

 <b>CONTRALORÍA</b> <small>GENERAL DE LA REPÚBLICA</small>	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>1</b>

## 1. OBJETIVO

Orientar al usuario en la instalación y uso básico de la herramienta de cifrado de información Kleopatra Gpg4win (GNU Privacy Guard para Windows).

## 2. ALCANCE

El siguiente instructivo aplica para los usuarios internos y usuarios externos que requieran remitir información confidencial a la Dirección de Información, Análisis y Reacción Inmediata de la Contraloría General de la República.

## 3. TERMINOS Y DEFINICIONES

**CIFRADO:** es un método de codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.

**CIFRADO SIMÉTRICO:** también conocido como algoritmo de clave/llave secreta, es un singular método de descodificación de mensajes que debe ser provisto al receptor antes de que el mensaje se pueda descodificar. La clave/llave que se usa en la codificación es la misma que se utiliza en la descodificación, lo que resulta más conveniente para los usuarios individuales y los sistemas cerrados. De lo contrario, se le tiene que enviar la clave/llave al receptor, lo que aumenta el riesgo de alteraciones en caso de que terceros, como un hacker, la intercepten. La ventaja es que este método es mucho más ágil que el método asimétrico.

**CIFRADO ASIMÉTRICO:** este método utiliza dos claves/llaves diferentes (pública y privada), que están vinculadas entre sí matemáticamente. Las claves/llaves son solo números extensos vinculados entre sí, pero no son idénticos, de ahí el término asimétrico. La clave/llave pública se puede compartir con cualquier persona, mientras que la clave/llave privada debe mantenerse en secreto. Ambas se pueden usar para cifrar un mensaje, y la clave/llave opuesta a la que se emplee para cifrarlo se utiliza luego para descodificarlo.

**GNU Privacy Guard (GnuPG o GPG)** es una herramienta de cifrado y firmas digitales desarrollado por Werner Koch, que viene a ser un reemplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.

	Macroproceso:		Proceso:
	Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win		
	Código:	Versión: 1.0	2

#### 4. DESARROLLO

##### 4.1. INSTALACIÓN DEL SOFTWARE GPG4WIN

4.1.1. Descargue la aplicación desde la url <https://www.gpg4win.org/>

4.1.2. En la ventana de descarga seleccione la opción \$0 y haga clic en Download.

[Home](#) » [Download](#)

## Download Gpg4win 3.1.11 (2019-12-17)

You can also use this installer to update an older version. Keys and configuration will be kept.

**Please donate for Gpg4win to support maintenance and development!**  
Pay what you want! – Thank you!

Donate with

PayPal

Bitcoin

Bank transfer



\$0

\$10

\$15

\$25

\$ \_\_\_\_\_

USD

EUR

onetime

monthly

Add me to the [list of sponsors](#) (from 20,- EUR/USD up)

I am using Gpg4win because ...

**Donate & Download**

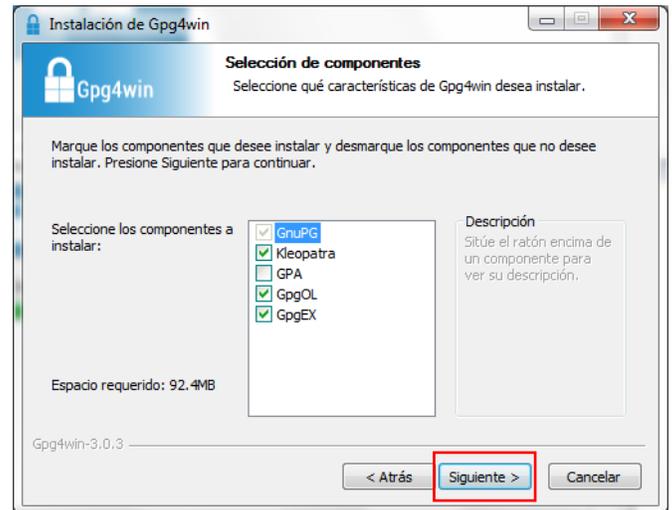
[OpenPGP signatures and source code package](#) »

4.1.3. Ubique la ruta donde se descargó el instalador del software **gpg4win-3.1.11.exe** o superior y haga clic sobre el archivo para proceder a iniciar la instalación.

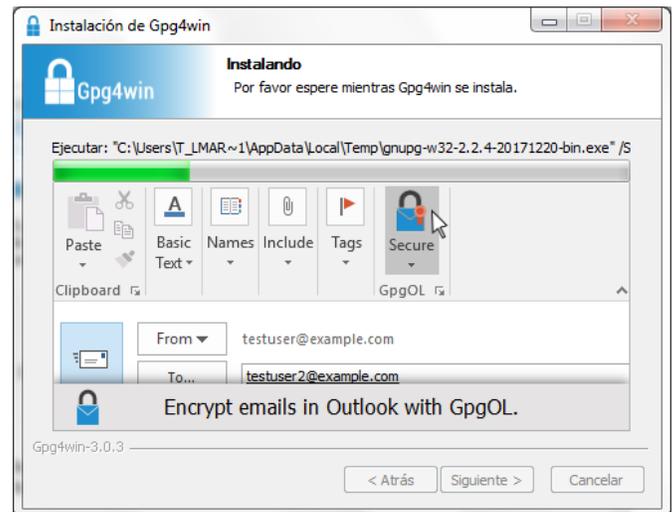
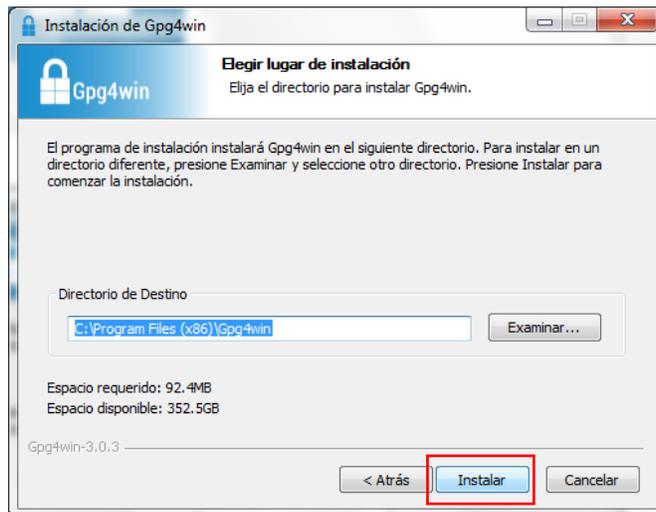


