TLP:WHITE

Guía para el uso de PGP en clientes de correo electrónico

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

incibe cert_

TLP:WHITE

Septiembre 2021

INCIBE_GUIA_USO_PGP_CORREO_2021_v2

Índice

Índice de figuras

1. Sobre esta guía

"El objeto de la presente guía es mostrar cómo mantener la confidencialidad, integridad y autenticidad en las comunicaciones por medio del correo electrónico"

El objeto de la presente guía es mostrar cómo mantener la confidencialidad, integridad y autenticidad en las comunicaciones por medio del correo electrónico. Para este cometido podemos utilizar PGP (*Pretty Good Privacy*), cuyo objetivo es proteger la información a través de la utilización de criptografía de clave pública. De esta manera, podremos enviar correos y archivos de forma segura y confidencial a través de Internet.

Para mantener los tres principios de confidencialidad, integridad y autenticidad, se presenta de una manera simple la utilización del estándar OpenPGP. Se enseñará el **uso básico** del paquete de cifrado Gpg4win, en el sistema operativo Windows y en particular a través de los clientes de correo electrónico Microsoft Outlook y Thunderbird.

La guía no tiene como finalidad explicar todos los aspectos de los paquetes de software empleados, ni entrar en los detalles más técnicos. Lo que se pretende es dar una visión general para que un usuario que posea unos conocimientos reducidos pueda implementar PGP en su cliente de correo electrónico.

Dentro de los aspectos particulares se partirán de aquellos puntos que hay que tener en cuenta en la gestión de las claves PGP para luego abordar la firma y verificación de correos electrónicos, así como el cifrado y descifrado de los mismos y de sus archivos adjuntos.

2. Introducción

2.1. ¿Qué es OpenPGP?

OpenPGP es un estándar de la organización internacional IETF (*Internet Engineering Task Force*), utilizado para la autenticación de documentos mediante firma digital y de correos electrónicos u otros tipos de compartición de información a través de Internet mediante criptografía de clave pública. Cualquier organización que implemente OpenPGP puede comunicarse con otras que también lo hagan.

Entre los principales usos de las aplicaciones que implementan este estándar se encuentran:

- Comprobar la integridad y autenticidad de los correos electrónicos por medio de técnicas de cifrado.
- Cifrar el contenido del correo para que éste sea solamente accesible por su destinatario.

Hay que tener en cuenta que tanto la dirección de correo del emisor, como las de los receptores, no se cifran.

2.2. Programas que implementan OpenPGP

En la actualidad, existen multitud de programas que implementan OpenPGP. Sin embargo, esta guía se centra en el uso de algunos componentes de Gpg4win, suite de software libre. Entre los componentes que ofrece la suite Gpg4win en esta guía solo se hará uso de dos de ellos:

- **Kleopatra:** es un gestor de certificados PGP. Mediante esta herramienta es posible crear certificados, modificarlos, destruirlos, añadir identidades o modificar fechas de expiración, entre otros.
- **GpgOL:** es un *plugin* de Outlook que añade las funcionalidades de cifrar, descifrar, firmar y comprobar la autenticidad e integridad tanto de los correos, como de sus posibles archivos adjuntos.

3. Cliente Outlook

3.1. Gestión de claves PGP

3.1.1. Creación

Para comenzar a utilizar PGP en nuestros correos electrónicos, antes será necesario crear un certificado con Kleopatra. Para ello, desde el menú «Archivo», se puede encontrar la opción «Nuevo par de claves», al seleccionarla se abrirá un cuadro de dialogo en el que se podrán visualizar dos opciones. Para crear el certificado PGP es necesario pulsar la primera opción.

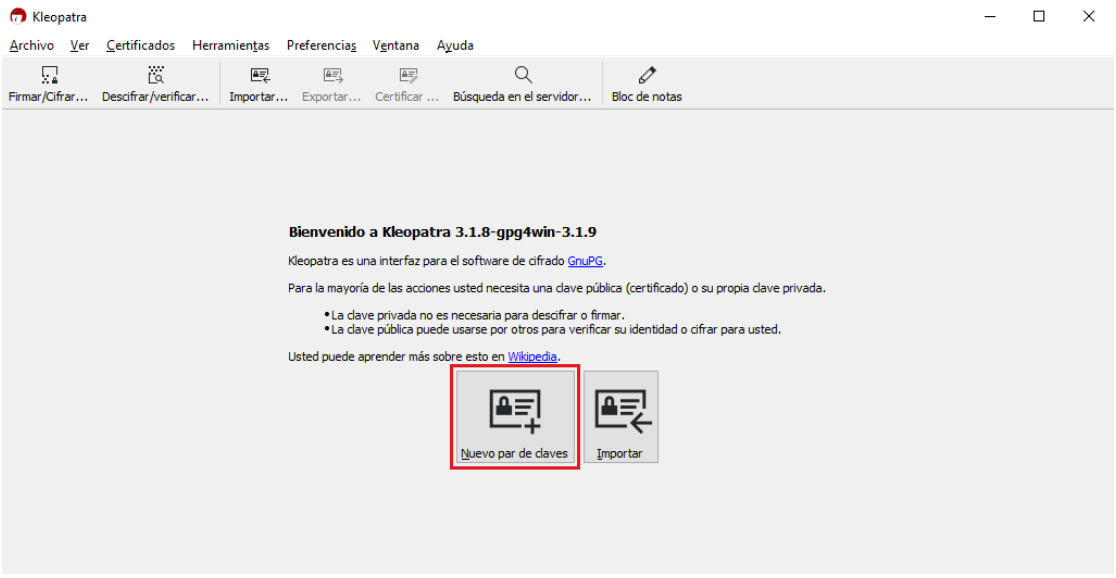

Figura 1 Ventana de elección de formato del par de claves

Acto seguido, aparecerá otra ventana en la que se definirá una identificación para el certificado que se está creando, mediante un nombre, que identifica al propietario del certificado y un correo electrónico del propietario, que se asociará al certificado. Como información adicional se puede definir un comentario como por ejemplo «Mi certificado PGP para el trabajo» o «Certificado personal».

Se debe tener en cuenta que tanto el nombre, como el comentario serán visibles para aquellos que vayan a usar nuestra clave pública para comunicarse con nosotros.

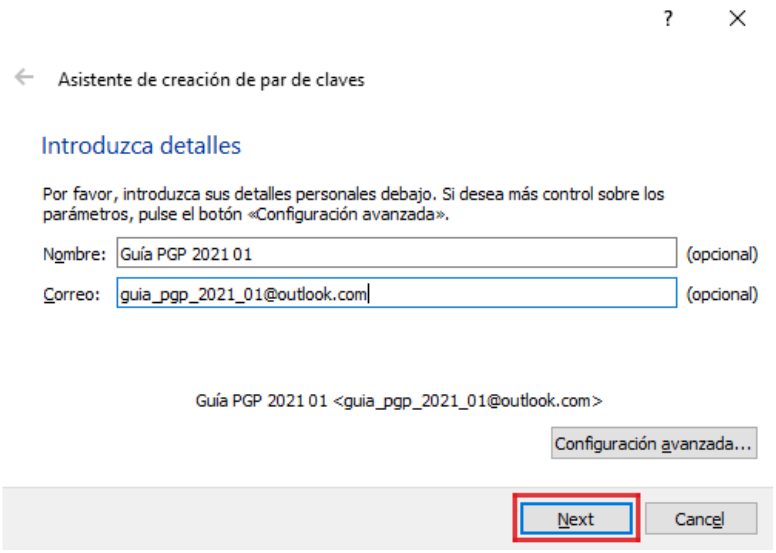

Figura 2 Introducción del nombre y correo del par de claves

En la pestaña «Configuración avanzada…» que se observa en la figura, se pueden definir características del certificado como son el algoritmo de cifrado (RSA, DSA y ECDSA), la fecha de caducidad o para qué se utilizará (firma, cifrado, certificación o autenticación).

Tras pulsar «Next» se mostrará otra ventana en la que se seleccionará la opción «Crear» para la generación del certificado:

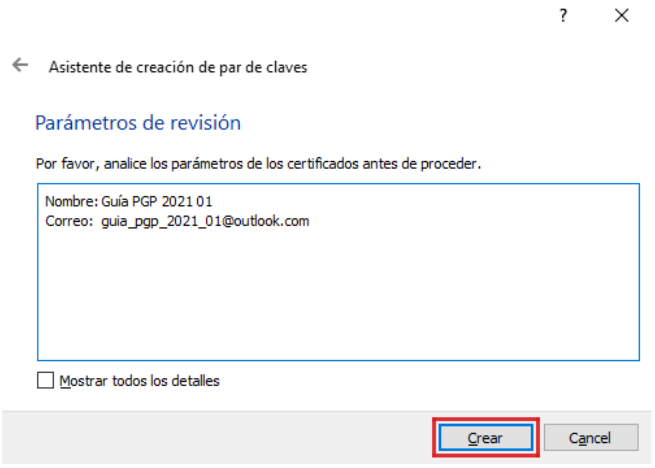

Figura 3 Parámetros de revisión del asistente

Antes de crearlo, se abrirá un nuevo cuadro de diálogo en el que se solicitará una contraseña que se usará para acceder al certificado que se va a generar. Esta contraseña debe ser robusta, por lo que es recomendable utilizar un mínimo de 8 caracteres entre los que se incluyan minúsculas, mayúsculas, números y símbolos. Será necesario conocer esta contraseña para poder firmar o descifrar información usando este certificado. En caso de que se olvide la contraseña, la única solución consistirá en revocar el certificado tal y como se detalla al final de este punto.

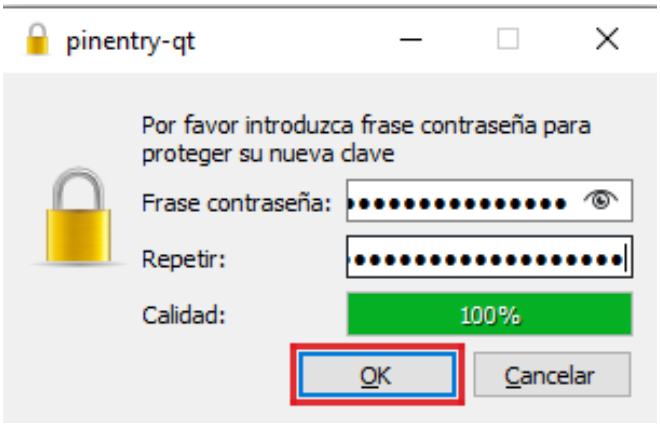

Figura 4 Introducción de la clave para el llavero de claves

Acto seguido, aparece una ventana donde se confirma la correcta creación de las claves, se muestra la huella digital del par de claves y se brindan 3 opciones:

- «Hacer copia de respaldo de su par de claves…», donde las claves se almacenarán en un directorio específico.
- «Enviar clave pública por correo…», como su propio nombre indica, enviará las claves a través de correo electrónico a la dirección que se elija.
- «Enviar clave pública a un servicio de directorio…», en esta última opción las claves se enviarán a un servicio público para que liste la clave en las búsquedas que le hagan.

"Esta contraseña debe ser robusta, por lo que es recomendable utilizar un mínimo de 8 caracteres entre los que se incluyan minúsculas, mayúsculas, números y símbolos"

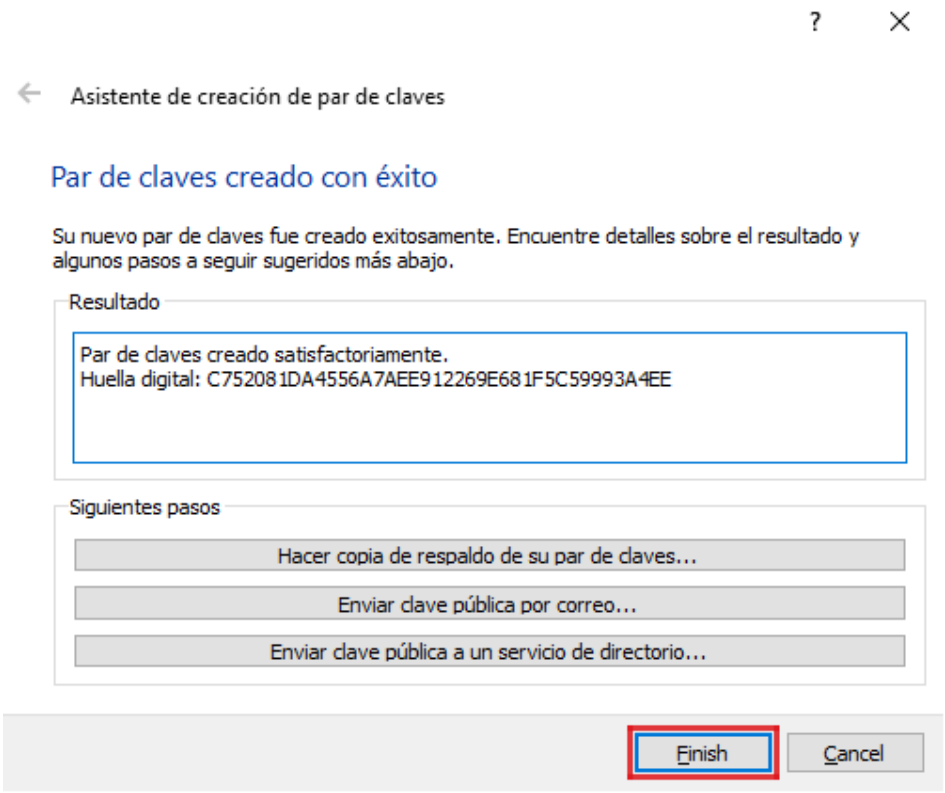

Figura 5 Ventana de creación exitosa del par de claves

Una vez creados, los certificados aparecen en la pantalla principal de Kleopatra.

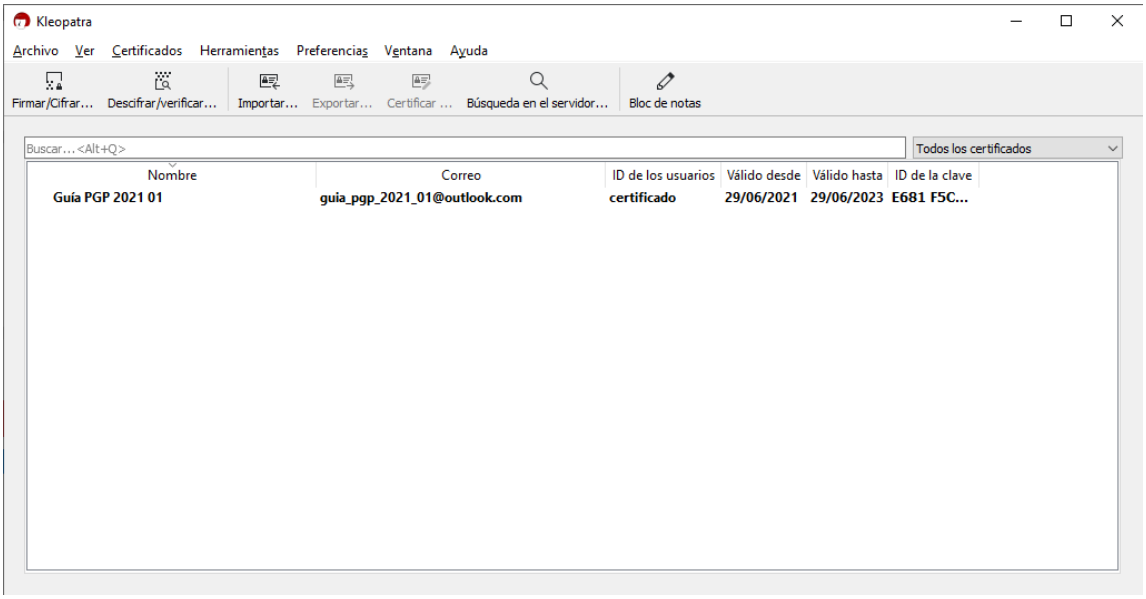

Figura 6 Ventana principal de Kleopatra con el par de claves creadas

En caso de haberse visto comprometida la seguridad de alguna de las claves o que éstas hayan expirado, es posible generar lo que se denomina un certificado de revocación, que otorga la posibilidad de cancelar la llave pública, siendo recomendable realizarlo y mantenerlo en un lugar seguro.

Para poder generarlo hay que hacer *clic* con el botón derecho sobre el certificado en cuestión, en el menú desplegable de propiedades y pulsar la opción «Detalles». Esto mostrará la ventana de «Detalles del certificado» tal y como se vio en puntos anteriores. En esta ventana se encuentra el botón «Generar certificado de revocación», cuando se pulsa sobre éste, permite generar un archivo con extensión *.rev* que se podrá almacenar donde se desee.

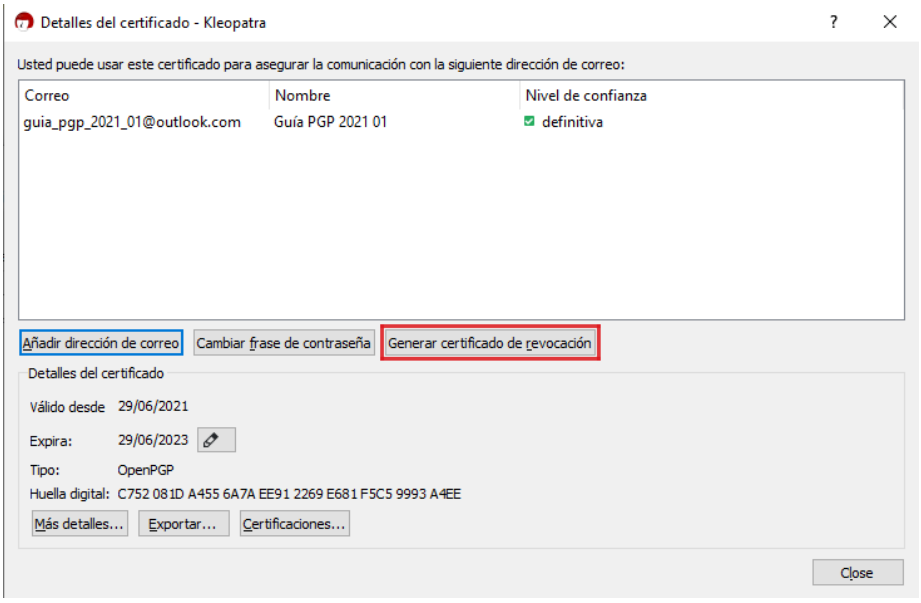

Figura 7 Detalles del certificado (incluye revocación)

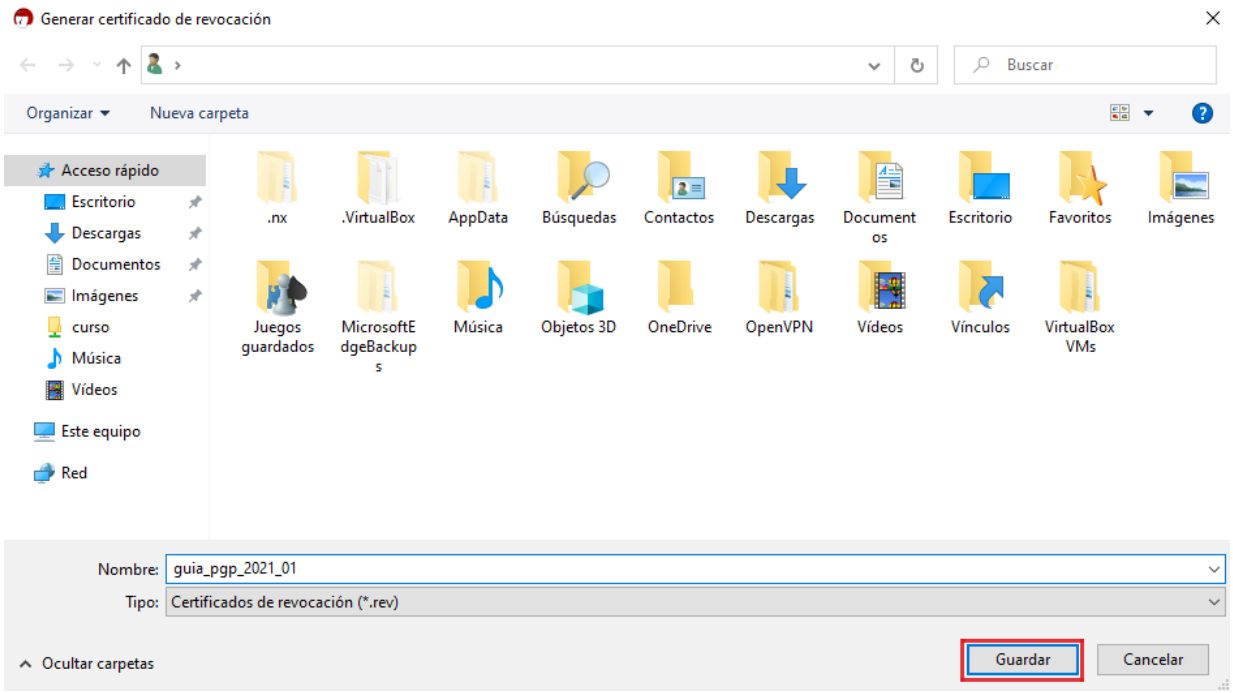

Figura 8 Ventana de guardado del certificado de revocación

Para poder generar este certificado de revocación es necesario introducir la clave que se tiene asociada a nuestro certificado. De este modo, se evita que si un tercero quiere acceder a nuestro equipo, pueda generar un certificado de revocación para nuestros certificados.

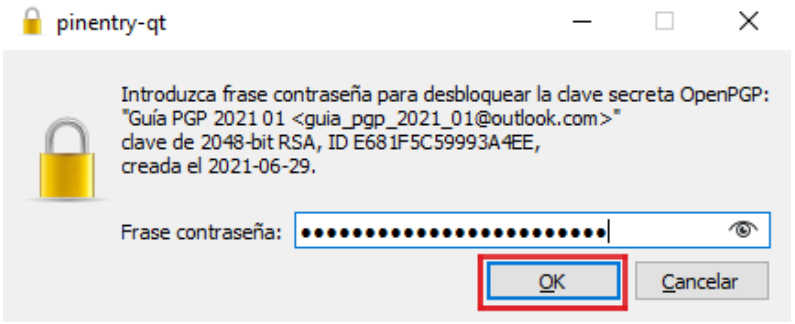

Figura 9 Ventana para la introducción de la clave

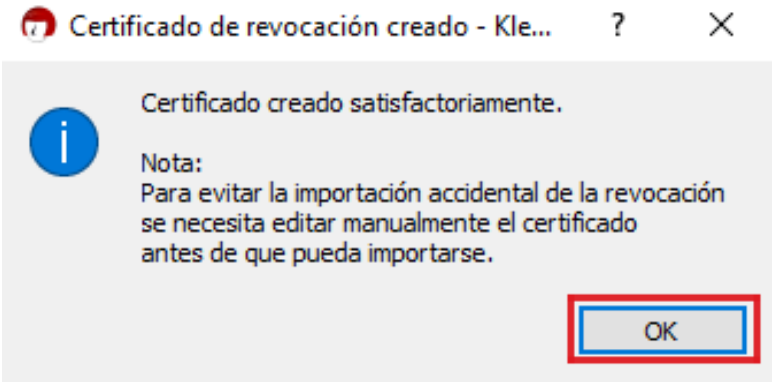

Figura 10 Ventana de certificado creado satisfactoriamente

3.1.2. Cambio de la contraseña de un certificado

En caso de ser necesario, es posible cambiar las contraseñas asignadas a cada certificado durante su creación. Si se realiza una copia del certificado PGP antes de modificar su contraseña, independientemente de si la realiza el usuario o un atacante, dicha copia seguirá teniendo la contraseña antigua, conservando una funcionalidad completa para su uso, por lo que podría utilizarse tanto para la firma como para el descifrado de documentos, incluso de aquellos que fueron cifrados después del cambio de contraseña.

Para ello, se pulsará con el botón derecho del ratón sobre el certificado al que se quiere aplicar dicho cambio en la pantalla principal de Kleopatra, seleccionando la opción de «Cambiar la frase de contraseña…» en el menú desplegable. Al seleccionarla se abrirá una ventana de diálogo donde se debe introducir la contraseña actual del certificado y, a continuación, la nueva contraseña del certificado en cuestión.

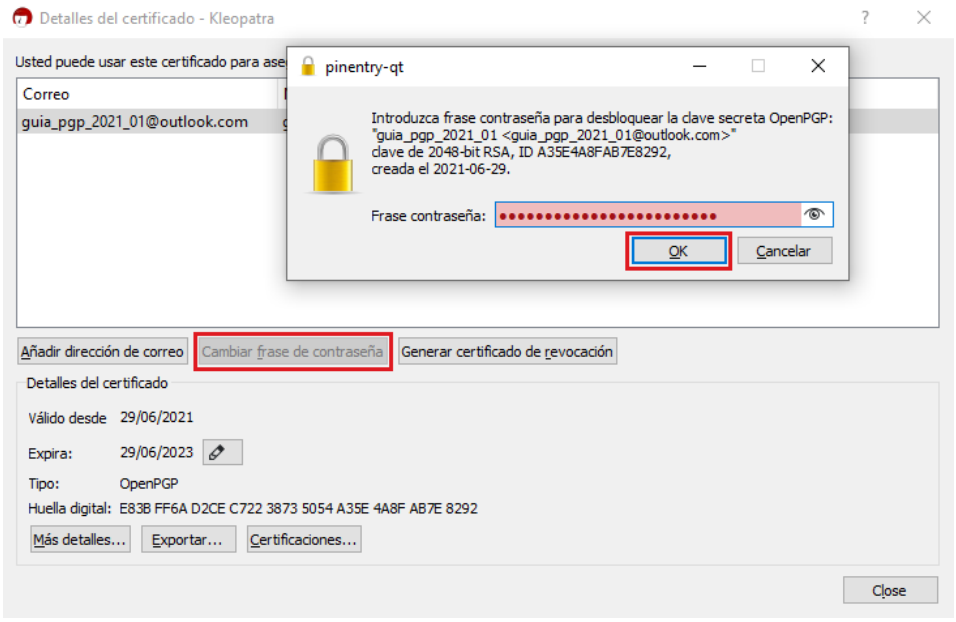

Figura 11 Ventana de cambio de contraseña de una clave PGP

3.1.3. Compartición de la clave pública de un certificado a través del correo electrónico

Para compartir la clave pública de un certificado PGP es necesario exportarla. Para ello, se debe pulsar con el botón derecho del ratón sobre el certificado en la pantalla principal de Kleopatra y elegir la opción «Exportar…».

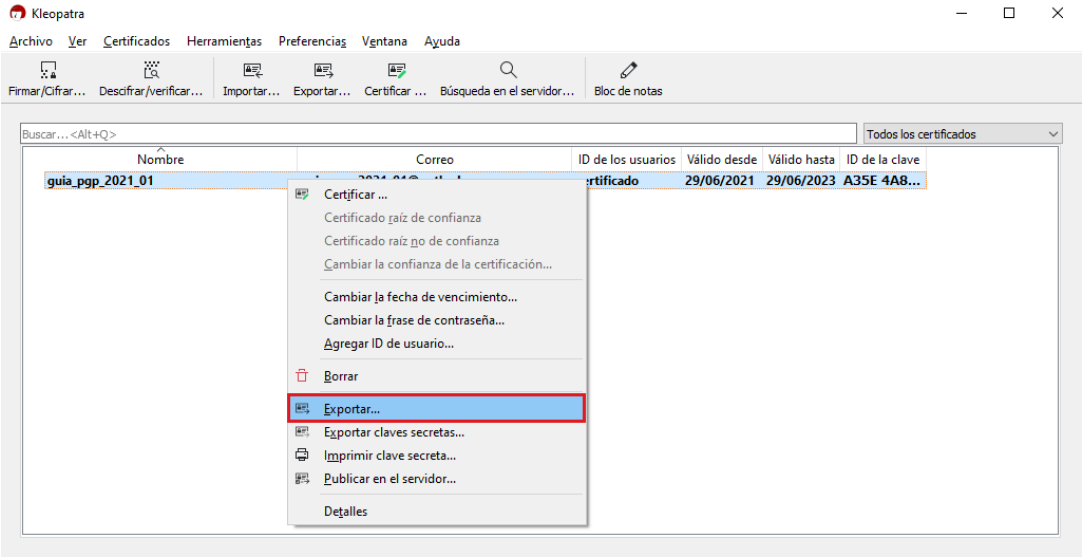

Figura 12 Ventana de exportar certificado

Tras esto, es necesario seleccionar una localización adecuada donde almacenar el archivo con extensión *.asc*

Para enviarlo a través del correo electrónico basta con adjuntarlo como un archivo más.

A la hora de importar una clave que se ha recibido en un correo electrónico, basta con pulsar dos veces sobre el archivo adjunto con extensión *.asc* que ha sido recibido. La ventana solicitará nuestra clave para añadirla.

3.1.4. Backup de la clave privada mediante la exportación a un fichero

No solo es posible exportar la clave pública de los certificados PGP. Además, es posible exportar el certificado en su totalidad, es decir, tanto la clave privada como la pública y las identidades que se le hayan asignado.

Para hacerlo, basta con pulsar el botón derecho del ratón sobre el certificado en la pantalla principal de Kleopatra. En el menú que se despliega se encuentra la opción «Exportar claves secretas…», tras ser pulsada, se abrirá una ventana de diálogo en la cual se debe seleccionar la localización donde se guardará el certificado en formato *.gpg*.

No se debe compartir esta copia de seguridad con terceros.

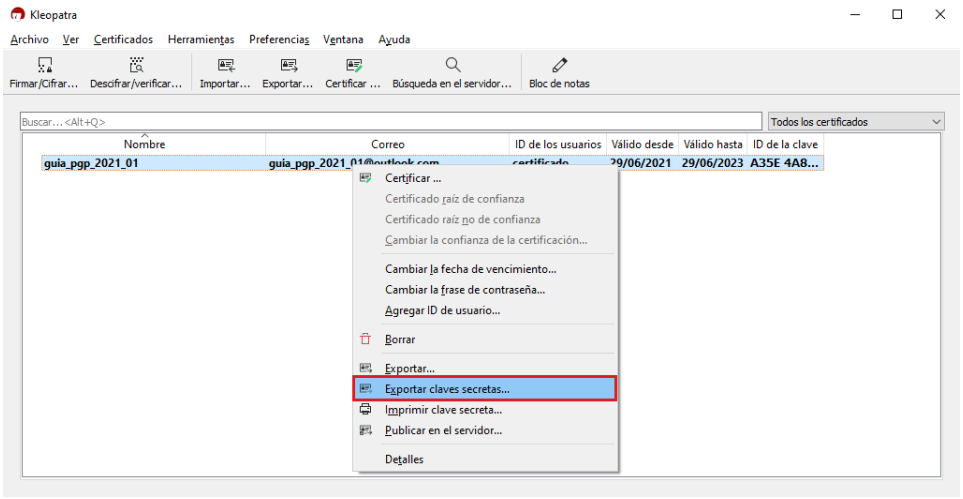

Figura 13 Ventana de exportación del par de claves

Si se quiere importar un certificado exportado de la manera anterior, basta con seleccionar la opción «Importar…» que se puede localizar en el menú superior de la pantalla principal de Kleopatra. Acto seguido, se abrirá una ventana de diálogo para seleccionar el certificado a importar.

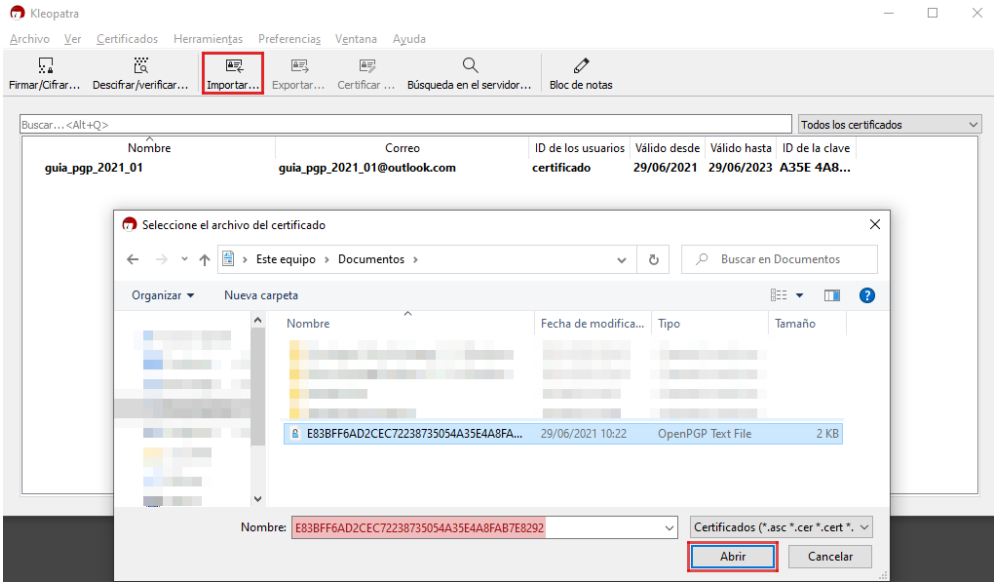

Figura 14 Ventana de importar un certificado

3.2. Firma y verificación de correos electrónicos

3.2.1. Firma

La acción de firmar se lleva a cabo para que el receptor del correo electrónico se cerciore de que la información que se transmitió no ha sido manipulada, es decir, que mantenga la integridad de los datos.

Para firmar un correo electrónico es necesario pulsar sobre el icono de Outlook llamado «GpgOL», donde se puede encontrar la opción «Sign» en el menú desplegable.

GpgOL selecciona automáticamente la firma en nuestros correos. Para poder elegir el certificado PGP en los emails enviados a través de Outlook, se deberá desactivar la opción «Automation» de la ventana de configuración de GpgOL. Para acceder a dicha ventana, primero se pulsa en la flecha situada en la parte inferior derecha del icono de Outlook llamado «GpgOL» (1), y seguidamente se desactiva la opción llamada «Automation» (2).

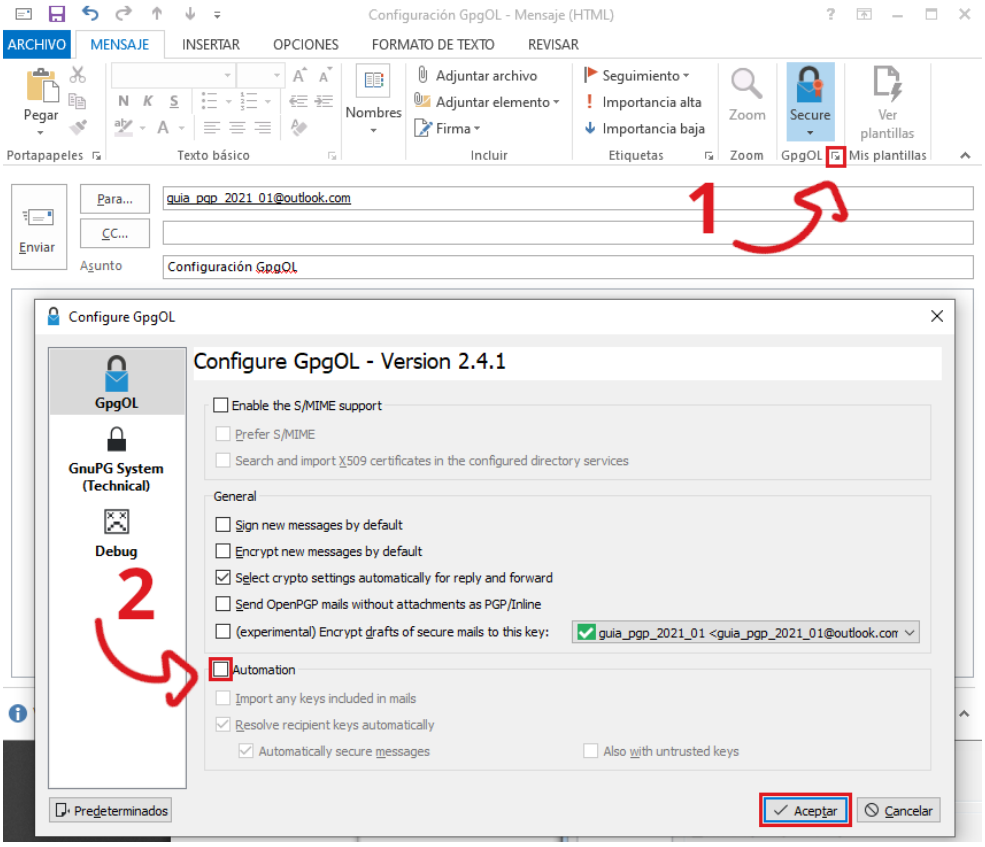

Figura 15 Configuración para la firma y cifrado de correos

Tras escribir el correo electrónico que se desea enviar, se pulsa «Enviar» y en la ventana que aparece se selecciona el certificado PGP que se utilizará para firmarlo.

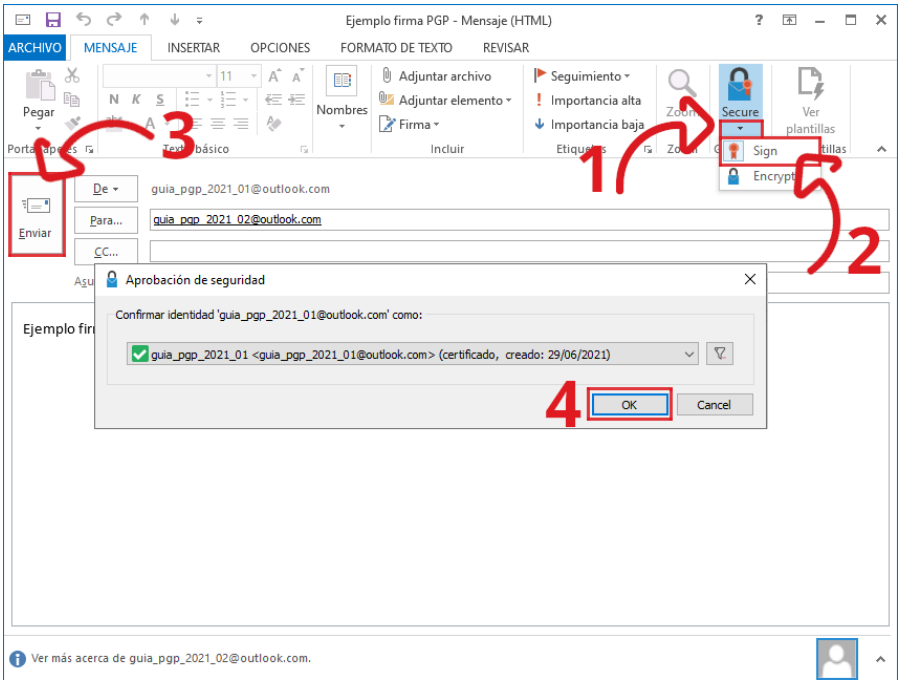

Figura 16 Firma de un correo electrónico en Outlook

3.2.2. Verificación

Para verificar los correos electrónicos firmados por PGP es necesario disponer de la clave pública del usuario que ha enviado el correo electrónico, como fue explicado en la sección 3.1.3 . La verificación se hace de forma automática, y es posible comprobarlo viendo el icono de GpgOL y la etiqueta en el correo «GpgOL: Level 4 trust in 'guia_pgp_2021_01@outlook.com'».

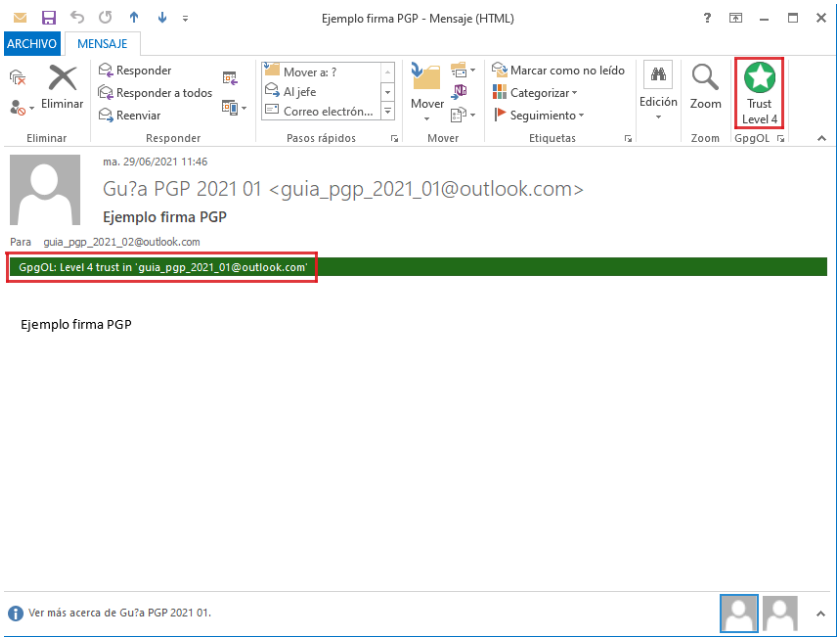

Figura 17 Verificación de la firma del correo electrónico

"Para verificar los correos electrónicos firmados por PGP es necesario disponer de la clave pública del usuario que ha enviado el correo electrónico"

3.3. Cifrado y descifrado de correos electrónicos

3.3.1. Cifrado

En primer lugar, es necesario disponer de la clave pública del certificado PGP del destinatario del correo electrónico. Para ello, se han de seguir los pasos descritos en el punto 3.1.1 para Outlook o 4.1.1 para Thunderbird.

Una vez hecho esto, y tras haber escrito el contenido del correo a enviar, en el icono de «GpgOL» localizado en la parte superior de la ventana de Outlook, se pulsará la opción «Encrypt» y luego el botón de «Enviar». De esta forma, nuestro correo irá cifrado y seleccionará la clave pública de forma automática, si por el contrario se quiere seleccionar manualmente la clave se deberá desactivar la opción «Automation» de la ventana de configuración de GpgOL.

Para acceder a dicha ventana, primero se pulsa en la flecha situada en la parte inferior derecha del icono de Outlook llamado «GpgOL», y seguidamente se desactiva la opción llamada «Automation», de manera similar a la "Figura 15 Configuración para la firma y cifrado de correos".

Ahora, cuando se pulse «Enviar», se mostrará una ventana en la que hay que seleccionar la clave pública del destinatario del correo electrónico a enviar, tal y como se muestra en la imagen inferior.

Figura 18 Aprobación de seguridad

Una vez seleccionado, se enviará el mensaje cifrado al destinatario.

3.3.2. Descifrado

A la hora de recibir un correo electrónico cifrado, para su lectura antes será necesario descifrarlo. Para ello, en el momento de recibir el correo cifrado, GpgOL mostrará una ventana en la cual habrá que introducir la contraseña de nuestro certificado PGP.

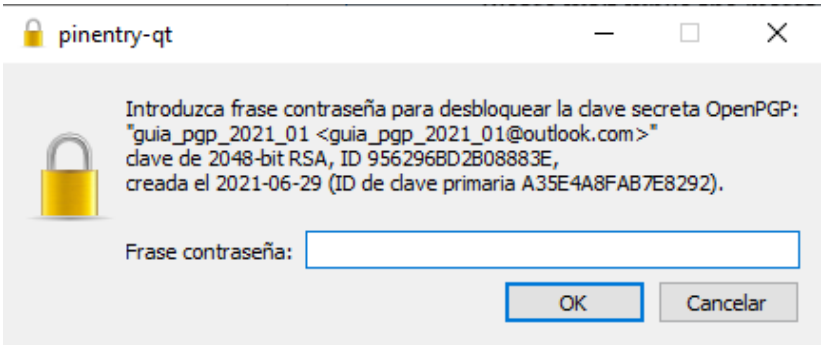

Figura 19 Ventana de inserción de la contraseña del llavero de claves para descifrar el correo

Una vez introducida, se mostrará el mensaje descifrado, y en el icono de GpgOL aparecerá un aviso para informar que el mensaje está cifrado, mostrando la etiqueta «GpgOL: Encrypted Message».

