



AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

INSTRUCTIVO DE CIFRADO DE DOCUMENTOS - PGP

BOGOTÁ D.C. JUNIO DE 2021



TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES.....	3
4. CONSIDERACIONES GENERALES.....	3
5. CIFRADO DE DOCUMENTOS	3
6. INSTALACIÓN DE GPG4WIN.....	3
7. CREACIÓN DE UN PAR DE CLAVES UTILIZANDO KLEOPATRA.....	4
8. EXPORTAR LA CLAVE COMPARTIDA (CLAVE PÚBLICA)	7
9. EXPORTAR LA CLAVE SECRETA.....	9
10. IMPORTAR UNA CLAVE.....	10
11. CIFRAR UN ARCHIVO CON UNA CLAVE PÚBLICA	12
12. DESCIFRAR UN ARCHIVO CON UNA CLAVE SECRETA.....	13

 ARN AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN	INSTRUCTIVO DE CIFRADO DE DOCUMENTOS - PGP	CÓDIGO: TI-I-01	
		FECHA 2021-06-03	VERSIÓN V- 1

1. OBJETIVO

Brindar información y explicar el paso a paso para la instalación de GPG4Win, la generación de claves de OpenGPG y exportación de clave pública.

2. ALCANCE

Este instructivo aplica para los funcionarios de la Entidad, que requieren realizar cifrado de información en el marco de sus funciones.

3. DEFINICIONES

CIFRADO O ENCRIPCIÓN: Consiste en la acción de transformar la información de archivos en cualquier formato, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta

CONTRASEÑA: Es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso o archivo.

FORMATO DE ARCHIVO: Es un estándar que define la forma en que la información se organiza y se codifica en un archivo informático

PGP: Es un programa cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública.

4. CONSIDERACIONES GENERALES

El presente documento tiene una primera versión del 4 de junio de 2020, como un documento complementario. A partir del mes de mayo de 2021 pasa a ser un documento controlado en su primera versión.

5. CIFRADO DE DOCUMENTOS

El presente documento ilustra paso a paso cómo se debe realizar la instalación, configuración, creación de claves y exportación de claves de GPG.

6. INSTALACIÓN DE GPG4WIN

1. Descargar gpg4win desde <https://www.gpg4win.de/>.
2. Instalar GpgWin incluyendo las siguientes opciones: GnuPG, Kleopatra y GpgEx (requiere reiniciar el sistema una vez finalizada la instalación):

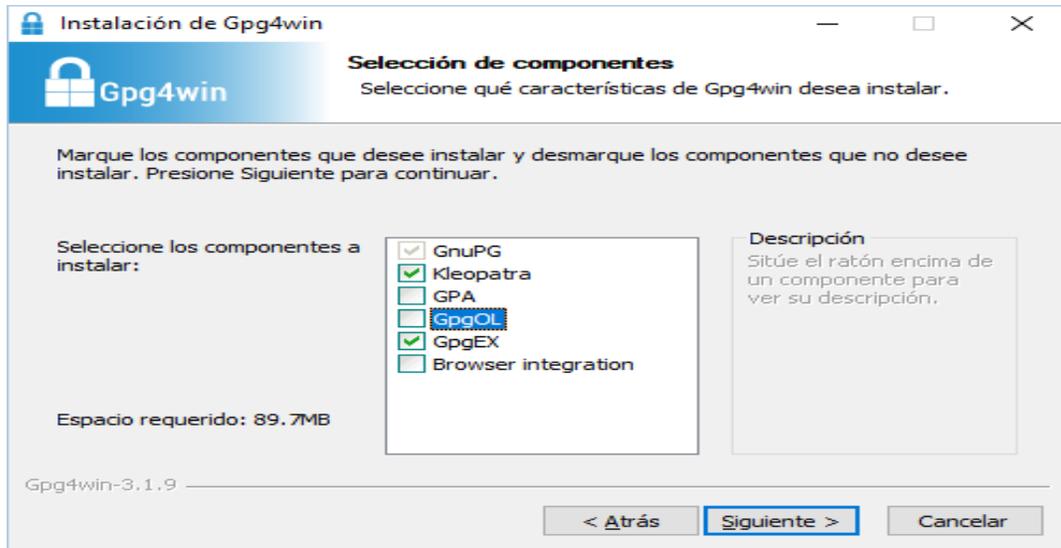


Ilustración 1 Instalación de Gpg4Win.

7. CREACIÓN DE UN PAR DE CLAVES UTILIZANDO KLEOPATRA

1. Iniciar Kleopatra:

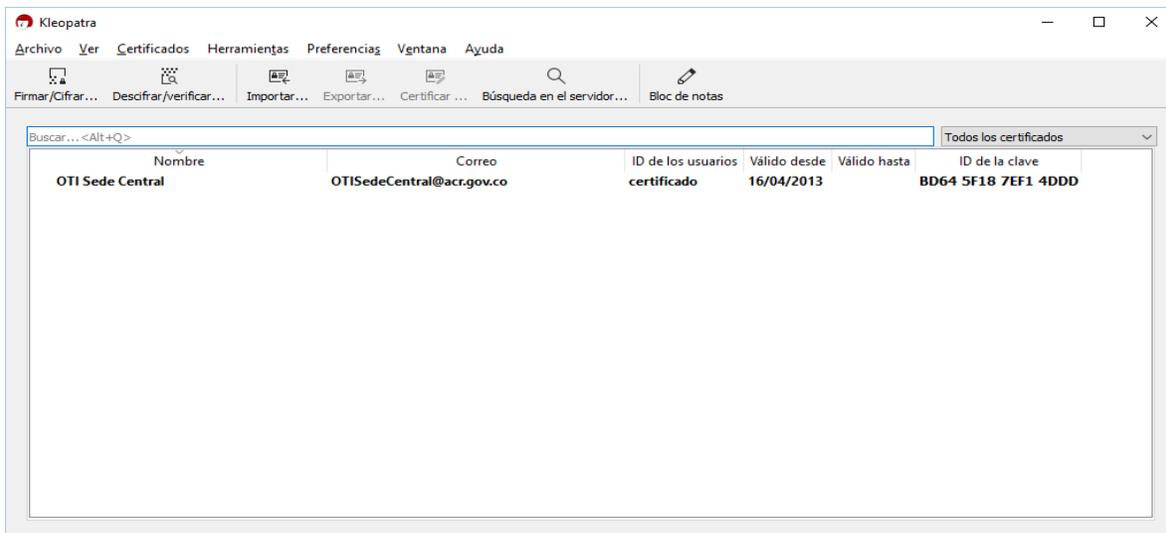


Ilustración 2 Ventana de inicio de Kleopatra.

2. En el menú seleccionar Archivo > Nuevo par de claves:

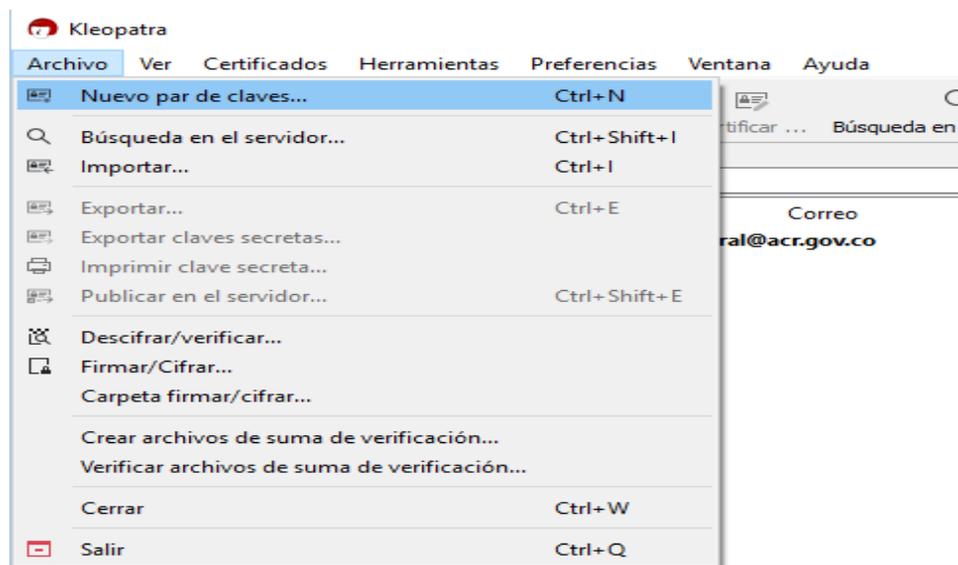


Ilustración 3 Nuevo par de claves

3. En elegir formato seleccione Crear un par de claves personales OpenPGP:

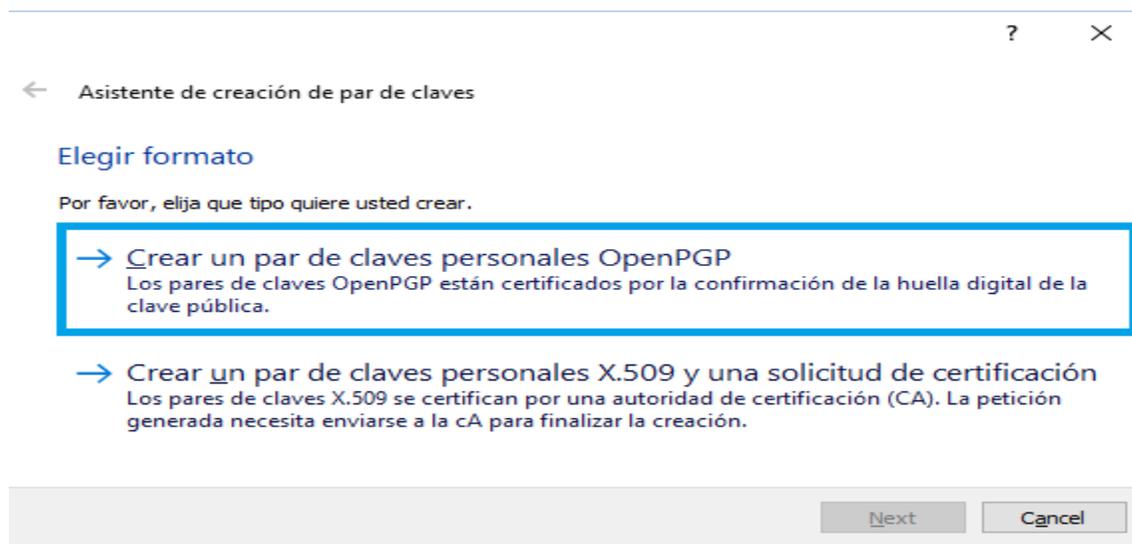


Ilustración 4 Crear un par de claves personales OpenPGP

4. En "Introduzca detalles", escriba el nombre y el correo electrónico. Oprima el botón Next.

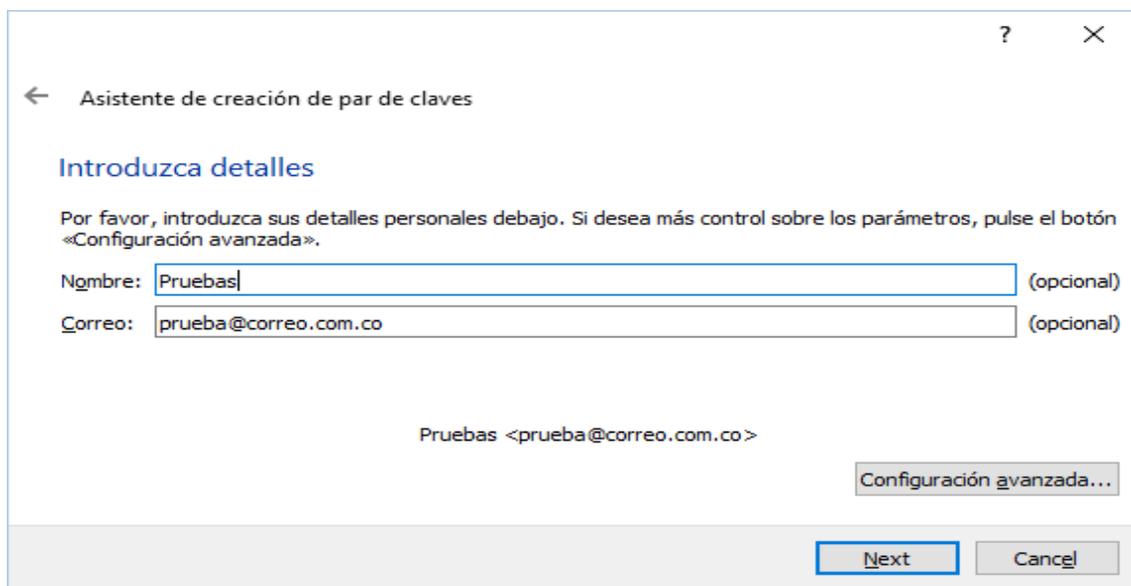


Ilustración 5 Introducir detalles del par de claves

- En "Parámetros de revisión" oprima el botón Crear.

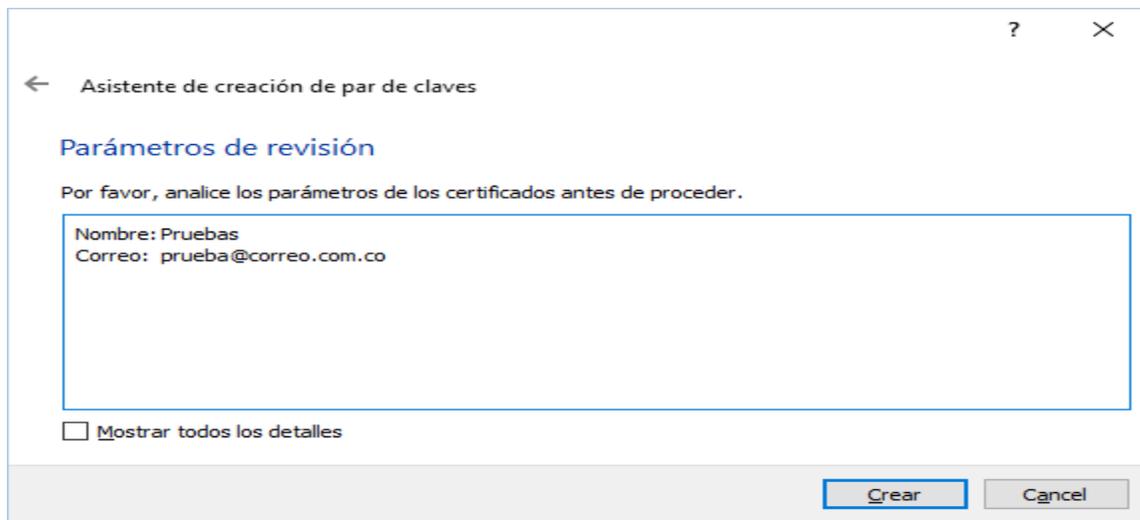


Ilustración 6 Parámetros de revisión del par de claves

- En "Creando par de claves" suministre una contraseña para el par de claves. Oprima el botón Ok:

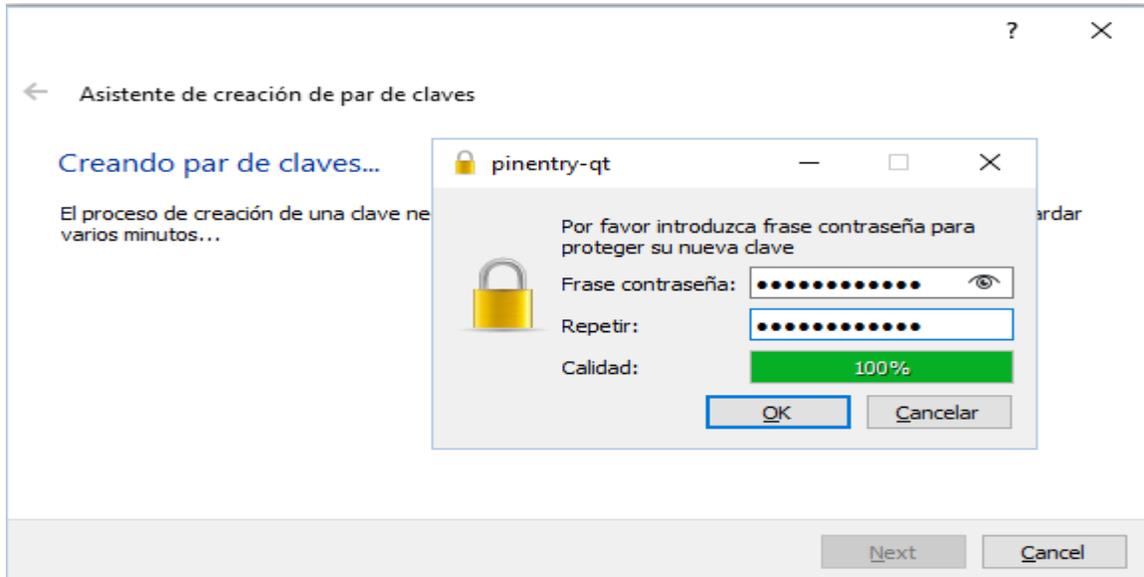


Ilustración 7 Crear contraseña para el par de claves

7. En "Par de claves creado con éxito" oprima el botón Finish:

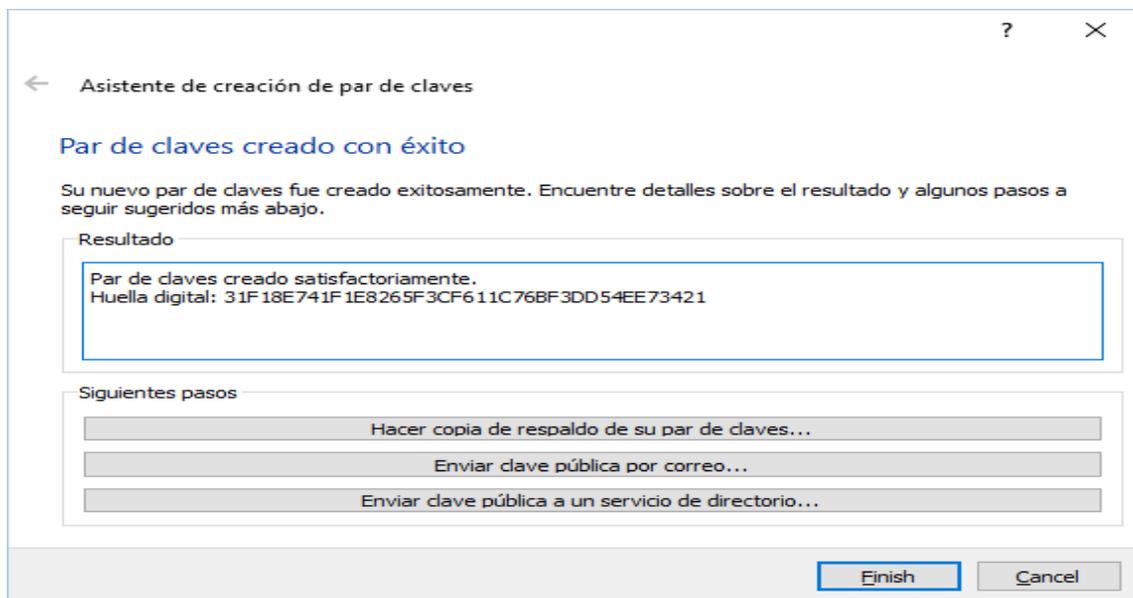


Ilustración 8 Par de claves creado con éxito.

8. EXPORTAR LA CLAVE COMPARTIDA (CLAVE PÚBLICA)

1. En Kleopatra, seleccione el Certificado que desea exportar:

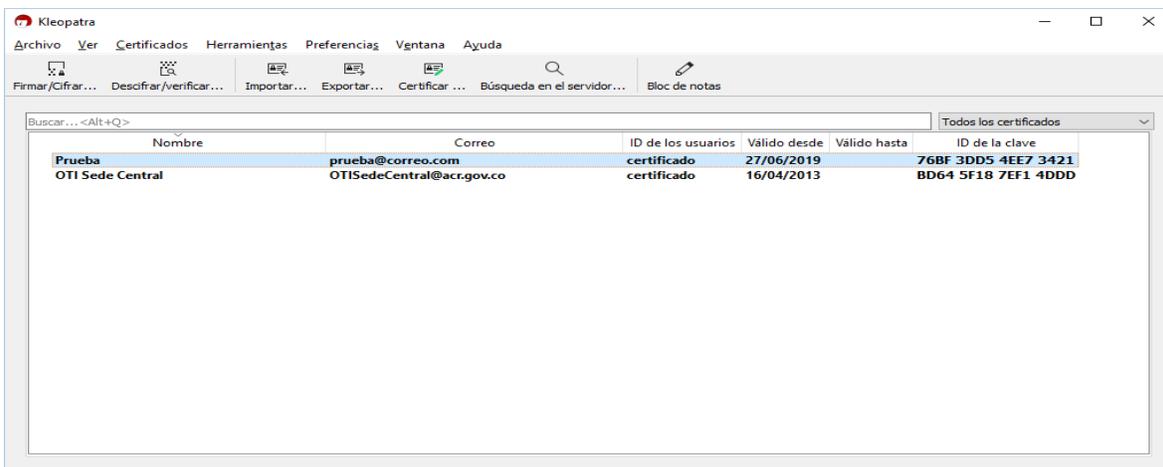


Ilustración 9 Seleccionar el certificado en Kleopatra para exportar la clave pública.

2. Desplegar el menú contextual, haciendo clic con el botón derecho del ratón sobre el nombre del certificado que desea exportar y seleccione la opción Exportar:

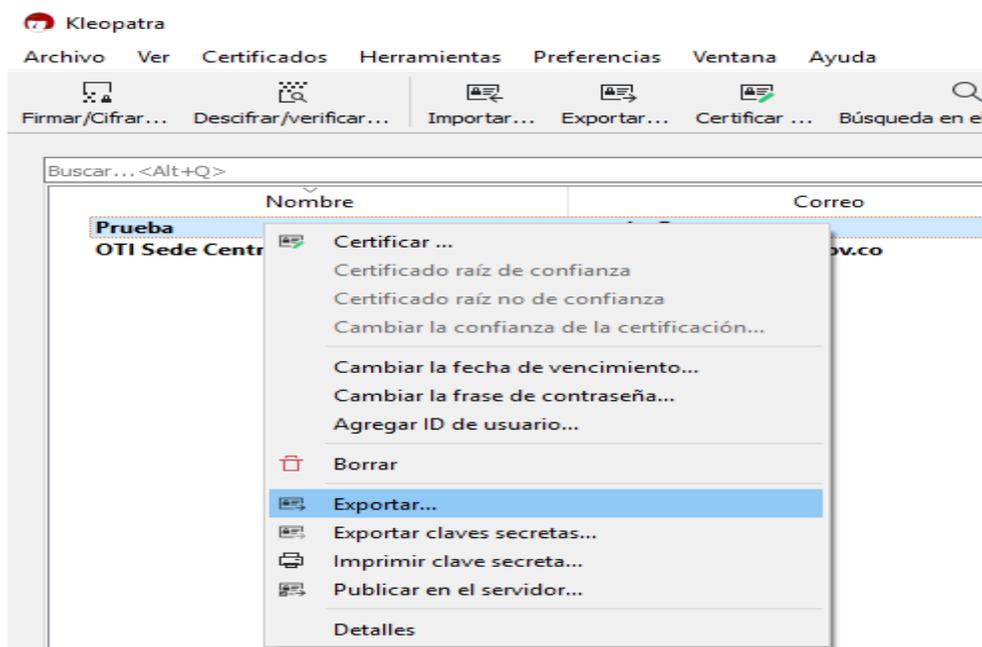


Ilustración 10 Menú contextual para exportar la clave pública.

3. Guardar el archivo de la clave pública con el nombre y en la ubicación de su preferencia:

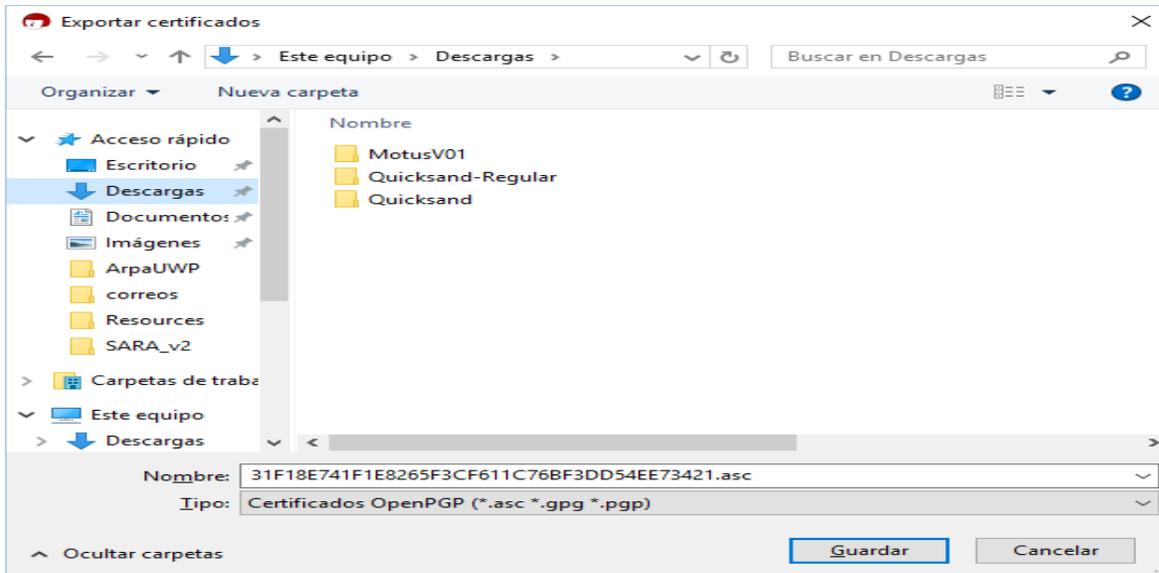


Ilustración 11 Guardar el archivo de la clave pública

9. EXPORTAR LA CLAVE SECRETA

Nota: La clave secreta debe ser almacenada en un lugar seguro y no debe ser compartida con nadie.

1. En Kleopatra, seleccione el Certificado que desea exportar:

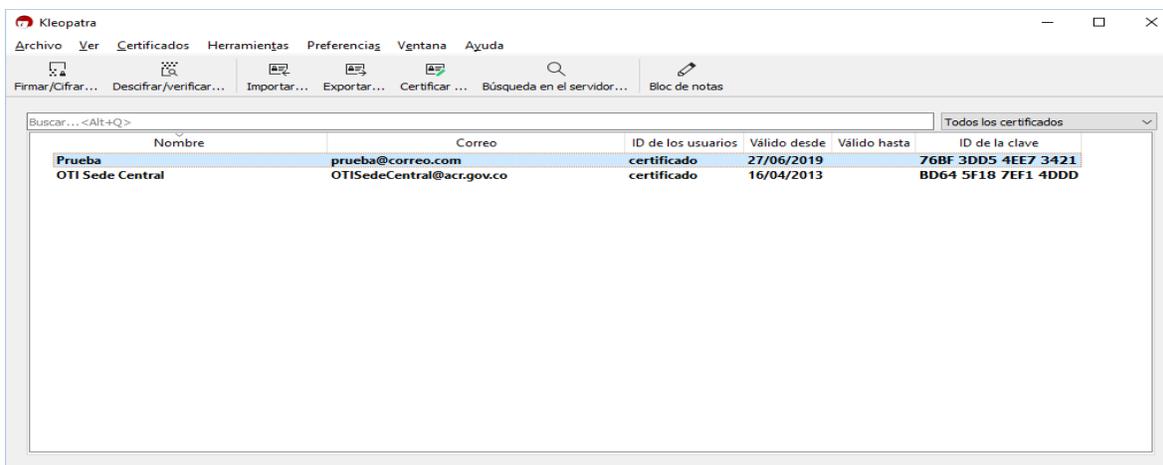


Ilustración 12 Seleccionar el certificado en Kleopatra para exportar la clave privada

2. Desplegar el menú contextual, haciendo clic con el botón derecho del ratón sobre el nombre del certificado que desea exportar y seleccione Exportar claves secretas:

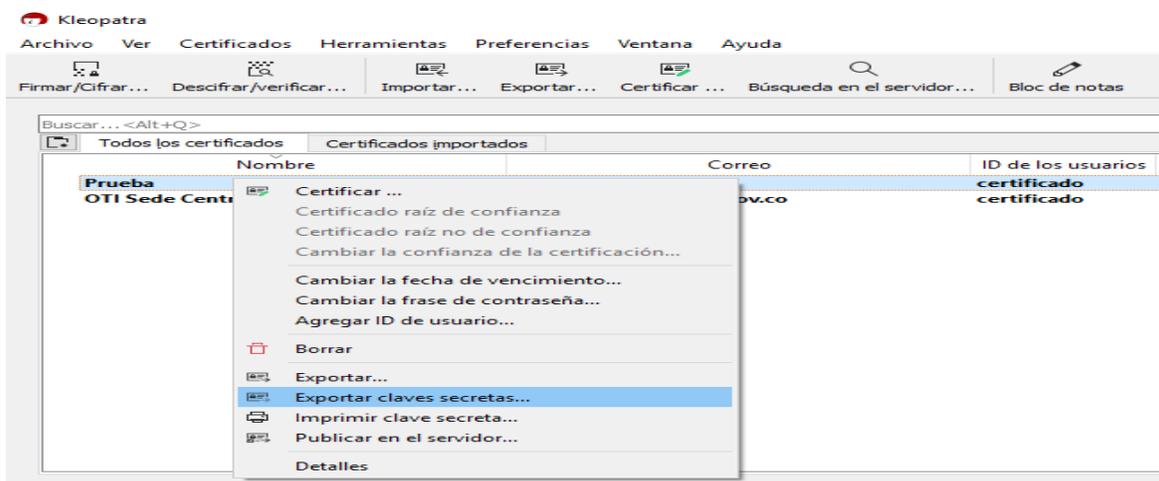


Ilustración 13 Menú contextual para exportar las claves secretas

3. Guardar el archivo de la clave secreta con el nombre y en la ubicación de su preferencia:

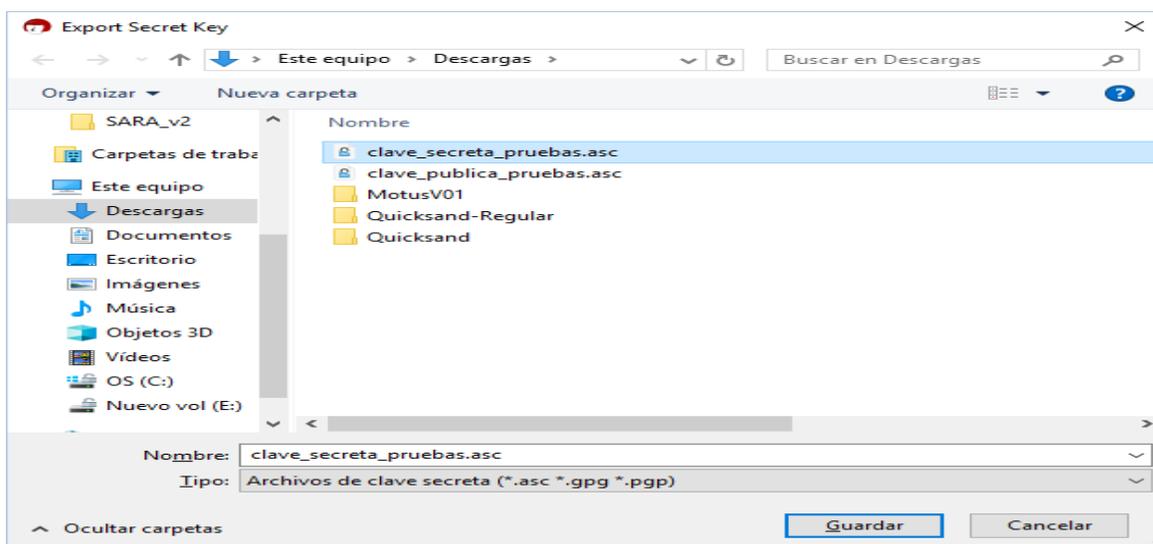


Ilustración 14 Guardar el archivo de la clave secreta.

10. IMPORTAR UNA CLAVE.

1. Para importar una clave, inicie Kleopatra y en el menú seleccione Archivo > Importar:

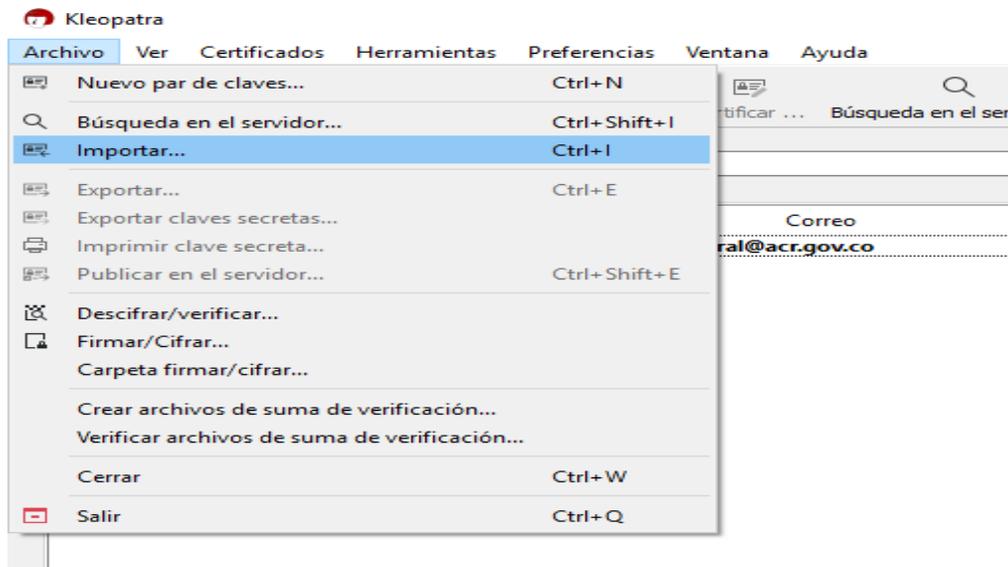


Ilustración 15 Menú para importar una clave en Kleopatra.

2. Seleccione el archivo a importar y haga clic en el botón Abrir:

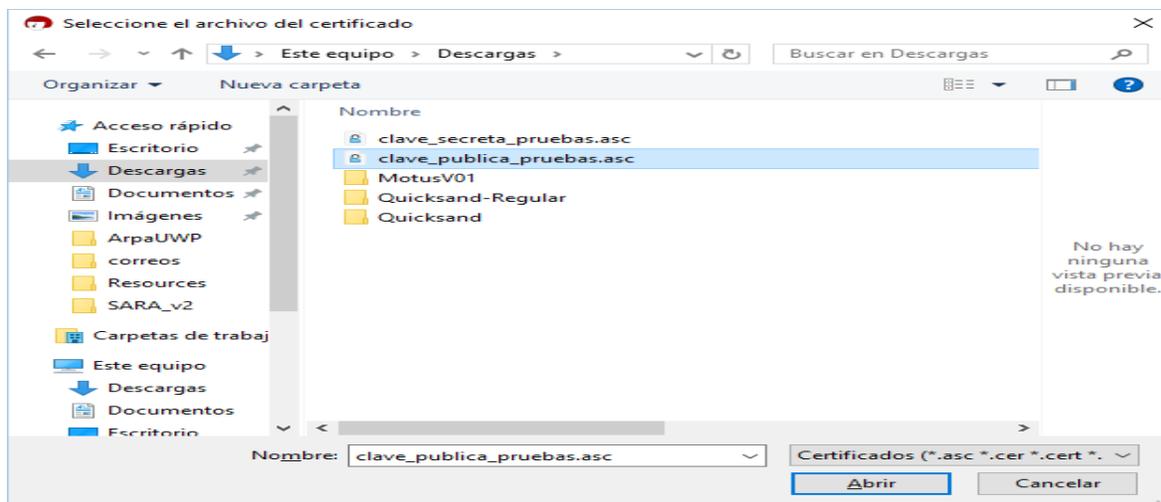


Ilustración 16 Seleccionar el archivo de clave para importar.

3. Al importar el archivo, Kleopatra le preguntará si desea marcar el certificado como válido. Haga clic en el botón No.

11. CIFRAR UN ARCHIVO CON UNA CLAVE PÚBLICA

1. En Kleopatra, en el menú Archivo seleccione la opción Firmar/Cifrar

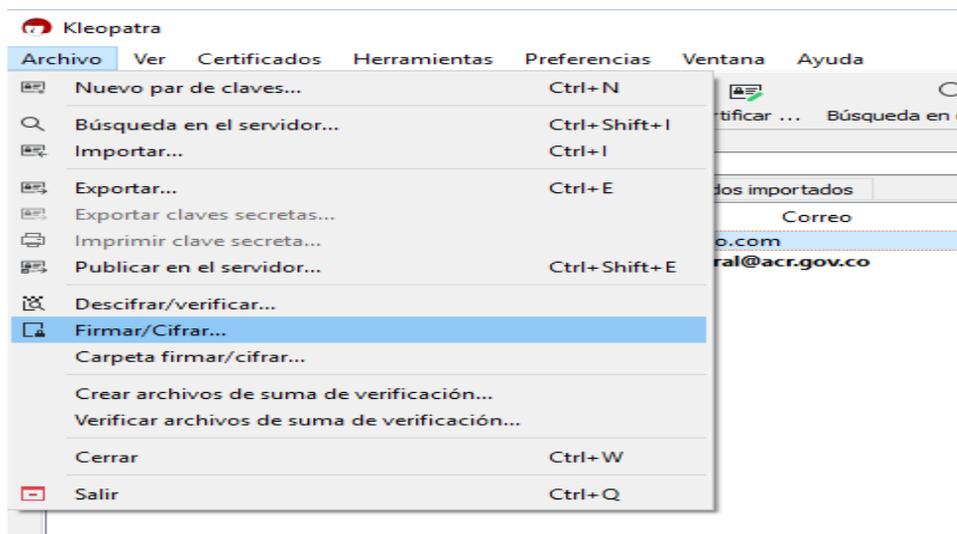


Ilustración 17 Menú para cifrar un archivo en Kleopatra.

2. Seleccione el archivo para cifrar y oprima el botón Abrir:

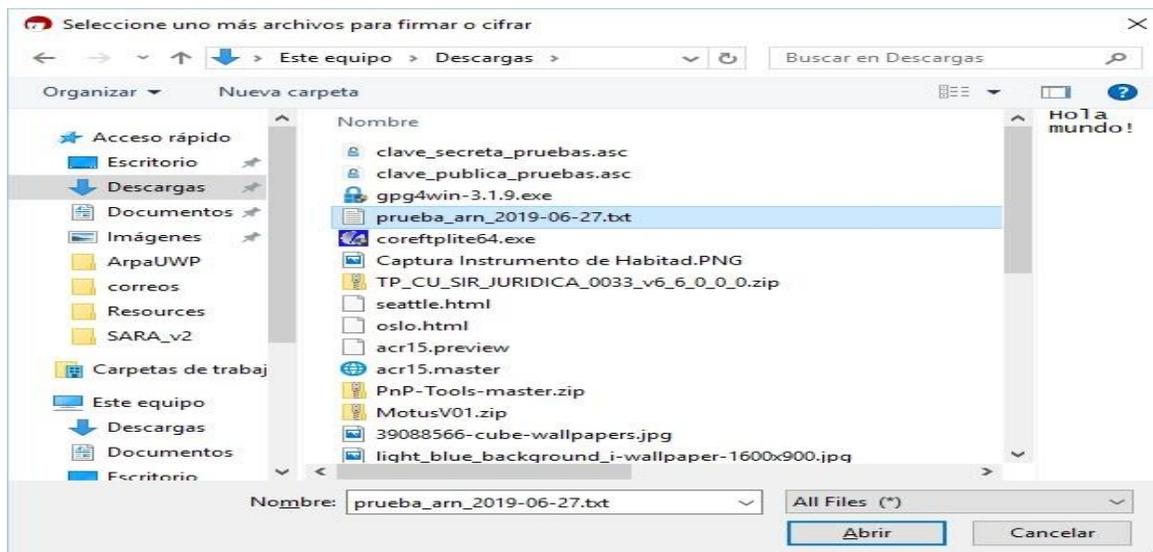


Ilustración 18 Abrir archivo para cifrar con Kleopatra.

3. En la ventana Firmar/cifrar archivos solo debe estar seleccionada la opción Cifrar para otros y se debe seleccionar la clave pública con la que se desea cifrar. Hacer clic en el botón Cifrar:

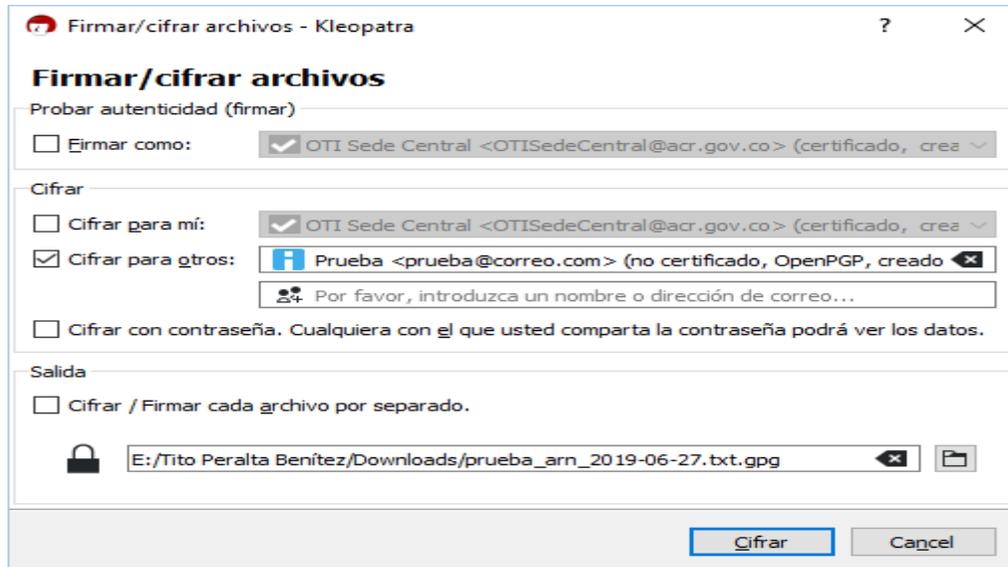


Ilustración 19 Seleccionar clave pública para el cifrado

4. Cuando se complete el cifrado, se muestra un mensaje informativo indicando el éxito de la operación:

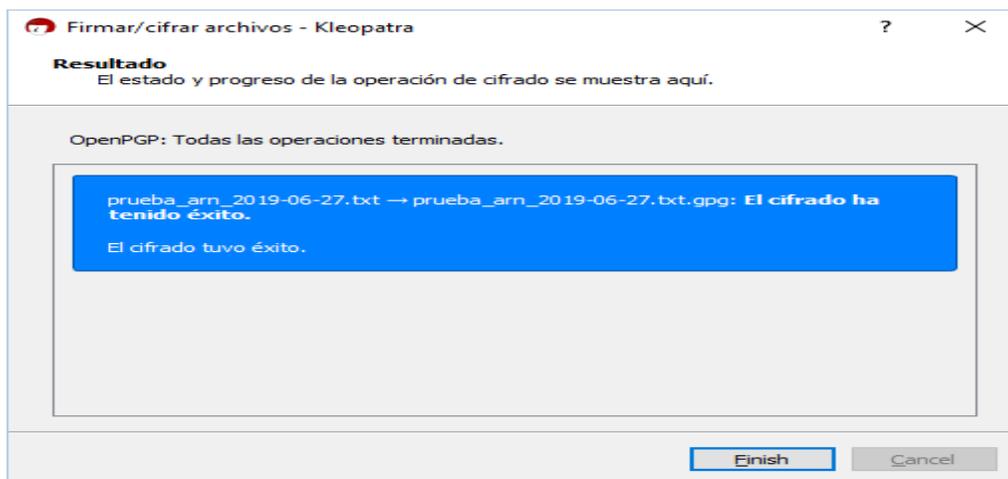


Ilustración 20 Mensaje que se muestra cuando se completa el cifrado de un archivo.

12. DESCIFRAR UN ARCHIVO CON UNA CLAVE SECRETA.

Nota: Para descifrar un archivo debe tener importada la clave secreta y conocer la contraseña del certificado. Para más información, consulte la sección Creación de un par de claves utilizando Kleopatra.

1. En Kleopatra, en el menú Archivo seleccione la opción Descifrar/Verificar:

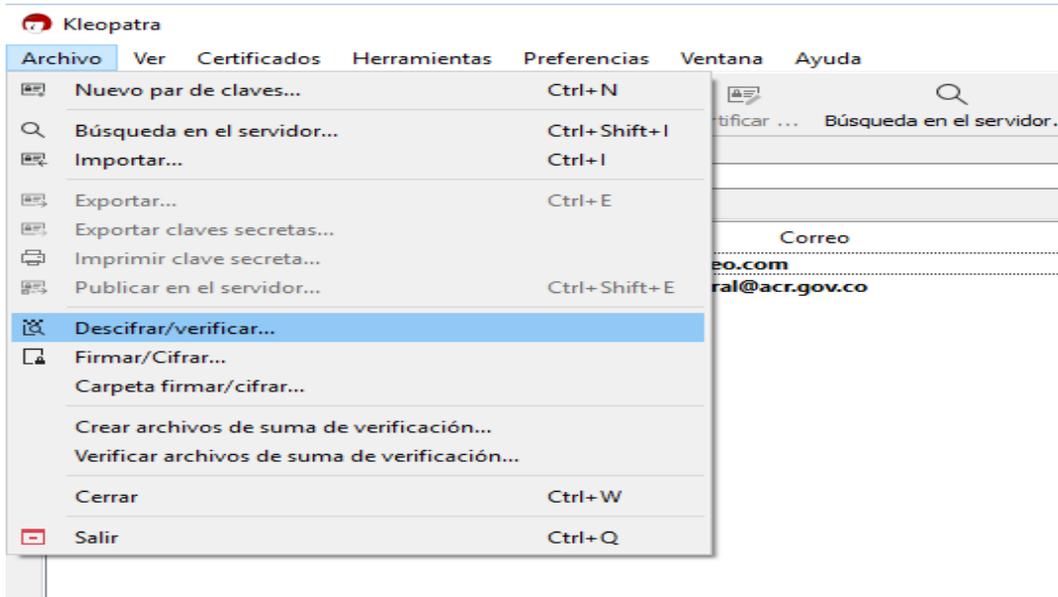


Ilustración 21 Menú para descifrar un archivo en Kleopatra.

2. Seleccione el archivo que quiere descifrar y oprima el botón Abrir:

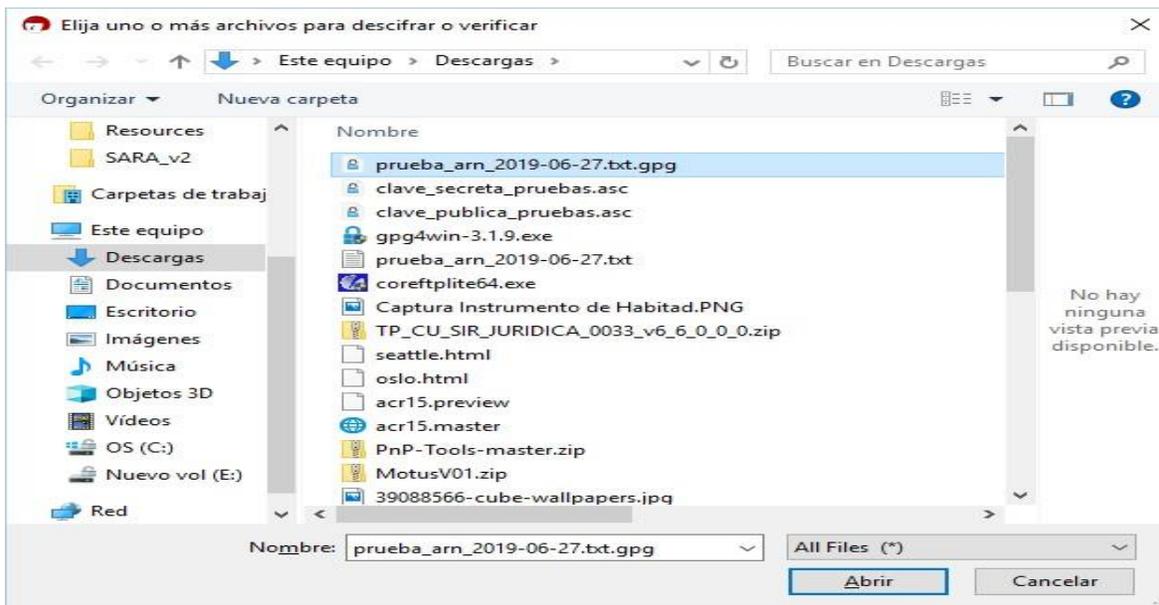


Ilustración 22 Abrir archivo para descifrar en Kleopatra

3. Cuando abra el archivo, le solicita la contraseña de la clave privada:

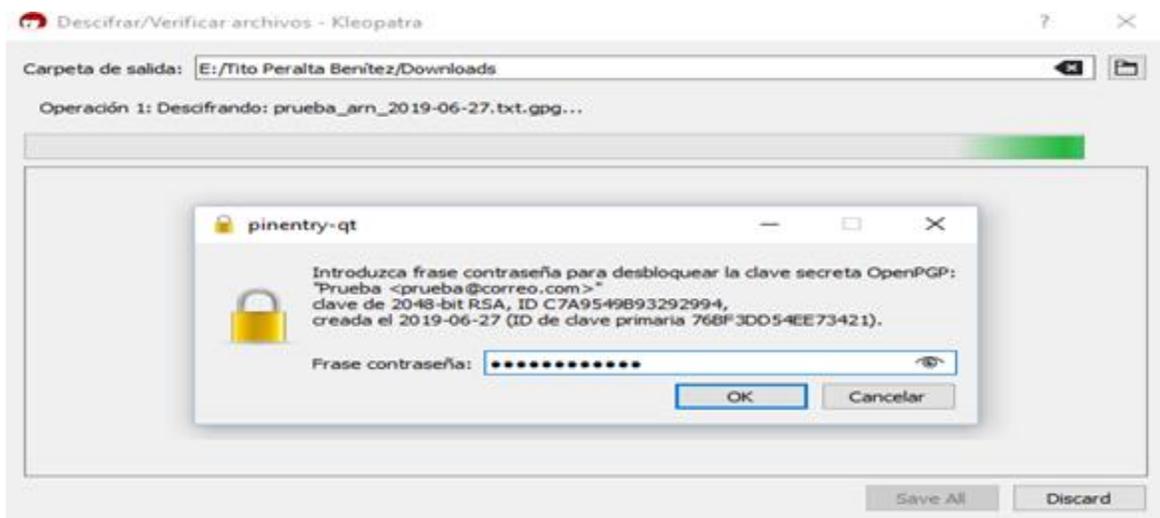


Ilustración 23 Insertar la contraseña de la clave privada

4. Si ingresó la contraseña correctamente, Kleopatra le informa que el archivo fue descifrado. Oprima el botón Save All para guardar el archivo en la ubicación Carpeta de salida:

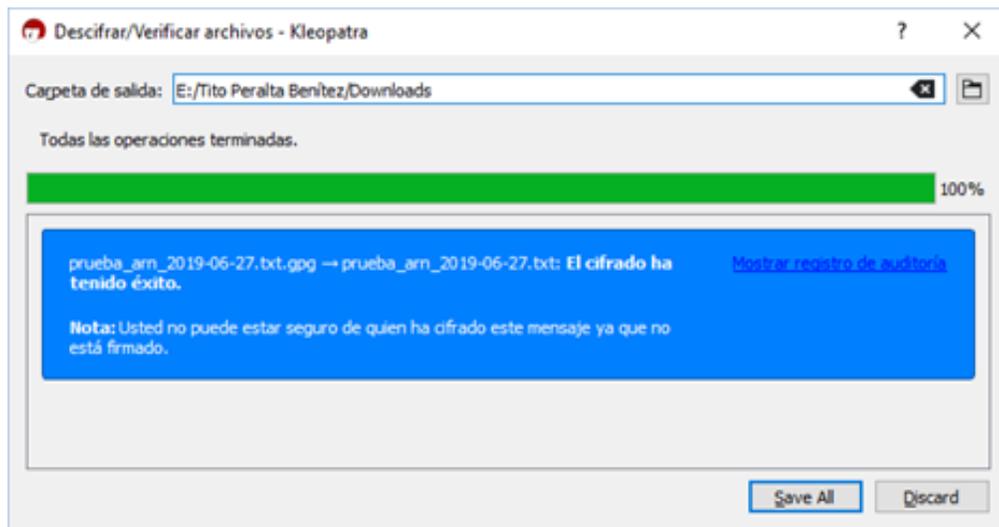


Ilustración 24 Mensaje informando que el archivo fue descifrado correctamente.