



Instructivo

Instalación y configuración de llaves GPG

Elaboró:	Especialista Ciberinteligencia		
Revisó:	Control documental		
Aprobó:	Gerente de Ciberinteligencia		
Responsable del documento:	Gerente Ciberinteligencia	Tiempo de retención:	1 año posterior a su vigencia
		Disposición final:	Eliminación del repositorio documental

Versión	Fecha	Descripción del cambio
1	27/09/21	Emisión inicial



Instructivo Instalación y configuración de llaves GPG

IT-CIB-001-V1
27 septiembre
2021

CONTENIDO

1. Objetivo.....	3
2. Alcance	3
3. Instructivo	4
Instalación.....	4
Integración de GPG en Outlook	28



Instructivo **Instalación y configuración de llaves GPG**

IT-CIB-001-V1
27 septiembre
2021

1. Objetivo

El presente documento tiene como objetivo dar a conocer los pasos a llevar a cabo la instalación y configuración de la herramienta GPG para cifrado de información.

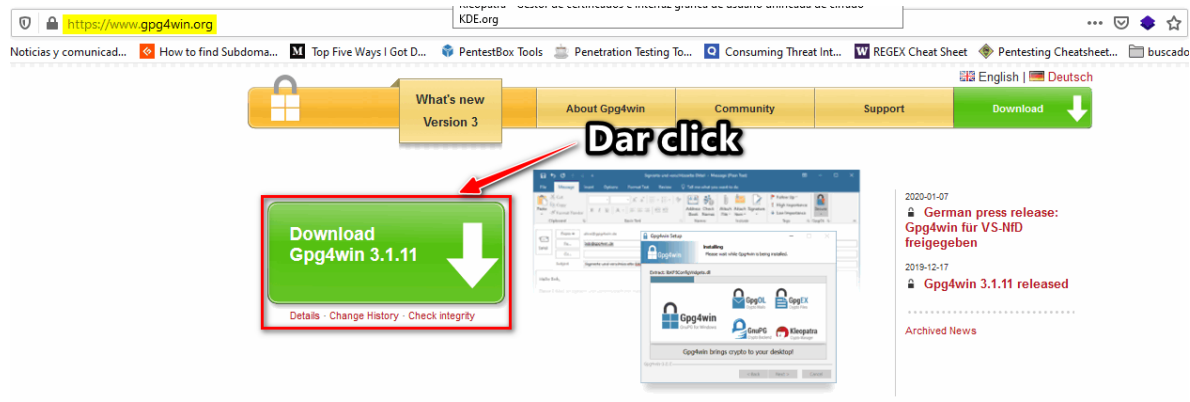
2. Alcance

El presente documento se limita a las actividades requeridas para instalar y configurar por primera vez ...

3. Instructivo

INSTALACIÓN

Ir a la dirección [gpg4win.org](https://www.gpg4win.org) y descargar la versión más reciente a continuación, dar click en el botón Download.



Download Gpg4win 3.1.11

Details · Change History · Check integrity

Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Discover Gpg4win

Learn what Gpg4win is and read more about the features of our solution!

[About Gpg4win »](#)

Getting started

We help you to use Gpg4win. Learn the basics about Gpg4win and get in the world of cryptography. The best point to start is with the illustrative Gpg4win Compendium.

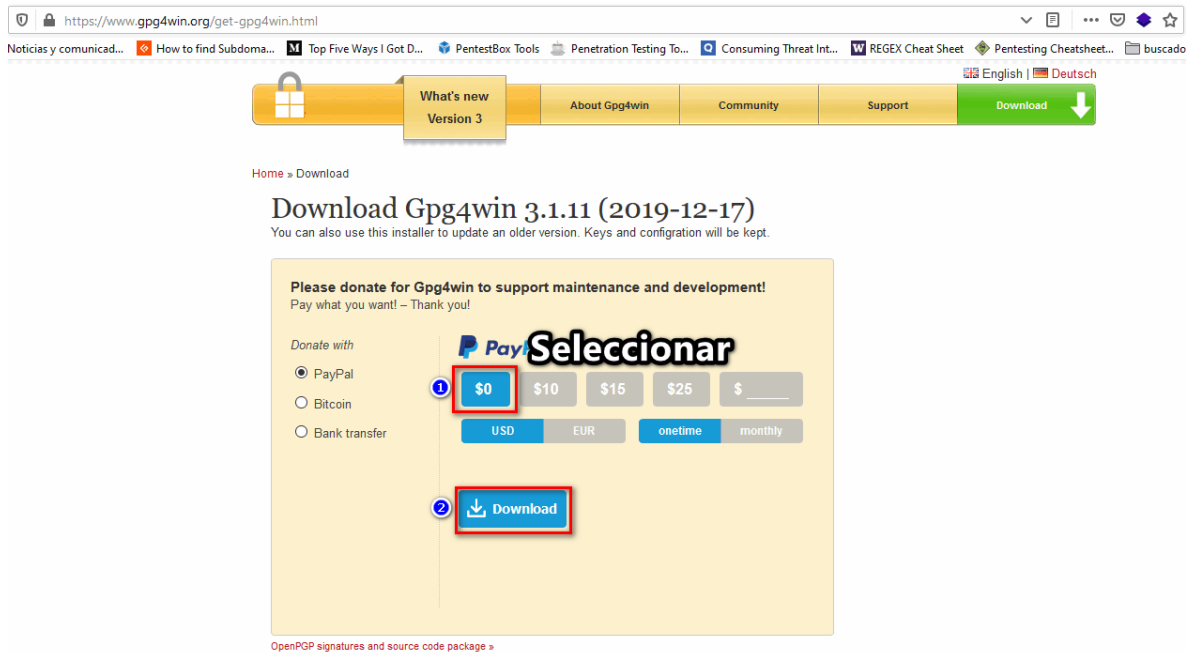
[Go to the Gpg4win Compendium »](#)

Join the community

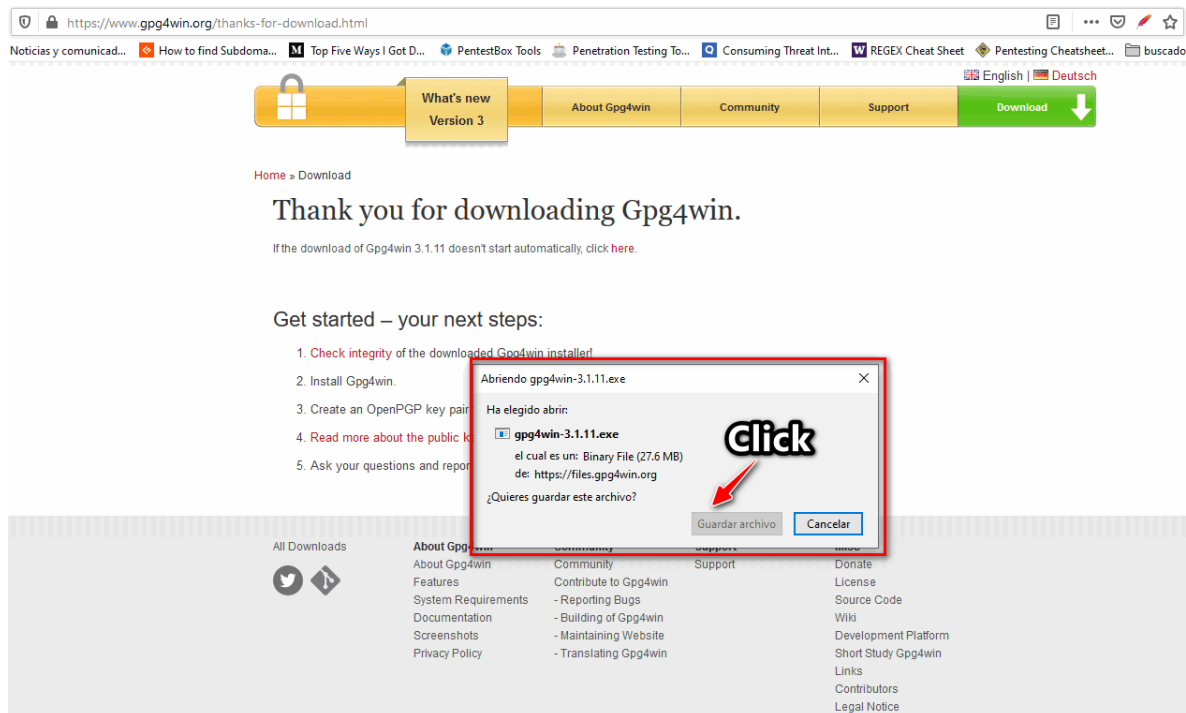
Gpg4win is Free Software. Join the community! We recommend subscribing to the [Gpg4win announcement mailing list](#) to be automatically informed about new releases and other important Gpg4win news.

[Go to the community »](#)

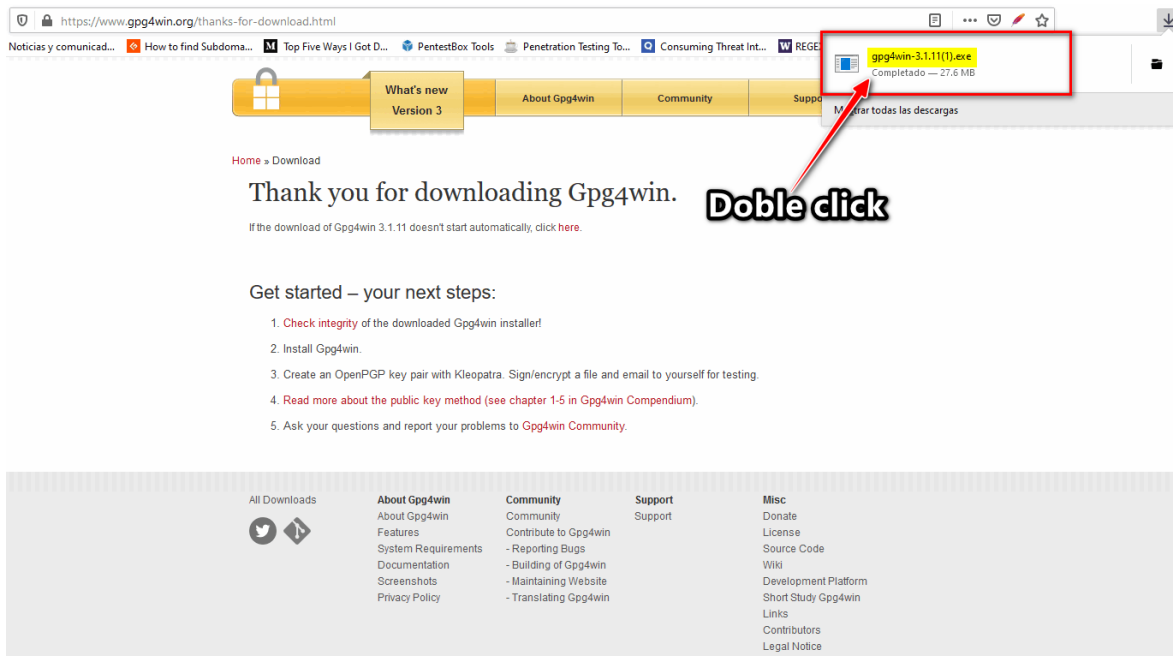
Si se desea realizar una aportación al proyecto se puede realizar a través de Paypal, si no se desea donar se debe seleccionar “\$0” y dar click en download