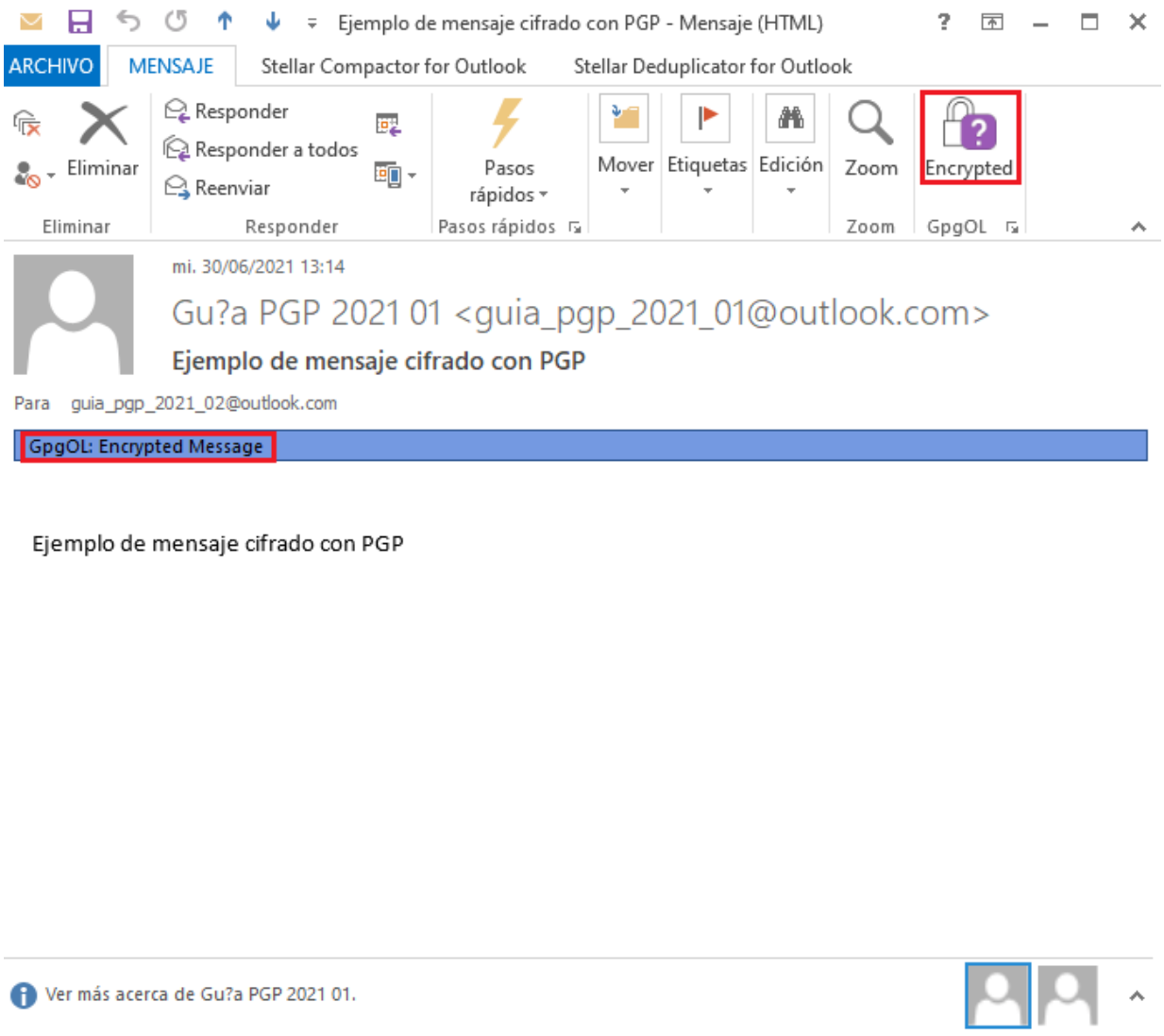

Figura 20 Verificación de mensaje cifrado

3.4. Cifrado y descifrado de un fichero para adjuntar a un correo electrónico

3.4.1. Cifrado

Cuando se envía un correo cifrado desde Outlook con uno o varios archivos adjuntos, los archivos se cifran automáticamente.

3.4.2. Descifrado

De la misma manera que los correos sin archivos adjuntos, Outlook reconoce cuándo un correo electrónico está cifrado, por lo que en el momento en que se quiera acceder a su contenido, el cliente de correo solicitará la contraseña asociada con la clave privada. Al introducirla se descifra tanto el cuerpo del correo, como el o los adjuntos que contenga.

"Outlook reconoce cuándo un correo electrónico está cifrado, por lo que en el momento en que se quiera acceder a su contenido, el cliente de correo solicitará la contraseña asociada con la clave privada"

4. Cliente Thunderbird

4.1. Gestión de claves PGP

En el caso de utilizar Thunderbird como cliente de correo electrónico, a partir de la versión 78.2.1 este cliente tiene soporte incorporado para dos estándares de encriptación, OpenPGP y S/MIME, por lo que el complemento Enigmail deja de utilizarse, sustituyendo el soporte por la versión nativa de OpenPGP que viene integrado en Thunderbird, y que es la que se explica en esta guía:

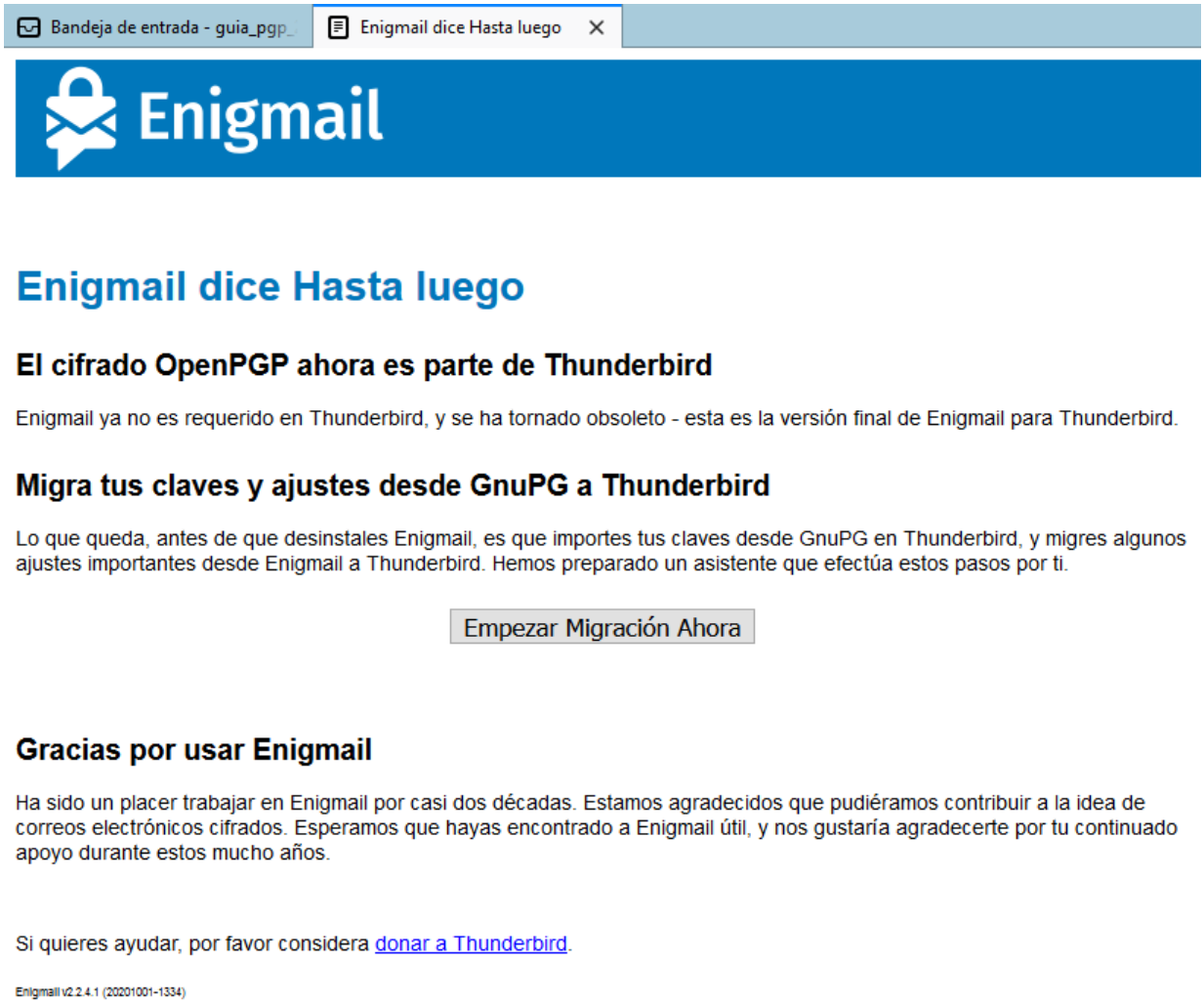

Figura 21 Mensaje de migración de Enigmail

Para configurar Thunderbird para usar OpenPGP, seleccione “Configuración de cuenta” desde el menú desplegable:

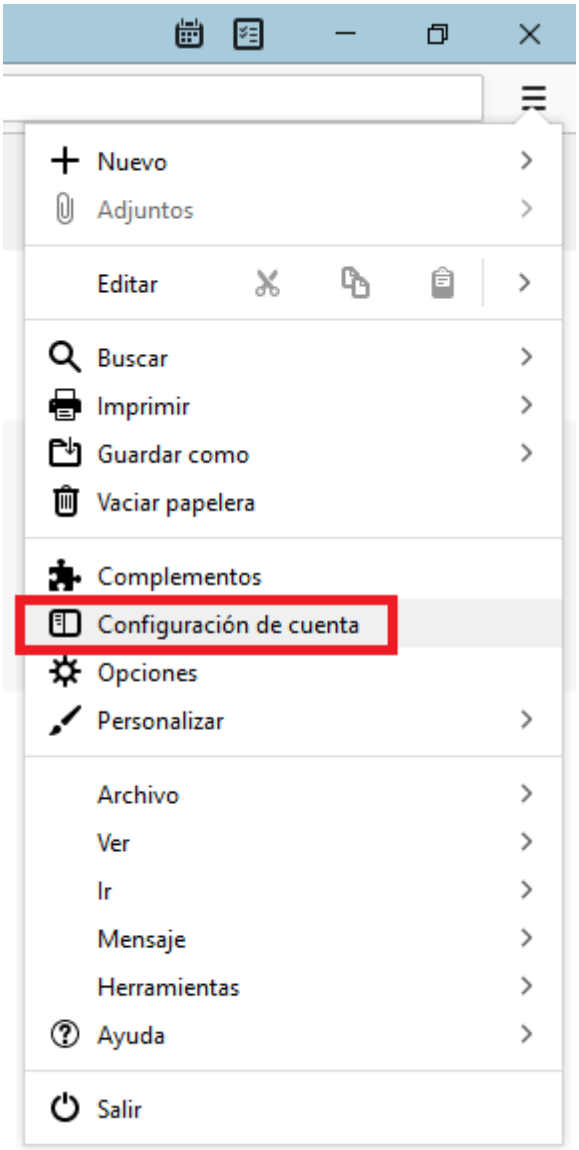

Figura 22 Configuración de cuenta de Thunderbird

4.1.1. Creación

Para comenzar a utilizar PGP como sistema de cifrado de los correos electrónicos, es necesario crear el par de claves que nos identifica. Para ello, en la opción «Cifrado extremo a extremo» de Thunderbird, se deberá seleccionar «Add Key…», con lo que se abrirá una nueva ventana:

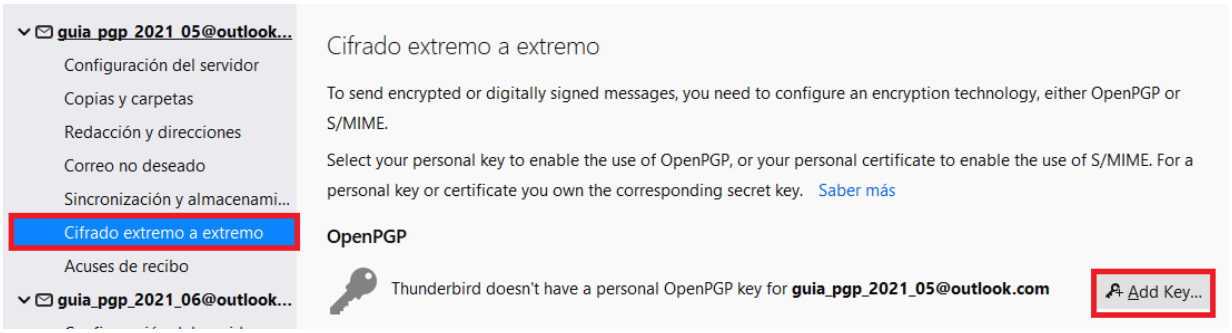

Figura 23 Cifrado extremo a extremo

A continuación, el asistente solicitará información referente a la creación de las claves, para lo que habrá 2 opciones:

1 Crear una nueva clave PGP con los valores de configuración deseados:

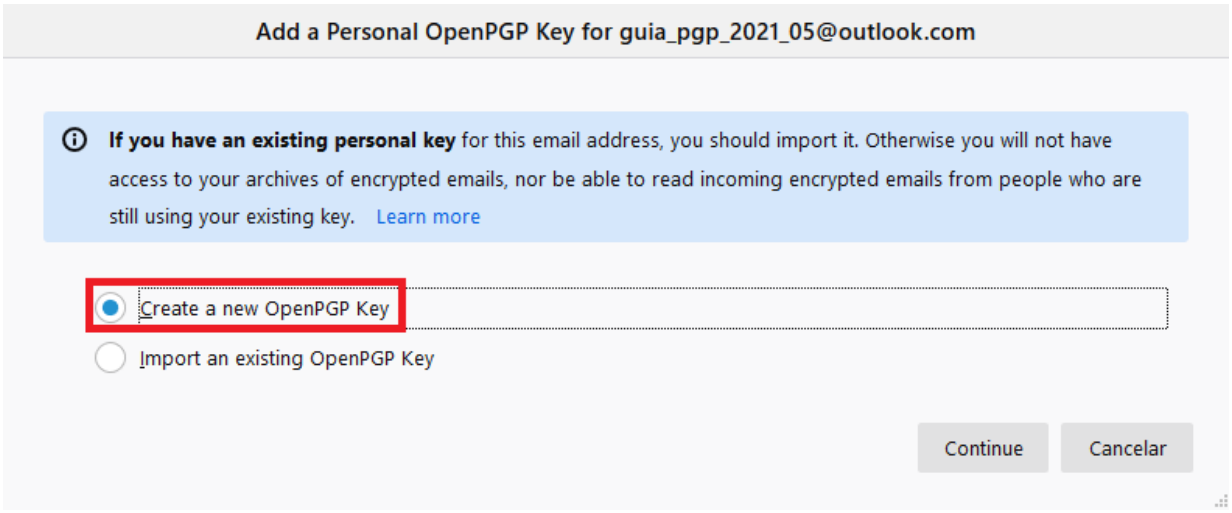

Figura 24 Crear nueva clave PGP

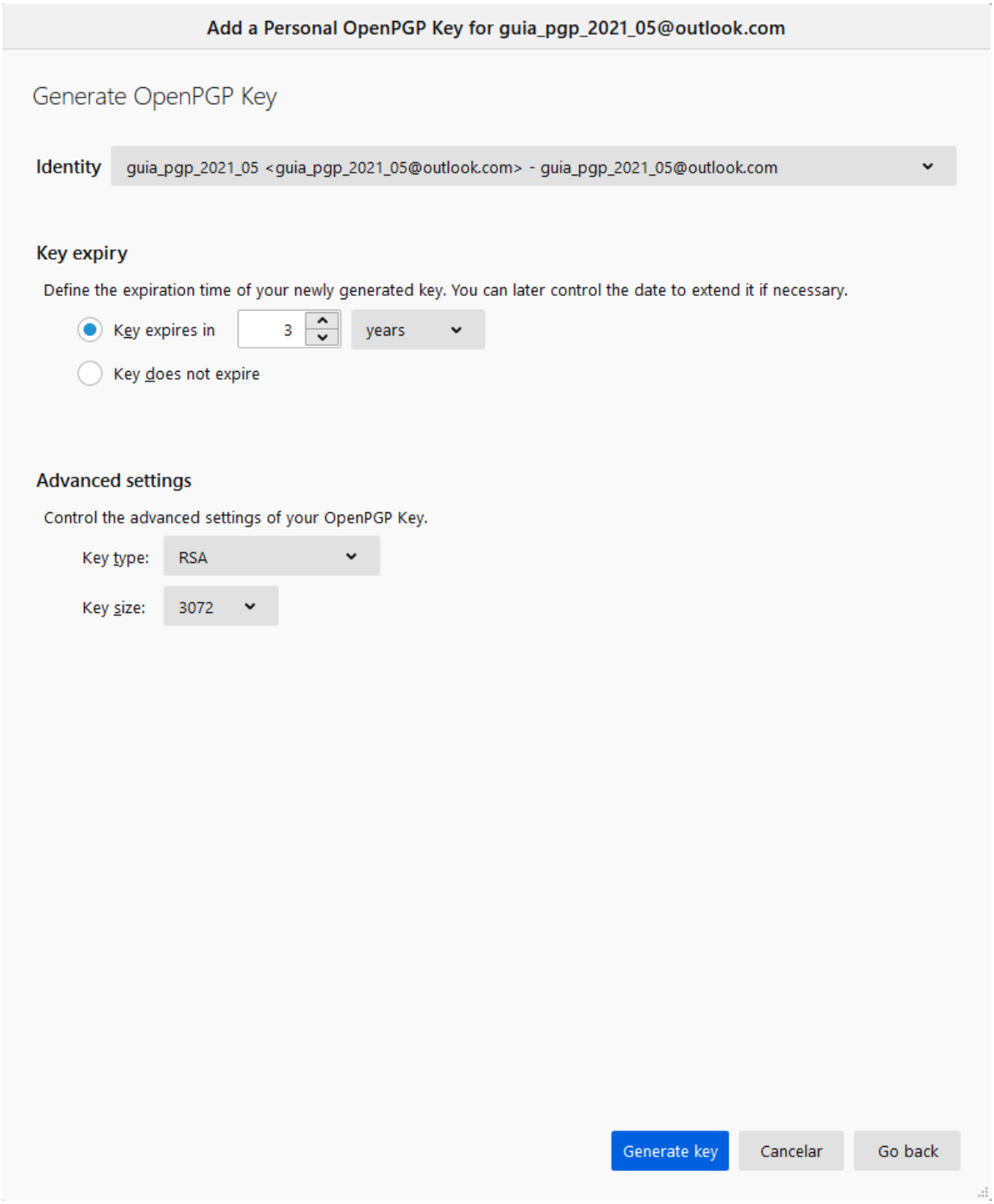

Figura 25 Configuración de nueva clave PGP

2 Si se dispone de un par de claves creadas previamente con Kleopatra, las detectará y preguntará si se desea utilizarlas. En caso contrario, ofrece la opción de crear un nuevo par de claves. Para continuar se pulsará sobre el botón «Siguiente».

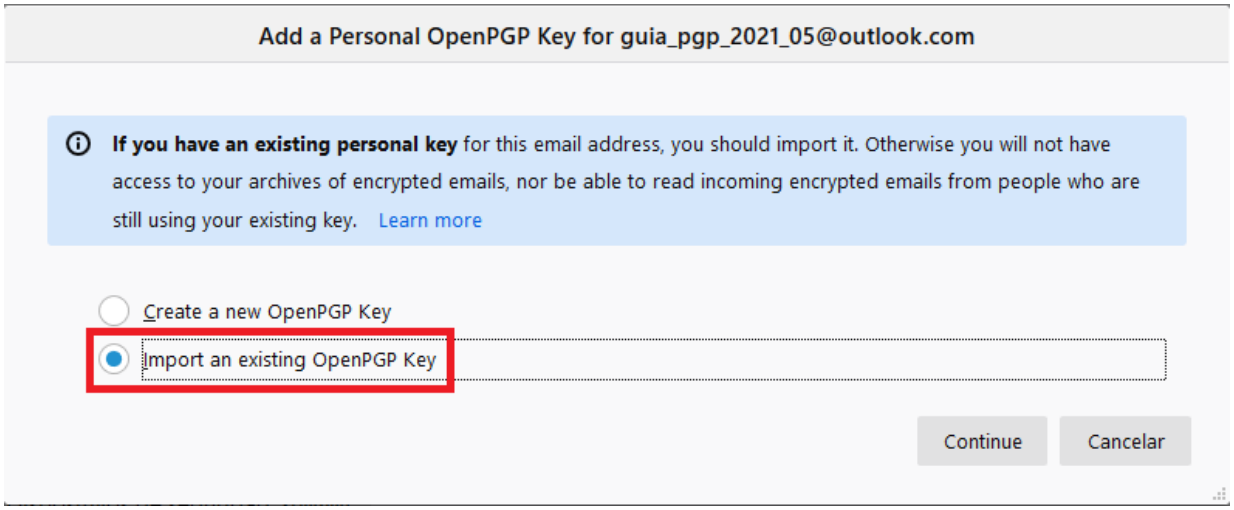

Figura 26 Importar clave PGP ya existente

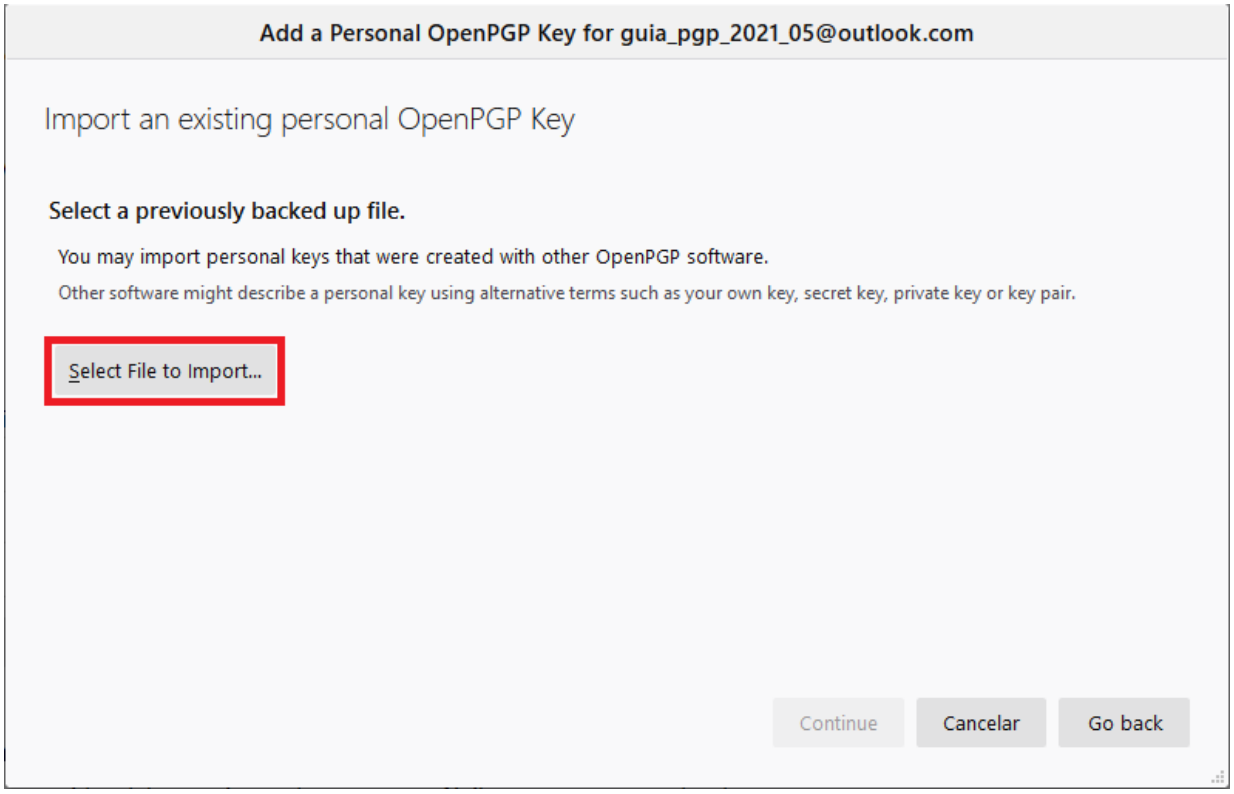

Figura 27 Seleccionar archivo a importar

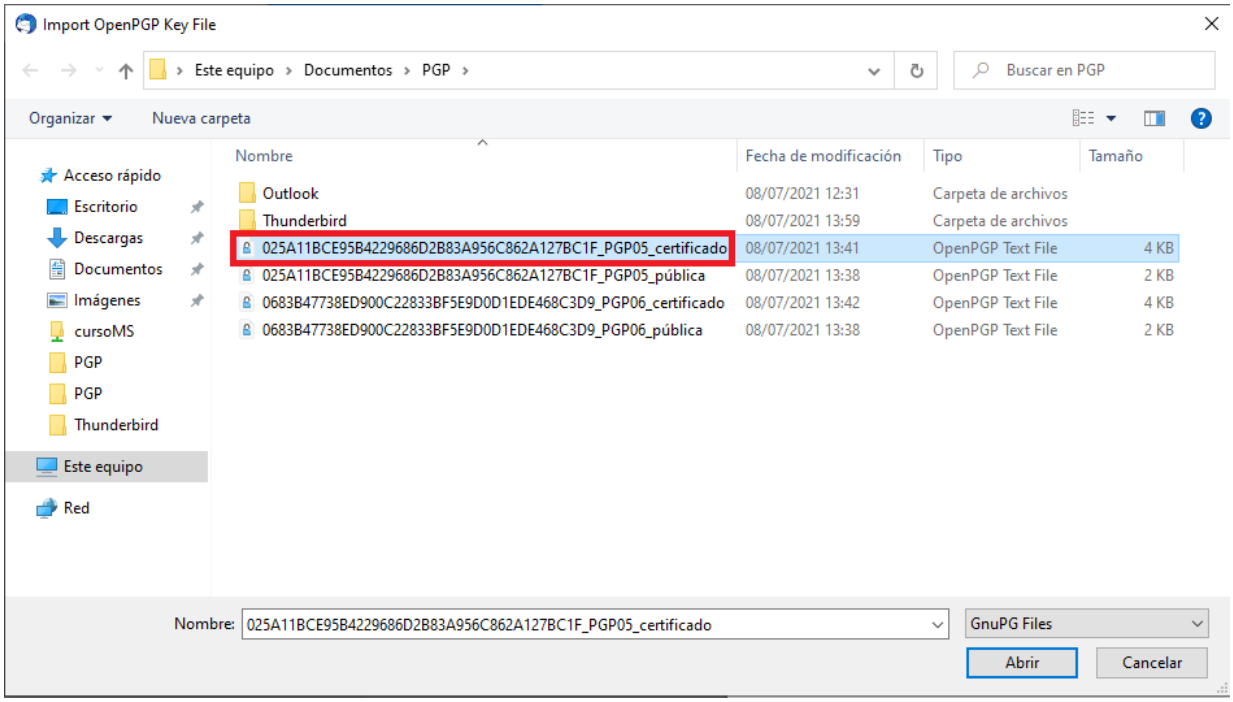

Figura 28 Clave PGP importada

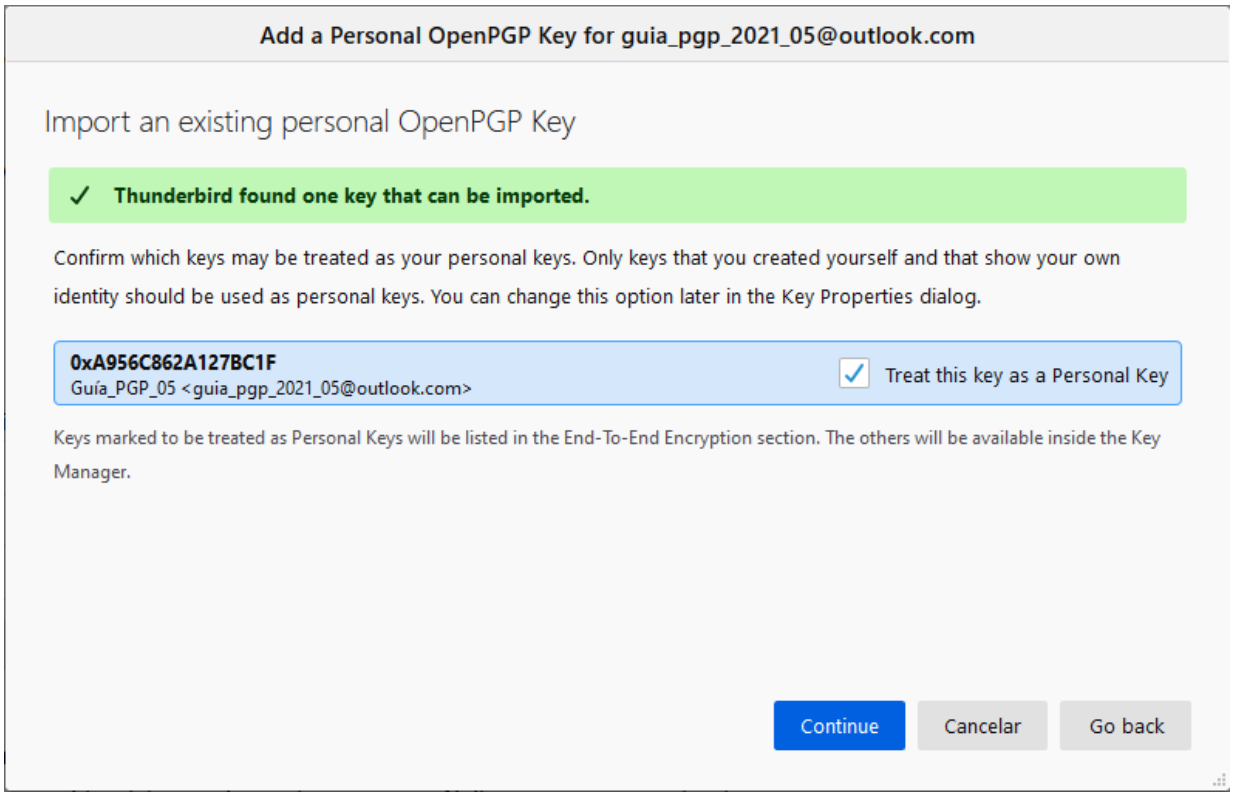

Figura 29 Clave importada con éxito

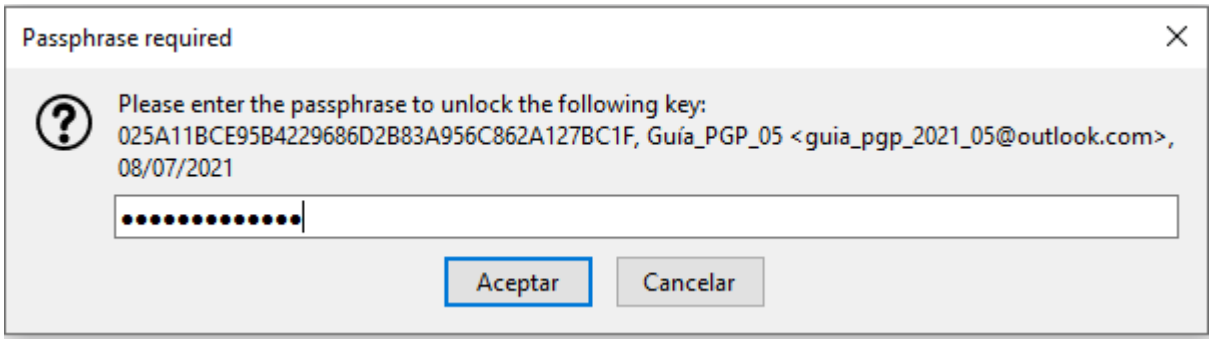

Figura 30 Contraseña para desbloquear la clave

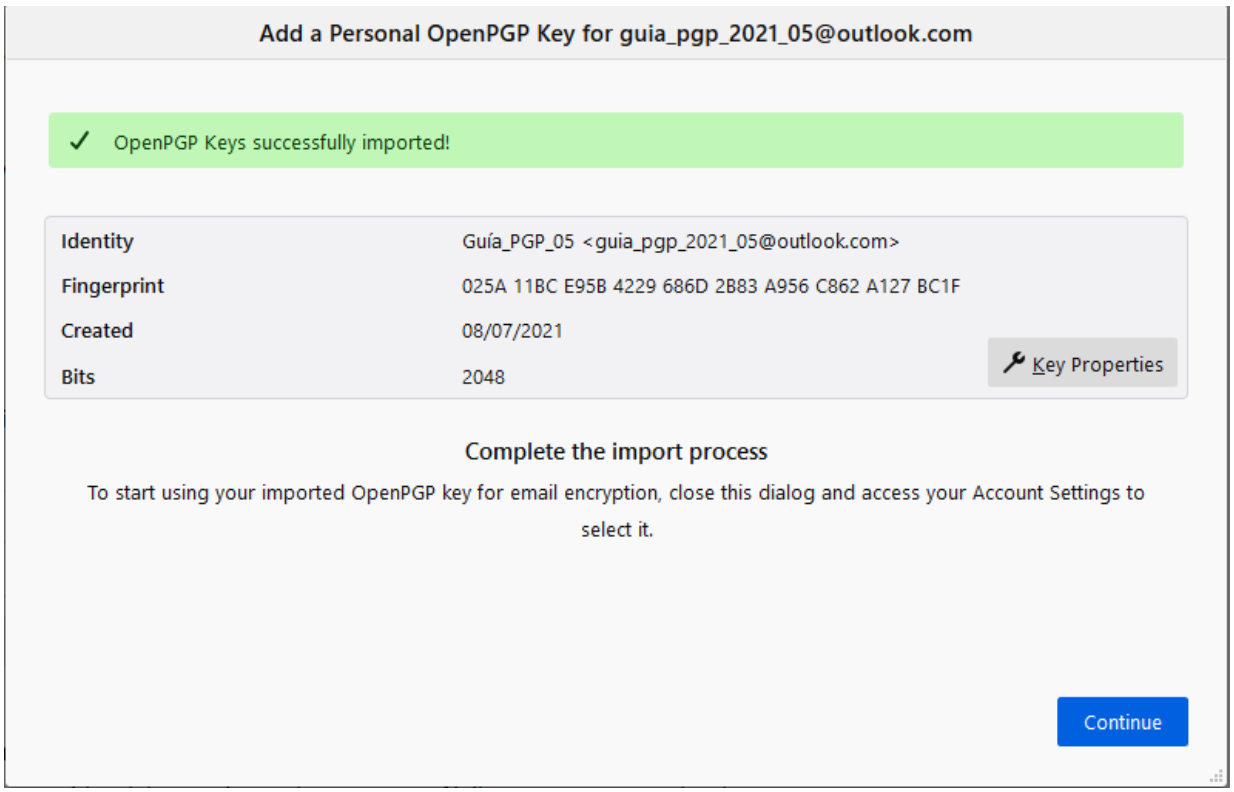

Figura 31 Proceso de importación completado

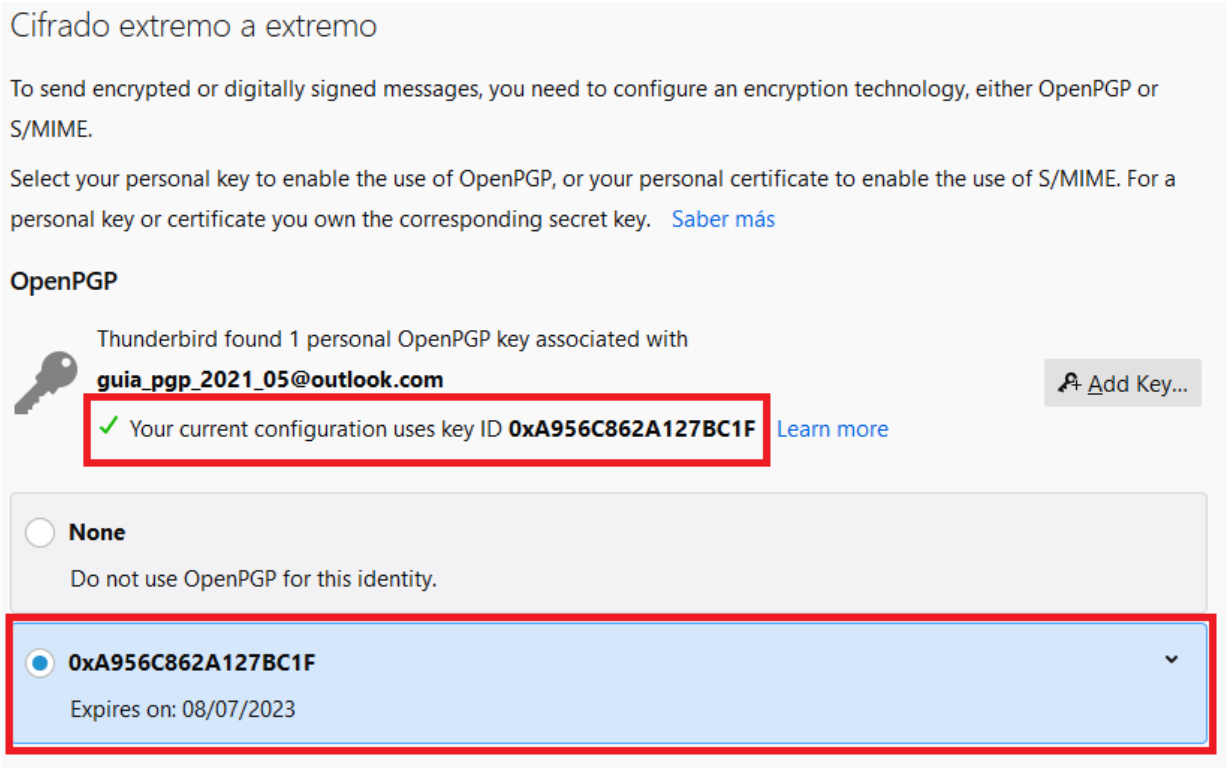

Figura 32 Clave personal OpenPGP asociada a email

3 Tras seguir los pasos de las siguientes ventanas del asistente de configuración, desde el desplegable “More” se puede generar un certificado de revocación. Este certificado es utilizado para que, en el caso de que nuestra clave privada haya sido comprometida, se pueda informar a todos nuestros contactos que nuestro certificado ya no es válido. En el caso de querer generarlo, se pulsaría sobre «Revoke key» y se confirmaría la acción:

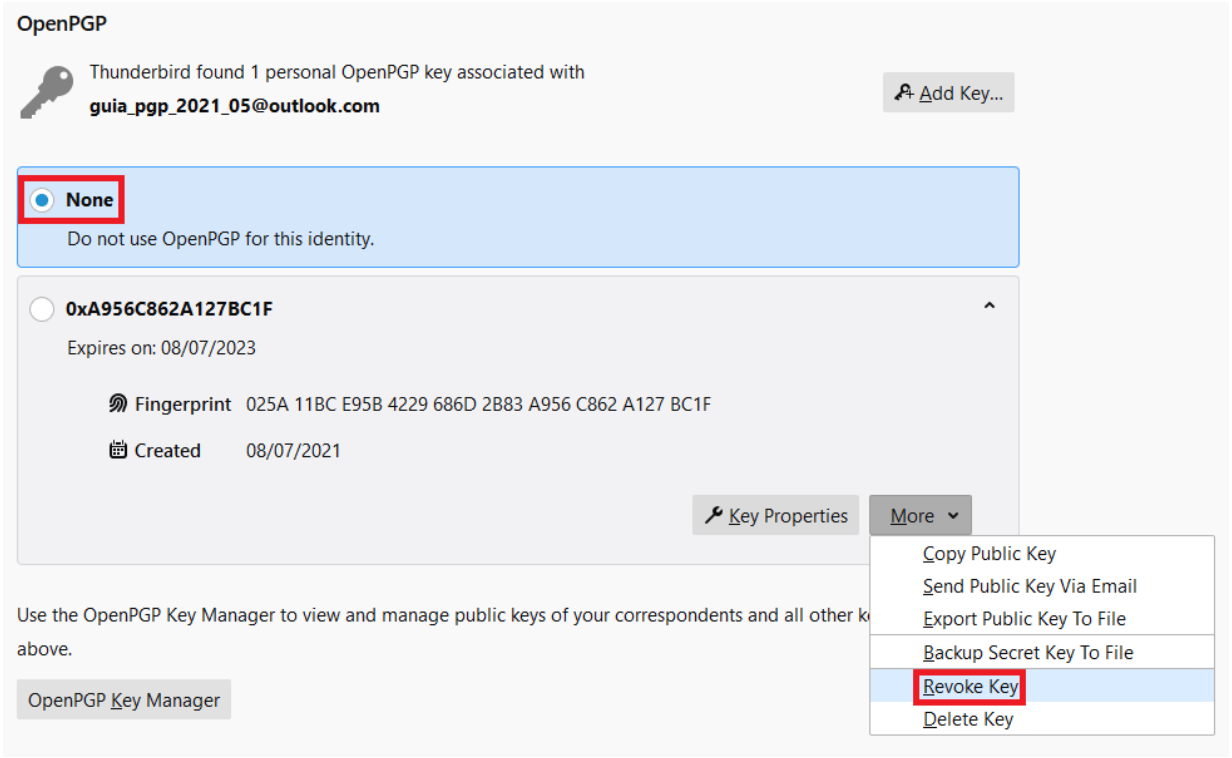

Figura 33 Generación de certificado de revocación

"Este certificado es utilizado para que, en el caso de que nuestra clave privada haya sido comprometida, se pueda informar a todos nuestros contactos que nuestro certificado ya no es válido"

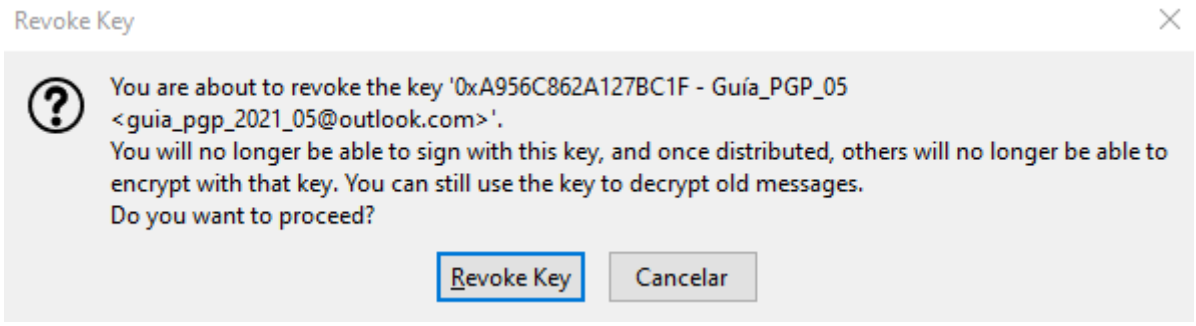

Figura 34 Mensaje de confirmación para la revocación

4.1.2. Cambio de la contraseña de un certificado

A raíz de la implementación de OpenPGP en Thunderbird 78, las claves no requieren una contraseña propia para ser usadas, Si se quiere evitar que un atacante que robe el disco pueda acceder a ellas, se necesita utilizar una clave maestra en el cliente de correo.

De cara al futuro, se está barajando la posibilidad de establecer una contraseña únicamente para descifrar las claves PGP y poder leer los correos cifrados, tal y como se describe en '*OpenPGP users in Thunderbird not aware of the recommendation to set up a Master Password*' y '*Thunderbird: Allow the optional use of user defined OpenPGP passphrases'.*

4.1.3. Compartición de la clave pública de un certificado a través del correo electrónico

Para compartir nuestra clave pública en un fichero adjunto en un correo electrónico, basta con seleccionar la pestaña «Seguridad» en la ventana de Thunderbird de redacción de mensajes, y seleccionar la opción «Adjuntar mi clave pública». También se puede utilizar la opción incluida en la barra de herramientas con el icono de clip «Adjuntar».

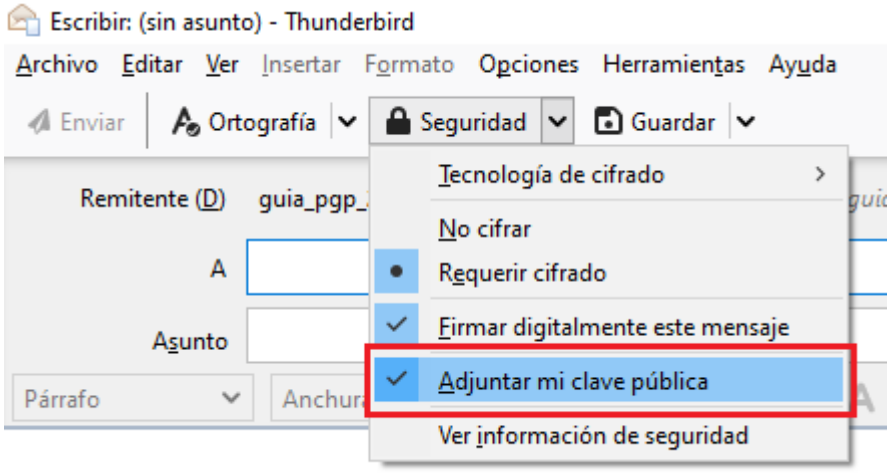

Figura 35 Compartir clave pública

A la hora de importar una clave que se ha recibido en un correo electrónico, basta con pulsar dos veces sobre el archivo adjunto con extensión *.asc* que ha sido recibido. La ventana solicitará nuestra clave para añadirla.

4.1.4. *Backup* del par de claves mediante la exportación a un fichero

En algunos casos, es necesario exportar las claves tanto públicas, como privadas, bien sea para realizar una copia de seguridad de las mismas o por la necesidad de usarlas en diferentes equipos informáticos.

Para exportar las claves se debe pulsar en la «Configuración de la cuenta» de Thunderbird, desplegar y acto seguido en «More». Ahí aparecerán, entre otras opciones, las de «Export Public Key To File» y « Backup Secret Key To File»:

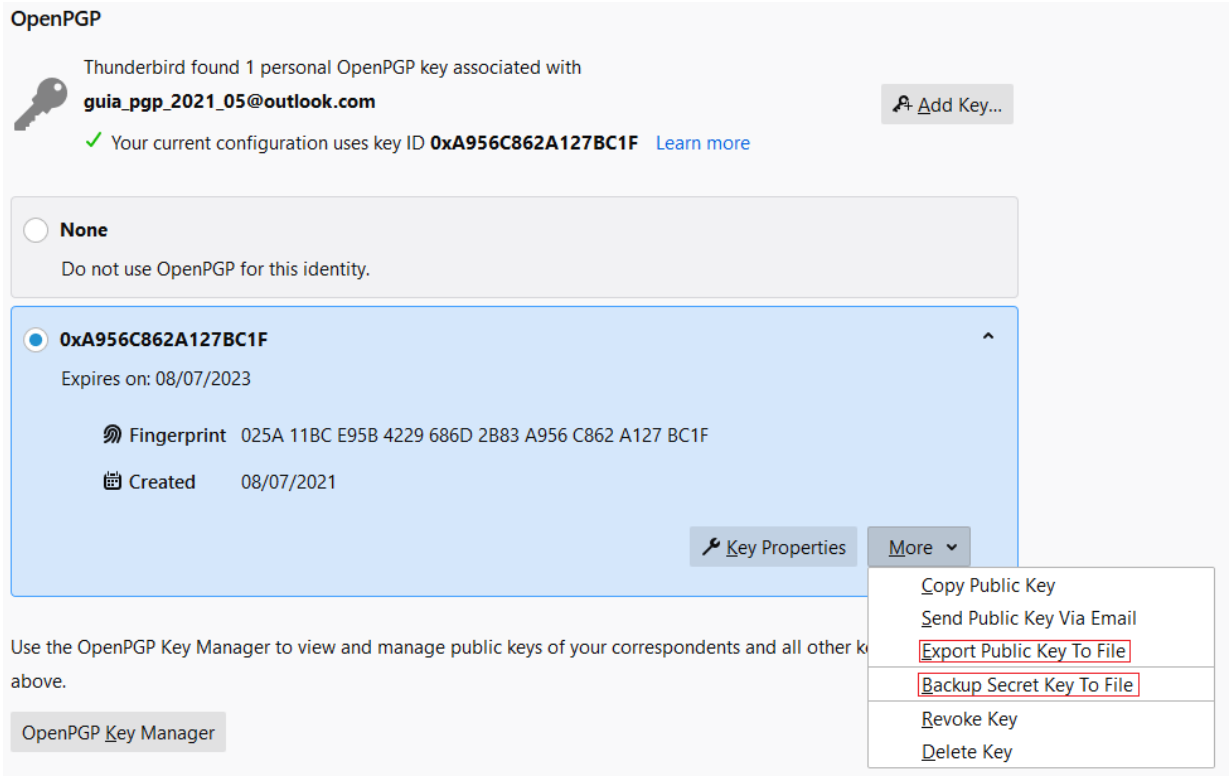

Figura 36 Backup del par de claves

Para la clave pública, el proceso será directo. Para la privada, se solicitará la contraseña de la clave a exportar:

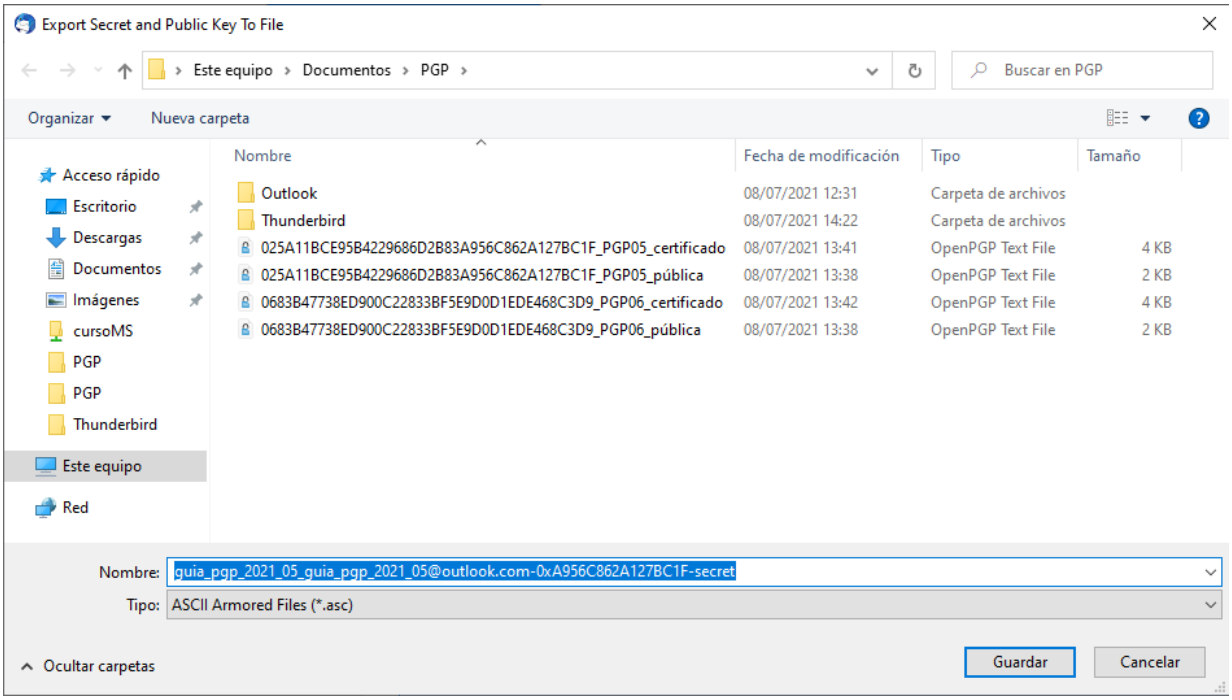

Figura 37 Backup clave privada

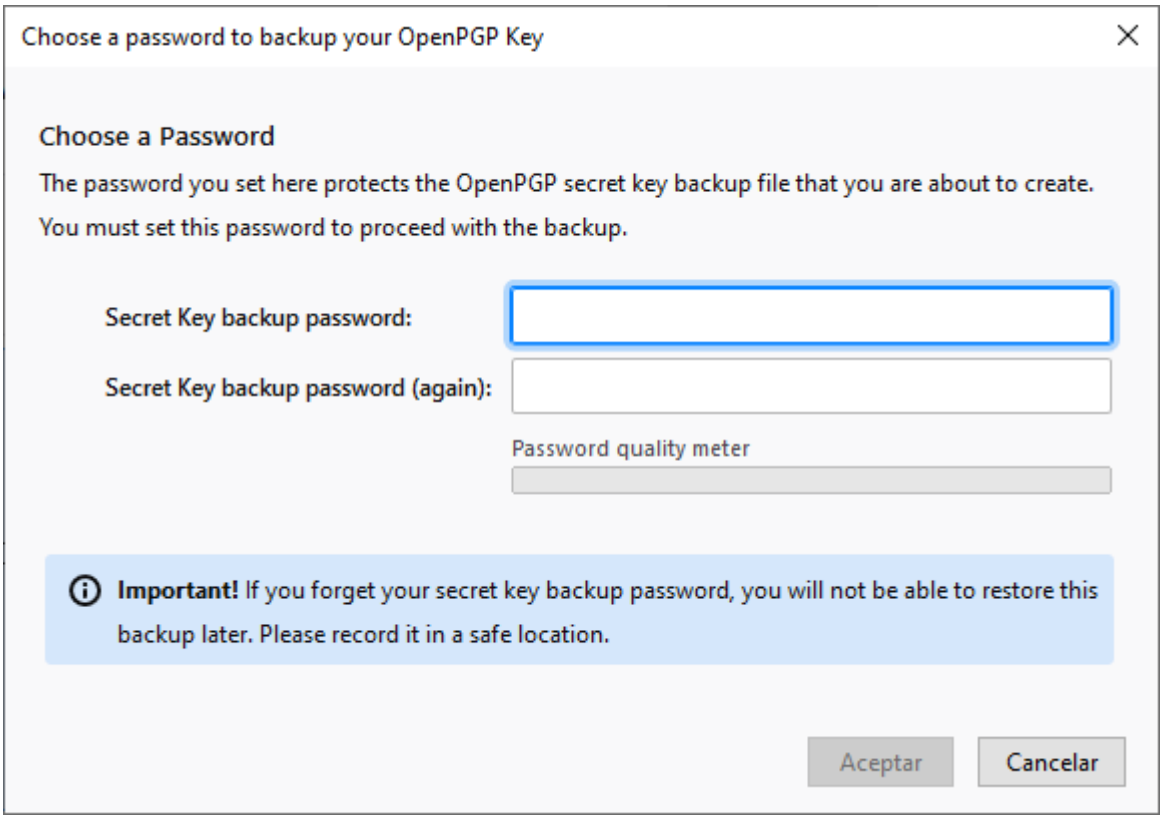

Figura 38 Contraseña de la clave privada

Finalmente, Thunderbird mostrará mensajes si todo ha sido correcto:

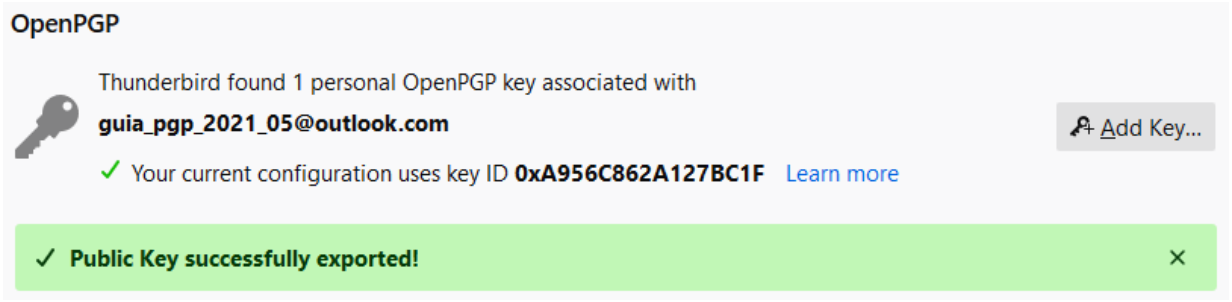

Figura 39 Exportación de clave pública correcta

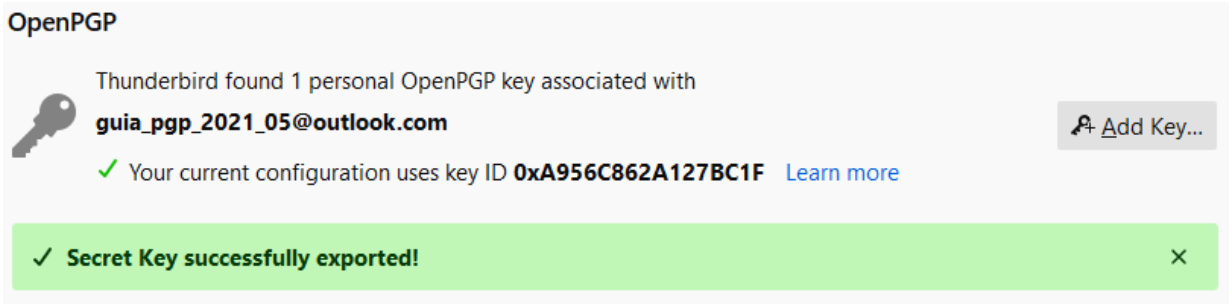

Figura 40 Exportación de clave privada correcta

4.2. Firma y verificación de correos electrónicos

4.2.1. Firma

La acción de firmar un correo electrónico permite al destinatario del mensaje verificar que el remitente sea realmente quien dice ser, teniendo importada la clave pública legítima del emisor.

Para llevar a cabo la firma de un correo electrónico en Thunderbird, en la pestaña «Seguridad» de la ventana del editor del mensaje deberá seleccionarse la opción de «Firmar digitalmente este mensaje» antes de enviar el correo de manera habitual.

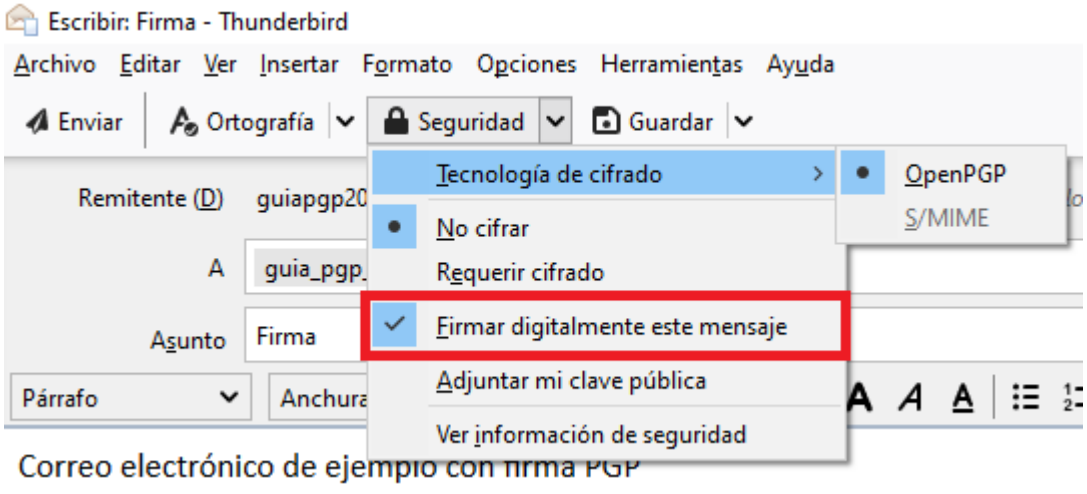

Figura 41 Firma digital del mensaje

“La acción de firmar un correo electrónico permite al destinatario del mensaje verificar que el remitente sea realmente quien dice ser”

4.2.2. Verificación

Para verificar la autenticidad de un correo electrónico firmado con Thunderbird no es necesario realizar ninguna acción. El propio cliente de correo electrónico mostrará un mensaje informando de que la firma es legítima.

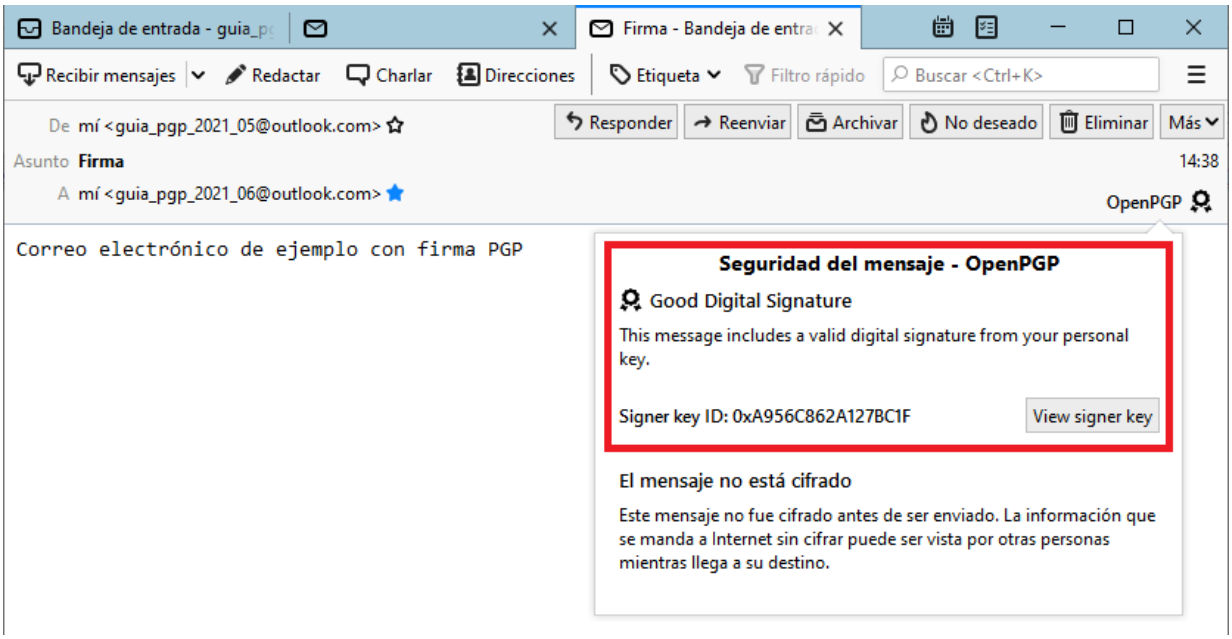

Figura 42 Mensaje de firma digital válida

4.3. Cifrado y descifrado de correos electrónicos

4.3.1. Cifrado

Para cifrar un correo electrónico se ha de seleccionar en la pestaña «Seguridad» la opción «Requerir cifrado». En el caso de que la clave pública del destinatario esté asociada a su correo electrónico, el mensaje se cifrará automáticamente. De no ser así, Thunderbird pedirá que se seleccione una clave de una lista.

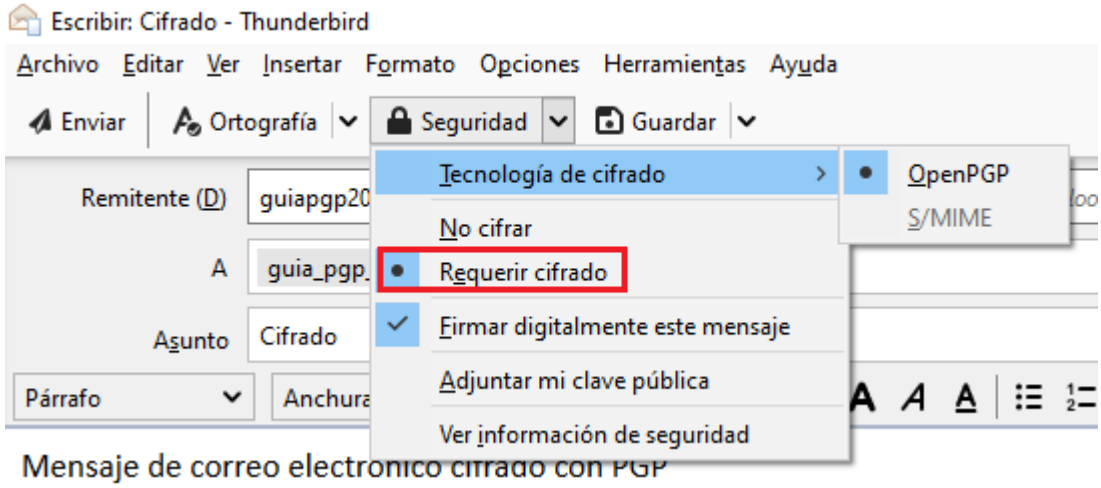

Figura 43 Cifrado de un correo electrónico con Thunderbird

En caso de no incluir texto en el asunto, Thunderbird nos los recordará:

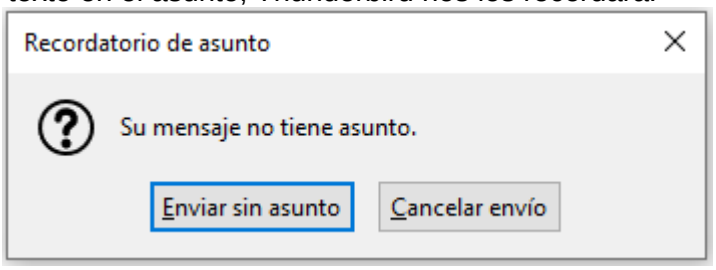

Figura 44 Recordatorio de asunto

Cuando se reciba el correo en la bandeja de entrada, el texto del asunto no será legible desde la vista previa, hasta que abramos el mensaje:

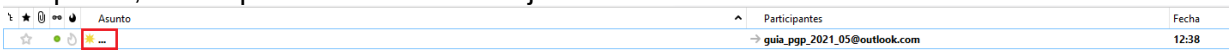

Figura 45 Asunto oculto en el correo electrónico

4.3.2. Descifrado

Thunderbird reconoce cuándo un correo electrónico está cifrado, por lo que en el momento en que se quiera acceder a su contenido, el cliente de correo solicitará, para poder descifrarlo, la contraseña asociada a la clave PGP utilizada.

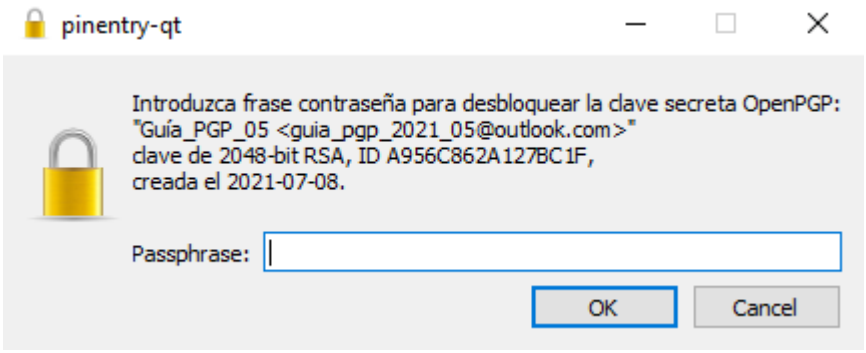

Figura 46 Ventana de solicitud de la contraseña del llavero de claves

Si el correo electrónico recibido está cifrado y firmado, se mostrará el siguiente mensaje:

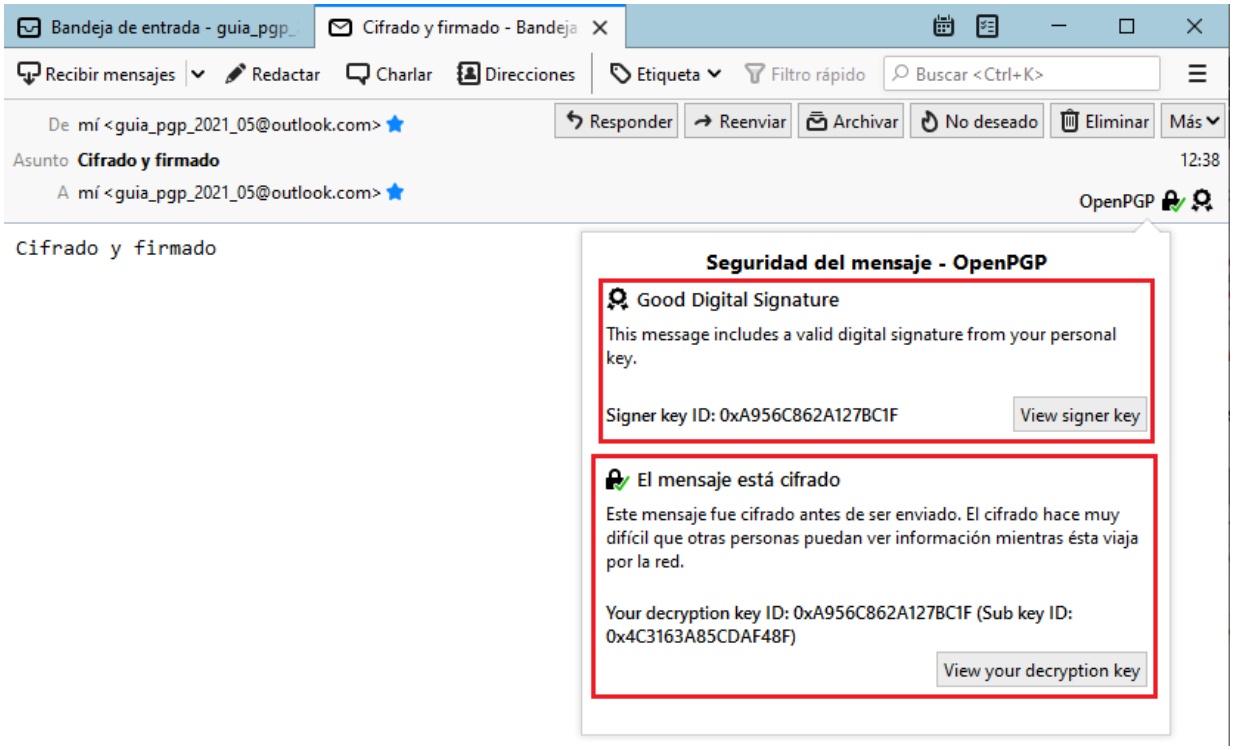

Figura 47 Correo electrónico cifrado y firmado

Por el contrario, si solo está cifrado, se mostrará otro mensaje:

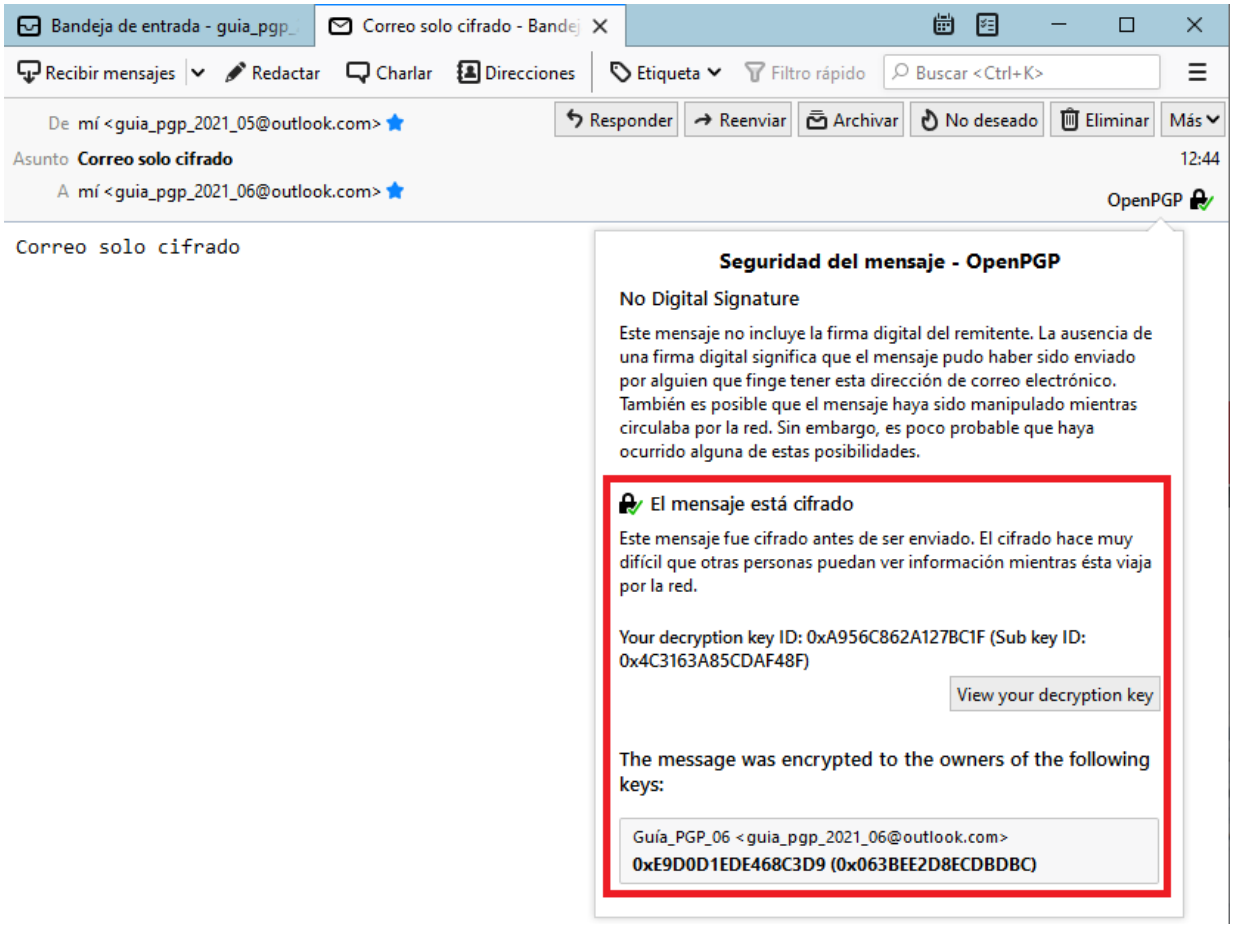

Figura 48 Correo electrónico descifrado

4.4. Cifrado y descifrado de un fichero para adjuntar a un correo electrónico

4.4.1. Cifrado

A la hora cifrar archivos adjuntos en un correo electrónico con Thunderbird, desde la versión 78 en adelante, hay que considerar las dos opciones que nos ofrece la aplicación:

- **OpenPGP**: es la opción por defecto desde la versión 78.2.1. Depende de la red de confianza descentralizada, en la que las claves son verificadas y firmadas por las de otros usuarios. Una clave firmada por una clave de confianza también puede ser de confianza y esas relaciones de confianza pueden extenderse de forma transitiva si se desea. OpenPGP se basa en niveles de confianza determinados individualmente, es decir, si alguien te envía una clave y confías en ella, puedes comunicarte con esa persona, no hay ninguna tercera parte implicada a mayores.
- **S/MIME**: adopta un enfoque de certificado para las claves, como con las claves TLS para HTTPS; las claves son firmadas por autoridades de certificación, que pueden ser internas o de terceros. S/MIME requiere certificados, y esto requiere la existencia de un servicio de certificados de terceros.

En esta guía se utilizará el primer método descrito, por lo que para cifrar el correo solo se necesitará adjuntar el archivo que se quiera enviar. Hay que recordar que el texto que se escriba en el cuerpo del mensaje se cifrará junto con el archivo adjunto.

Una vez adjuntado el archivo y escrito el cuerpo, en la pestaña «Seguridad» del editor del mensaje, se seleccionará la opción «Tecnología de cifrado».

NOTA: Los correos electrónicos que contengan un archivo adjunto también pueden ser firmados de la misma manera que los que no contienen ningún adjunto, por lo que si se desea firmarlo, se seleccionará la opción «Firmar mensaje».

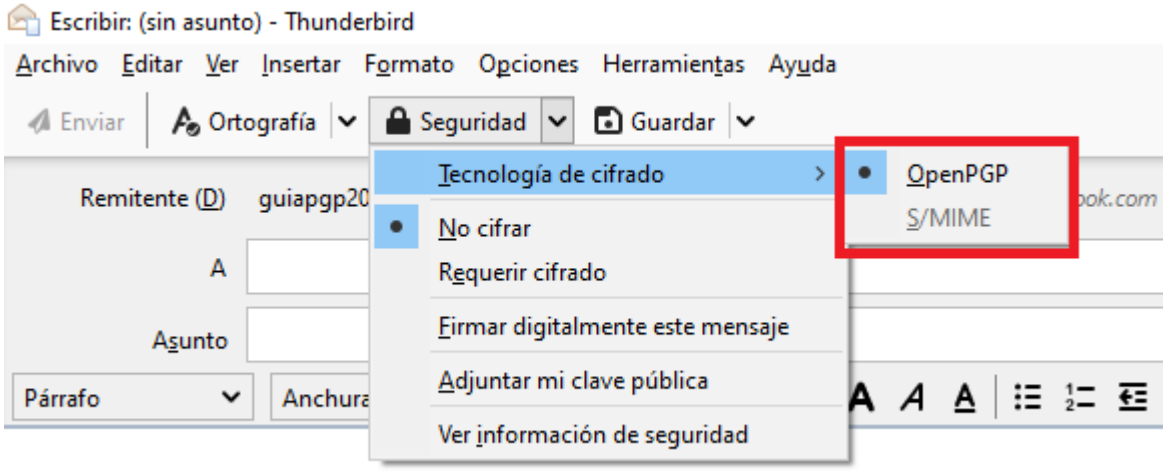

Figura 49 Menú de selección del protocolo de cifrado en Thunderbird

4.4.2. Descifrado

De la misma manera que los correos sin archivos adjuntos, Thunderbird reconoce cuándo un correo electrónico está cifrado, por lo que en el momento en que se quiera acceder a su contenido, el cliente de correo solicitará la contraseña asociada con la clave privada. Al introducirla se descifra tanto el cuerpo del correo, como el o los adjuntos que contenga.

"En el momento en que se quiera acceder a su contenido, el cliente de correo solicitará la contraseña asociada con la clave privada"

5. Referencias

[1] Gpg4win - https://www.gpg4win.org/

[2] Documentación disponible del Servidor de Claves Públicas PGP RedIRIS - https://www.rediris.es/cert/doc/pgp/keyserver.html.es

[3] The certificate server - https://www.gpg4win.org/doc/en/gpg4win-compendium_22.html