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>3</b>

4.1.4. Una vez iniciada la instalación del Software haga clic en el botón “siguiente” de acuerdo a la imagen.



4.1.5. Ubique el directorio destino donde va a realizar la instalación y haga clic en “instalar”.



	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>4</b>

4.1.6. Una vez realizada la instalación, haga clic en **“Terminar”**.

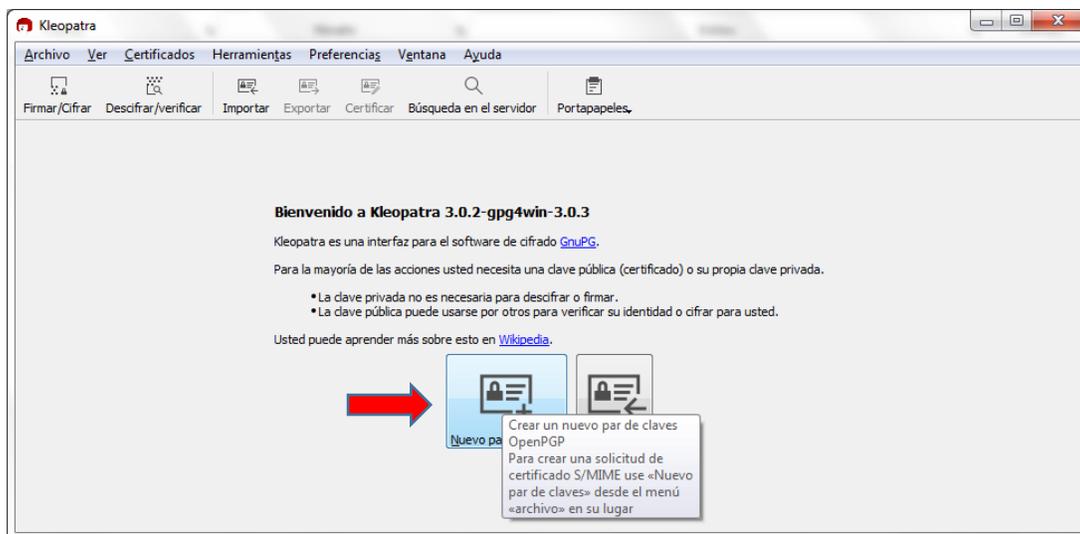


## 4.2. CREACIÓN DE LAS CLAVES/LLAVES PARA EL CIFRADO ASIMÉTRICO

4.2.1. Ubique el ícono del software “Kleopatra” y haga doble clic para ejecutarlo.

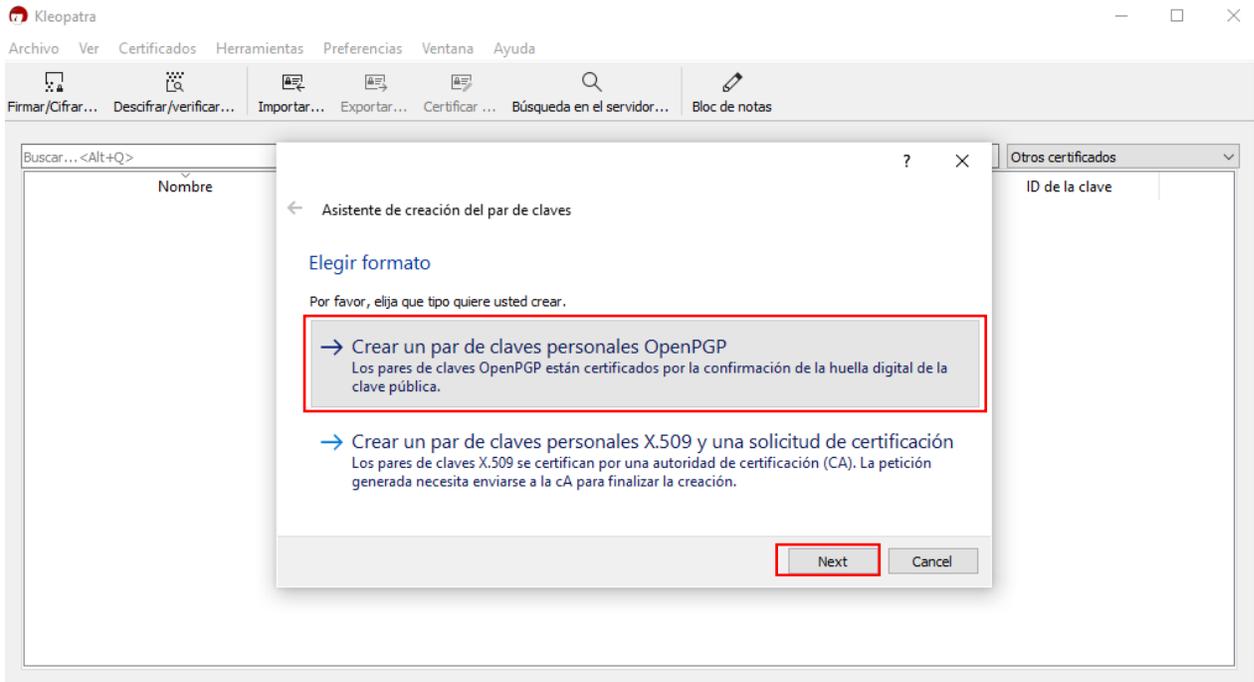


4.2.2. Al abrir por primera vez el software se visualiza la siguiente ventana para la creación de las claves/llaves de cifrado. Haga clic en **“Nuevo par de claves”**.

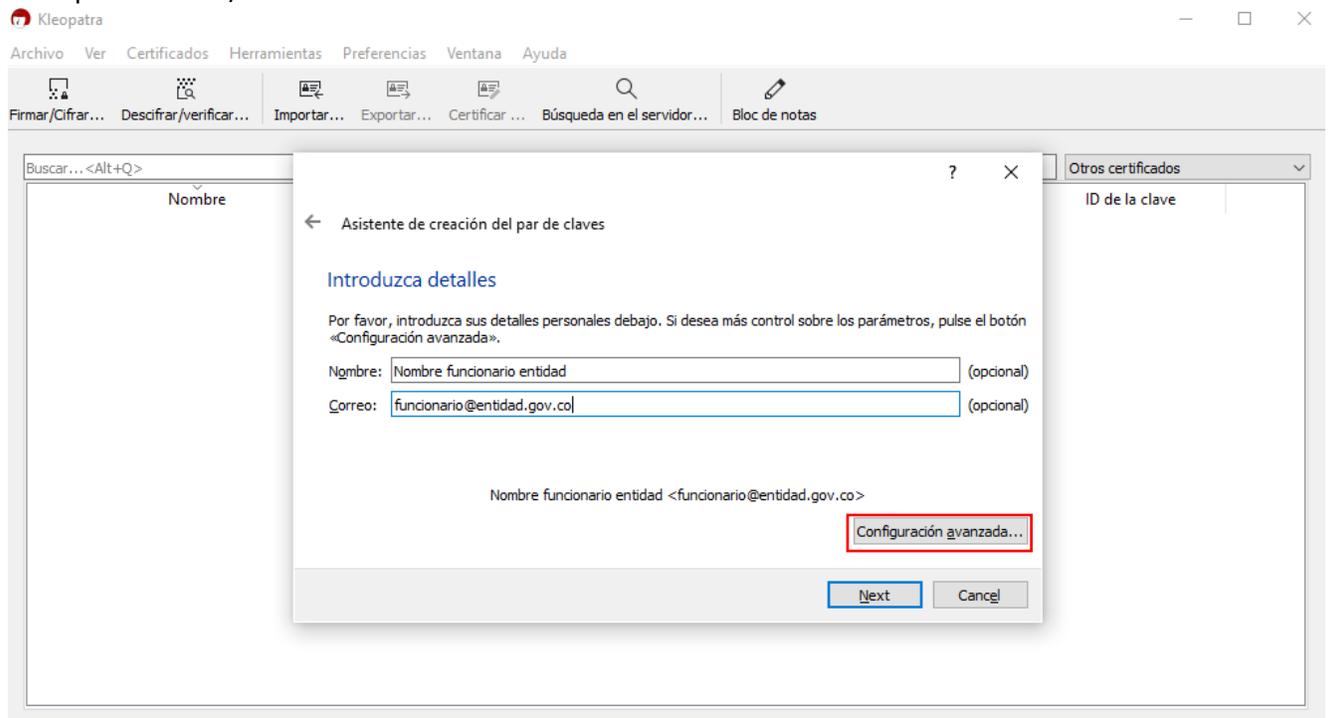


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>5</b>

4.2.3. Se inicia el asistente de creación de las claves/llaves de cifrado; seleccione la opción **“Crear un par de claves personales OPenPGP”** y en el botón **“Next”**.

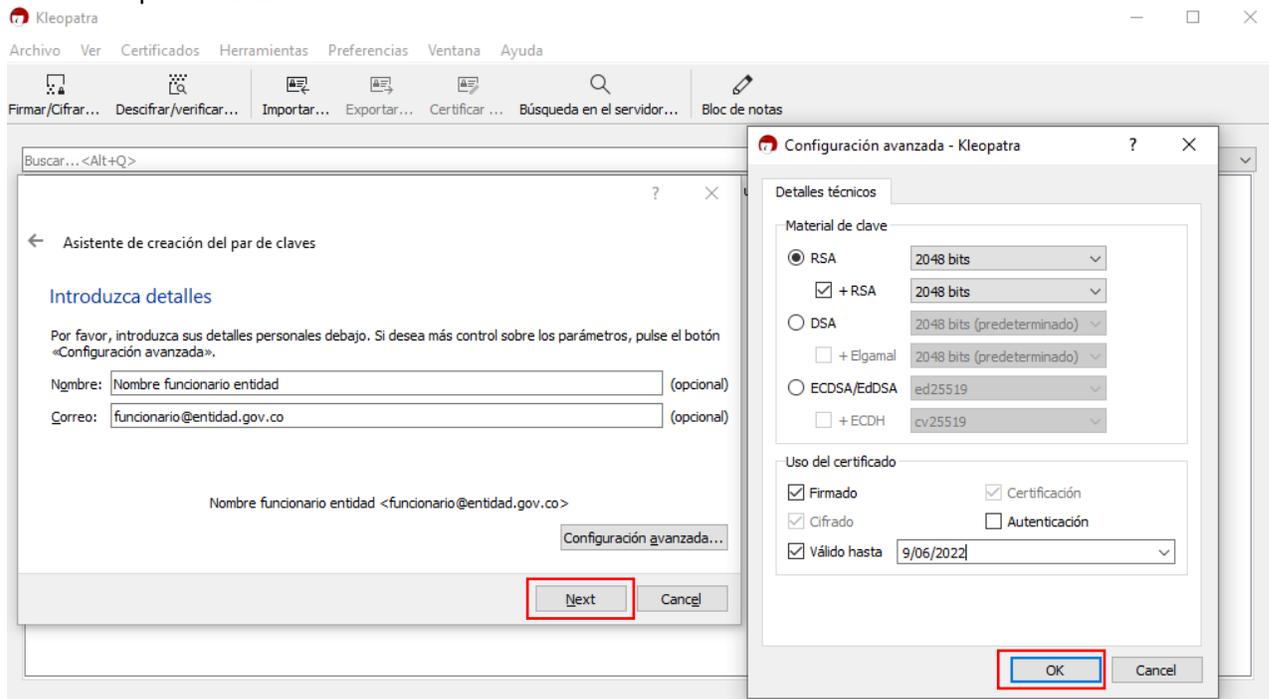


4.2.4. Digite la información relacionada con el nombre y correo del funcionario al cual se le generará el par de claves/llaves de cifrado.

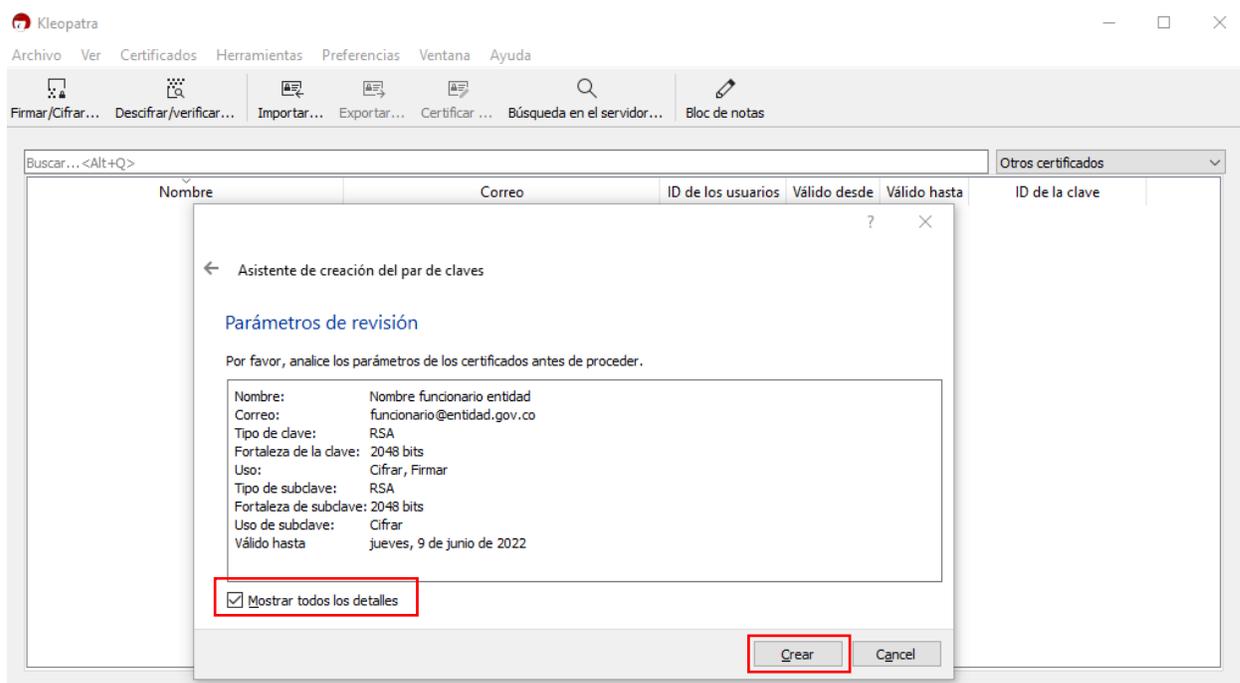


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>6</b>

En la opción de configuración avanzada seleccione el tiempo de validez que va a definir para las claves/llaves de cifrado. Una vez definido haga clic en la opción **“OK”** y posteriormente en la opción **“Next”**.

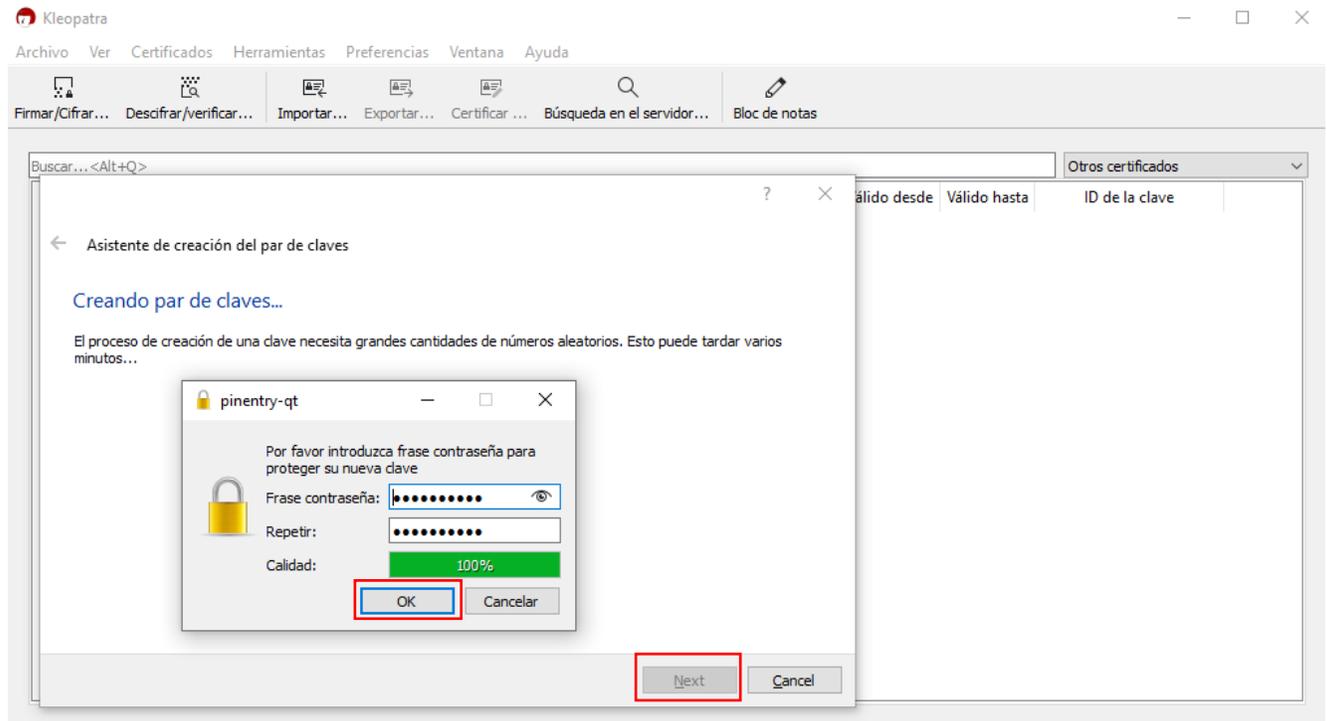


4.2.5. Al hacer clic en la opción **“Mostrar todos los detalles”**, se visualizará la siguiente ventana con la información de los parámetros del par de claves/llaves de cifrado asimétrico. Haga clic en **“crear”**.

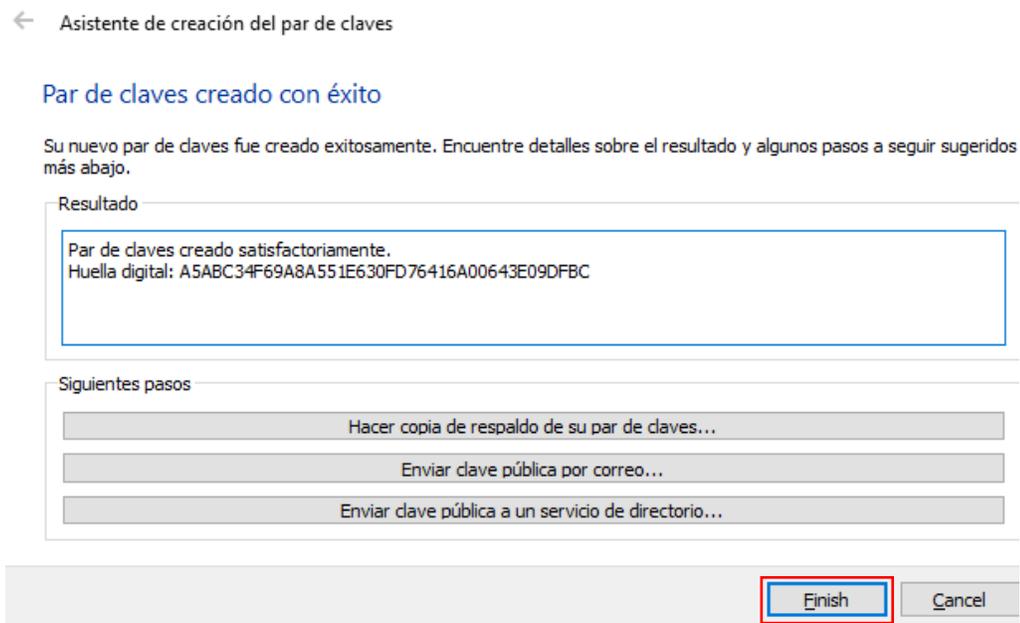


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>7</b>

4.2.6. Digite la contraseña para proteger el par de claves/llaves y haga clic en el botón **“OK”** y posteriormente en **“Next”**.



4.2.7. Una vez ingresada la contraseña, se visualizará una ventana donde confirma la creación exitosa del par de claves/llaves de cifrado. Para finalizar el proceso seleccione la opción **“Finish”**



	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>8</b>

4.2.8. Haga una copia del par de claves/llaves y envíe vía correo electrónico la llave pública con la cual el receptor de los archivos cifrados podrá hacer su apertura, haciendo clic en las opciones respectivas.

← Asistente de creación del par de claves

### Par de claves creado con éxito

Su nuevo par de claves fue creado exitosamente. Encuentre detalles sobre el resultado y algunos pasos a seguir sugeridos más abajo.

**Resultado**

Par de claves creado satisfactoriamente.  
 Huella digital: 597C8E841F359A5D305E78645D70C4404C4C316D

**Siguientes pasos**

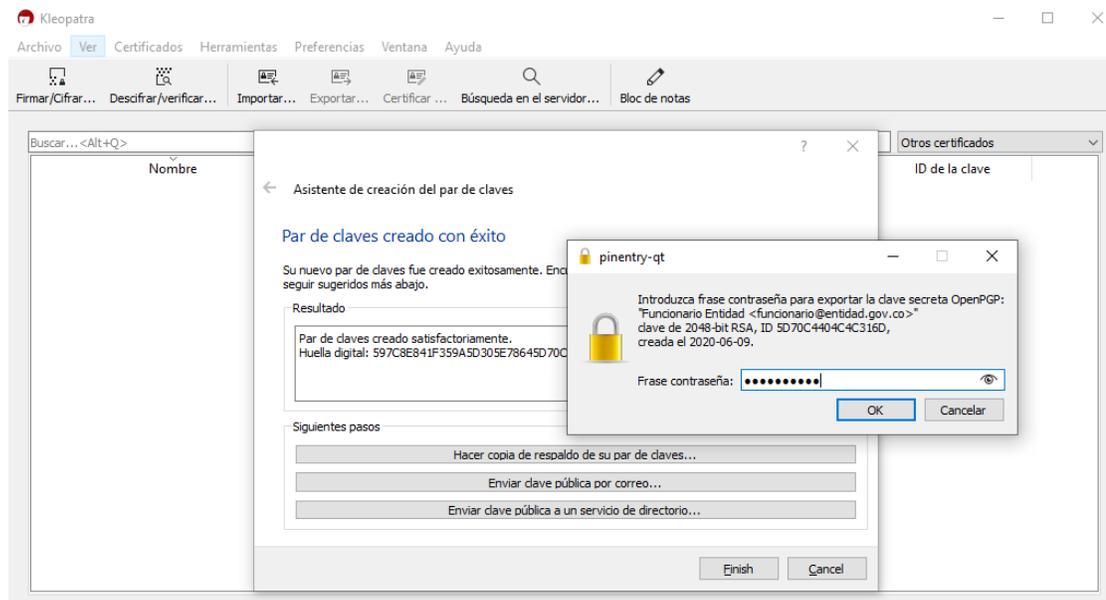
→
Hacer copia de respaldo de su par de claves...

→
Enviar clave pública por correo...

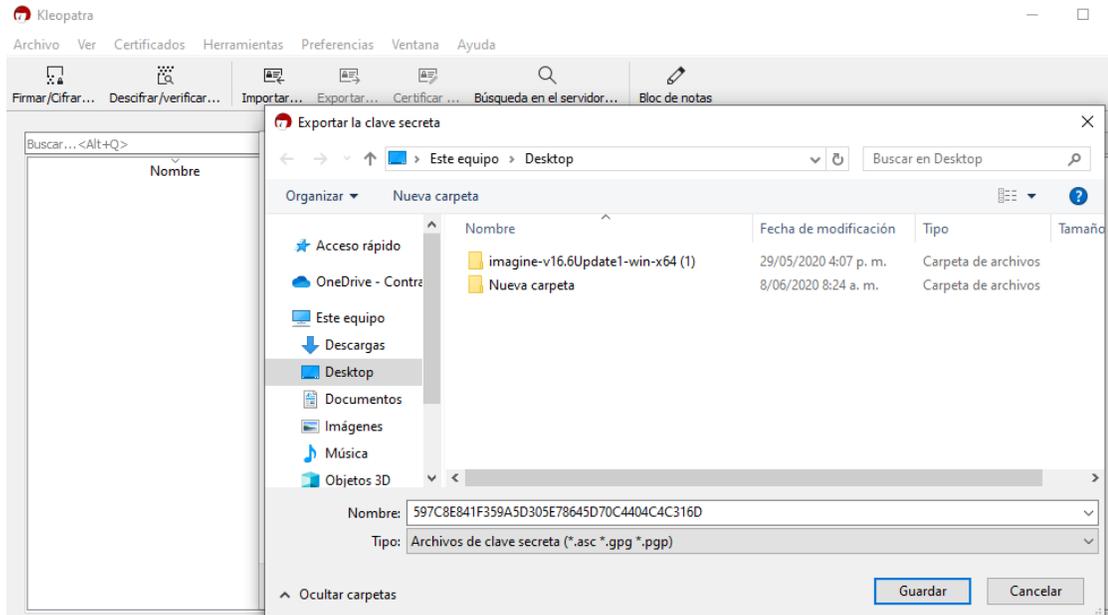
→
Enviar clave pública a un servicio de directorio...

Finish Cancel

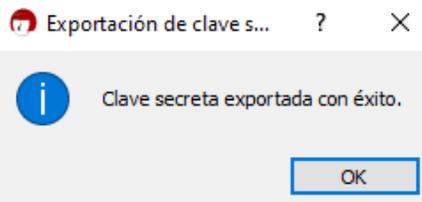
Al hacer clic en la opción correspondiente a “**hacer copia de respaldo de su par de claves...**” se desplegará un cuadro de dialogo para digitar la contraseña digitada en el paso descrito en el numeral 4.2.6; digite la contraseña y seleccione la ruta donde guardará la copia de las claves/llaves.



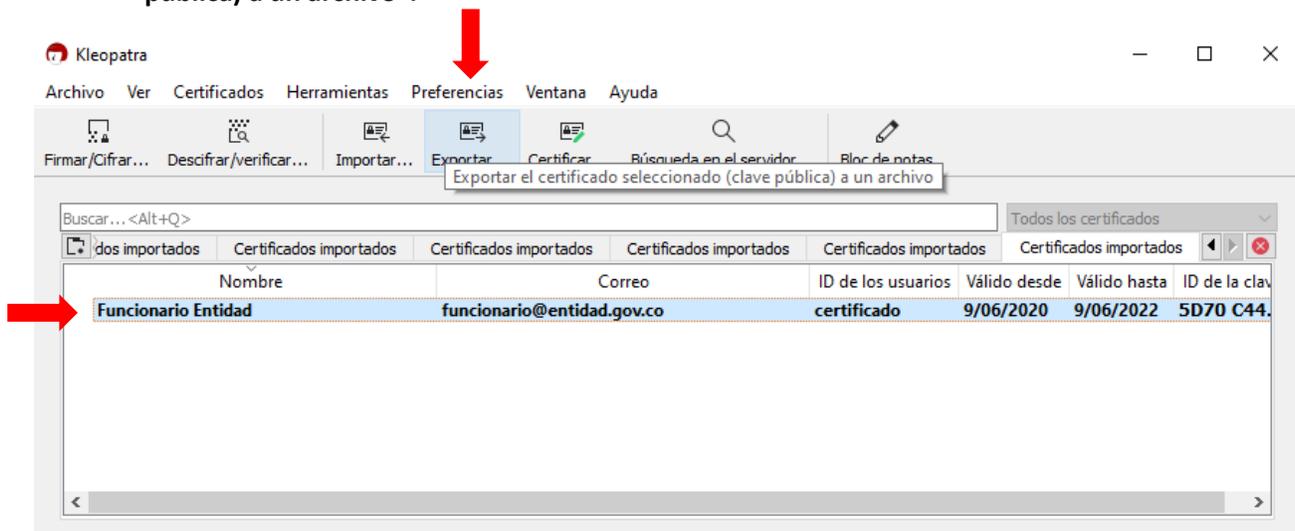
	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>9</b>



Asígnele un nombre al archivo de su par de claves/llaves. Una vez ha hecho clic sobre la opción **“Guardar”** se desplegará un cuadro de diálogo que le informará la creación exitosa del par de claves/llaves.

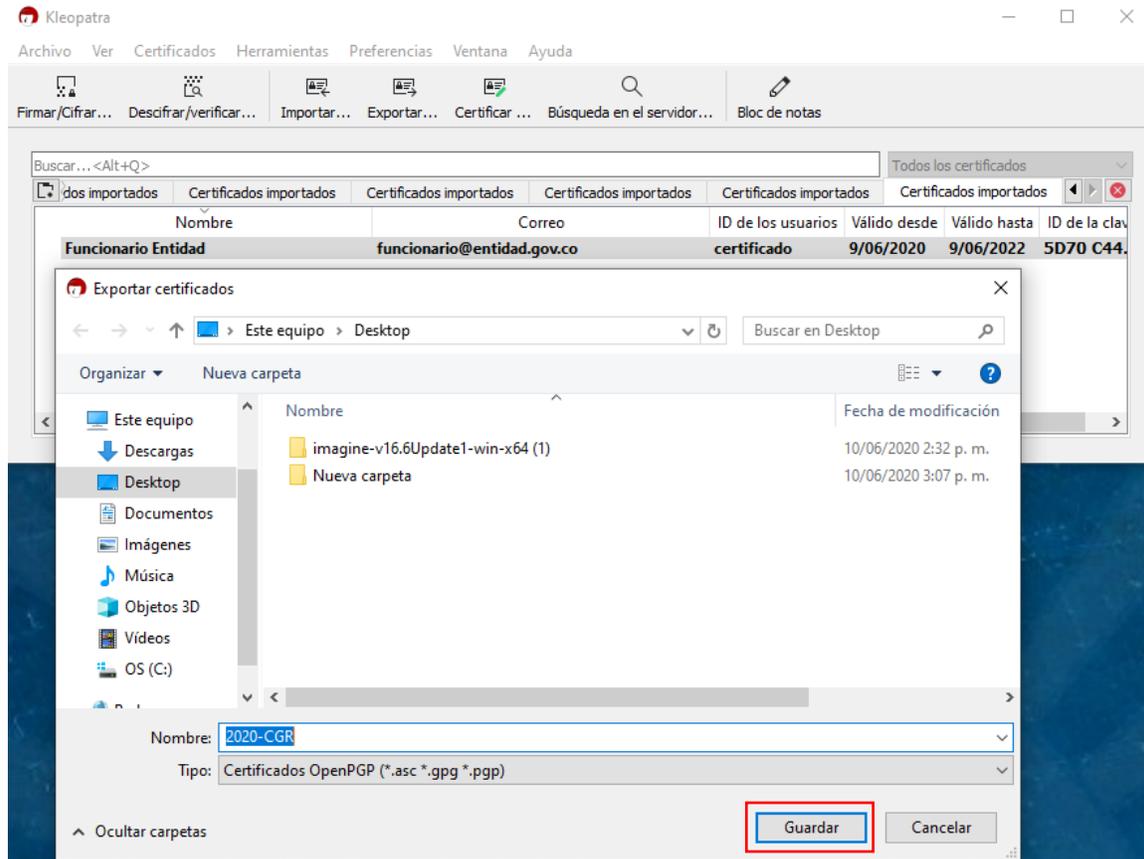


**Nota:** Si no es posible enviar la clave/llave pública con la opción **“Enviar clave pública por correo...”** seleccione el certificado y posteriormente la opción **“Exportar el certificado seleccionado (clave pública) a un archivo”**.

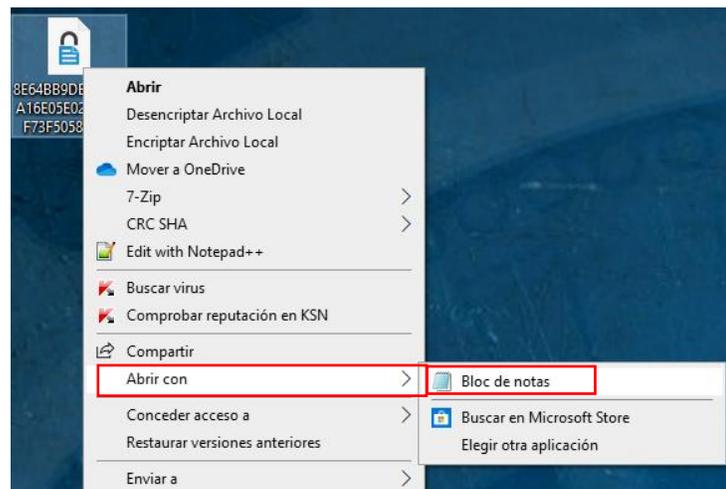


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>10</b>

Automaticamente se despliega una ventana para exportar los certificados donde solicita la ubicación donde se guardará la clave/llave, defina el nombre del archivo con el año y las siglas de su Entidad (por ejemplo (2020-CGR))

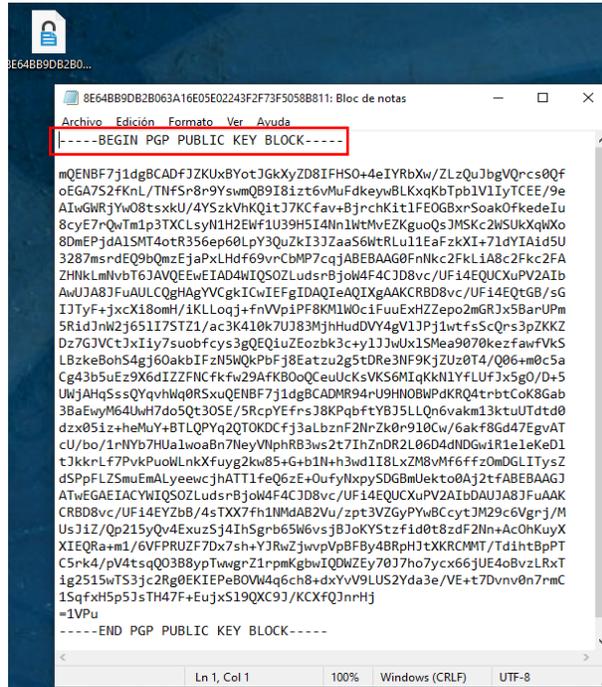


Inmediatamente se generará un archivo como el que se muestra en la imagen. Si desea verificar que ha exportado la clave/llave pública, haga clic derecho en el archivo y seleccione la opción **“Abrir con”** y seleccione **“Bloc de notas”**.

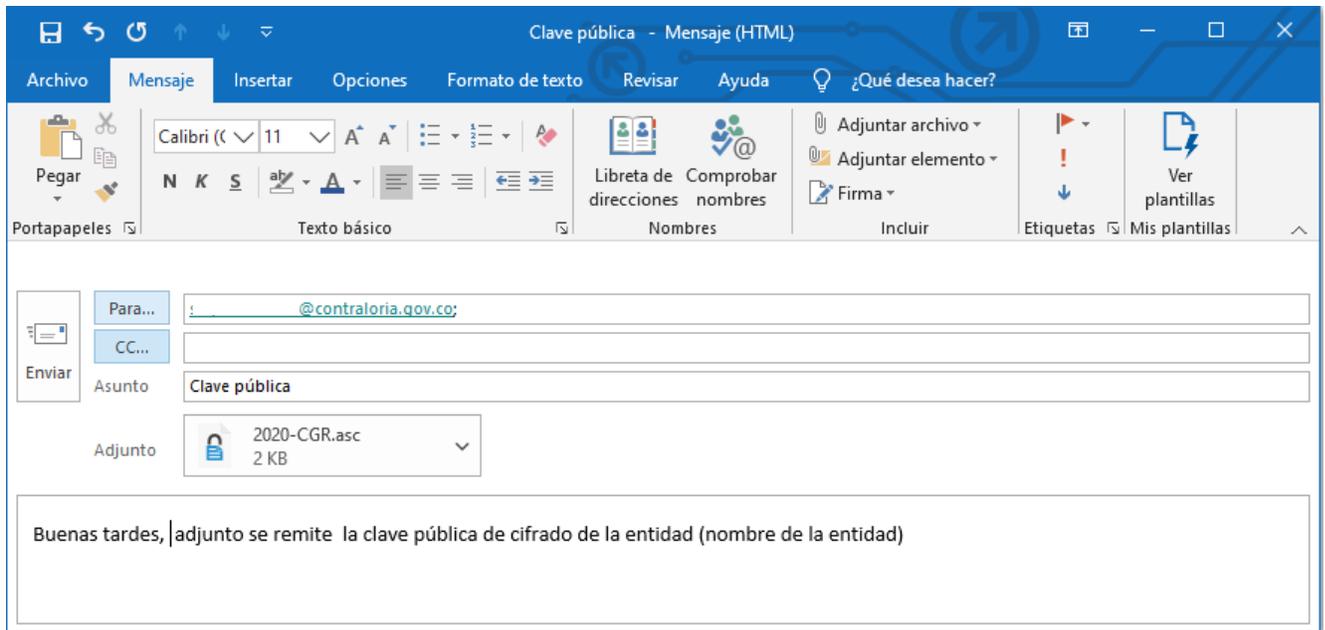


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>11</b>

El contenido del archivo será similar al de la imagen y en texto legible se leerá “-----BEGIN PGP PUBLIC KEY BLOCK-----”



4.2.9. Seleccione el archivo generado y envíelo al correo electrónico que haya sido definido por la contraloría General de la República para su envío.



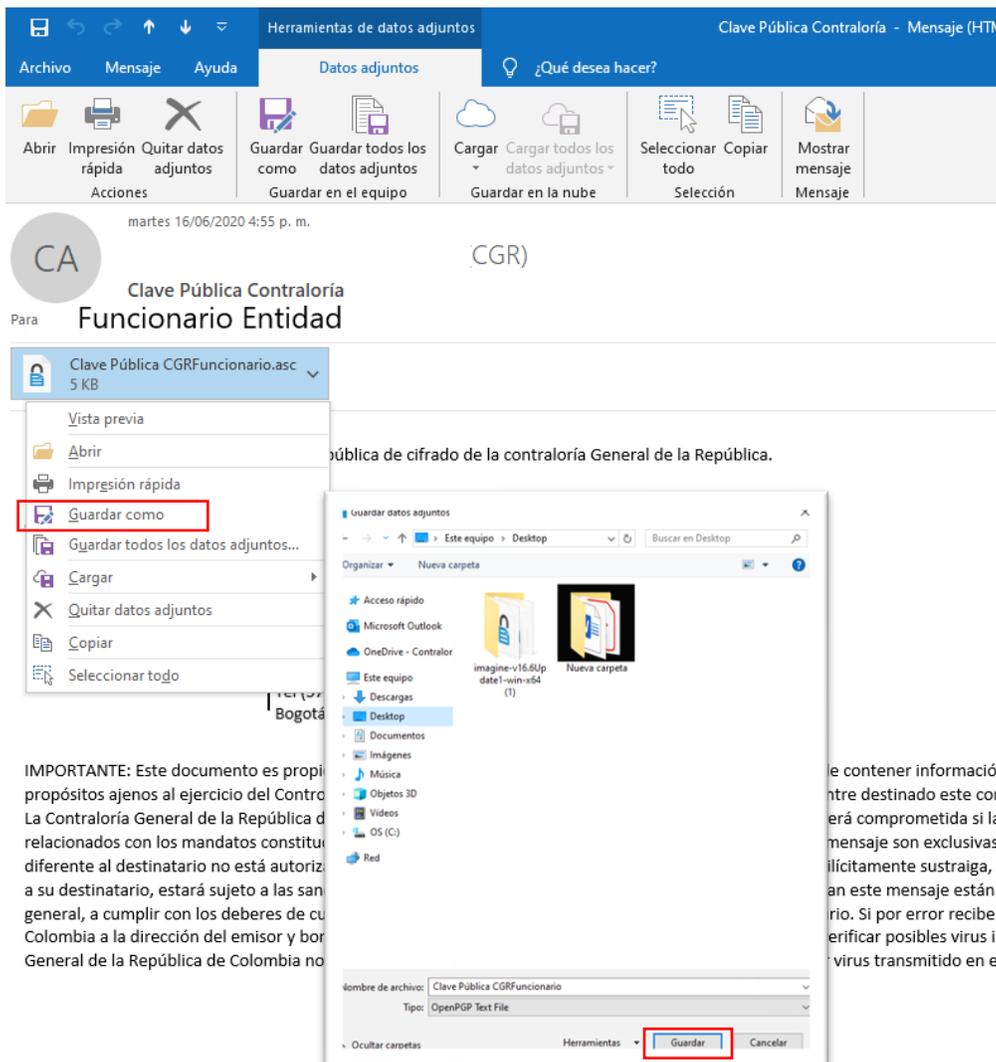
	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>12</b>

### 4.3. IMPORTAR CLAVE/LLAVE PÚBLICA

Si usted va a realizar la importación de la clave/llave Pública de cifrado de la Contraloría General de la República siga las instrucciones de este numeral, de lo contrario salte al numeral 4.4 cifrado de documentos y/o carpetas.

4.3.1. La importación de la clave/llave pública de la contraloría General de la República inicia con su recepción por correo electrónico, para ello la Entidad deberá tener el mismo software para poder seguir el presente instructivo.

Haga clic derecho sobre el archivo adjunto de la clave/llave pública y guárdelo.



martes 16/06/2020 4:55 p. m.

CA (CGR)

Clave Pública Contraloría  
Para Funcionario Entidad

Clave Pública CGRFuncionario.asc  
5 KB

Guardar como

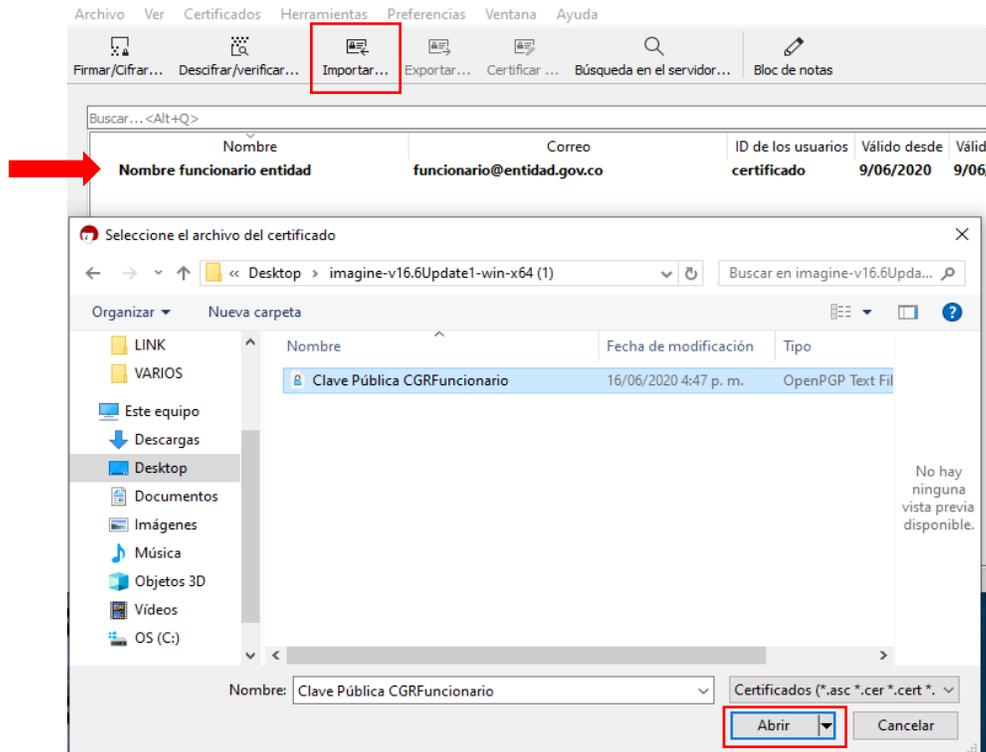
Guardar como  
Nombre de archivo: Clave Pública CGRFuncionario  
Tipo: OpenPGP Text File  
Guardar

**IMPORTANTE:** Este documento es propiedad de la Contraloría General de la República de Colombia y no debe ser utilizado para fines ajenos al ejercicio del Control. La Contraloría General de la República de Colombia no se responsabiliza por los daños o perjuicios relacionados con los mandatos constitucionales que no están autorizados a su destinatario, estará sujeto a las sanciones generales, a cumplir con los deberes de confidencialidad de la Contraloría General de la República de Colombia no debe ser utilizado para fines ajenos al ejercicio del Control.

Este documento contiene información confidencial y no debe ser divulgada ni utilizada para fines ajenos al ejercicio del Control. Si por error recibe este mensaje, se le solicita que no lo divulgue ni lo utilice para fines ajenos al ejercicio del Control. Si por error recibe este mensaje, se le solicita que no lo divulgue ni lo utilice para fines ajenos al ejercicio del Control.

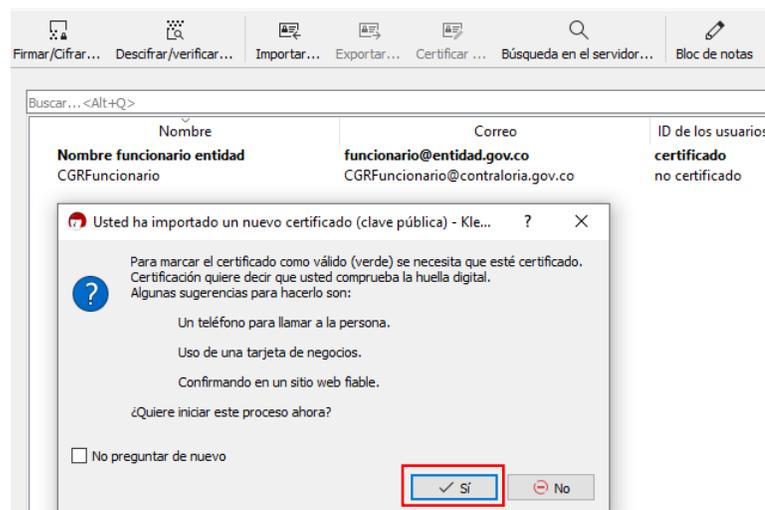
	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>13</b>

4.3.2. Haga clic en el icono importar, ubique la ruta donde guardó previamente la clave/llave pública remitida por la Contraloría General de la República, seleccionala y haga clic en la opción “Abrir”.



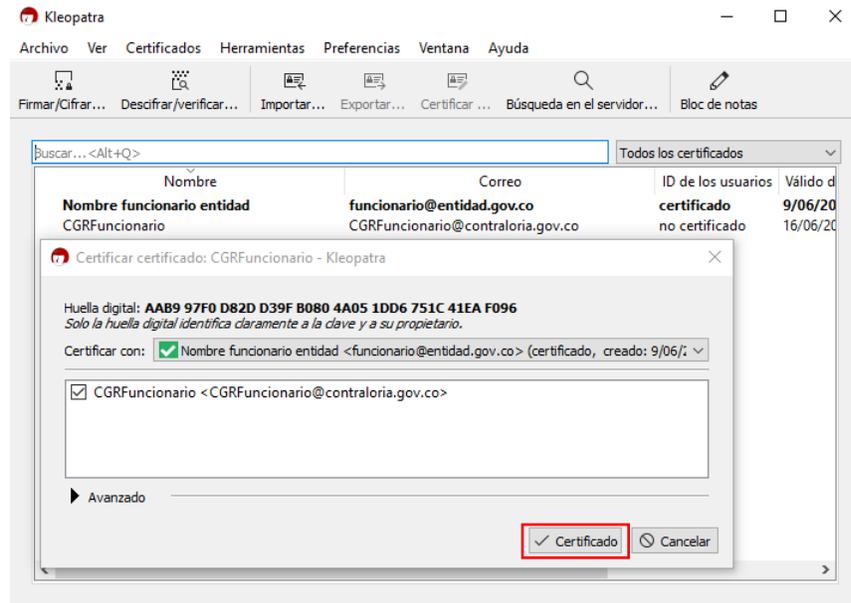
**Nota:** Si usted ha generado un par de claves/llaves previamente, su clave/llave privada aparecerá en la ventana de inicio del software Kleopatra en negrilla como se muestra en la imagen anterior.

4.3.3. Una vez importado la clave/llave pública aparecerá un mensaje para verificar su validez; realice la verificación a través de llamada telefónica al número que aparece en la firma del correo remitido por la Contraloría General de la República y posteriormente seleccione la opción “Sí”.

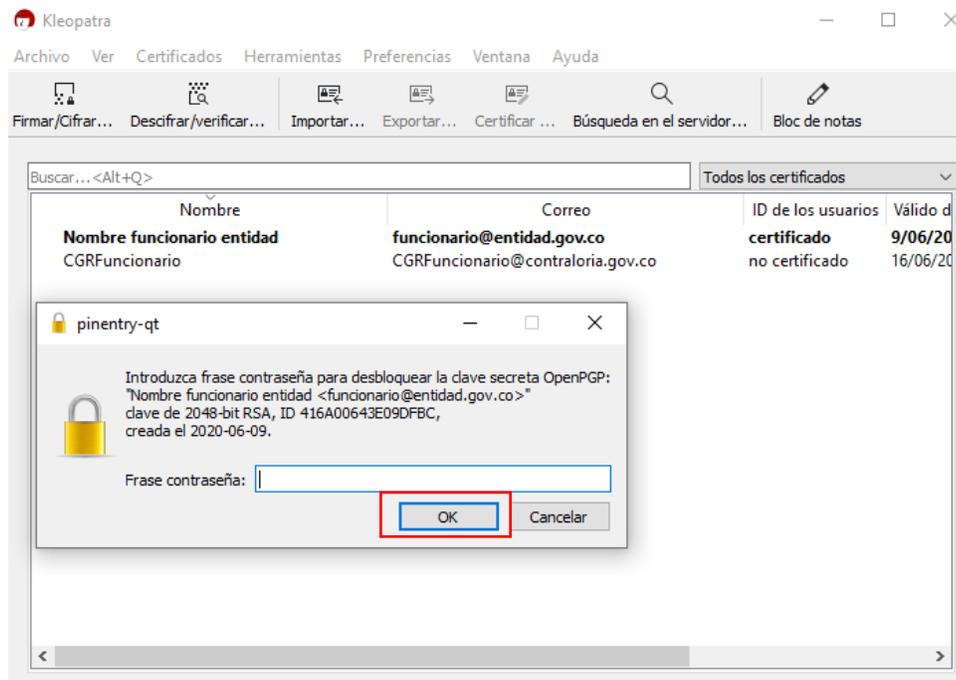


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>14</b>

4.3.4. Si ha verificado la validez de la clave/llave pública seleccione la opción **“Certificado”**.

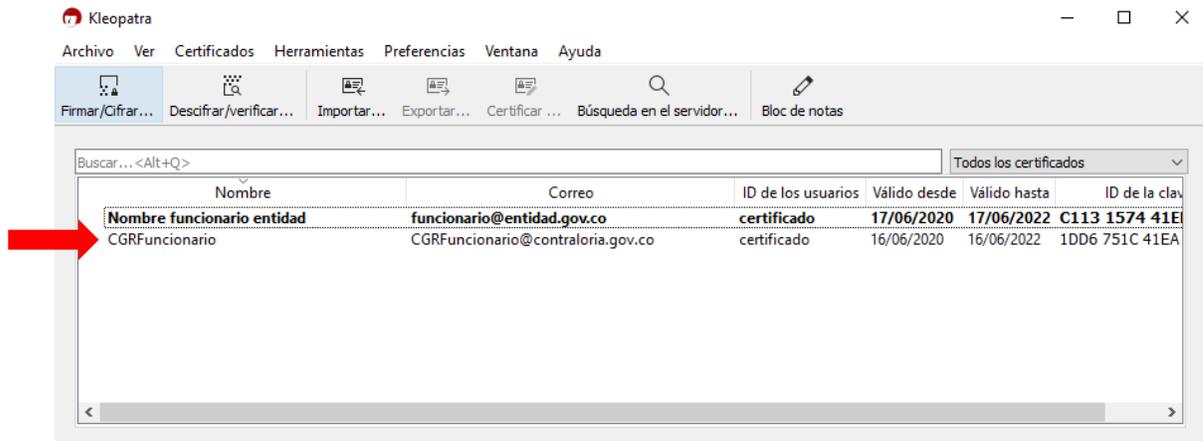


Inmediatamente se desplegará un cuadro de diálogo donde le solicitará la contraseña con la cual creó su clave/llave privada en el numeral 4.2.6. Una vez digitada seleccione la opción **“OK”**



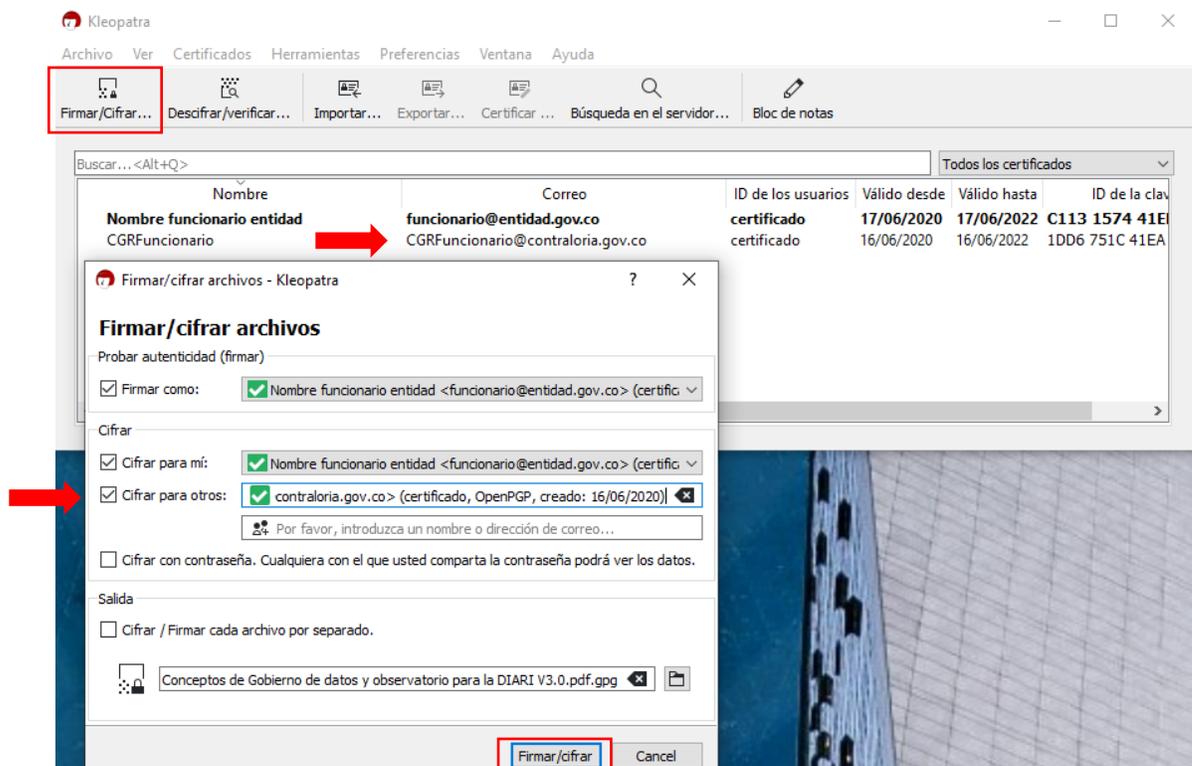
	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>15</b>

4.3.5. Una vez se ha certificado la validez de la clave/llave pública remitida por la Contraloría General de la República aparecerá relacionada en la ventana principal de la aplicación (sin negrilla).



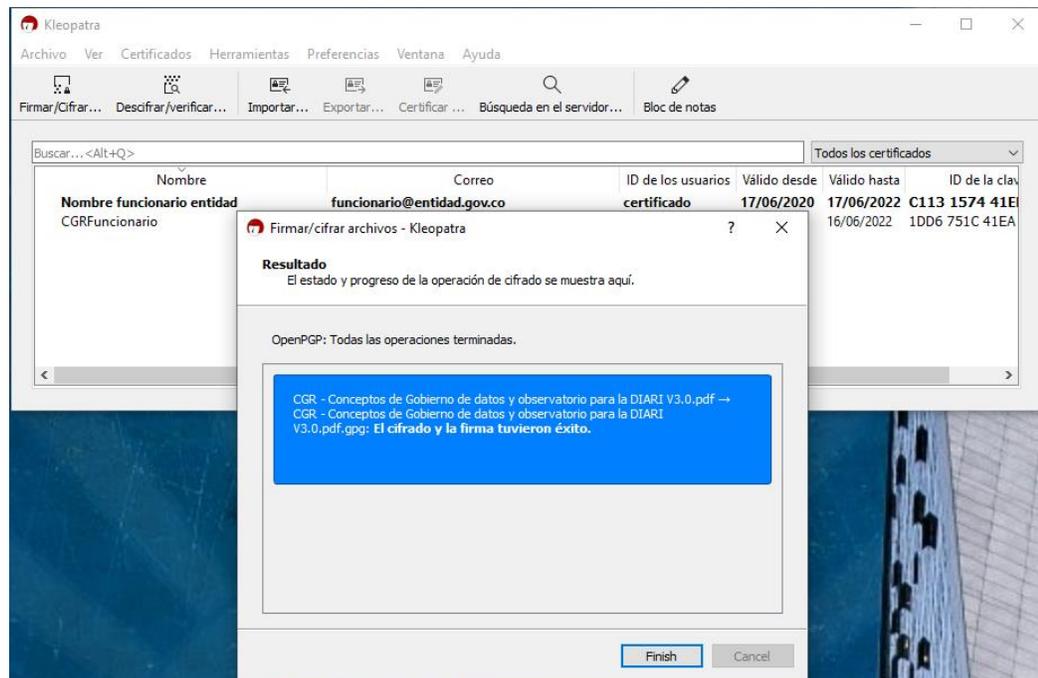
#### 4.4. CIFRAR Y FIRMAR DOCUMENTOS

4.4.1. Este paso se realiza cuando va a cifrar un documento y remitirlo a la Contraloría General de la República. Para cifrar un documento seleccione la opción **“Firmar y Cifrar”**, seleccione el documento que desea cifrar y coloque los parámetros requeridos en las casillas señaladas; en la opción cifrar para otros, ingrese los datos del correo que aparecen en la clave/llave pública remitida por la contraloría y seleccione la opción **“Firmar/cifrar”**.