A continuación, aparecerá una ventana en la cual se le tiene que dar click en el botón “Guardar archivo”



Una vez completada la descarga se debe dar en el archivo “gpg4win-3.XX.exe” doble

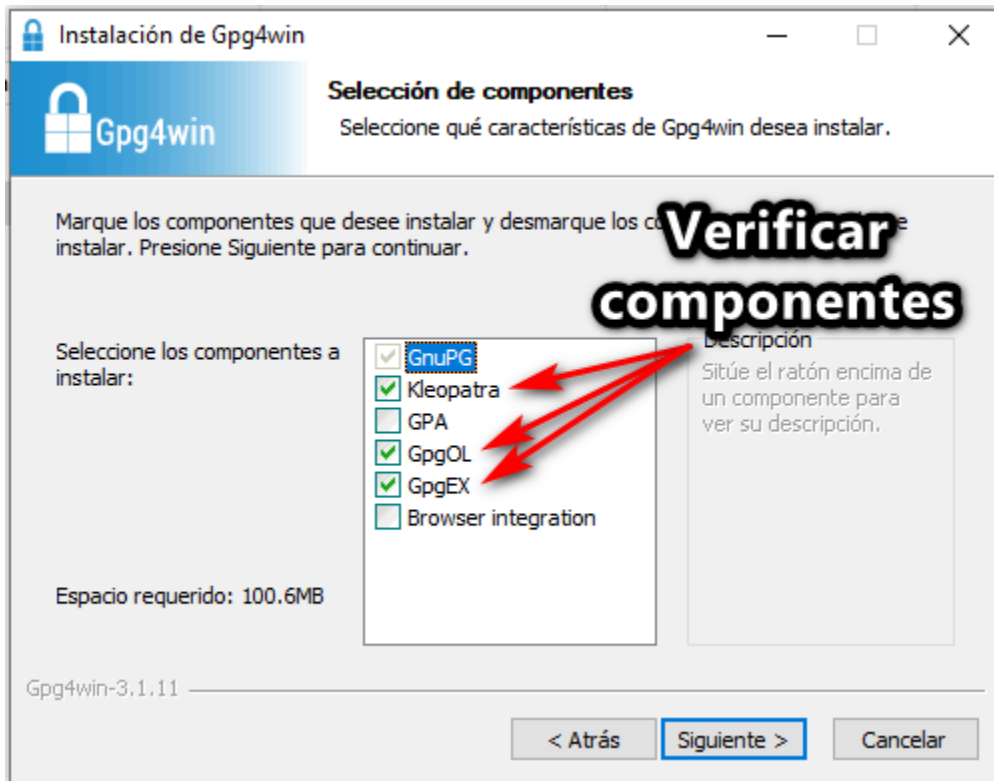


Una vez ejecutado el programa se inicializará la secuencia de instalación.

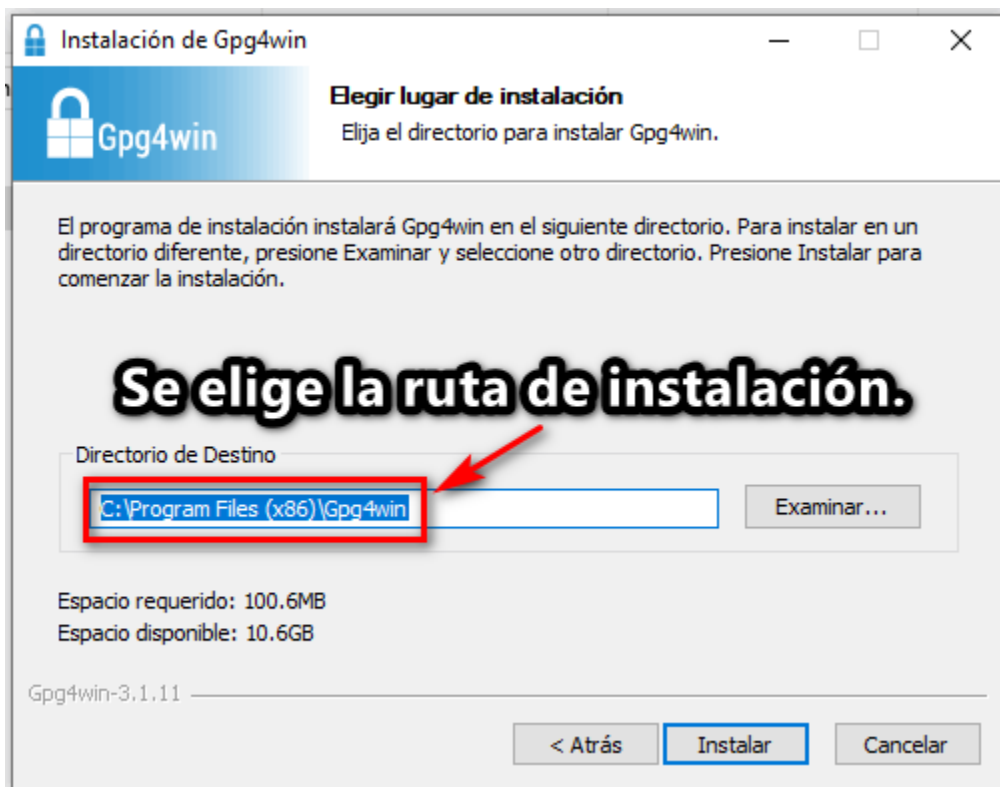
Programa de instalación.



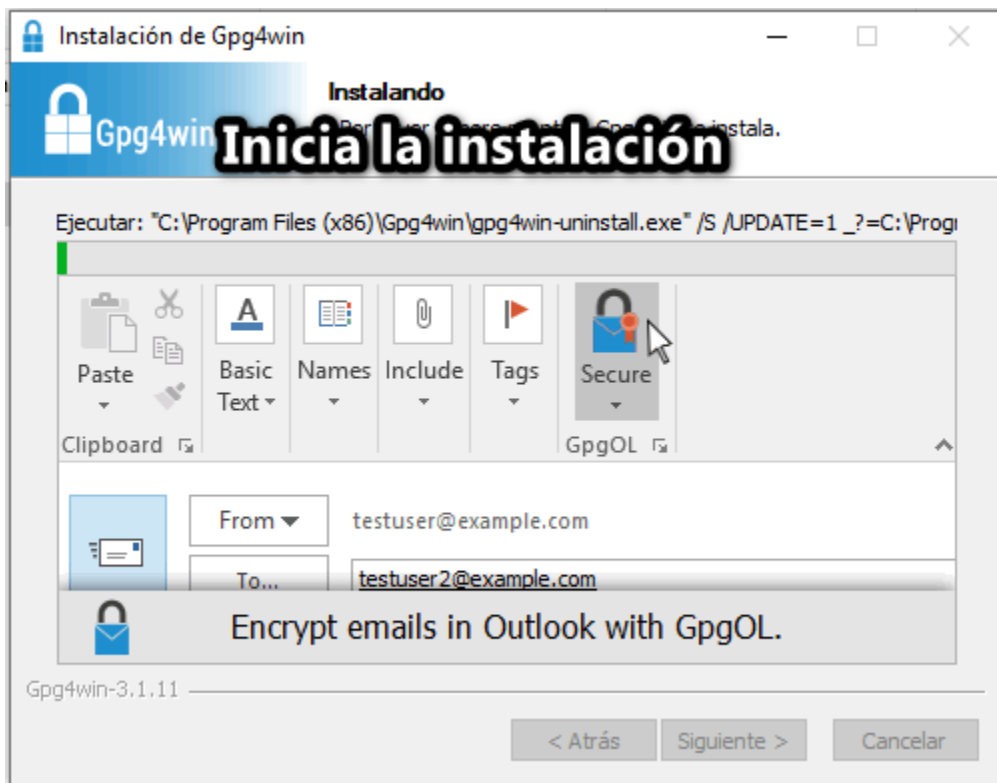
Verificar que los componentes Kleopatra, GpgOL y GpgEX estén marcados



Se elige la ruta de instalación.



Inicia la instalación.

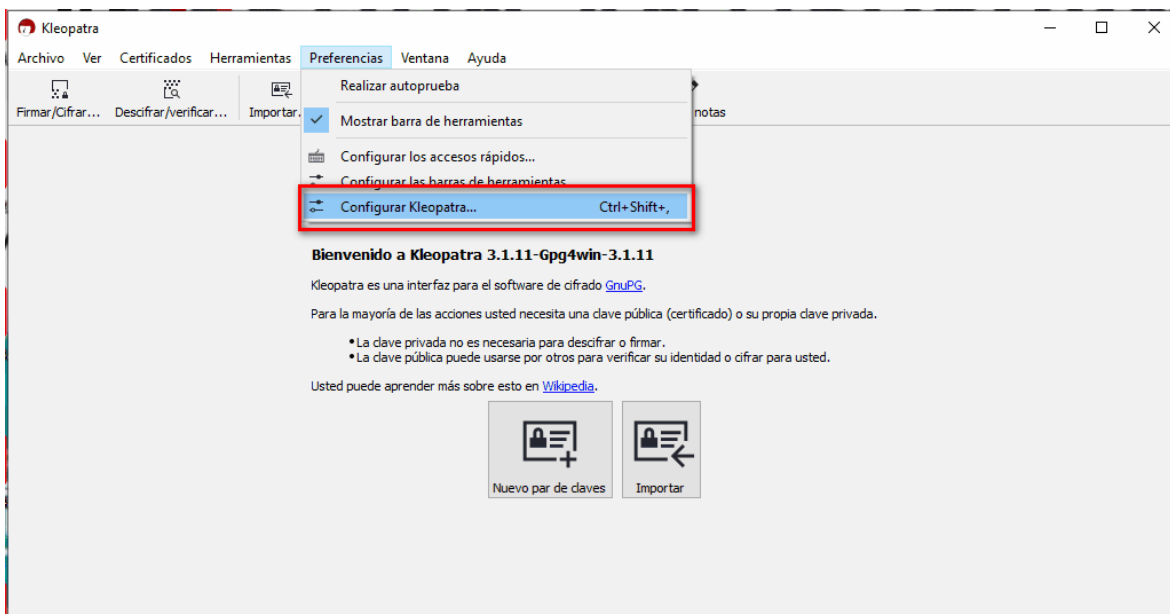


Una vez finalizada la instalación el programa podrá solicitar el reinicio del equipo

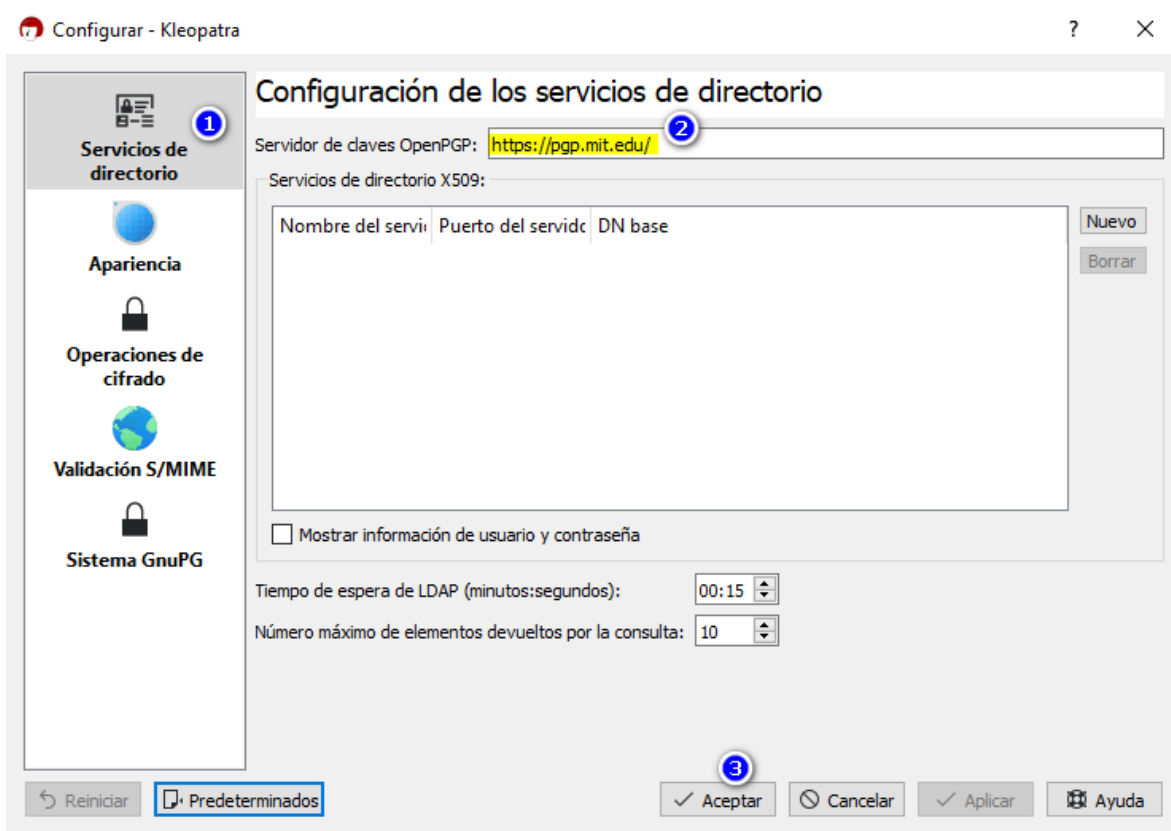


Después del reinicio del dispositivo, se tiene que acceder al programa “Kleopatra”.

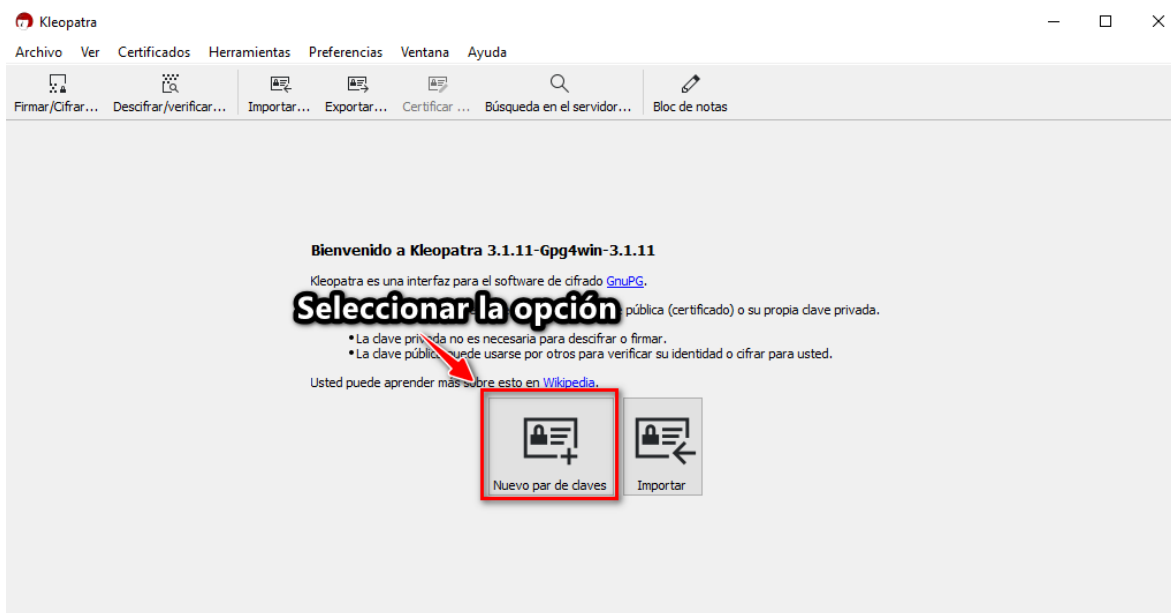
Una vez inicializado el programa se debe de ir a la ruta Preferencias > Configurar Kleopatra



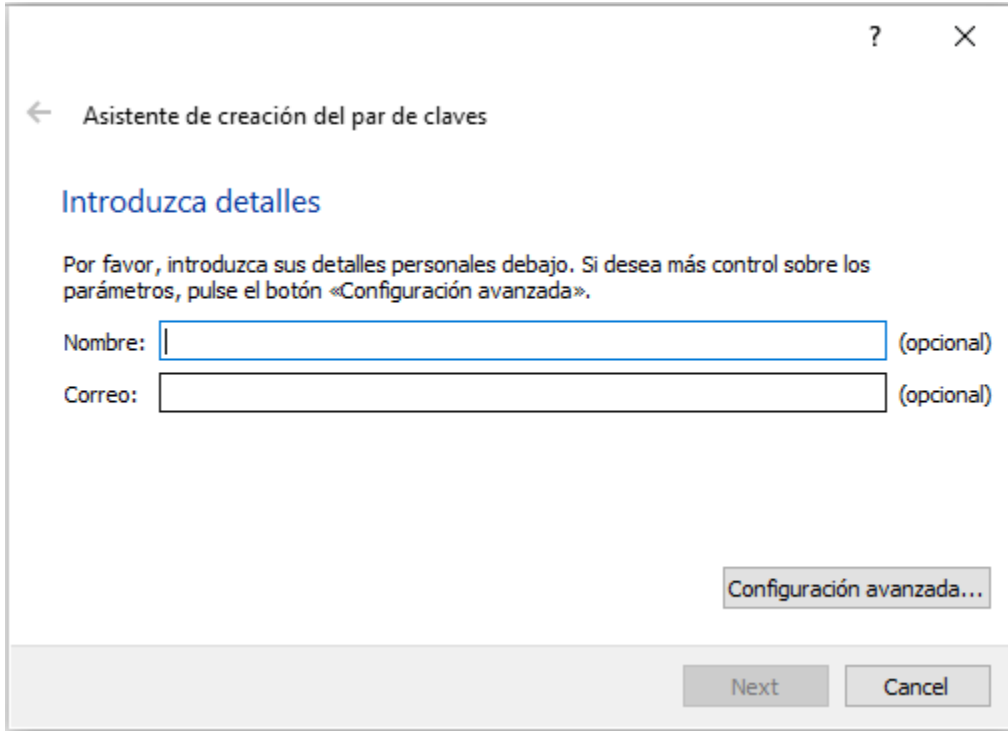
Dentro del menú de configuración se debe ir a la pestaña “Servicios de directorio”, y después agregar el siguiente servidor <https://pgp.mit.edu/>, a continuación se debe de dar click en aceptar.



Después de realizar la configuración se mostrará la pantalla de inicio. En esta pantalla se tiene que seleccionar la opción “Nuevo par de claves”.



Una vez seleccionada la opción se mostrará un cuadro como el siguiente, en el cual se solicitará el nombre de la llave, así como el correo electrónico.



← Asistente de creación del par de claves

Introduzca detalles

Por favor, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, pulse el botón «Configuración avanzada».

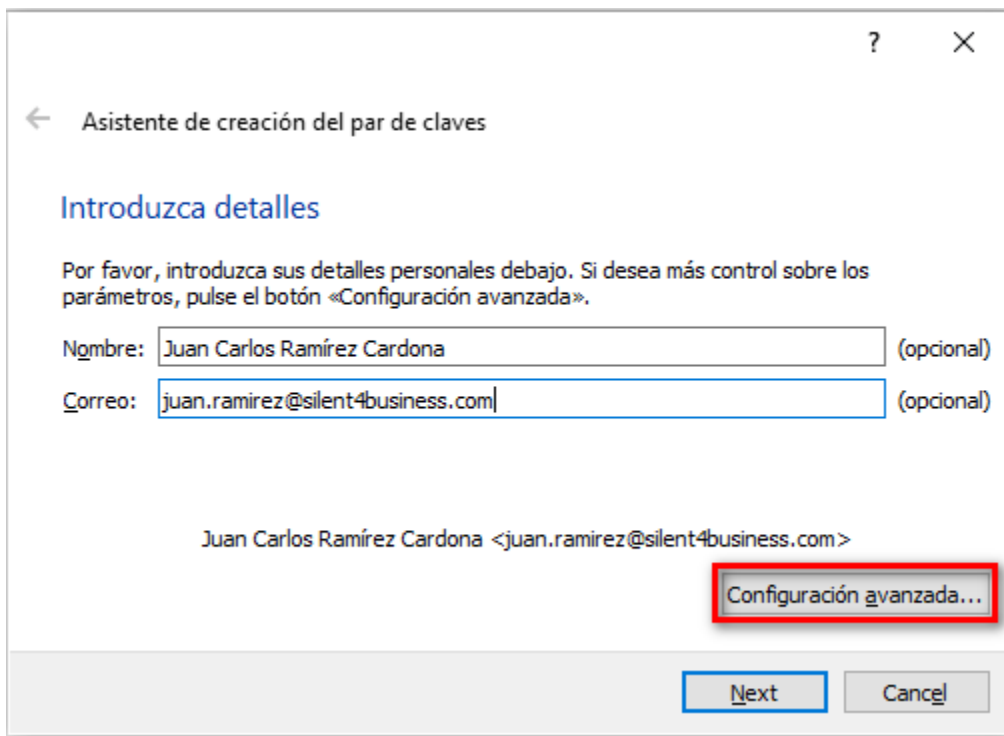
Nombre: (opcional)

Correo: (opcional)

Configuración avanzada...

Next Cancel

Una vez que se introducen los campos solicitados se tiene que seleccionar el botón “Configuración avanzada”



Asistente de creación del par de claves

Introduzca detalles

Por favor, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, pulse el botón «Configuración avanzada».

Nombre: Juan Carlos Ramírez Cardona (opcional)

Correo: juan.ramirez@silent4business.com (opcional)

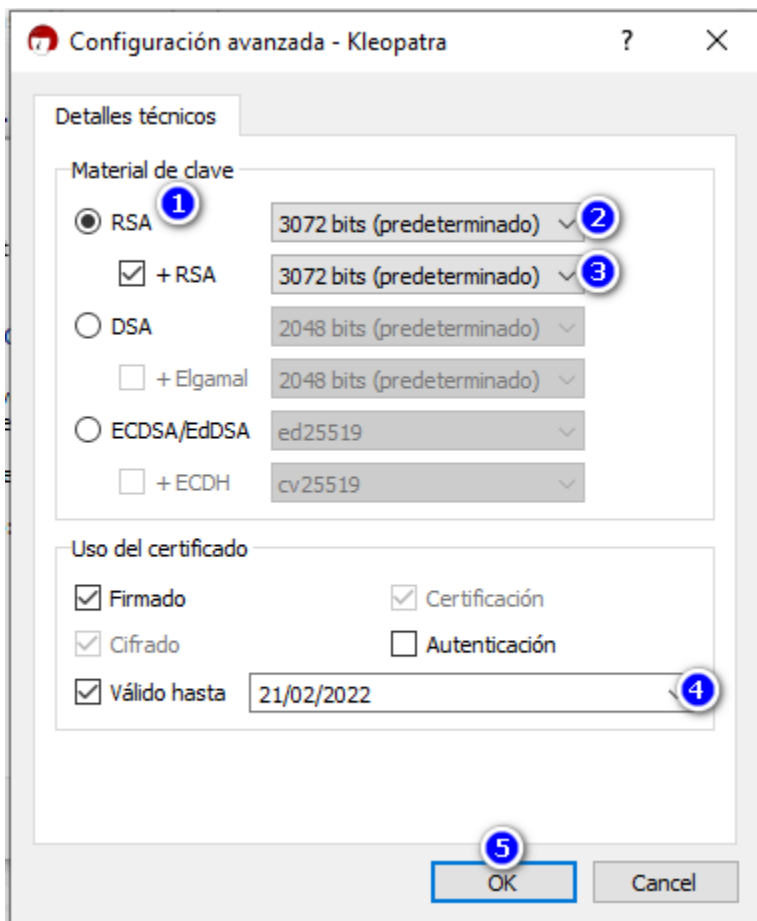
Juan Carlos Ramírez Cardona <juan.ramirez@silent4business.com>

Configuración avanzada...

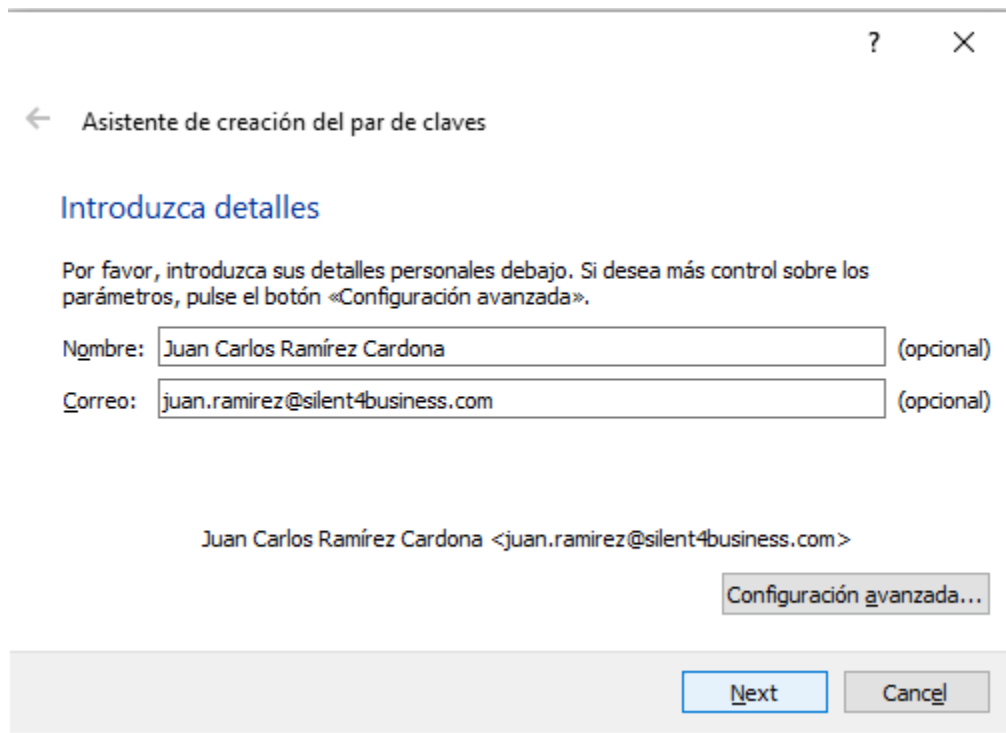
Next Cancel

En la configuración avanzada se deben seleccionar los siguientes valores:

- Se debe seleccionar el cifrado “RSA”(recomendable)
- Seleccionar el tamaño del cifrado del primer cifrado
- Seleccionar el tamaño del cifrado del segundo cifrado
- Modificar la fecha de caducidad del certificado



Una vez finalizado la configuración se debe de dar click en “Next”



← Asistente de creación del par de claves

Introduzca detalles

Por favor, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, pulse el botón «Configuración avanzada».

Nombre: (opcional)

Correo: (opcional)

Juan Carlos Ramírez Cardona <juan.ramirez@silent4business.com>

Configuración avanzada...

Next Cancel

A continuación, se muestran las modificaciones que se realizaron al certificado, al dar click en mostrar detalles del certificado.

← Asistente de creación del par de claves

Parámetros de revisión

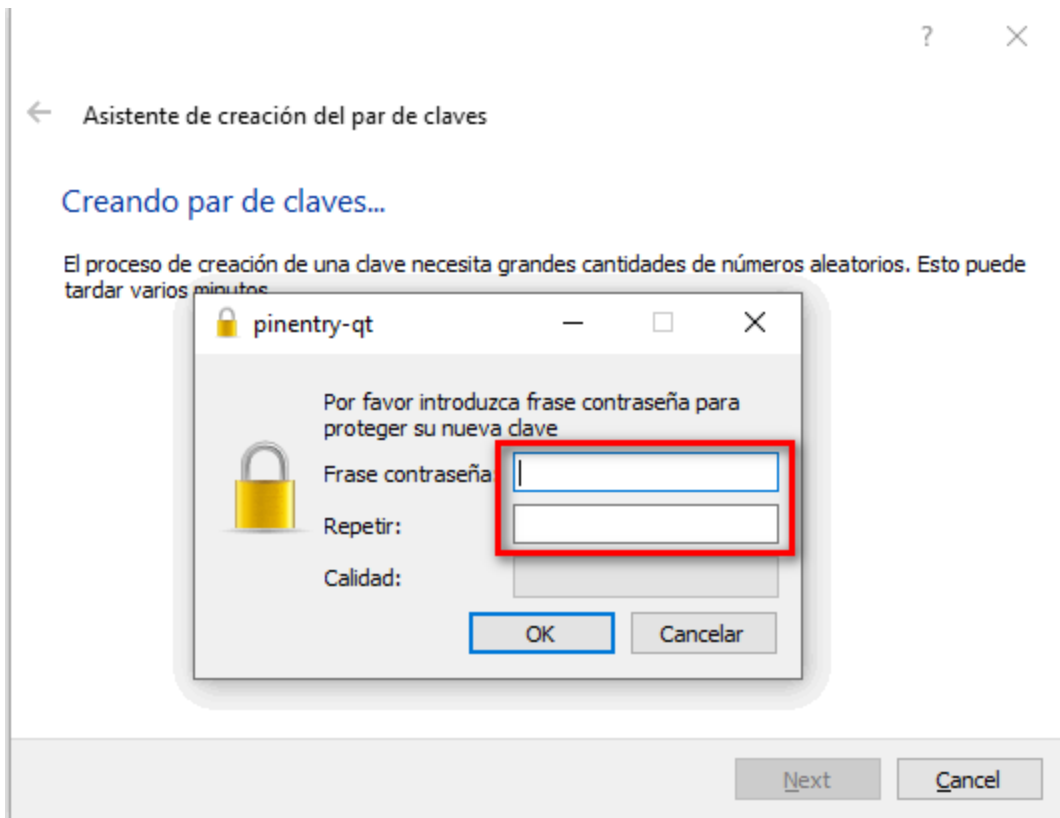
Por favor, analice los parámetros de los certificados antes de proceder.

Nombre:	Juan Carlos Ramírez Cardona
Correo:	juan.ramirez@silent4business.com
Tipo de clave:	RSA
Fortaleza de la clave:	3072 bits
Uso:	Cifrar, Firmar
Tipo de subclave:	RSA
Fortaleza de subclave:	3072 bits
Uso de subclave:	Cifrar
Válido hasta	jueves, 31 de diciembre de 2020

☒ Mostrar todos los detalles

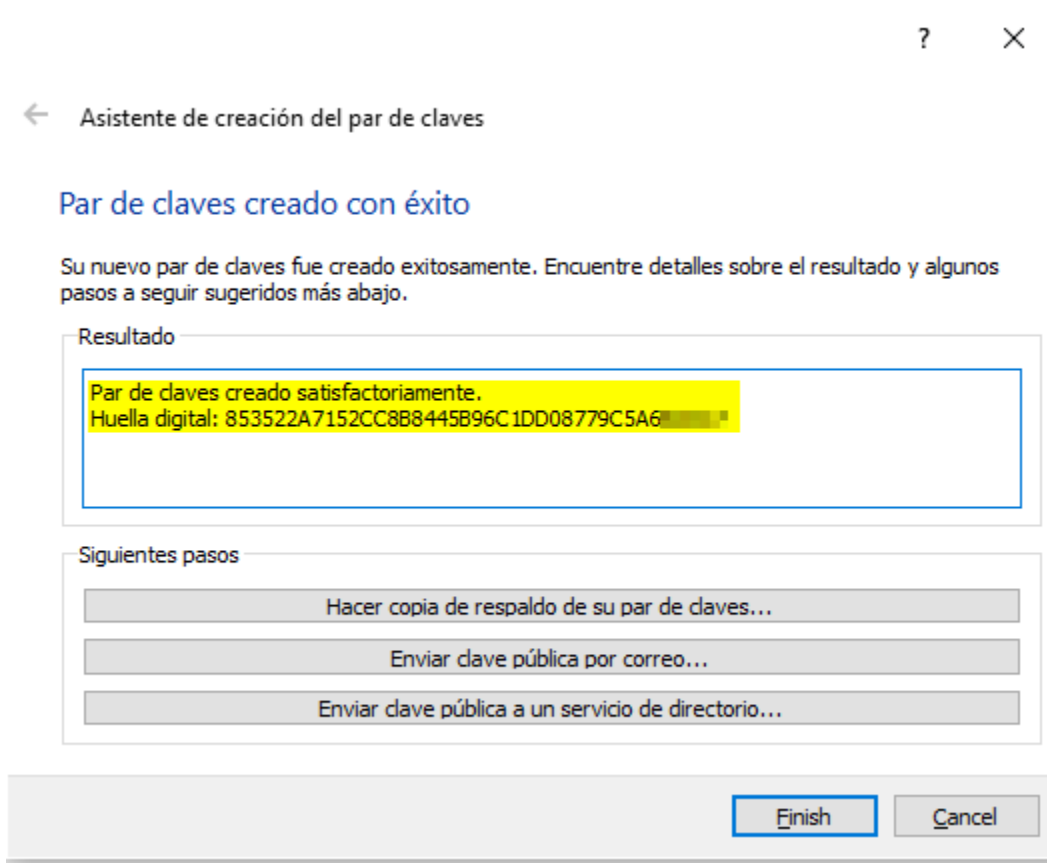
[Crear](#) [Cancel](#)

A continuación el programa solicitará una contraseña para el certificado.

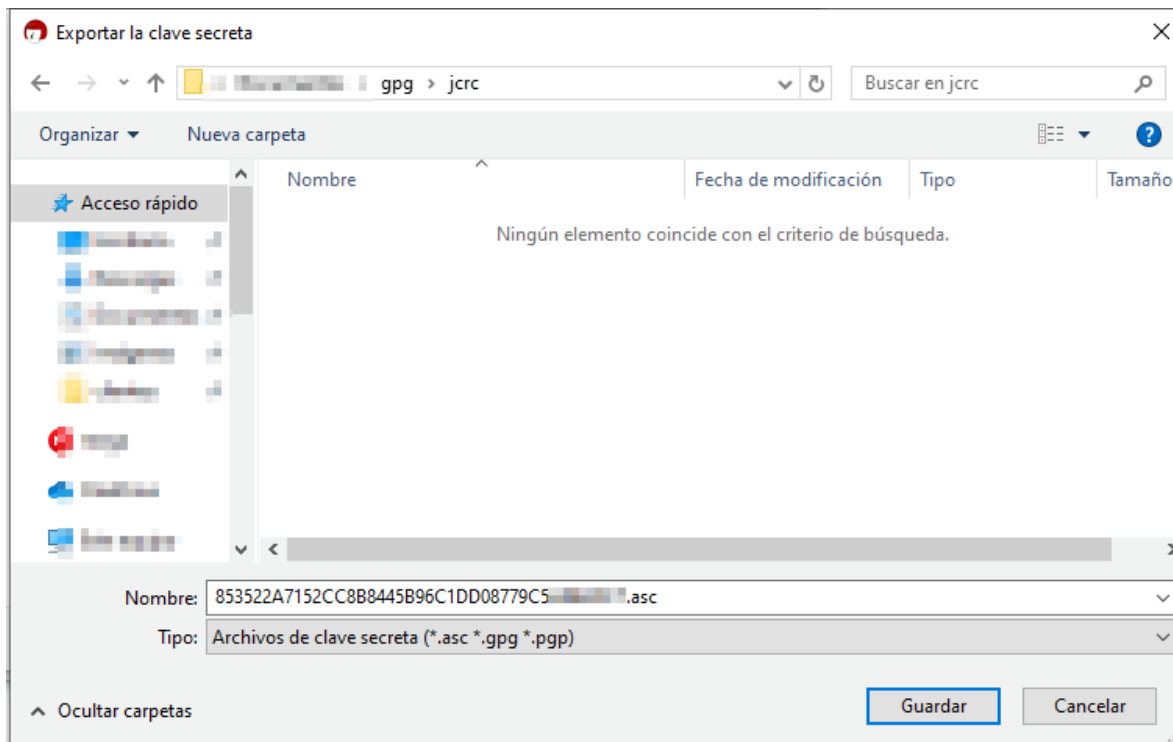


Una vez introducida la contraseña se mostrara un mensaje donde se indica que el par de claves se crearon con éxito.

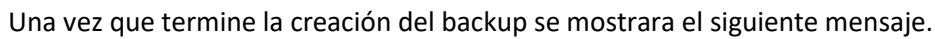
Ahora será necesario hacer un respaldo del par de claves, dando click en “Hacer una copia de respaldo de su par de claves”

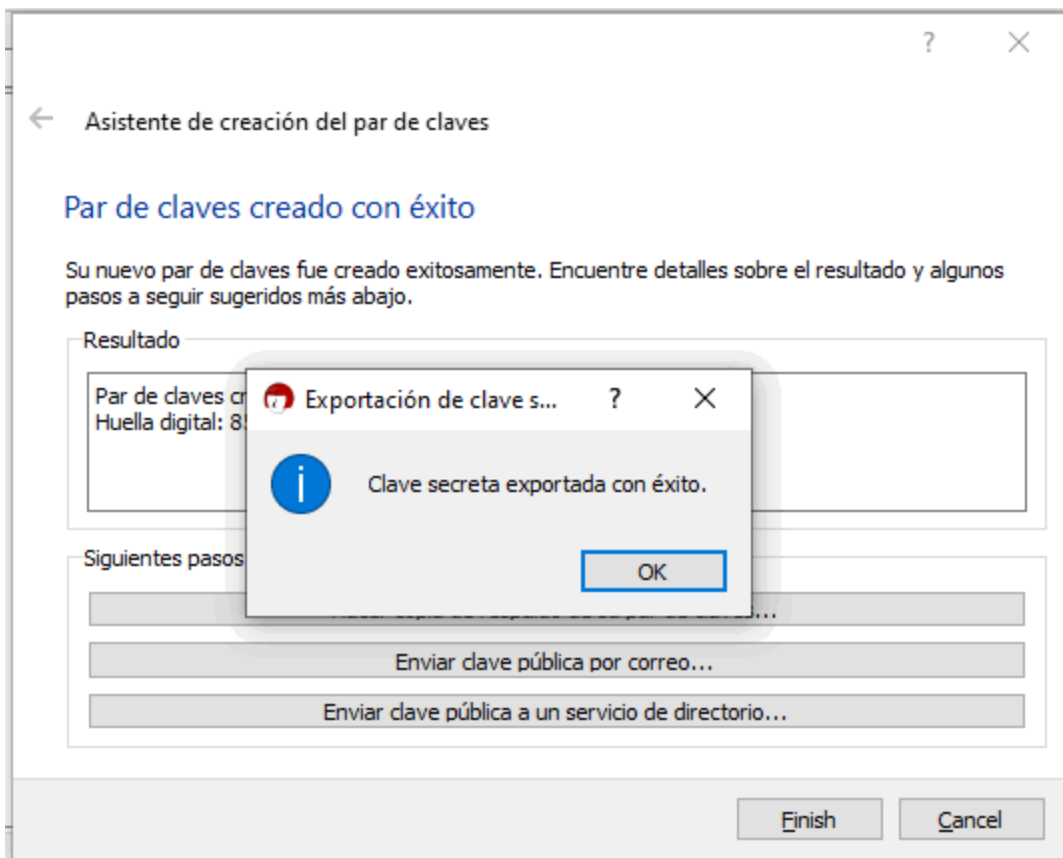


Se mostrará una ventana donde se debe seleccionar la localización del respaldo de los archivos.



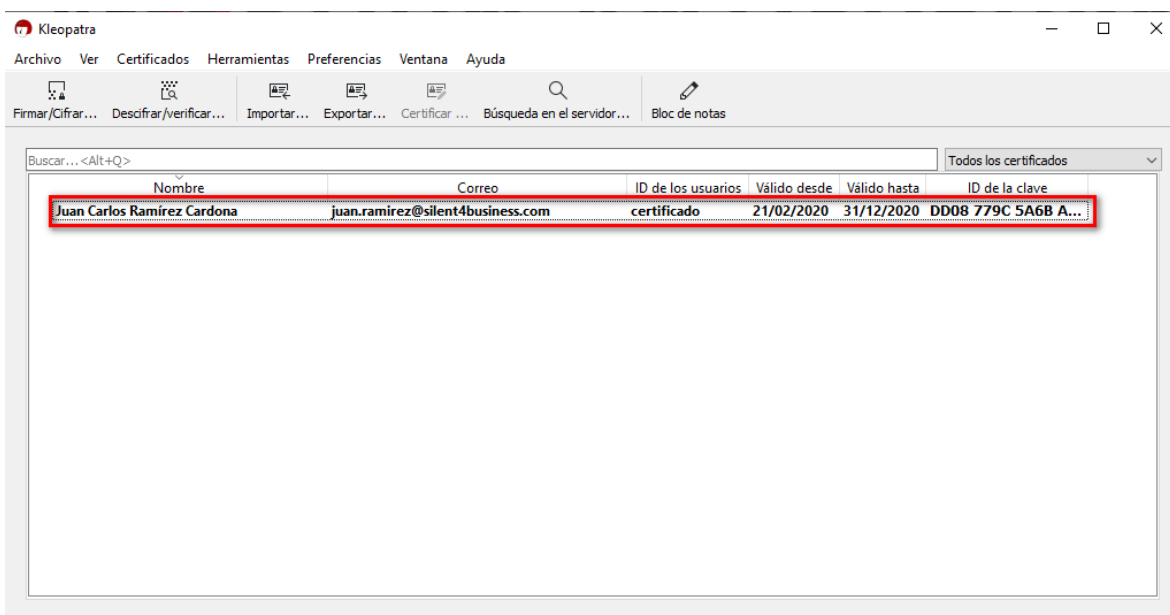
A continuación, se solicitará de la contraseña.





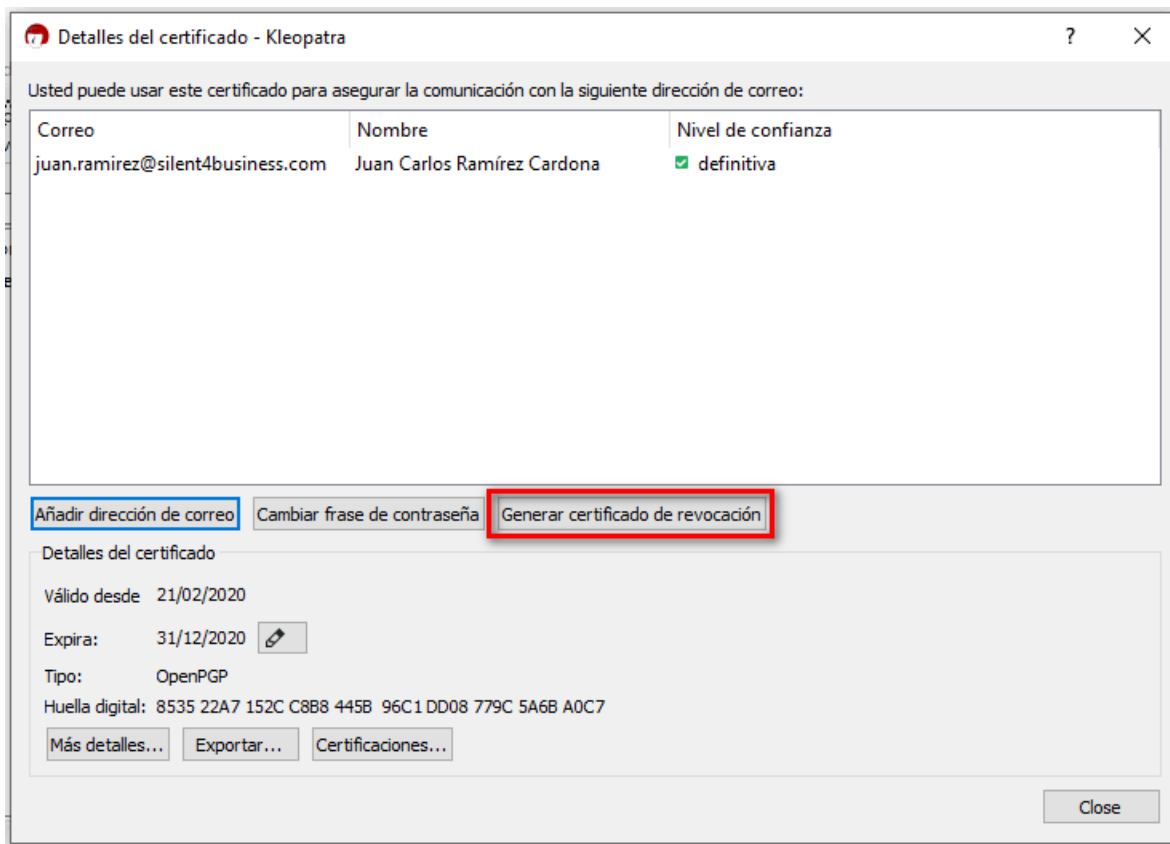
A continuación, se debe de dar click en el botón “Finish”

Ahora se mostrará una ventana como la siguiente, en la cual se mostrarán los certificados creados.

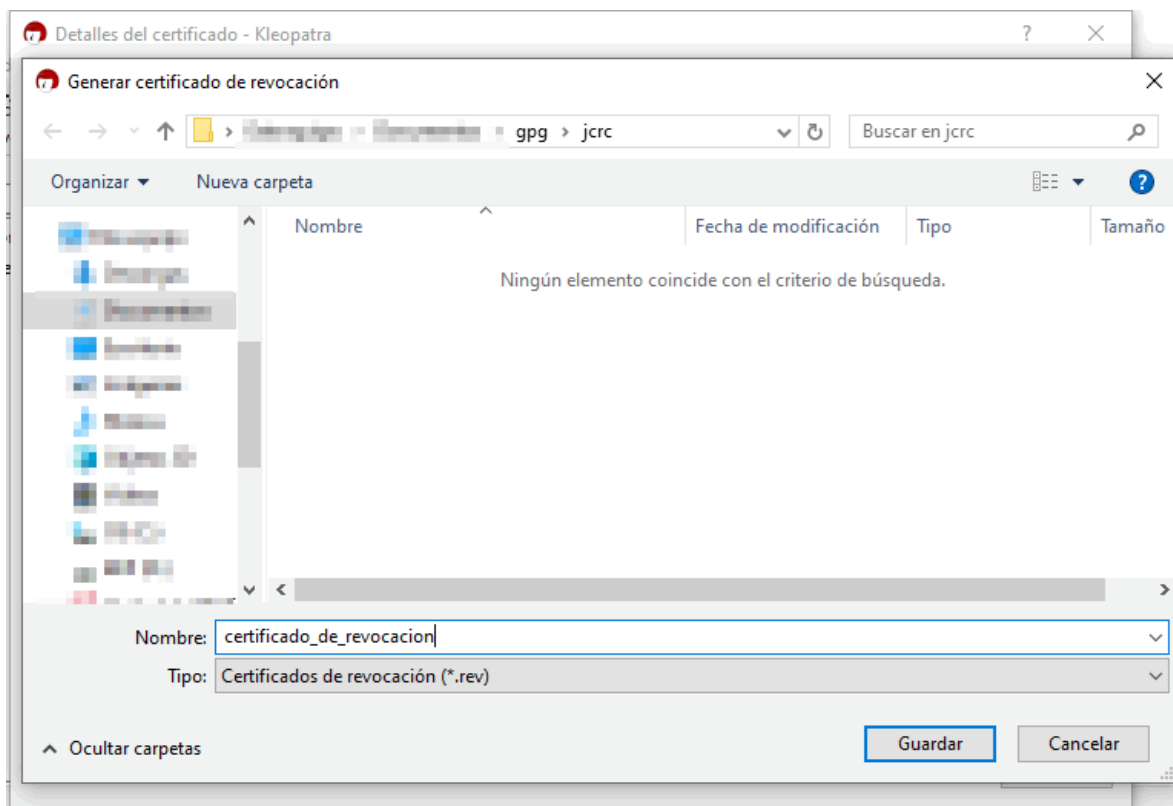


Previo a compartir el certificado es necesario crear un certificado de revocación, esto con la finalidad de que el certificado sea eliminado si el colaborador por cualquier razón salga del equipo del CSRIT.

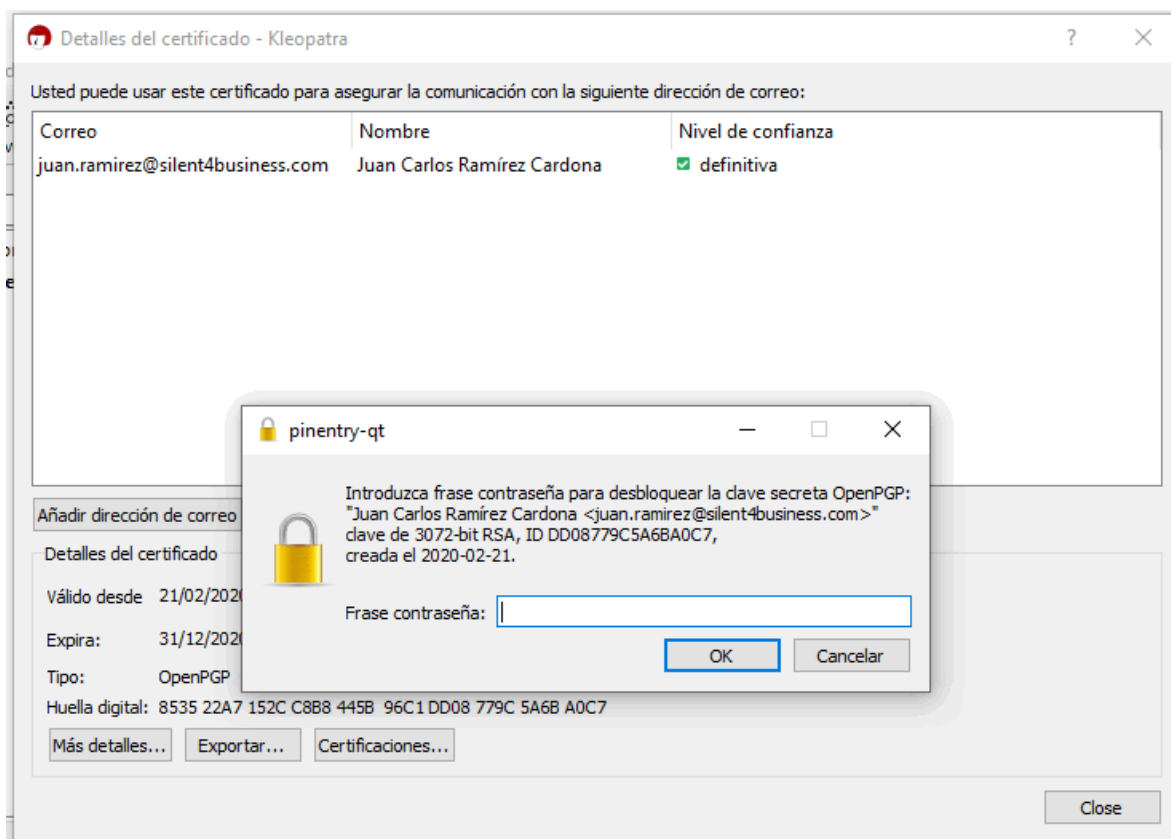
Para ello es necesario dar click derecho en el certificado e ir a los detalles del certificado, a continuación es necesario dar click en “Generar certificado de revocación”



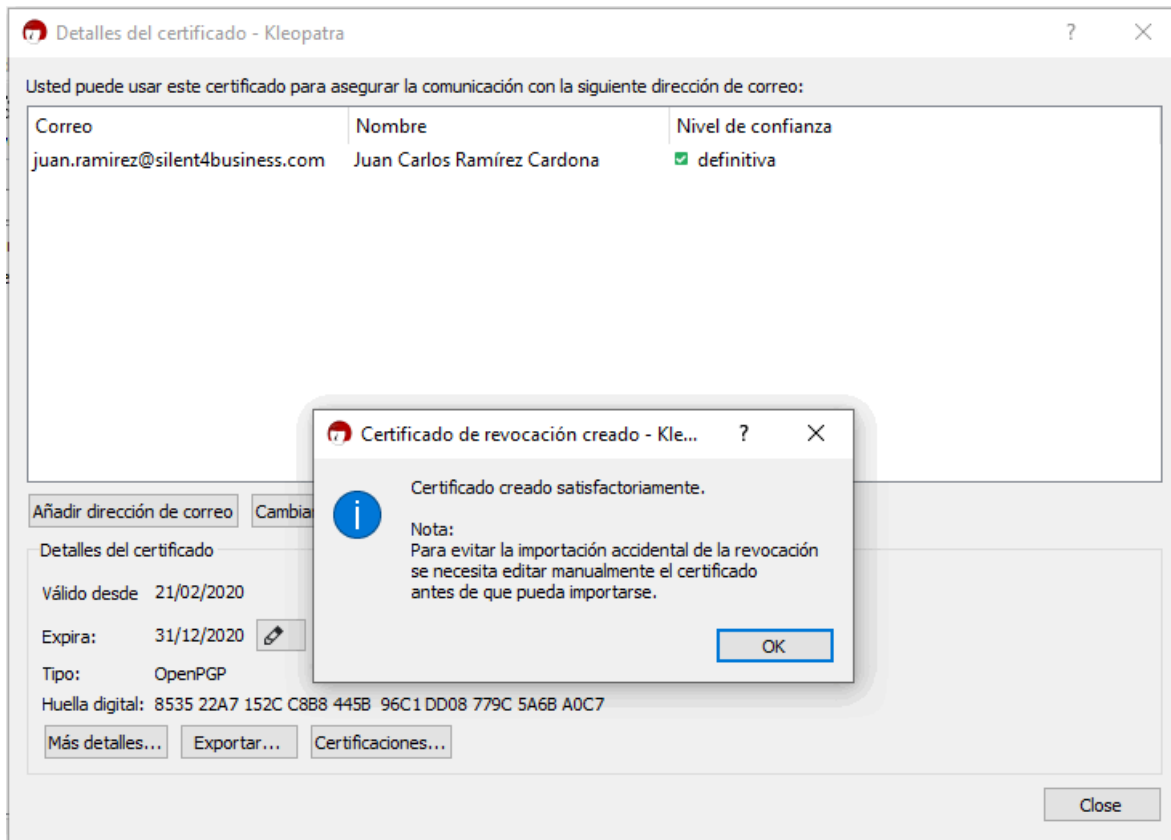
A continuación, es necesario elegir la ruta donde se almacenará el certificado de revocación.



El programa solicitará la contraseña para confirmar la acción.

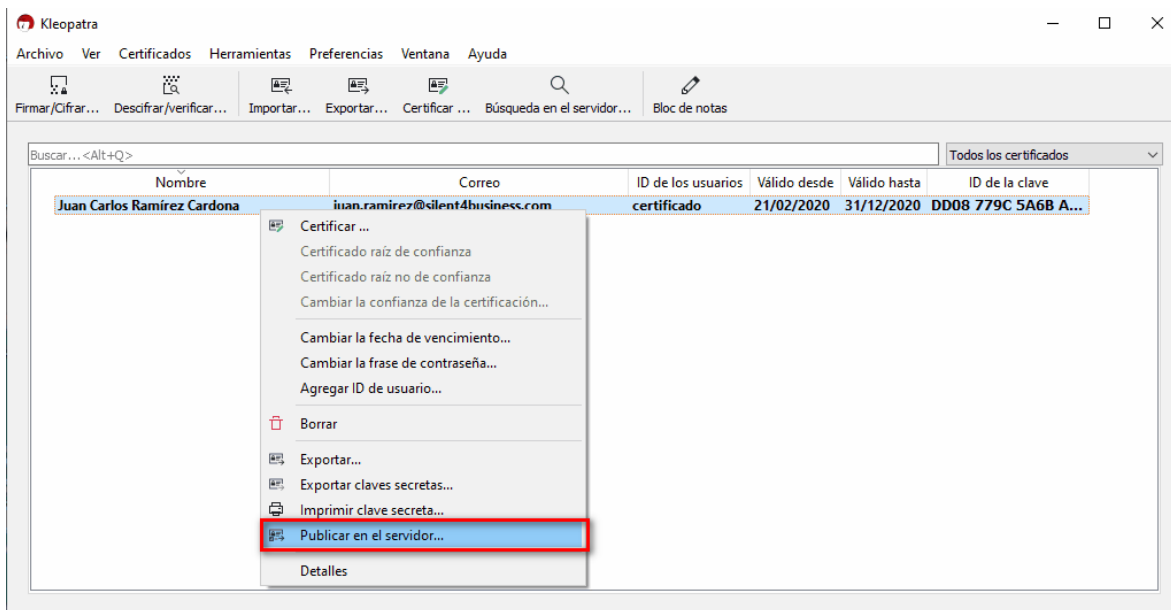


Una vez realizado la acción mostrara el mensaje de confirmación, en la que enuncia que implica la creación del certificado de revocación.

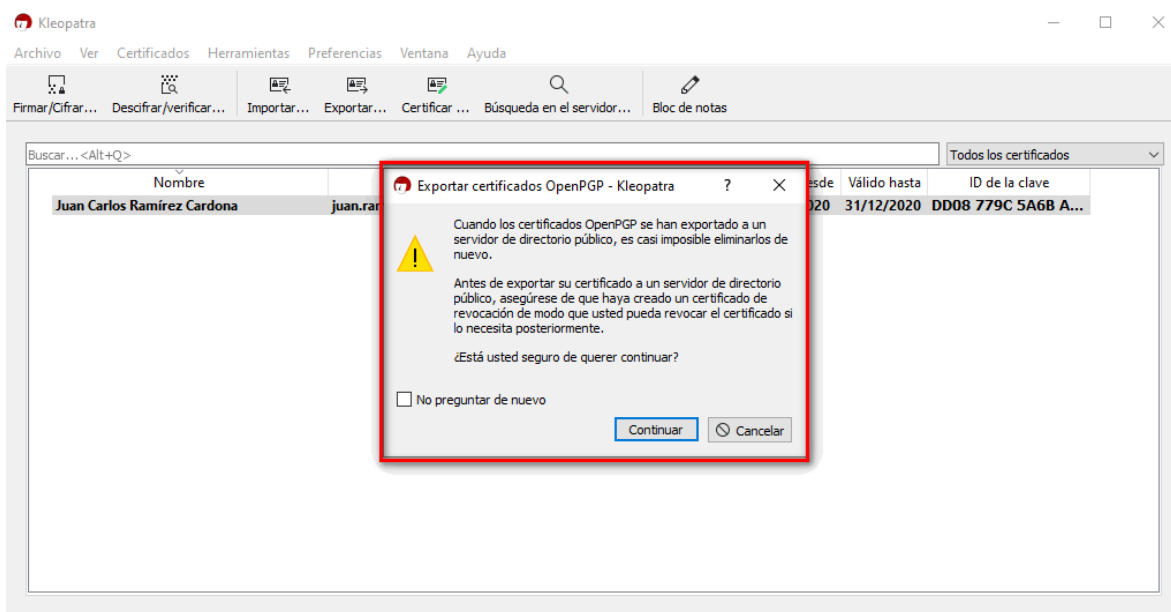


Una vez que se tiene el certificado de revocación es necesario publicar el certificado en el servidor GPG que se configuro en pasos previos.

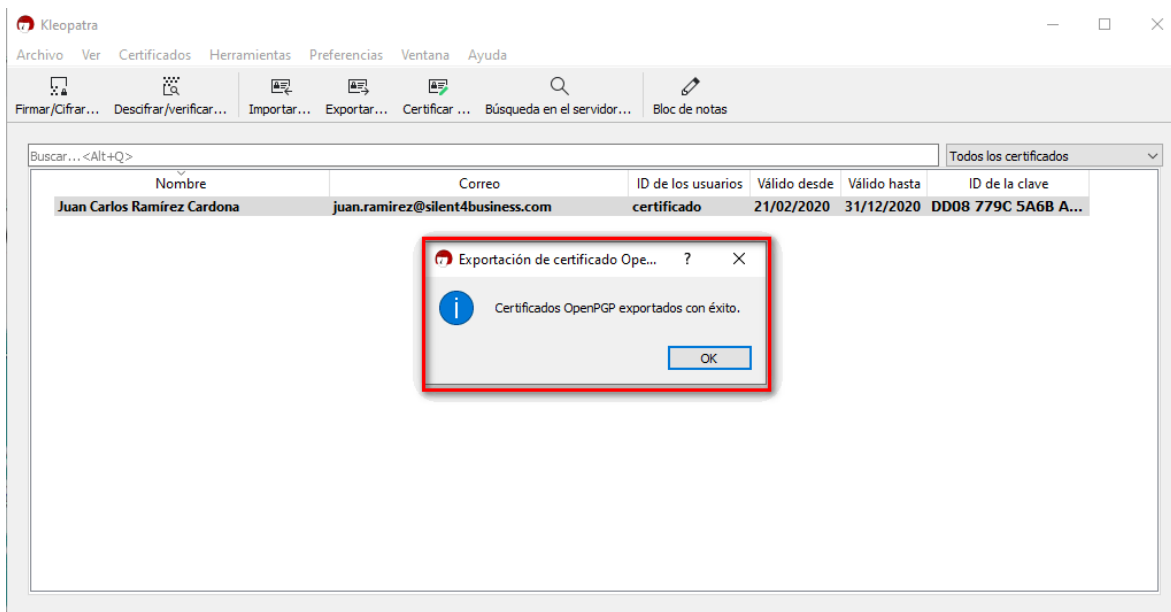
Para realizar esta acción es necesario dar click derecho sobre el nombre del certificado, y dar click en "Publicar en el servidor"



Al dar click en “Publicar en el servidor” se mostrara la siguiente alerta, que hace referencia al certificado de revocación que se creó en pasos anteriores, a la cual se debe de presionar “continuar”.



Una vez que el certificado fue exportado aparecerá la siguiente notificación.

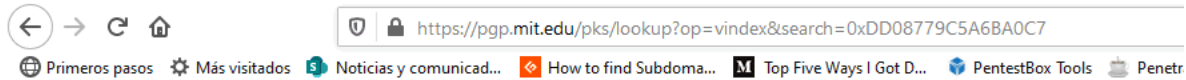


Una vez realizada esta acción se puede ir al sitio <https://pgp.mit.edu> y buscar el certificado exportado.

Nota. El proceso de actualización de un nuevo usuario es de aproximadamente en 5 minutos.



Al darle click se al usuario mostrara el detalle del certificado.



Search results for '0xdd08779c5a6ba0c7'

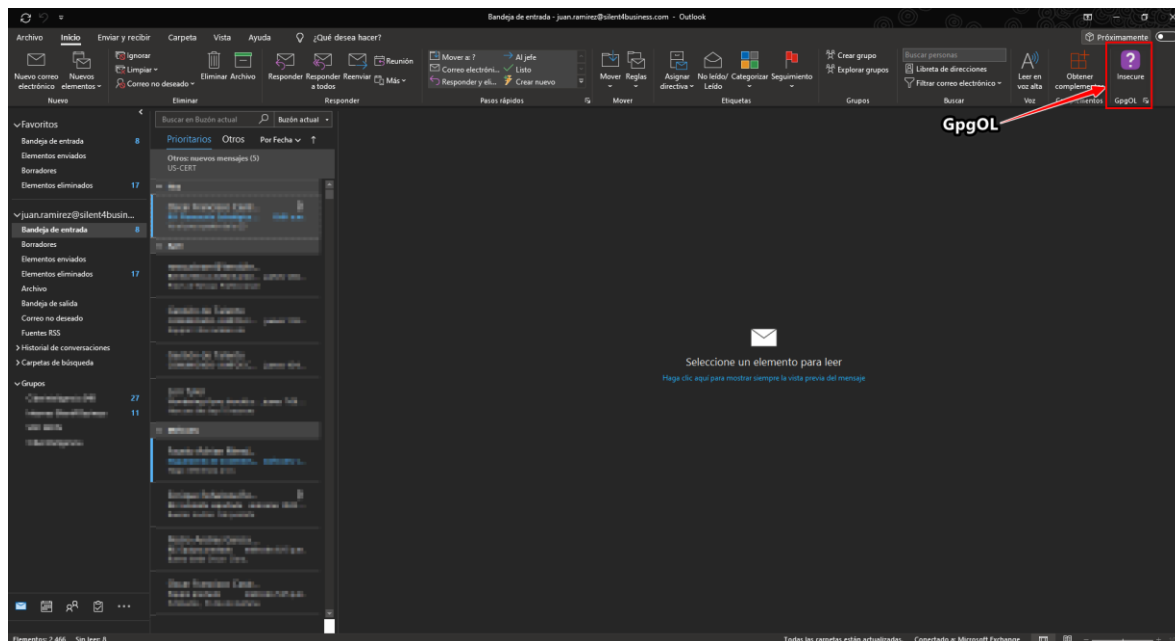
Type bits/keyID cr. time exp time key expir

```
pub 3072R/5A6BA0C7 2020-02-21
uid Juan Carlos Ramirez Cardona <juan.ramirez@silent4business.com>
sig sig3 5A6BA0C7 2020-02-21 2020-12-31 [selfsig]
sub 3072R/DE0139A5 2020-02-21
sig sbind 5A6BA0C7 2020-02-21 2020-12-31 []
```

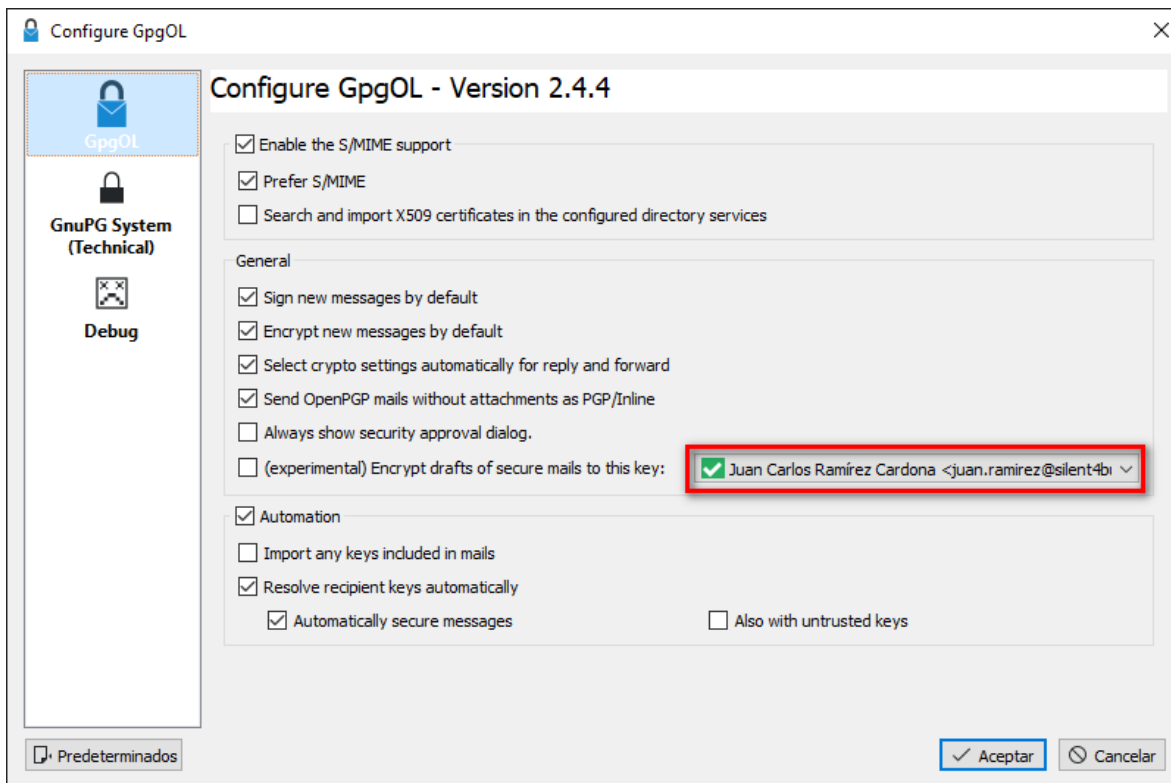
INTEGRACIÓN DE GPG EN OUTLOOK

Reiniciar Outlook

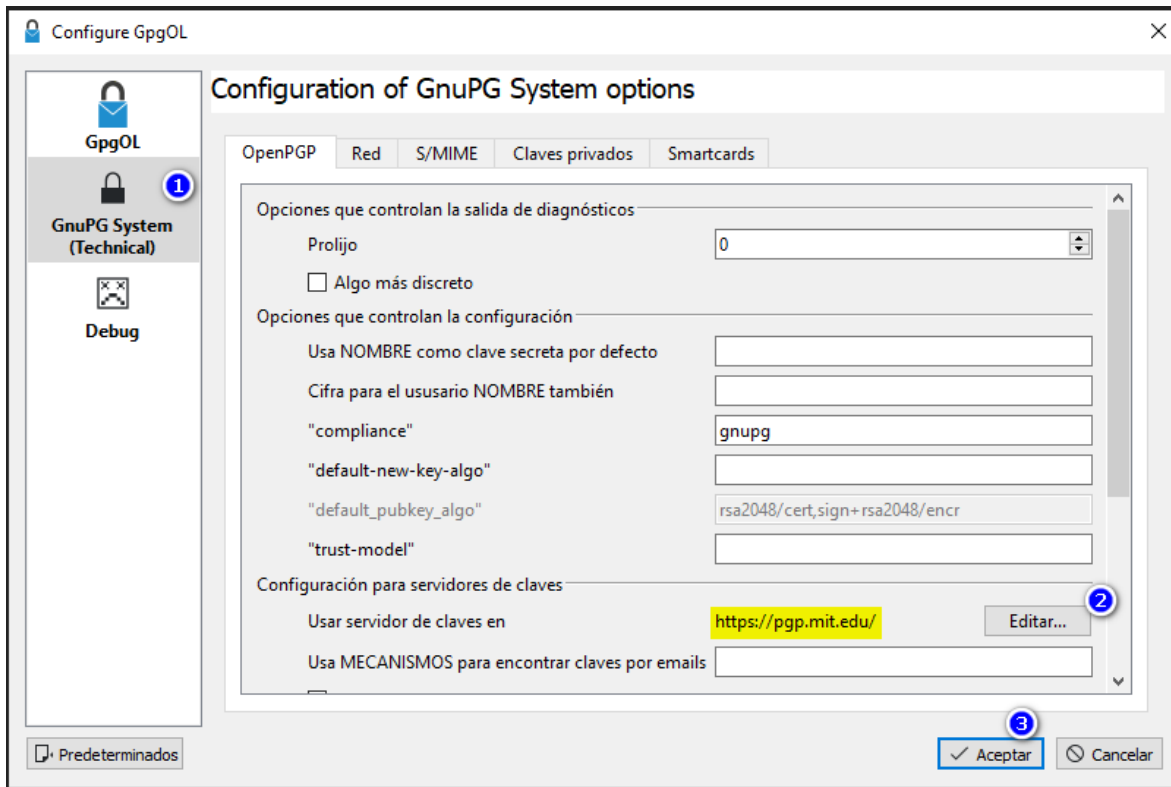
Al abrir Outlook se podrá verificar la integración de GpgOL.



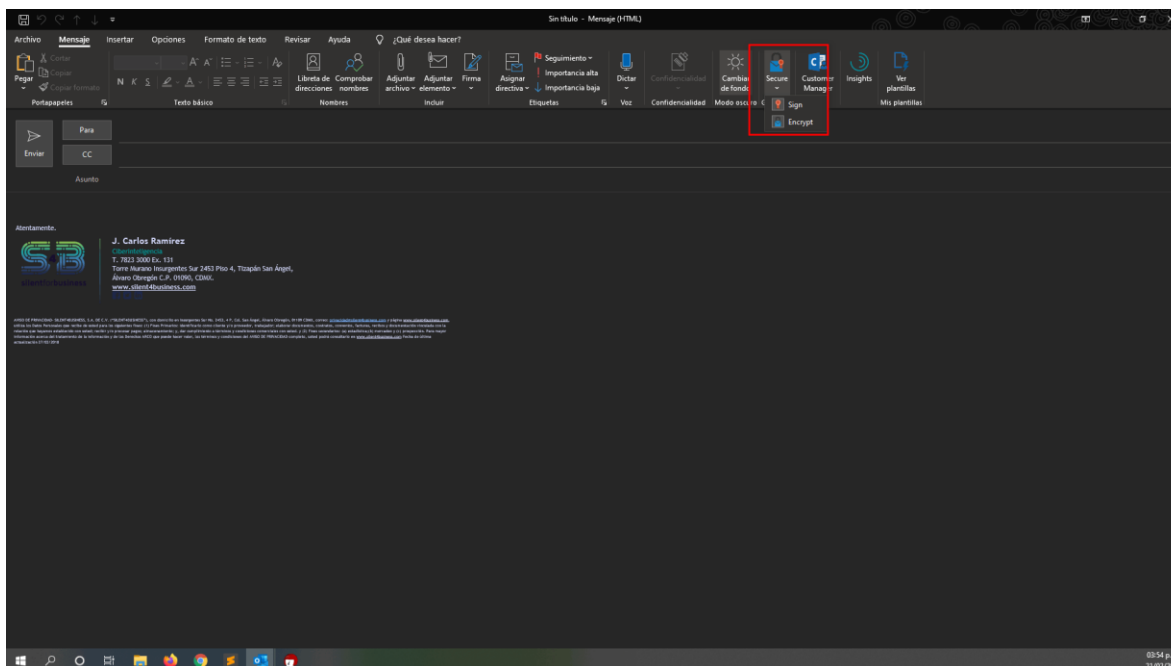
Al presionar la pestaña inferior izquierda del recuadro GpgOL se mostrará el siguiente menú. En el se debe verificar que la cuenta de correo quede asociada al certificado previamente emitido.



A continuación se debe ir a la pestaña “GnuPG System(Technical)”, y editar(en caso de no se encuentre el servidor previamente configurado) el servidor de claves, el cual deberá de tener el valor <https://pgp.mit.edu> y luego dar click en aceptar para guardar los cambios.



Una vez realizado esto, al abrir un nuevo correo se podrá observar que en la opción “Secure”, con la cual será posible firmar y cifrar la información que sea intercambiada via correo electrónico haciendo uso de GPG.





Instructivo Instalación y configuración de llaves GPG

IT-CIB-001-V1
27 septiembre
2021

Es importante mencionar que para que funcione de manera adecuada el intercambio de correos es necesario que el destinatario tenga dado de alta su llave GPG en el servidor que previamente configuramos.