GUÍA PARA GENERACIÓN DE LLAVES PÚBLICAS PGP PARA INTERCAMBIO DE COMUNICACIONES CIFRADAS.

Descripción

Este documento es una guía referencial para la generación de llaves públicas PGP, que serán utilizadas para el intercambio de comunicaciones cifradas mediante correo electrónico, entre el EcuCERT y los prestadores de servicios de telecomunicaciones respecto de la gestión de vulnerabilidades e incidentes, en cumplimiento a lo establecido en la norma técnica de gestión de incidentes y vulnerabilidades

Requisitos

Para la generación y administración de llaves públicas PGP se requiere los siguientes elementos:

- Computador con sistema operativo Windows.
- Programa GPG4Win. Descargable en https://gpg4win.org/thanks-for-download.html.

Contenido

Este documento está estructurado de la siguiente manera:

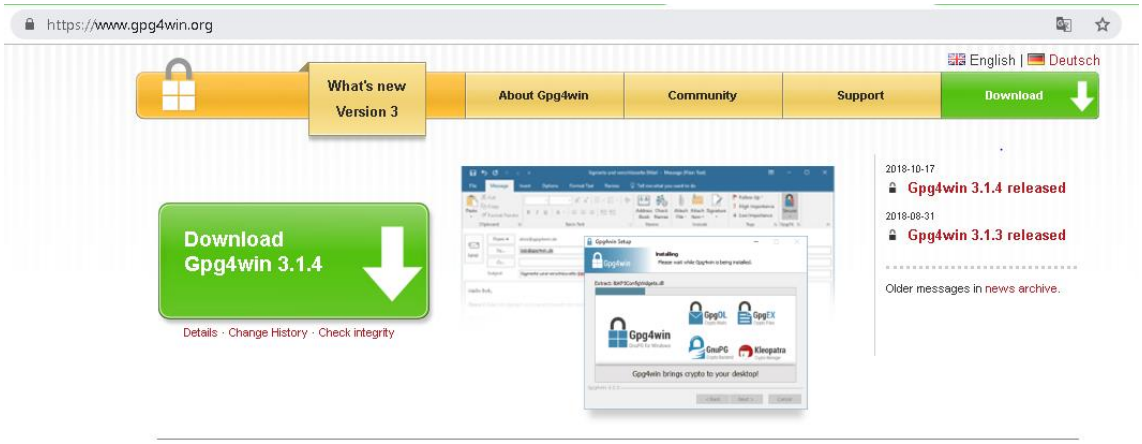
1. Instalación de la Aplicación GPG4Win.
2. Creación del par de llaves (pública y secreta) PGP.
3. Generación del archivo de llave pública.
4. Generación del archivo de llave secreta.
5. Importación del archivo llave pública de otros usuarios.
6. Importación del archivo que contiene la llave secreta.
7. Observaciones.

Cada número contiene los pasos que deben ser ejecutados de manera secuencial.

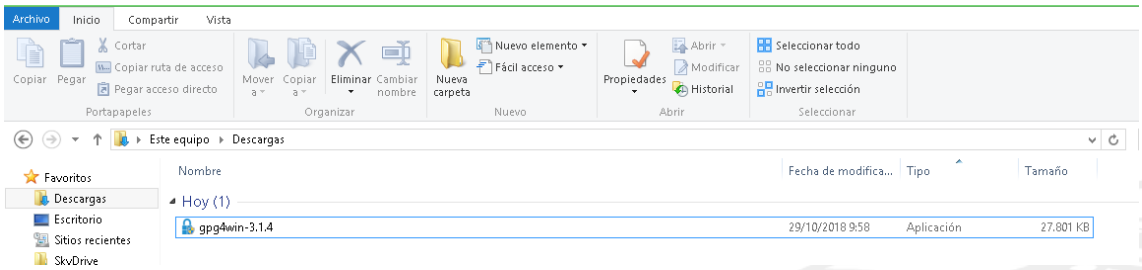
1. INSTALACION DE LA APLICACIÓN GPG4WIN

Paso No. 1
Descargar la aplicación Gpg4win, la cual se encuentra en el enlace https://gpg4win.org/thanks-for-download.html.

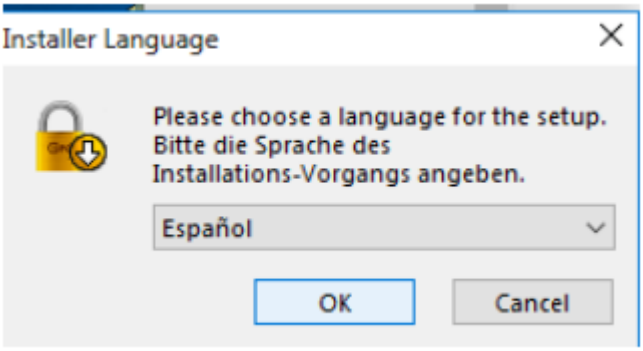
Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec



Paso No. 2
Ejecutar el archivo descargado para iniciar la instalación de la aplicación gpg4win.

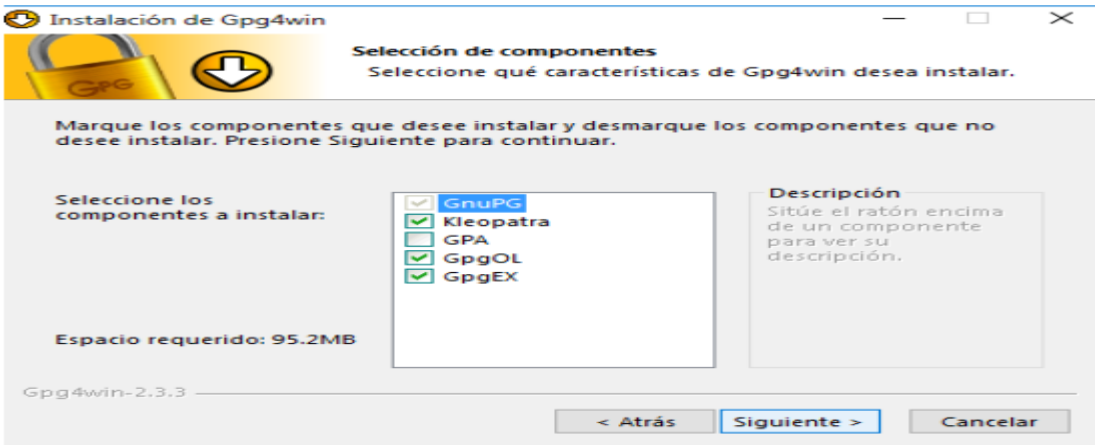


Paso No. 3
Escoger el lenguaje y hacer click en OK.

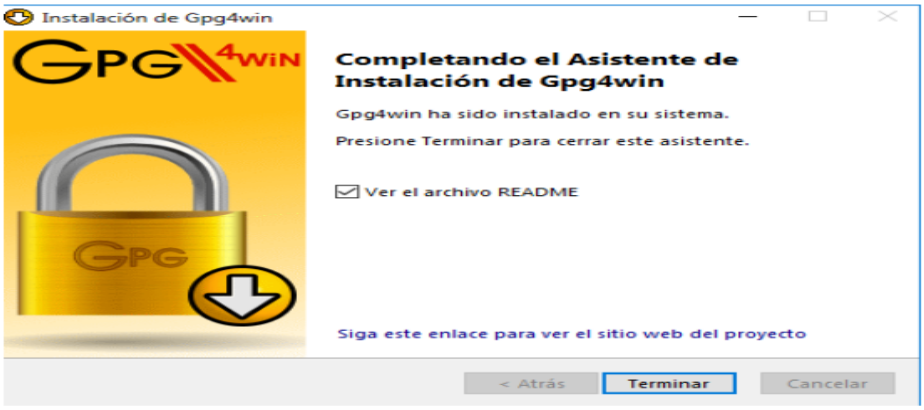


Paso No. 4
Luego de hacer click en OK, aparecerá la siguiente ventana en la cual se debe seleccionar de manera obligatoria los casilleros correspondientes a GnuPG, Kleopatra, GpOL y GpgEX.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

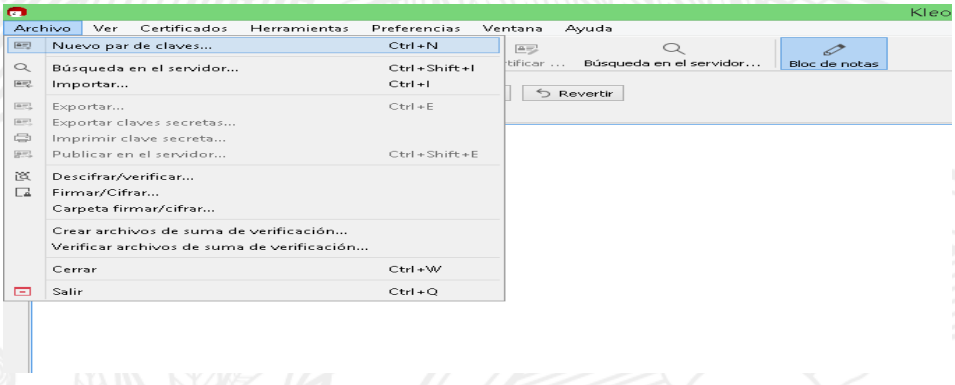


Paso No. 5
Finalizar la instalación



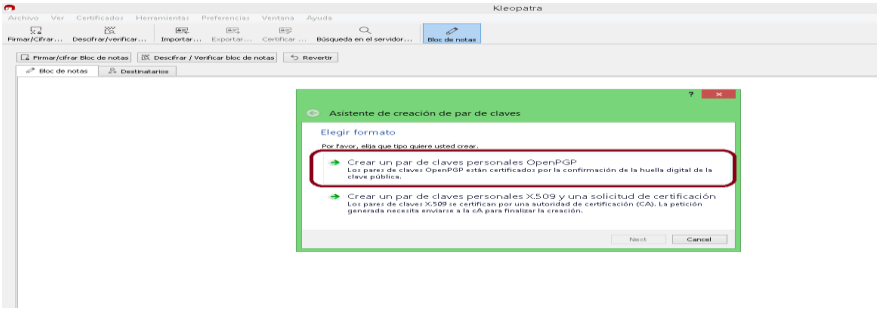
2. GENERACIÓN DE LAS LLAVES (PÚBLICA Y PRIVADA) PGP

Paso No. 6
En la aplicación Kleopatra hacer click en la pestaña Archivo y luego en la opción "Nuevo par de claves".

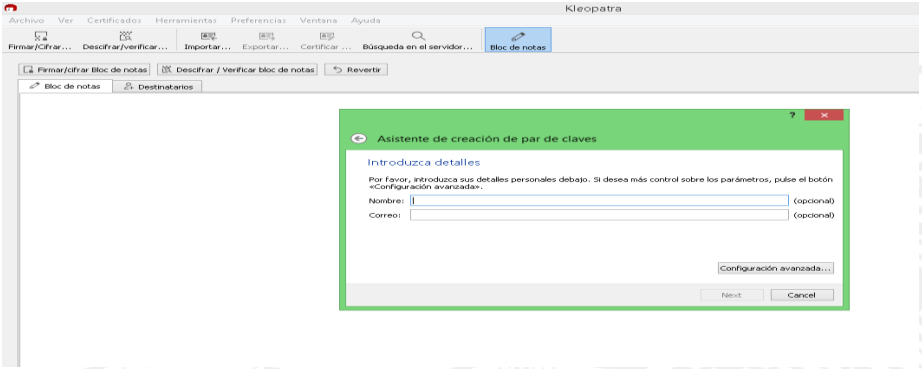


Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

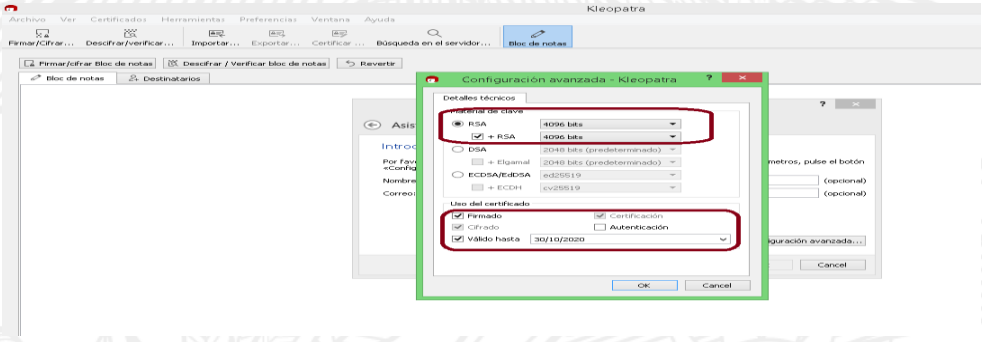
Paso No. 7
Seleccionar la opción “Crear un par de claves personales open PGP”.



Paso No. 8
Registro de datos administrativos del propietario de las claves públicas PGP. En esta ventana se deberán ingresar los datos correspondientes a Nombre y correo electrónico.



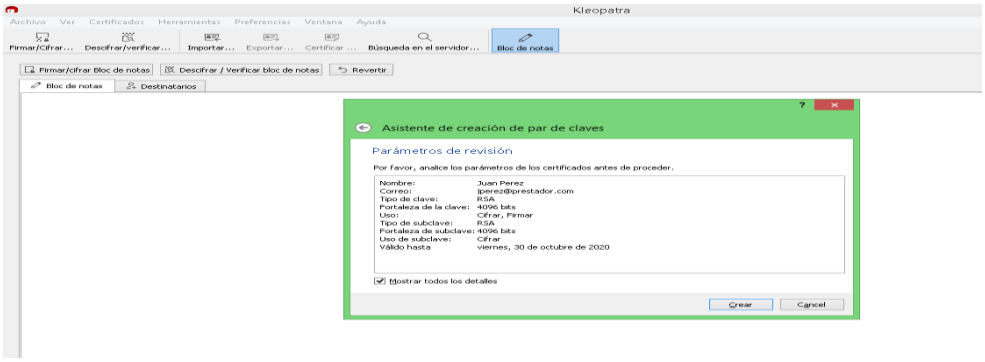
Paso No. 9
Hacer click en configuraciones avanzadas y seleccionar las siguientes opciones.



Paso No. 10

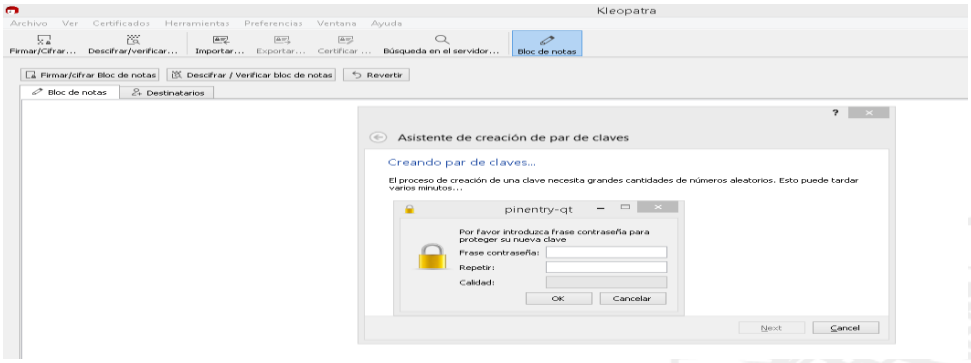
Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

Luego de verificar los datos administrativos y parámetros técnicos configurados, hacer click en “Crear”.



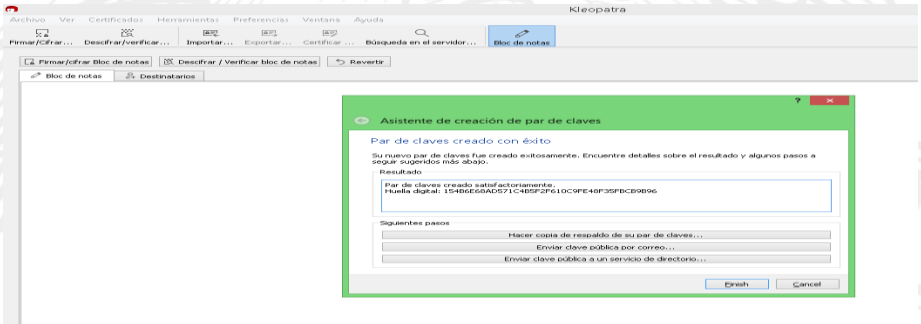
Paso No. 11

Ingresar una contraseña para la protección de las llaves públicas creadas.



Paso No. 12

La aplicación Kleopatra notificará la creación satisfactoria de las llaves públicas PGP, hacer click en “Finish”.

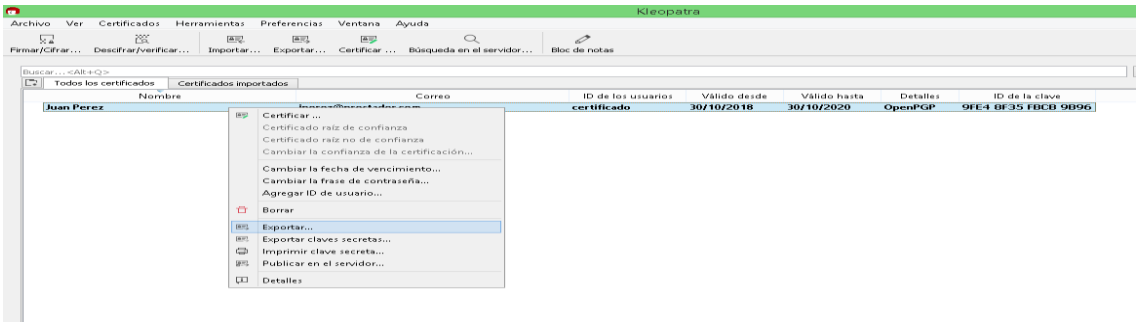


3. GENERACIÓN DEL ARCHIVO DE LLAVE PÚBLICA

Paso No. 13

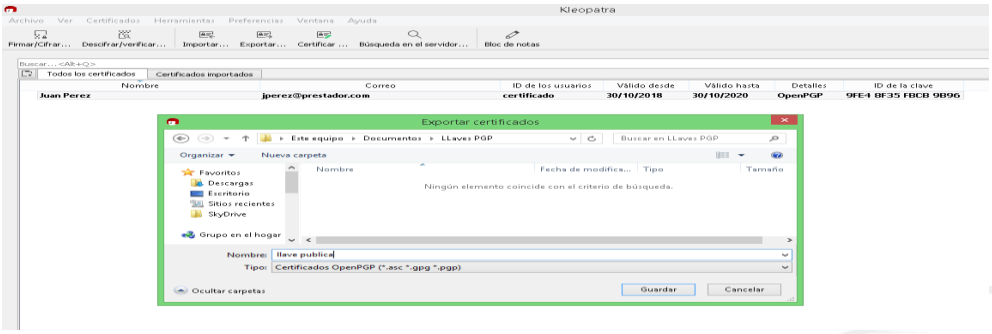
En la aplicación Kleopatra en la pestaña “Todos los certificados” hacer click derecho sobre el usuario creado y luego hacer click en el botón exportar.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec



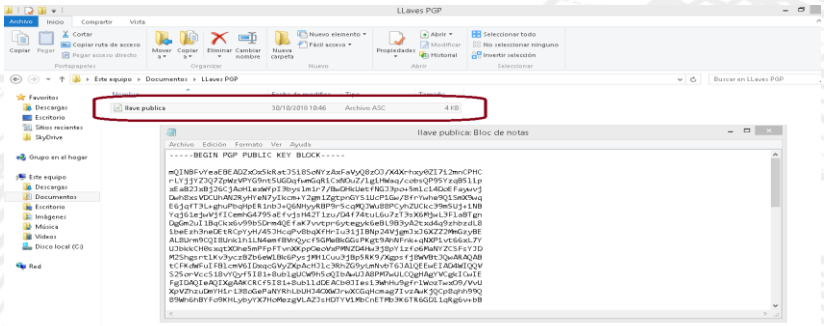
Paso No. 14

Seleccionar la ubicación en donde se almacenará el archivo que contiene la llave pública.



Paso No. 15

Verificación de la clave pública creada. Con un editor de texto abrir el archivo generado en el paso anterior.



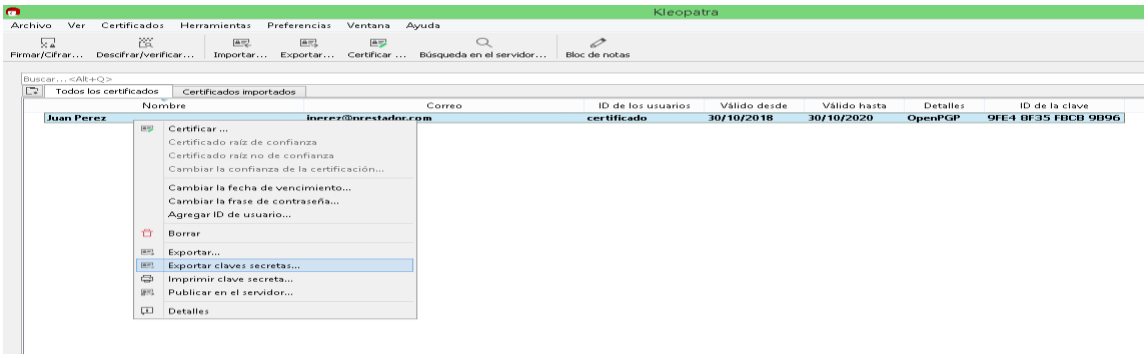
Esta llave pública es el archivo que se debe intercambiar con los destinatarios de los mensajes cifrados que se vayan a enviar.

4. GENERACIÓN DEL ARCHIVO DE LLAVE SECRETA

Paso No. 16

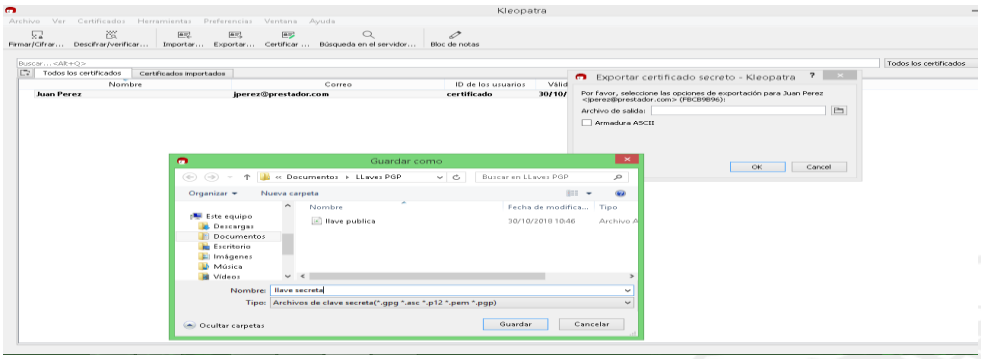
En la aplicación Kleopatra en la pestaña “Todos los certificados” hacer click derecho sobre el usuario creado y luego hacer click en el botón Exportar claves secretas.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec



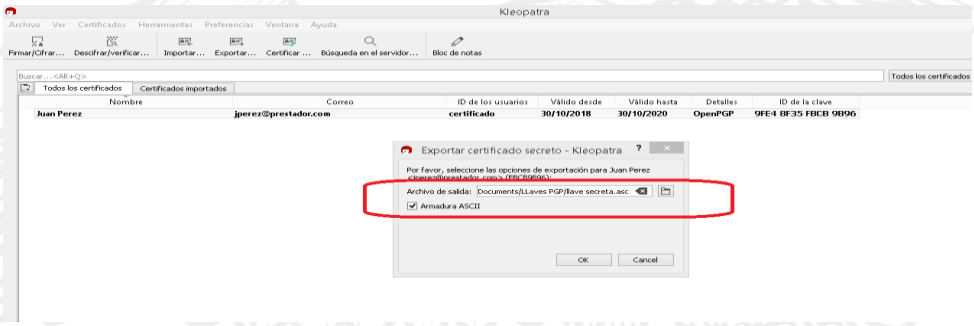
Paso No. 17

Seleccionar la ubicación en donde se almacenará el archivo que contiene la llave secreta.



Paso No. 18

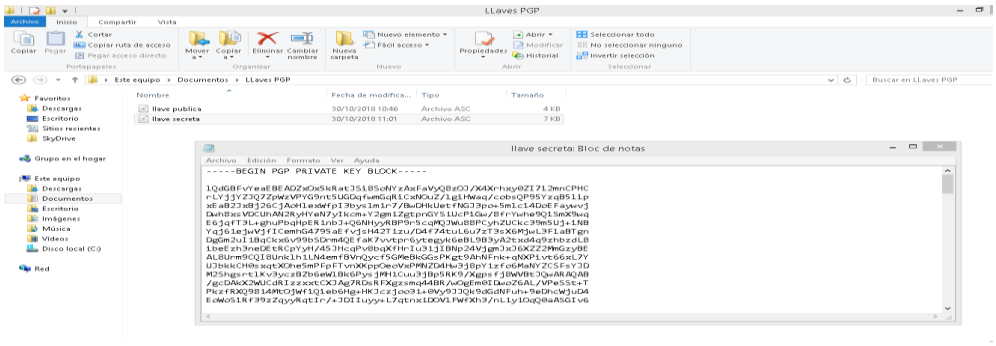
Seleccionar la opción Armadura ASCCI y luego hacer click en Ok.



Paso No. 19

Verificación de la clave secreta creada. Con un editor de texto abrir el archivo generado en el paso anterior.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

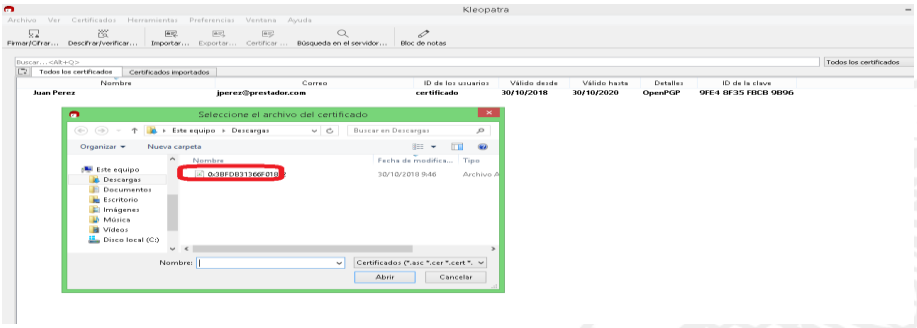


Esta llave secreta es el archivo que bajo ninguna circunstancia debe ser accedido por otra persona que no sea el usuario o propietario de las llaves.

5. IMPORTAR LLAVE PUBLICA DE OTROS USUARIOS

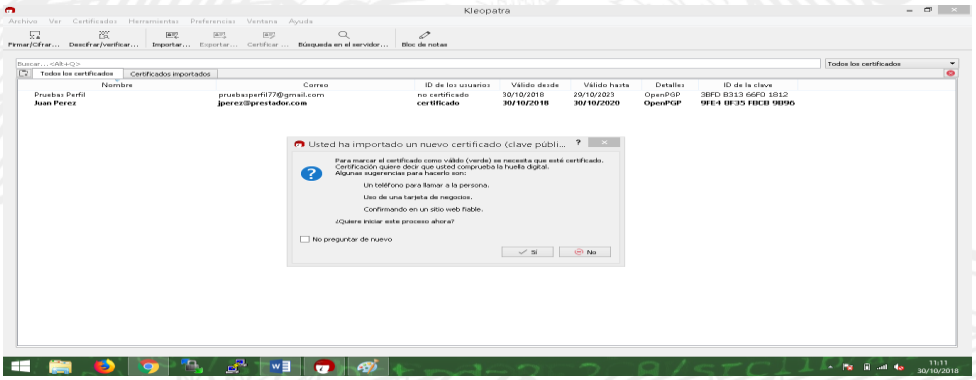
Paso No. 20

En la aplicación kleopatra en la pestaña archivo hacer click en el botón Importar, y luego escoger el archivo que contiene la llave pública del destinatario.



Paso No. 21

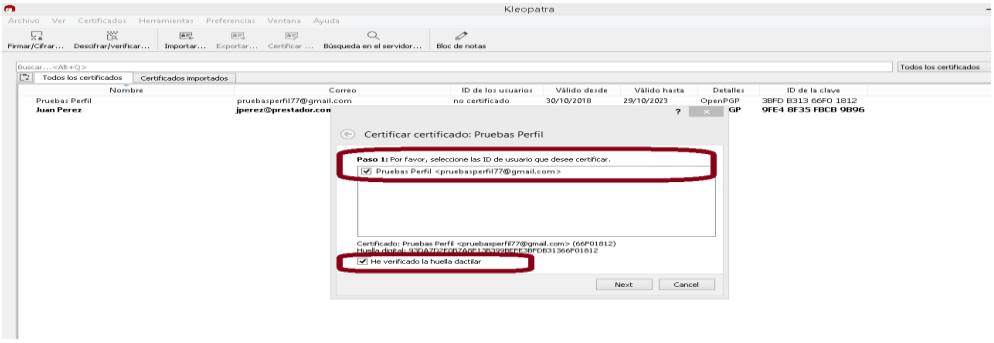
En la siguiente ventana hacer click en el botón “SI”.



Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

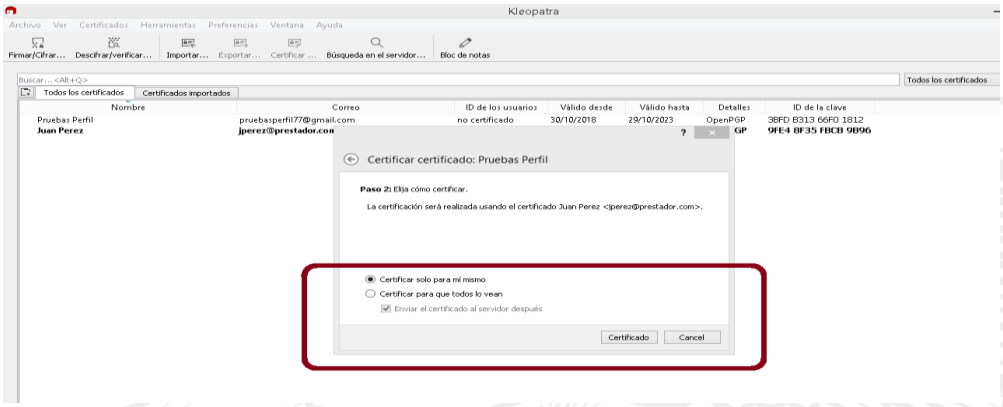
Paso No. 22

En la siguiente ventana hacer seleccionar los dos casilleros que se indican en la figura, los cuales corresponden al usuario del cual se está importando la llave pública, y el proceso de verificación de huella dactilar.



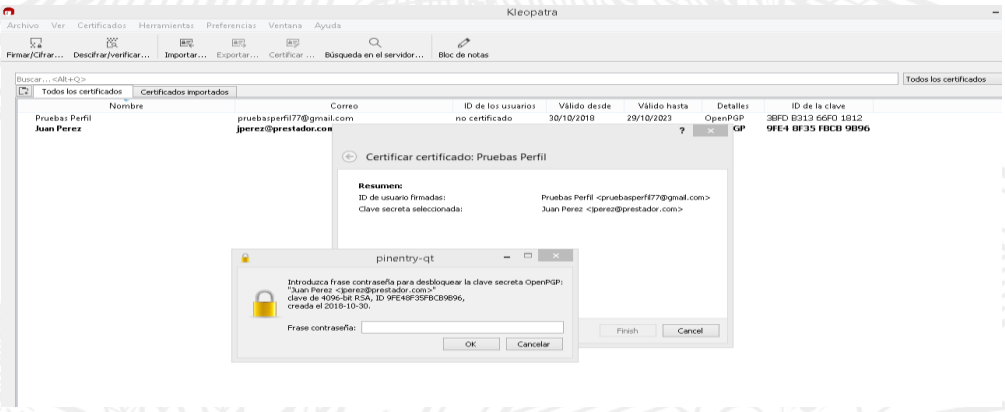
Paso No. 23

En la siguiente ventana seleccionar la opción certificar solo para sí mismo y luego hacer click en el botón Certificado.



Paso No. 24

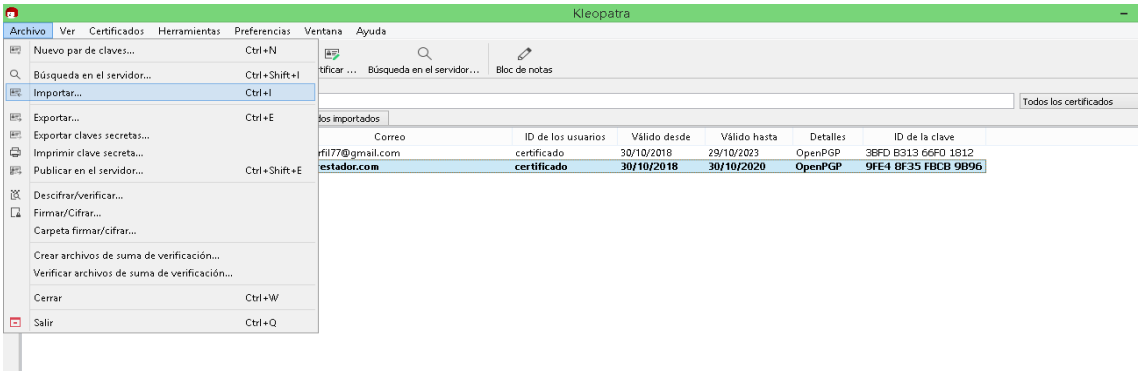
Para finalizar la importación se debe ingresar la clave con la que se protege la clave secreta de acuerdo al paso No. 11.



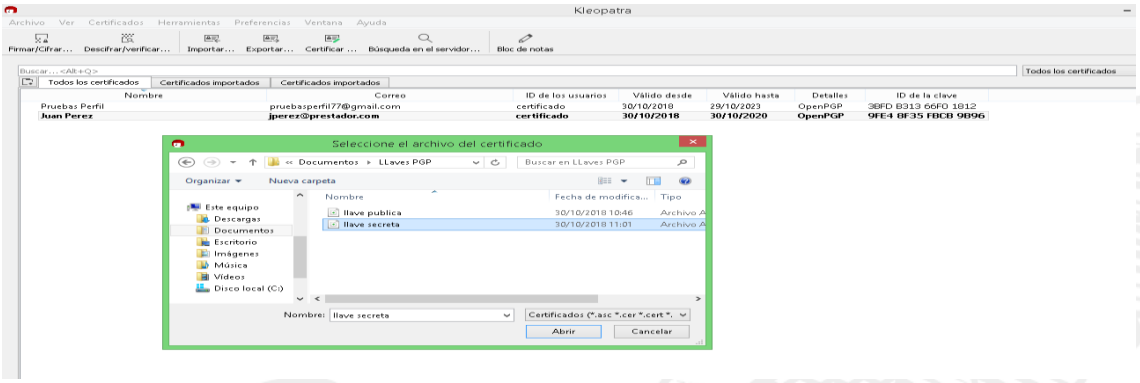
Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

6. IMPORTACIÓN DEL ARCHIVO QUE CONTIENE LA LLAVE SECRETA

Paso No. 25
En la aplicación kleopatra en la pestaña archivo hacer click en el botón importar.



Paso No. 26
Seleccionar el archivo correspondiente a la llave secreta.



Observaciones
Las llaves publicadas PGP deberán ser configuradas en sus sistemas de correo electrónico, y la llave pública debe ser compartida con el Centro de Respuestas a Incidentes Informáticos del EcuCERT.

La llave pública del EcuCERT se encuentra publicada en su página web www.ecucert.gob.ec

Referencia:

https://www.deepdotweb.com/2015/02/21/pgp-tutorial-for-windows-kleopatra-gpg4win/

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec