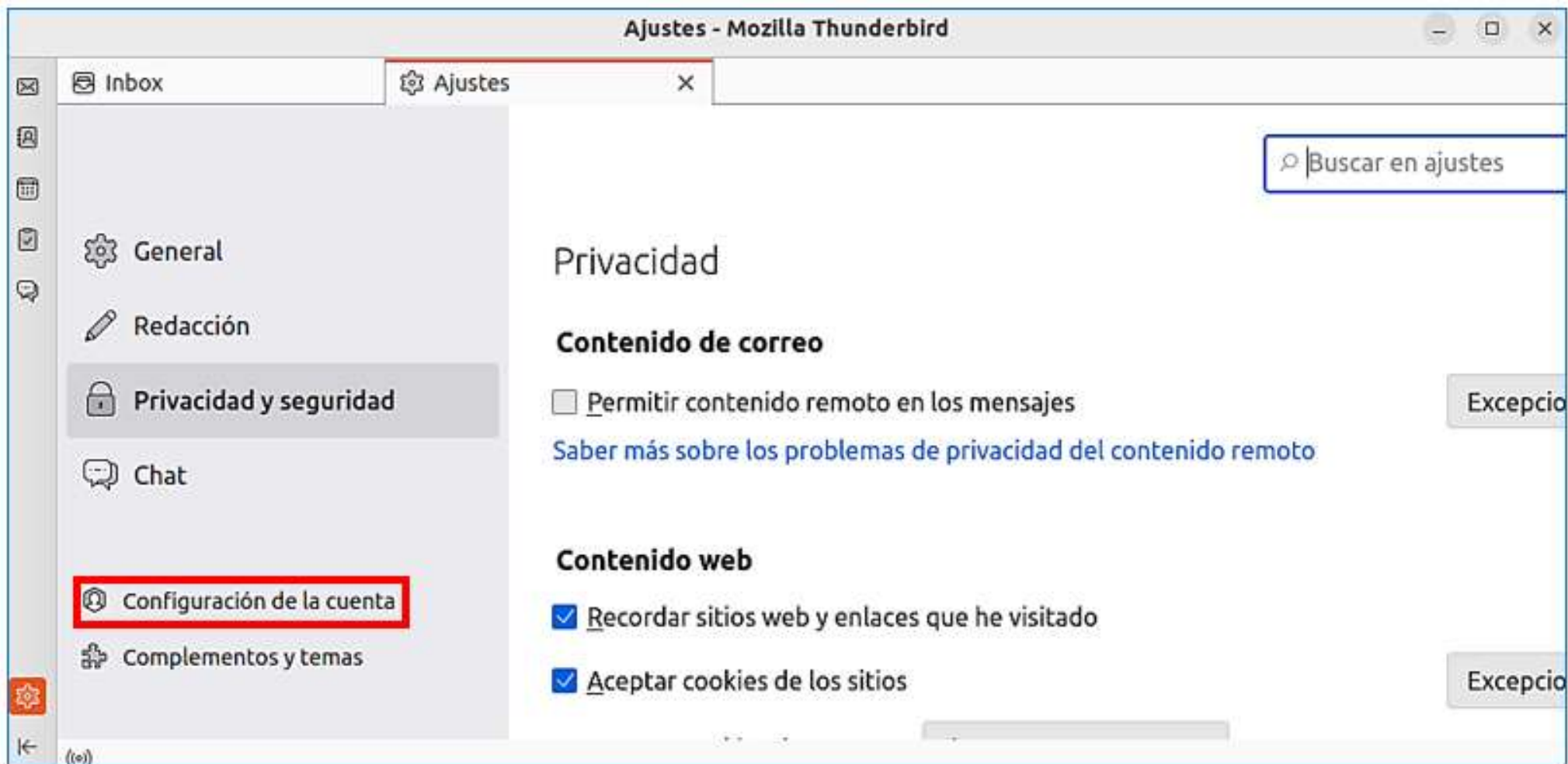
## Añadir claves a Thunderbird:

Para añadir la clave, vamos a **Configuración**:

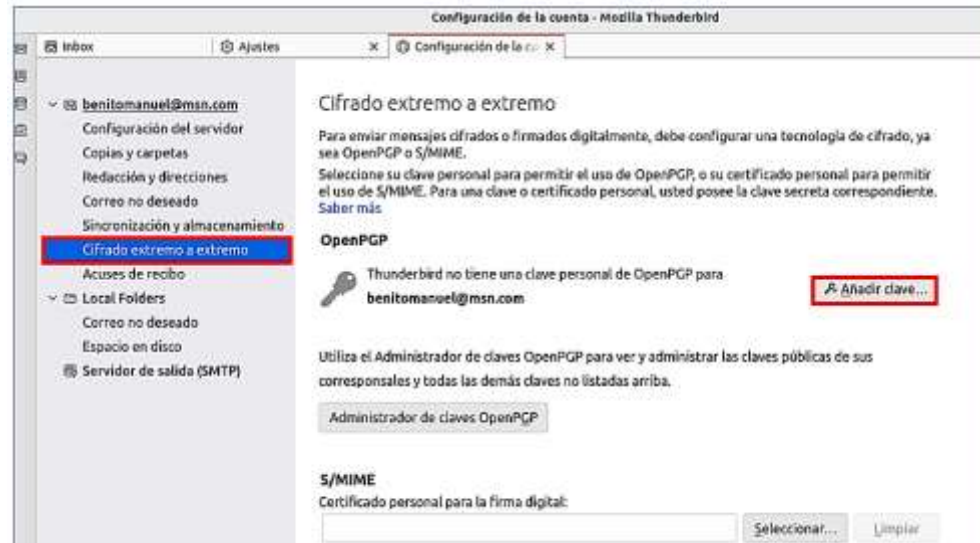


Seleccionamos **Configuración de la cuenta**:

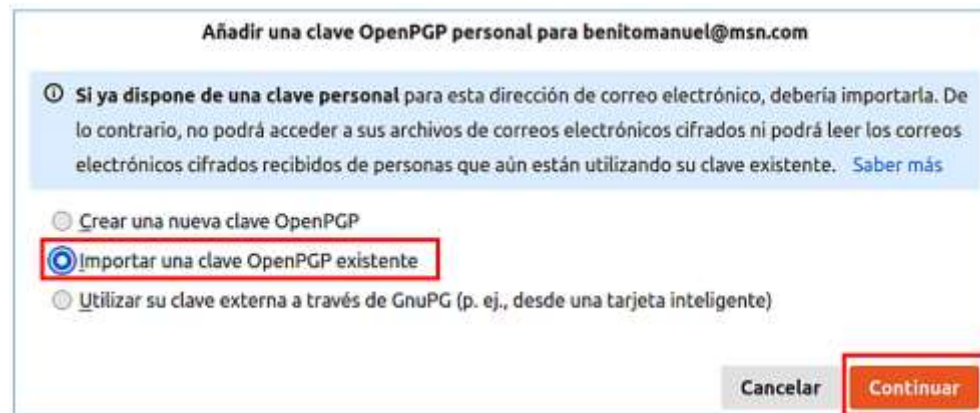




Seleccionamos **Cifrado extremo a extremo, Añadir clave:**



Seleccionamos **Importar una clave OpenPGP existente**. Pulsamos **Continuar**:



Pulsamos **Seleccionar archivo para importar**:





Buscamos la clave secreta que hemos exportado en **Kleopatra**, y pulsamos **Abrir**:



Pulsamos **Continuar**:

**Añadir una clave OpenPGP personal para benitomanuel@msn.com**

Importar una clave OpenPGP personal existente

✓ **Thunderbird encontró una clave que puede ser importada.**

Confirme qué claves pueden utilizarse como sus claves personales. Sólo las claves que creó usted mismo y que muestran su propia identidad deberían usarse como claves personales. Puede cambiar esta opción más adelante en el cuadro de diálogo Propiedades de la clave.

**0xAC85AD898EEE7841**  
clave2 <benitomanuel@msn.com>

☒ Utilizar esta clave como una clave personal

Las claves marcadas para ser utilizadas como claves personales se enumerarán en la sección Cifrado de extremo a extremo. Las demás estarán disponibles dentro del Administrador de claves.

Atrás

Cancelar

Continuar

Termina el proceso de importación. Pulsamos **Cerrar**:

**Añadir una clave OpenPGP personal para benitomanuel@msn.com**

✓ ¡Las claves OpenPGP se han importado correctamente!