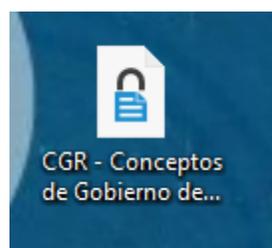


	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>16</b>

**Nota:** En el evento en que dentro del proceso de firma y cifrado de archivos le solicite una contraseña, digite la contraseña con la cual creó su clave/llave privada en el numeral 4.2.6. Una vez finalizado el proceso aparecerá un mensaje como el que se visualiza en la imagen:



4.4.2. Una vez cifrado el documento, se crea un archivo con un ícono como el observado en la imagen.

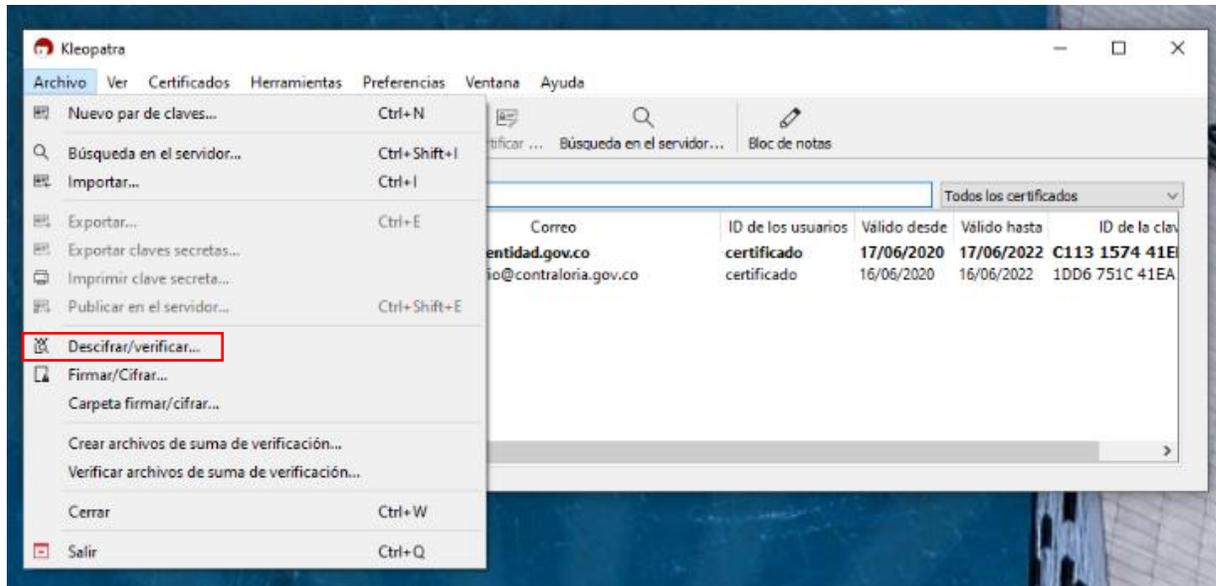


Esto significa que el archivo ha sido cifrado y puede enviarse al destinatario de la Contraloría General de la República por medio de correo electrónico.

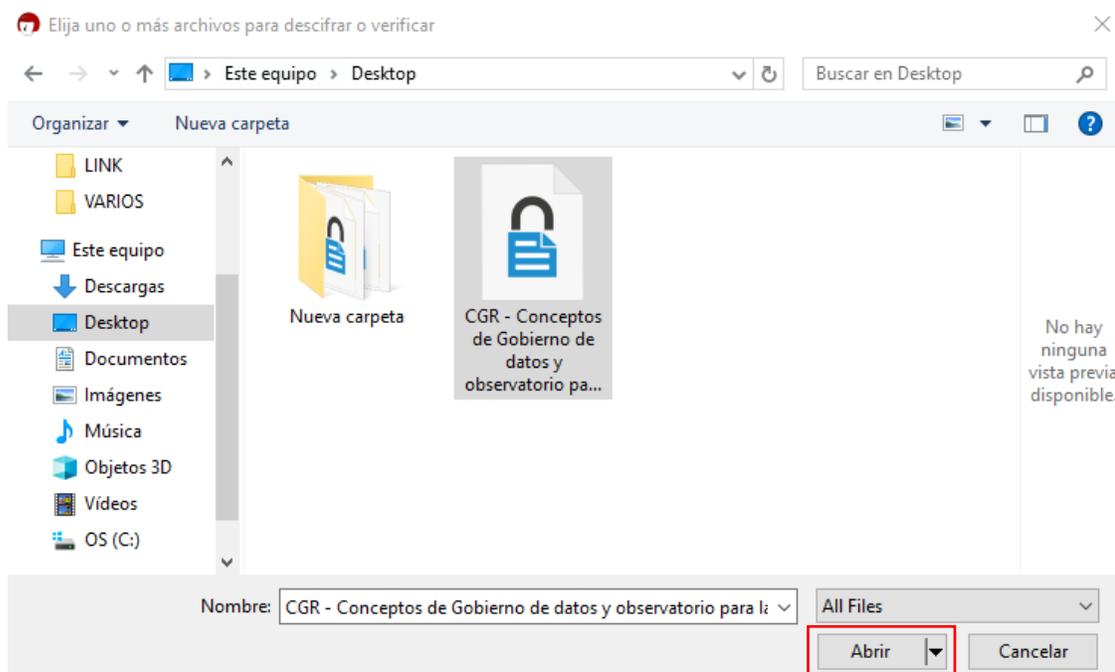
	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>17</b>

## 4.5. DESCIFRAR DOCUMENTOS

4.5.1. Una vez recibido el archivo, abra la aplicación y seleccione del menú **“Archivo”** la opción **“Descifrar/Verificar”**.

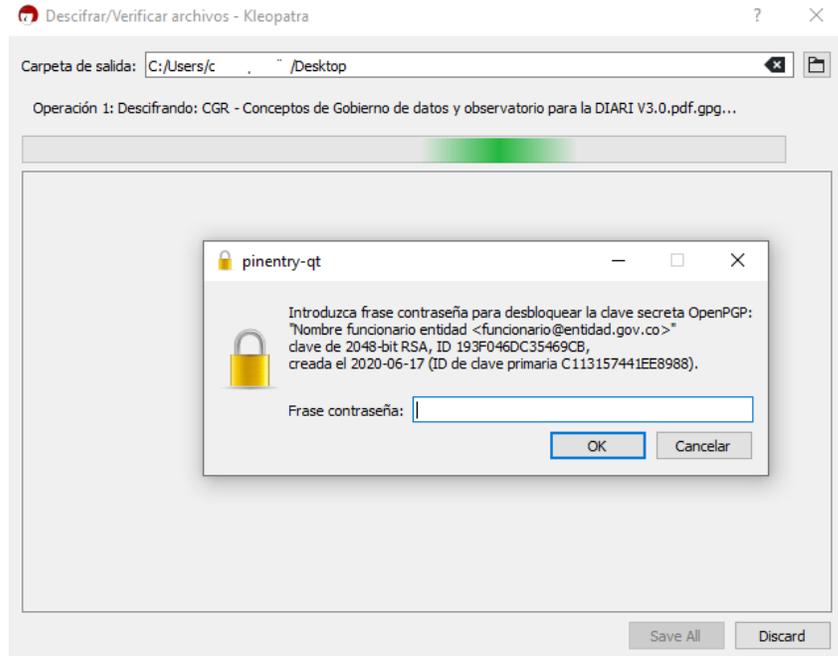


Ubique la ruta donde se encuentra el archivo a descifrar, selecciónelo y haga clic en **“Abrir”**.



	<b>Macroproceso:</b>		<b>Proceso:</b>
	<b>Instructivo de instalación y uso de herramienta de cifrado de información Gpg4win</b>		
	<b>Código:</b>	<b>Versión: 1.0</b>	<b>18</b>

Inmediatamente se desplegará un cuadro de diálogo donde le solicitará la contraseña con la cual creó su clave privada en el numeral 4.2.6. Digitela y haga clic en **“OK”**.



Una vez ingresada la contraseña le aparecerá la siguiente ventana, seleccione la opción **“Save All”**. Inmediatamente se guardará el archivo sin cifrar en la misma ruta donde guardó el archivo cifrado.