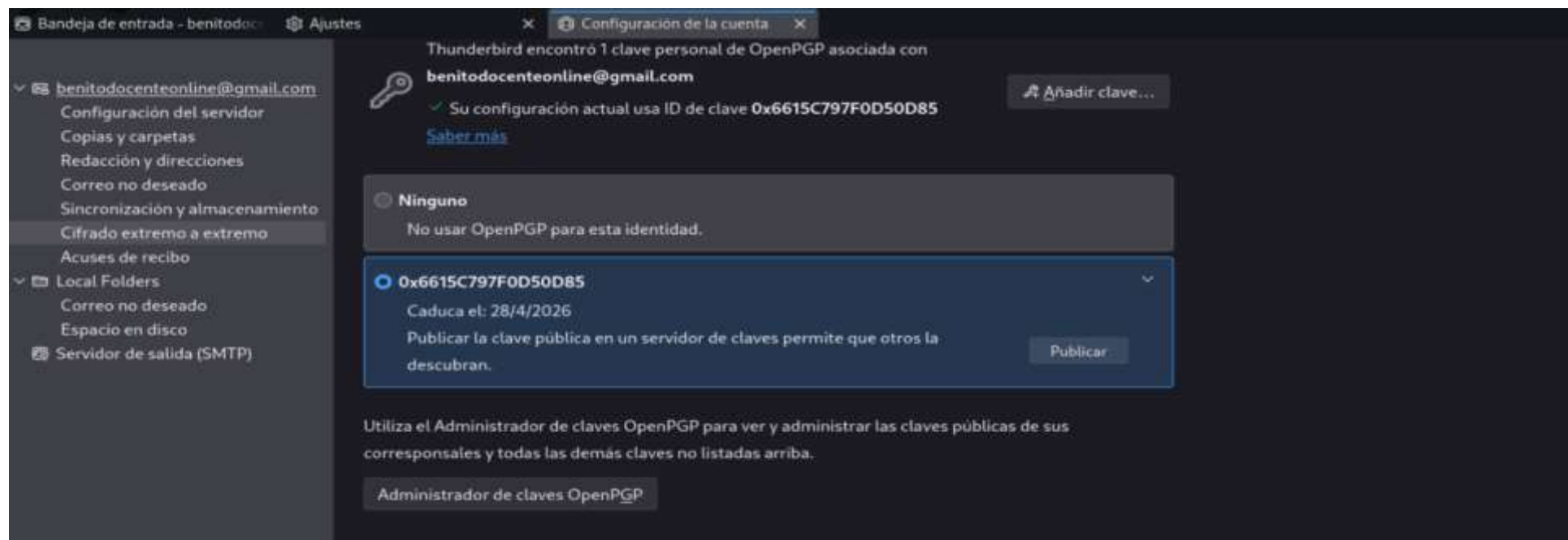
<b>Identidad</b>	clave2 <benitomanuel@msn.com>
<b>Huella digital</b>	C700 4002 0135 7791 9F8E 7AD8 AC85 AD89 8EEE 7841
<b>Creada</b>	14/6/2023
<b>Bits</b>	3072

🔑 Propiedades de la clave

**Completar el proceso de importación**  
Para empezar a utilizar su clave OpenPGP importada y cifrar los mensajes de correo electrónico, cierre este cuadro de diálogo y acceda a la configuración de su cuenta para seleccionarla.

Continuar

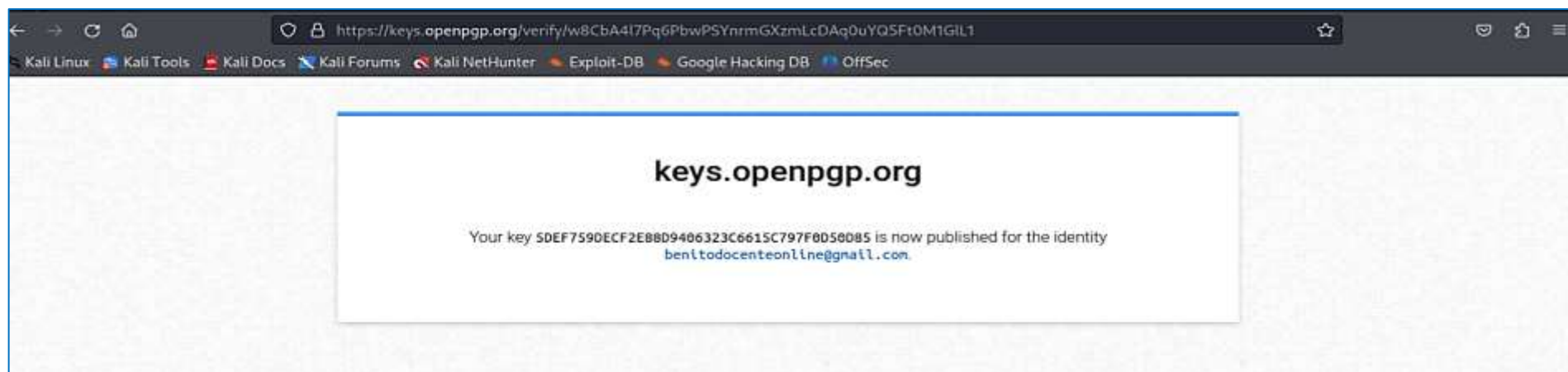
Por último, seleccionamos la clave personal y pulsa **Publicar**:



Recibirás un correo en tu cuenta para verificar la publicación del certificado:

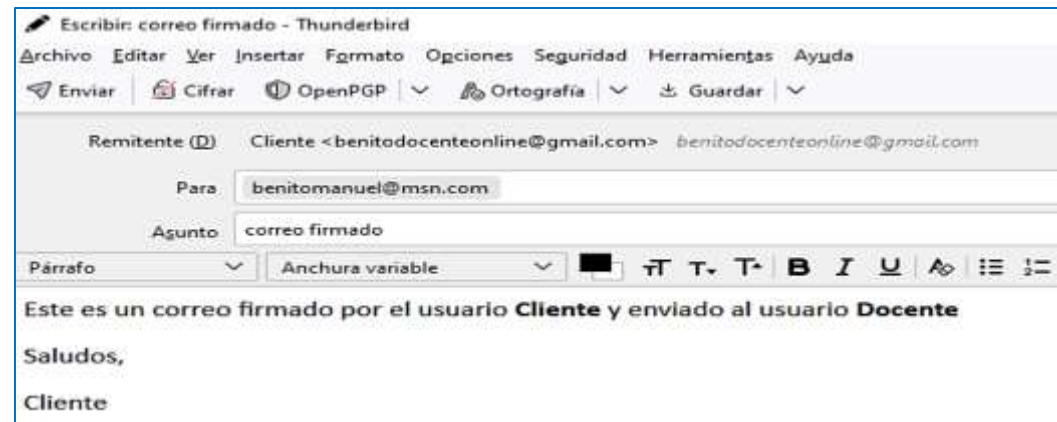


La clave ha sido publicada para la cuenta de correo indicada:



## Envío de correo firmado

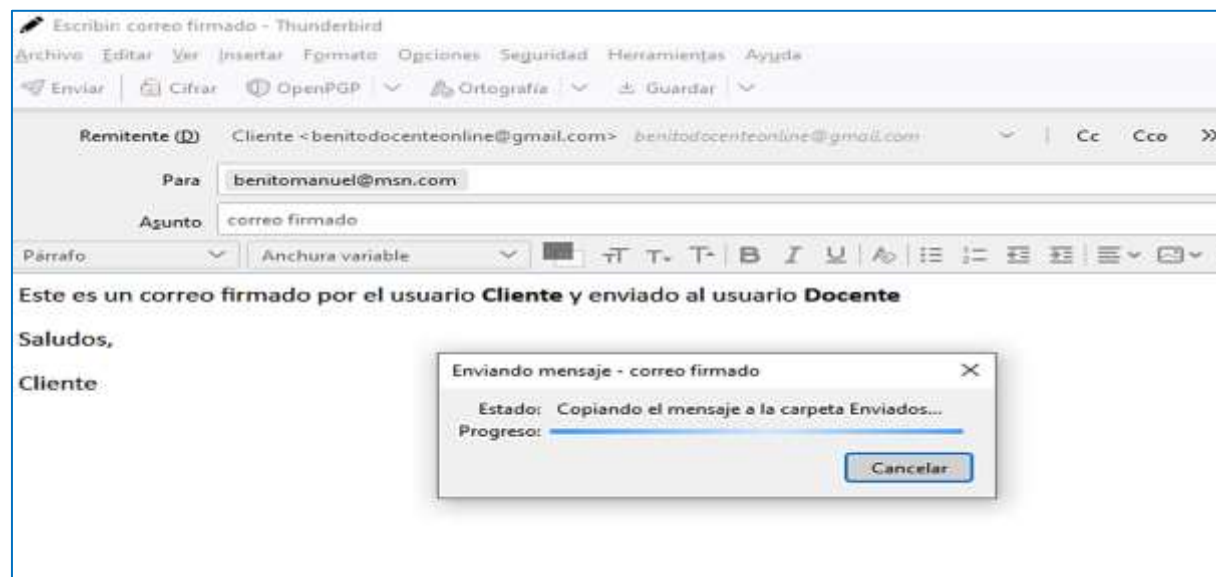
Preparamos un correo para enviar:



En la pestaña OpenPGP, seleccionamos la opción **Firmar digitalmente**:

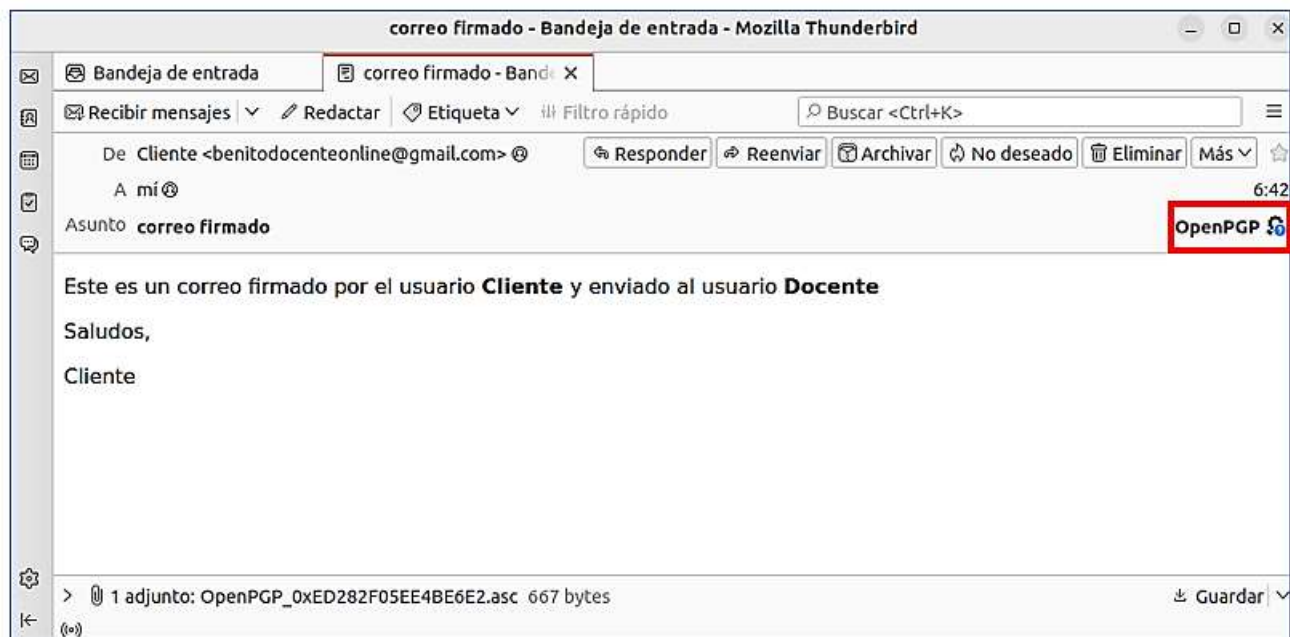


Enviamos el correo:

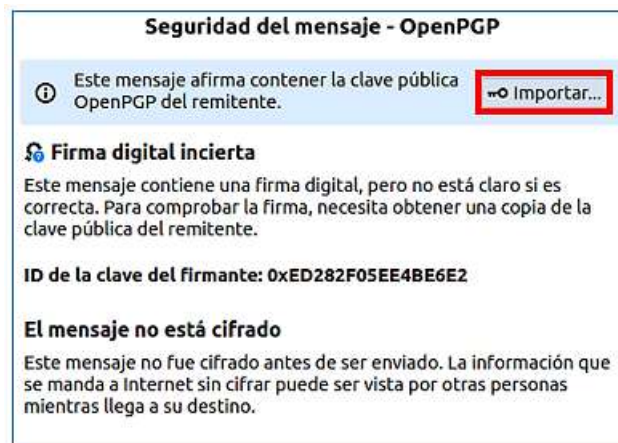


El Usuario (Docente) recibe el correo. En la parte superior izquierda, nos indica que está firmado. Pulsamos en **OpenPGP**:



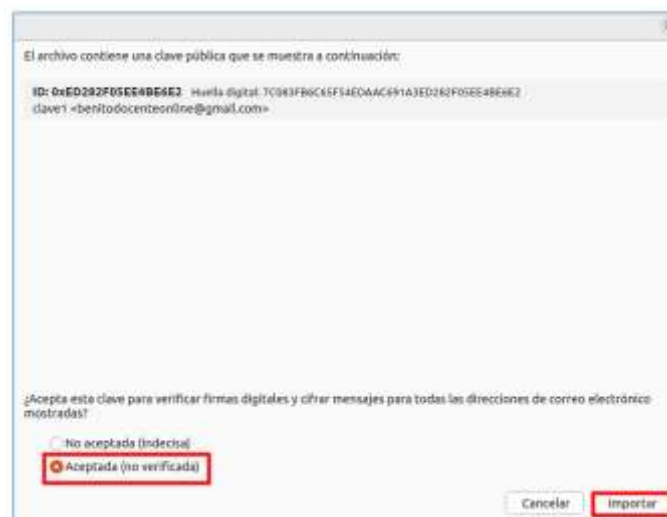


Nos indica que está firmado, pero indica que necesita la clave pública del firmante para comprobarlo. El mensaje incluye la firma. Pulsamos **importar**:

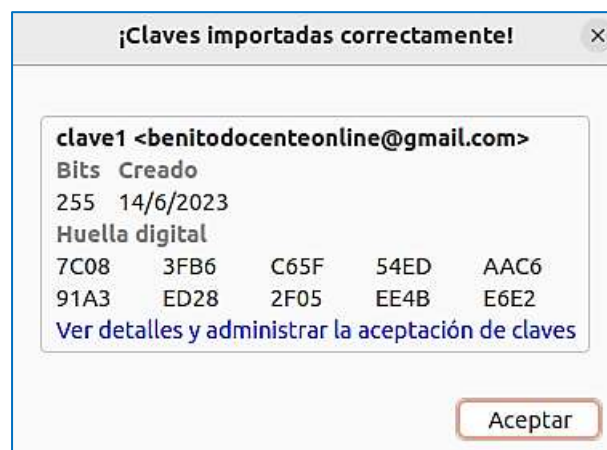




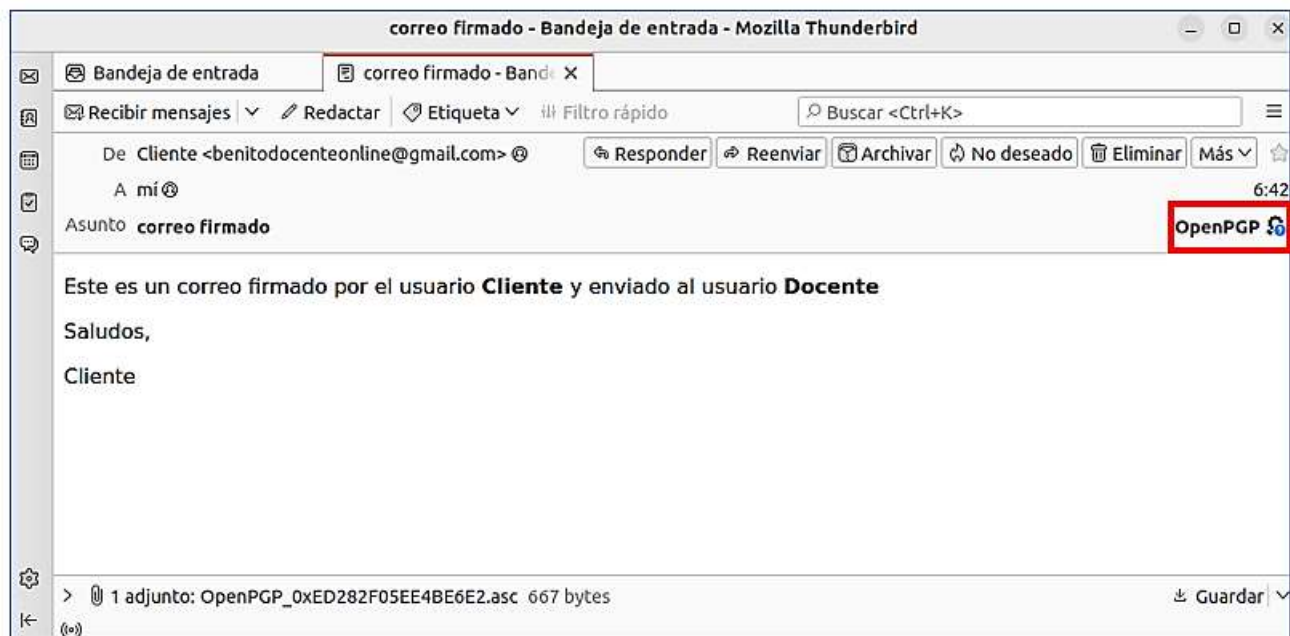
Seleccionamos **Aceptada** y pulsamos **Importar**:



Nos indica que la clave ha sido importada correctamente y pulsamos **Aceptar**:




Volvemos a comprobar la firma:




Ahora nos indica la clave. Pulsamos **ver la clave del firmante**:

**Seguridad del mensaje - OpenPGP**



Este mensaje afirma contener la clave pública OpenPGP del remitente.

[Importar...](#)



**Firma digital incierta**

Este mensaje contiene una firma digital, pero no está claro si es correcta. Para comprobar la firma, necesita obtener una copia de la clave pública del remitente.

ID de la clave del firmante:  
0xED282F05EE4BE6E2

[Ver la clave del firmante](#)

**El mensaje no está cifrado**

Este mensaje no fue cifrado antes de ser enviado. La información que se manda a Internet sin cifrar puede ser vista por otras personas mientras llega a su destino.

Seleccionamos la opción **Sí, he verificado en persona que esta clave tiene la huella digital correcta**. Pulsamos **Aceptar**:

Propiedades de la clave

Propietario de la clave reclamada	clave1 <benitodocenteonline@gmail.com>
Tipo	clave pública
ID de clave	0xED282F05EE4BE6E2
Huella digital	7C08 3FB6 C65F 54ED AAC6 91A3 ED28 2F05 EE4B
Creado	14/6/2023
Caducidad	14/6/2025

Actualizar en línea

Su aceptación   Certificaciones   Estructura

¿Acepta esta clave para verificar firmas digitales y para cifrar mensajes?

☐ No, rechazar esta clave.

☐ Todavía no, quizás más tarde.

☐ Sí, pero no he verificado que sea la clave correcta.

☒ Sí, he verificado en persona que esta clave tiene la huella digital correcta.

Verifique la huella digital de la clave utilizando un canal de comunicación seguro que no sea el correo electrónico para asegurarse de que realmente sea la clave de benitodocenteonline@gmail.com.

Cancelar   Aceptar

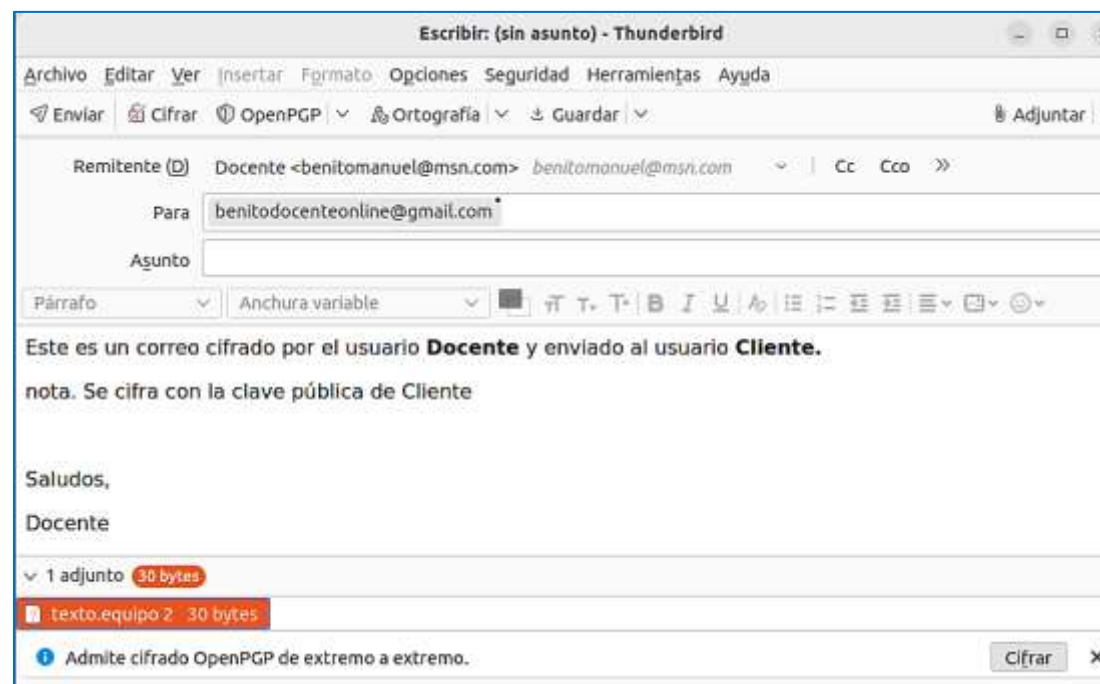
Ahora nos aparece la firma como válida:



OpenPGP 

## Envío de correo cifrado

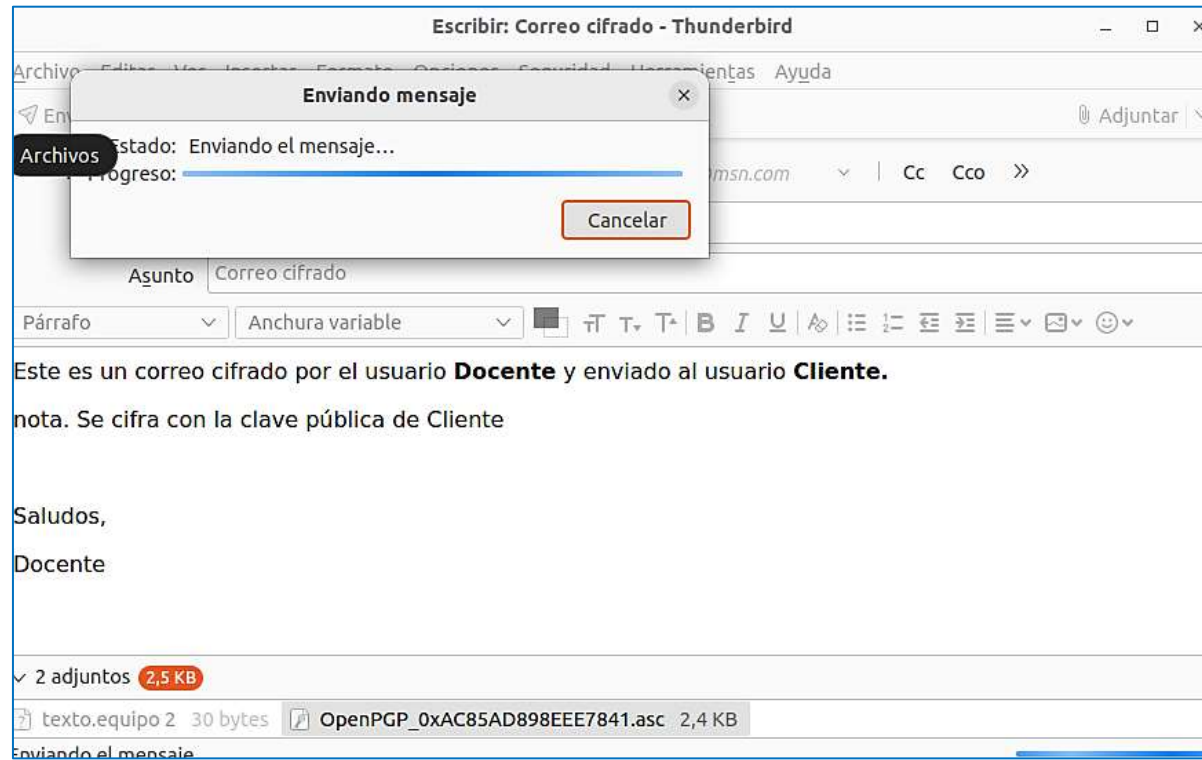
Preparamos un correo para enviar con un archivo adjunto:



Como **Thunderbird** tiene la clave pública del usuario al que se va a enviar el correo, indica que admite cifrado. Pulsamos **Cifrar**:



Enviamos el correo:

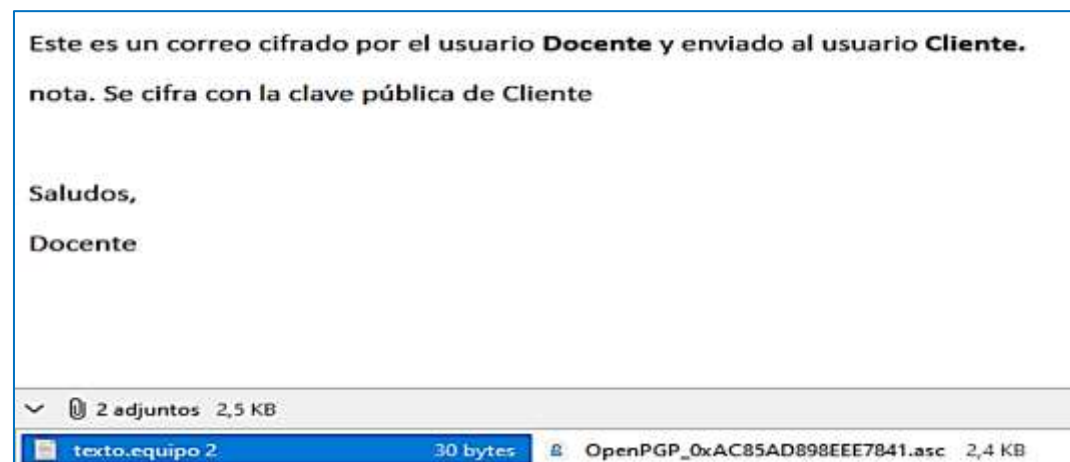


El Usuario (Cliente) recibe el correo. En la parte superior izquierda, nos indica que está firmado y cifrado. Pulsamos en **OpenPGP**:

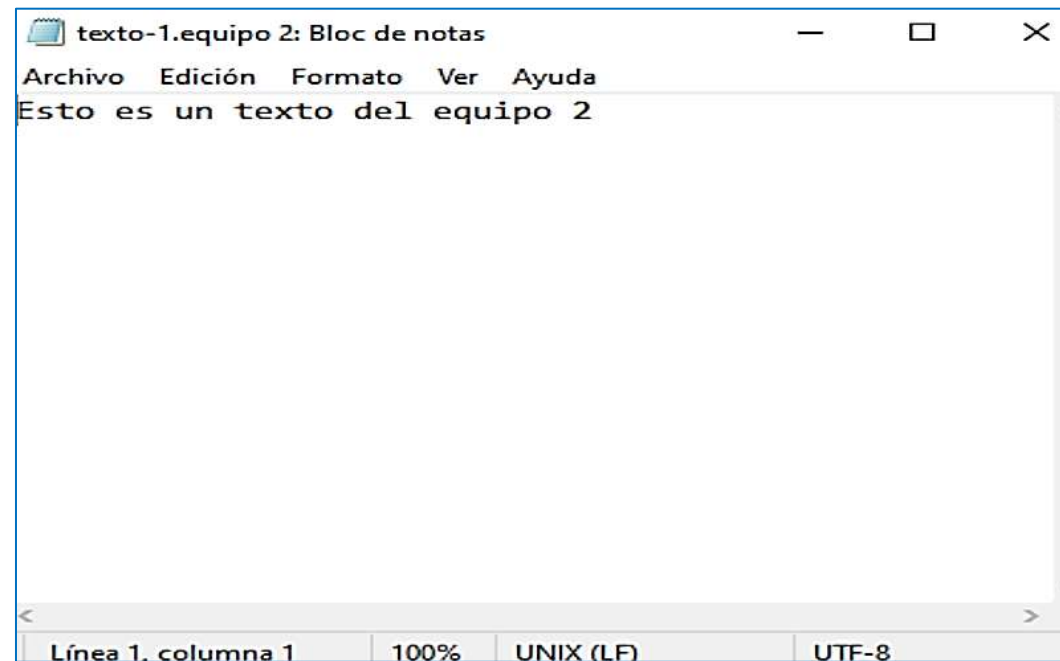


Nos indica que el cifrado es válido y la firma es incierta, ya que no tenemos la clave pública del emisor (Docente). Procedemos a validarla como vimos en el apartado de firmar.

Si descargamos el archivo, vemos que es visible:







Si vemos el correo desde un navegador (Gmail), observaremos que el contenido del correo no es visible:



