UT01: ADOPCIÓN DE PAUTAS DE SEGURIDAD INFORMÁTICA – ENCRIPTAR Y DESENCRIPTAR FICHEROS

FRANCISCO JESÚS GARCÍA – UCEDA DÍAZ - ALBO

ÍNDICE

INTRODUCCIÓN

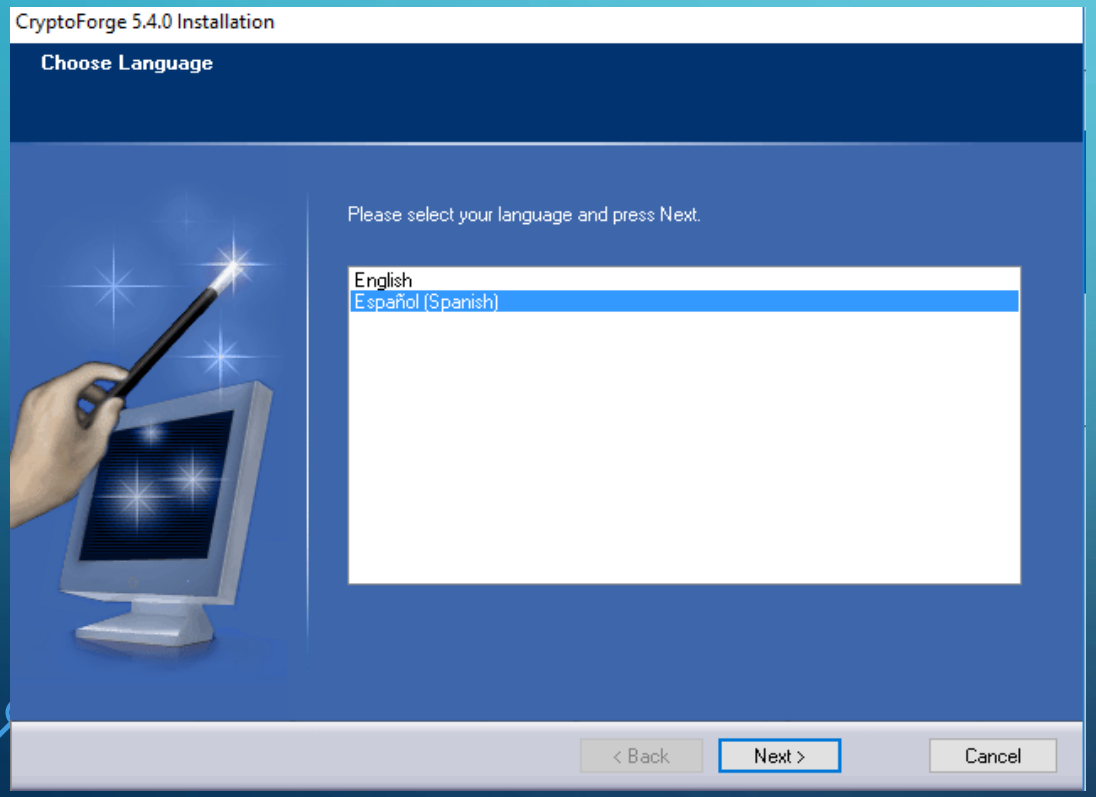
- En esta práctica utilizaremos varios programas para realizar encriptación y desencriptación de ficheros. Utilizaremos para ello dos aplicaciones en entornos Windows y un comando que viene por defecto en Linux.

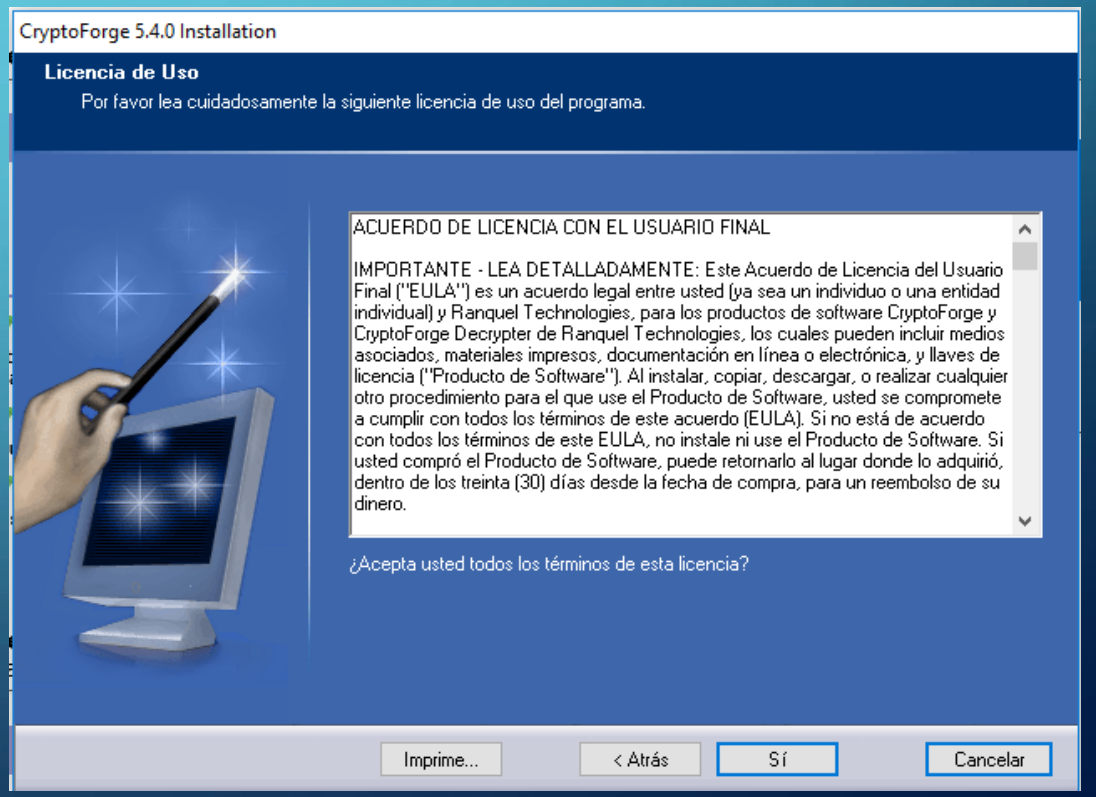
CRYPTOFORGE

- Iremos a la página oficial del programa para descargarlo e instalarlo. Link.

CRYPTOFORGE

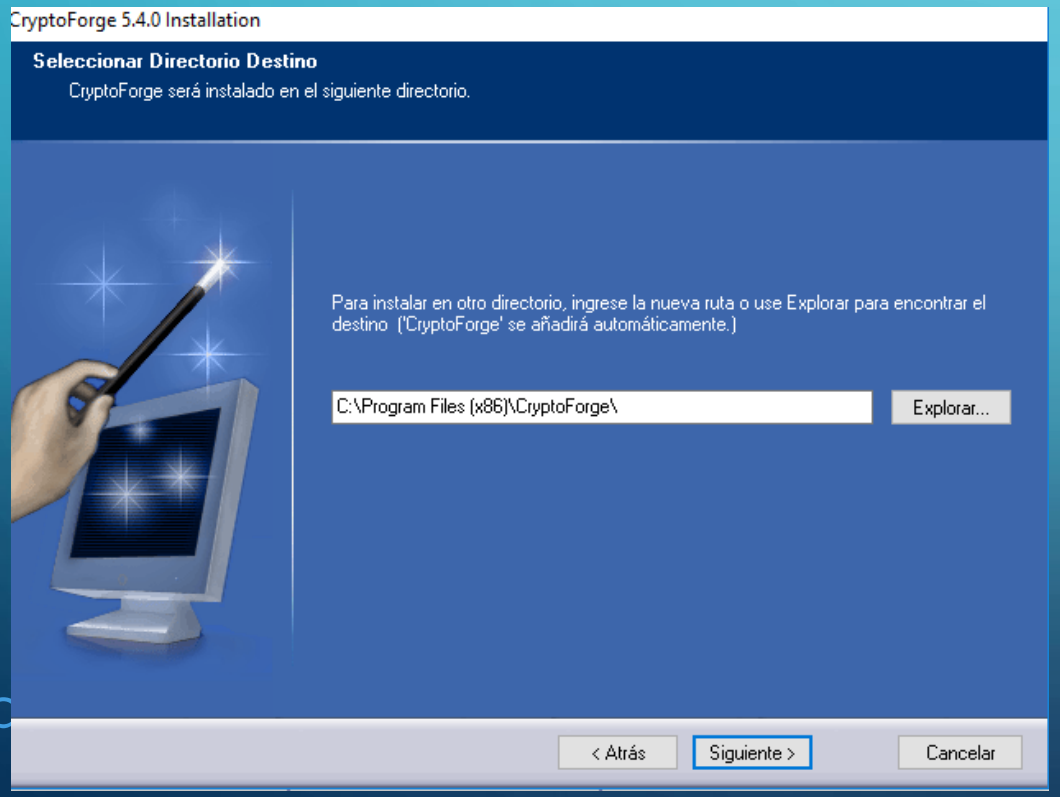
- Ejecutaremos el programa y escogemos nuestro idioma, después aceptaremos los términos y condiciones

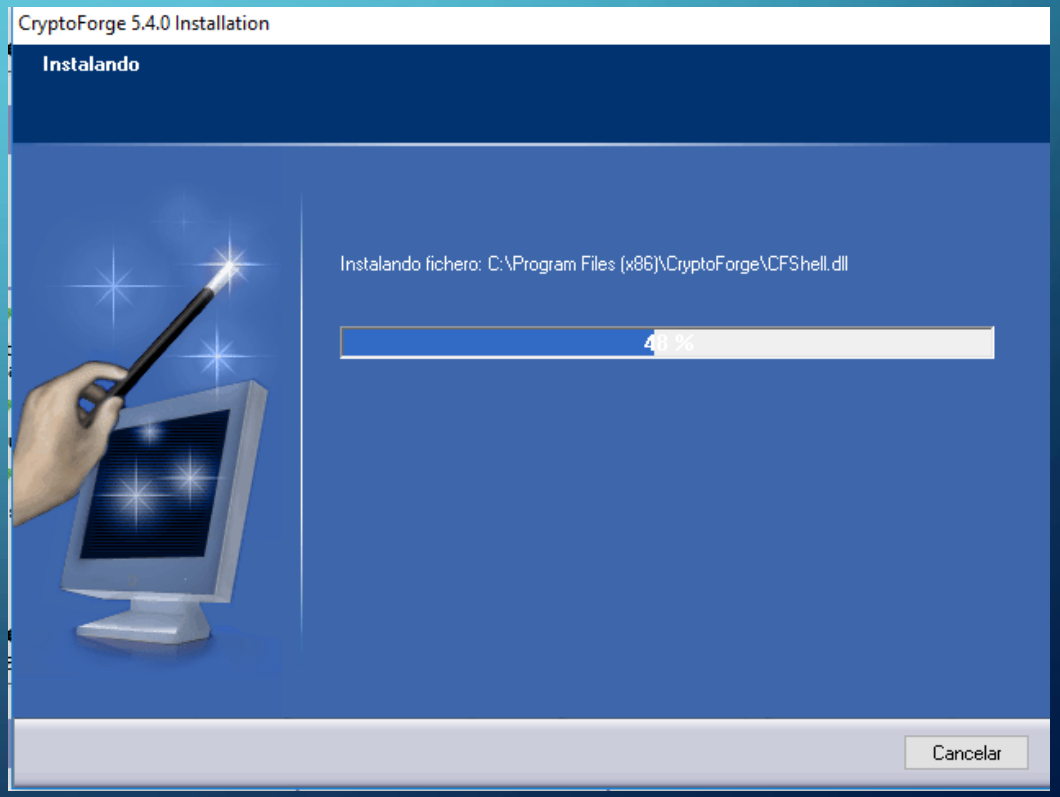




CRYPTOFORGE

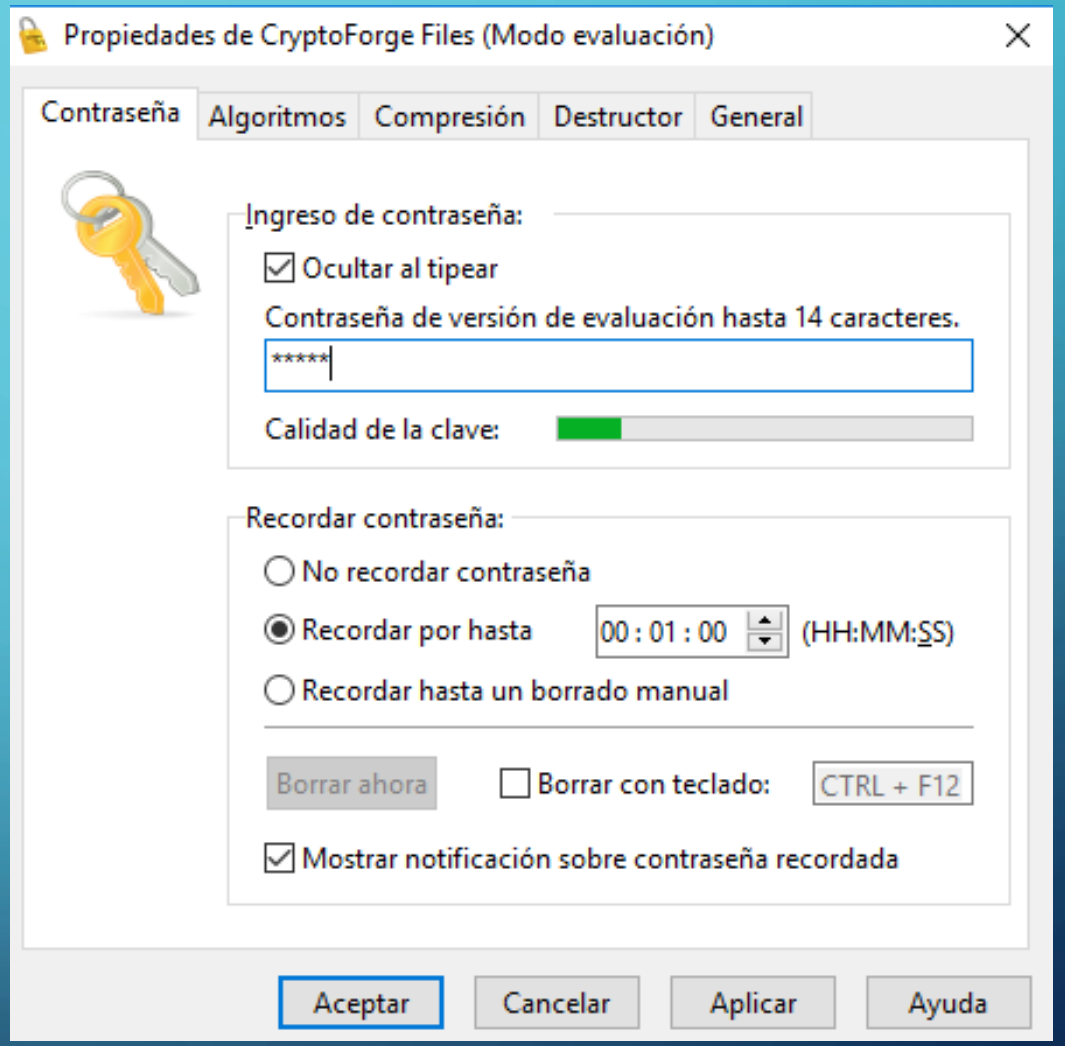
- Elegiremos la ruta de instalación y esperamos a que se instale.





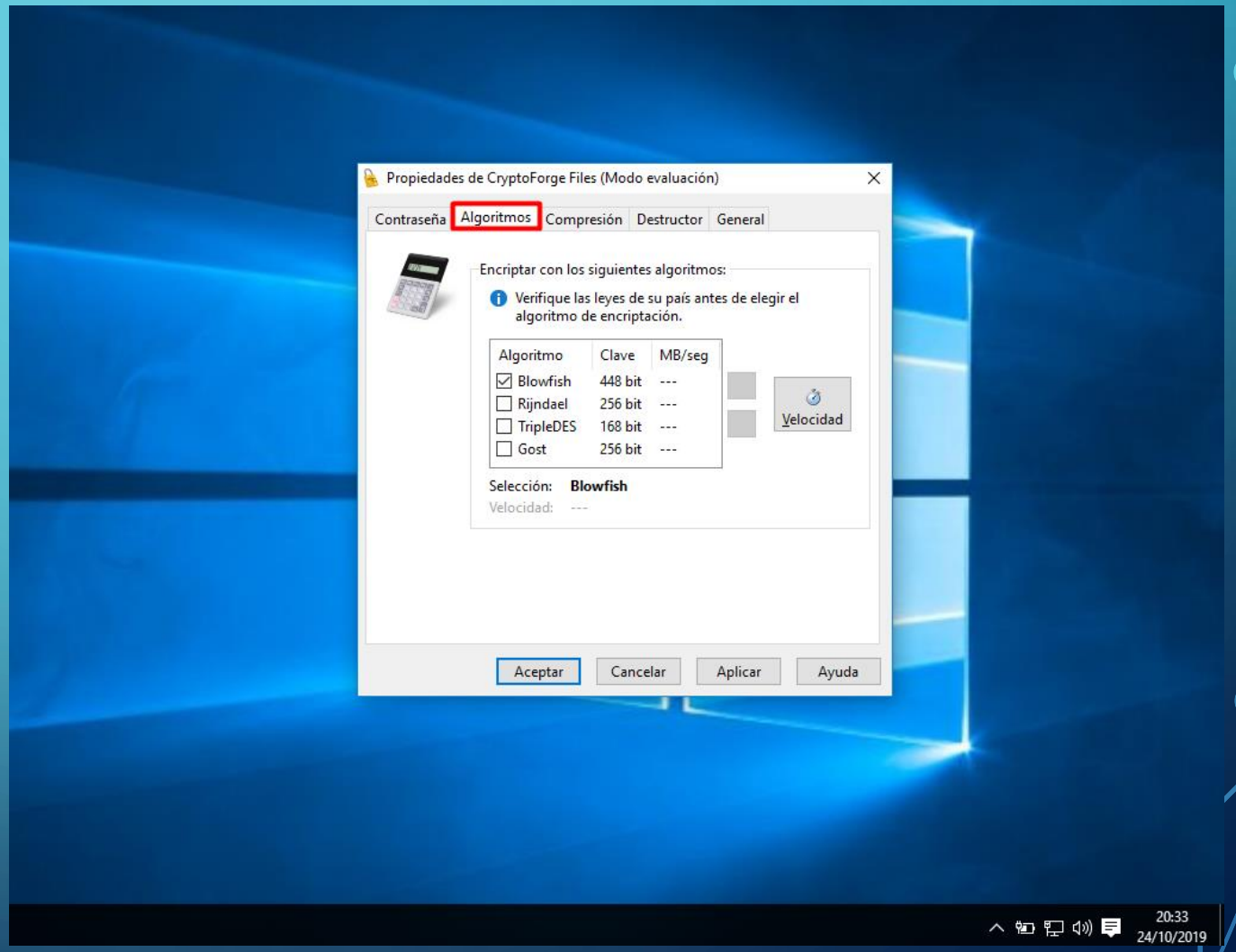
CRYPTOFORGE

- Una vez descargado lo ejecutamos, podemos ver como en la primera pestaña podremos configurar la contraseña a utilizar en cifrado/descifrado.



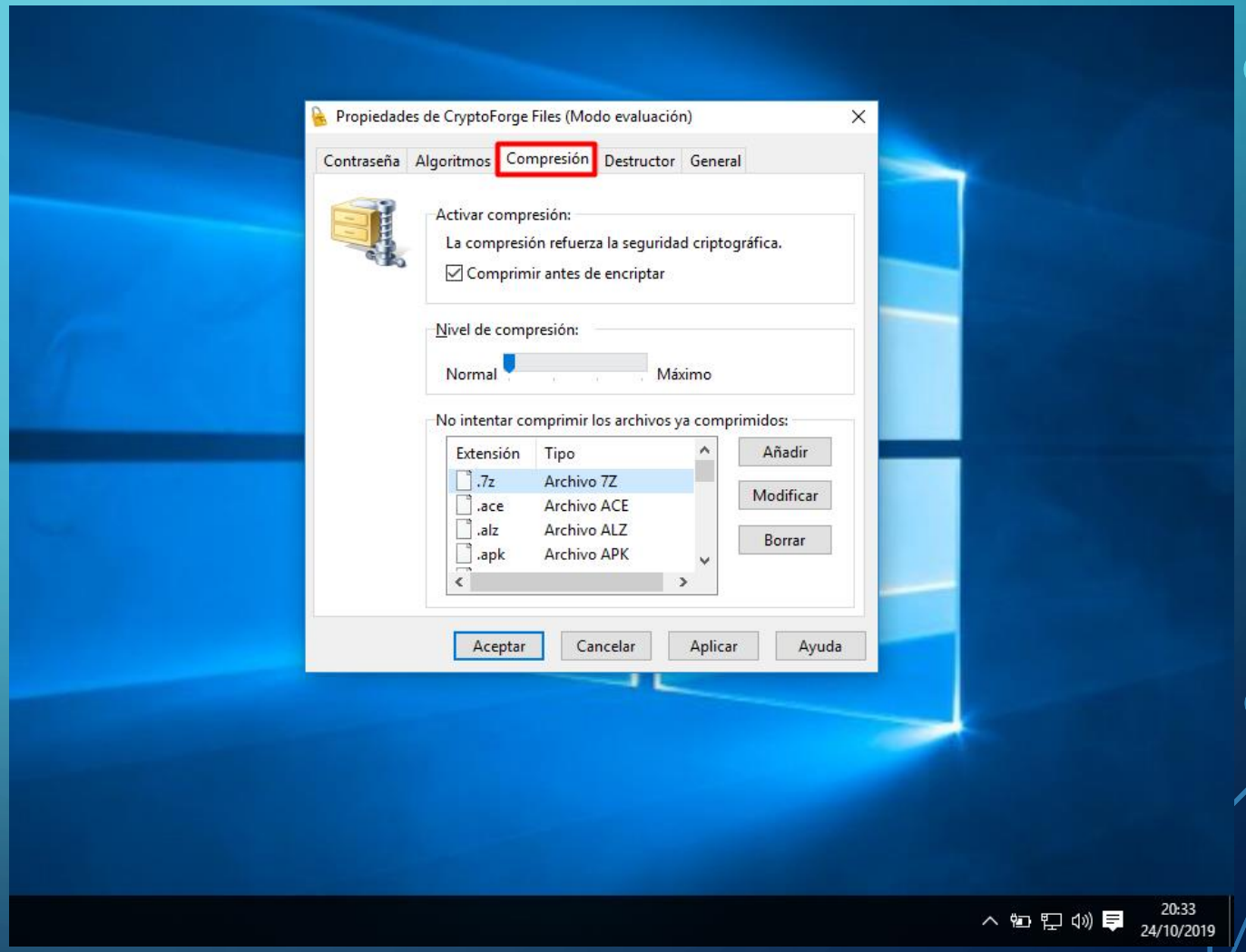
CRYPTOFORGE

- En la pestaña *Algoritmo*, podremos cambiar el algoritmo con el que se cifra.



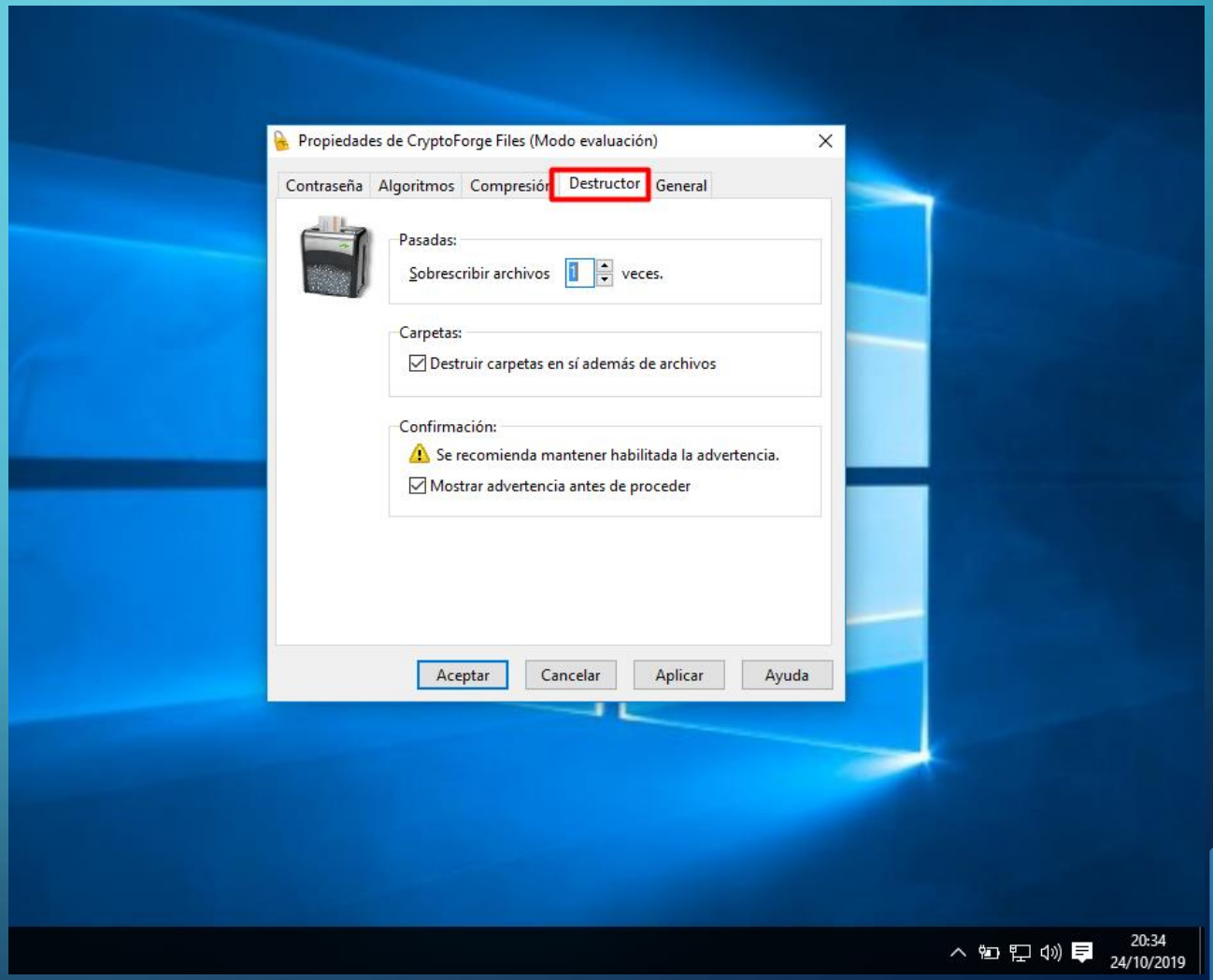
CRYPTOFORGE

- En la pestaña *Compresión* podemos escoger como comprimir el archivo a cifrar. En caso de que sea un archivo ya comprimido no lo cifrará si esta en la lista de abajo.



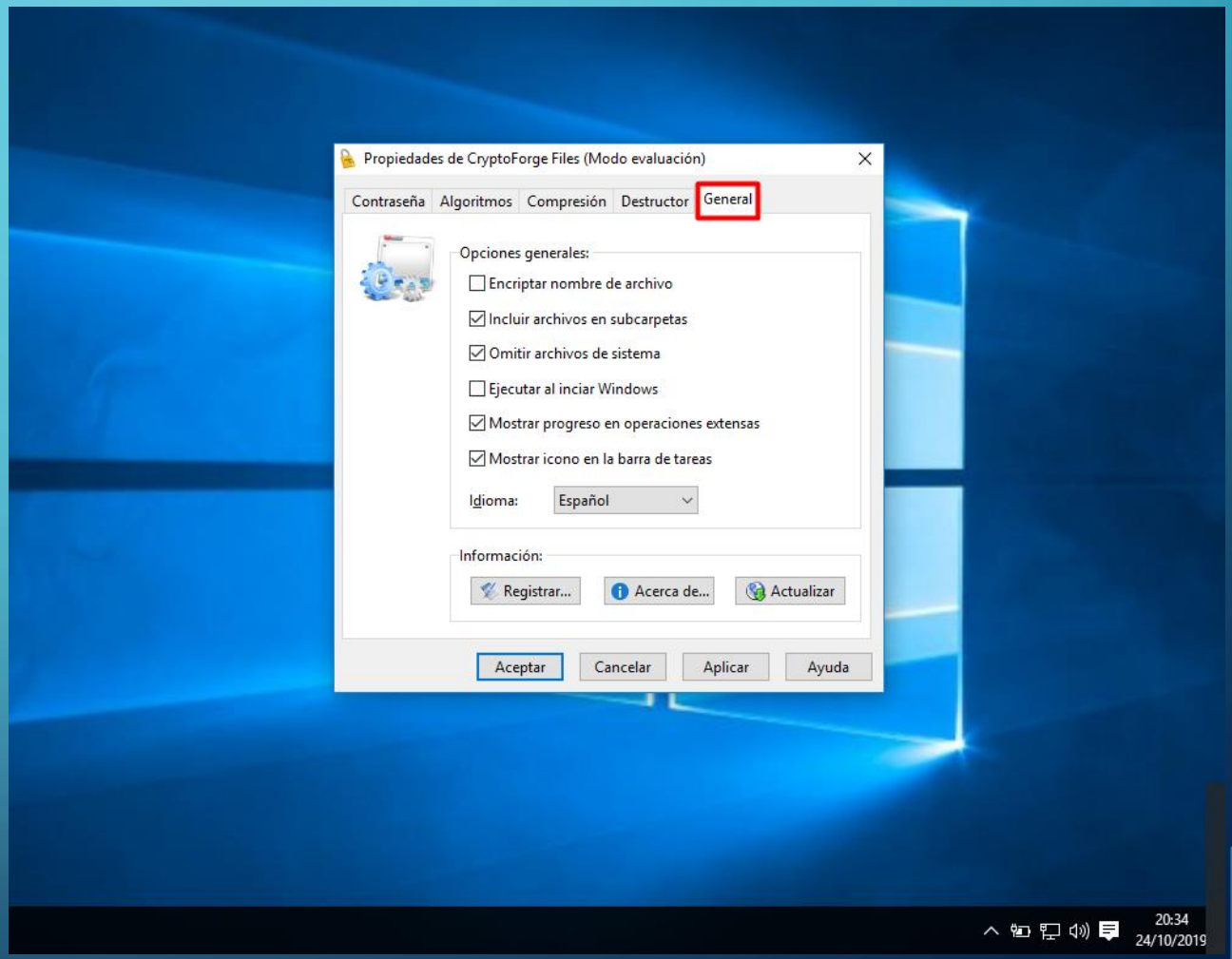
CRYPTOFORGE

- En la pestaña *Destructor* podemos escoger de que manera destruir archivos, carpetas, comprimidos… seleccionados.



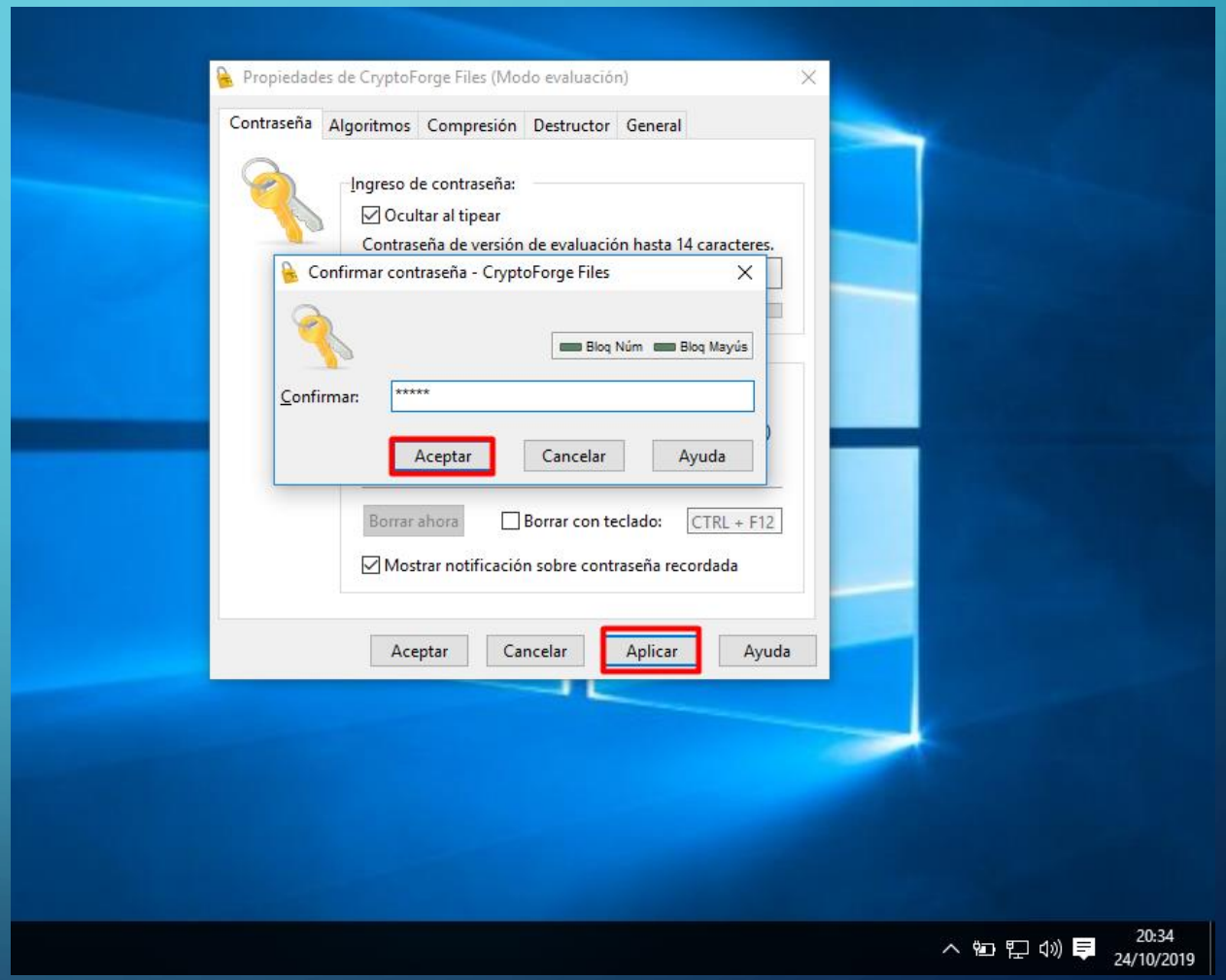
CRYPTOFORGE

- En la pestaña *General* podemos ver opciones generales.



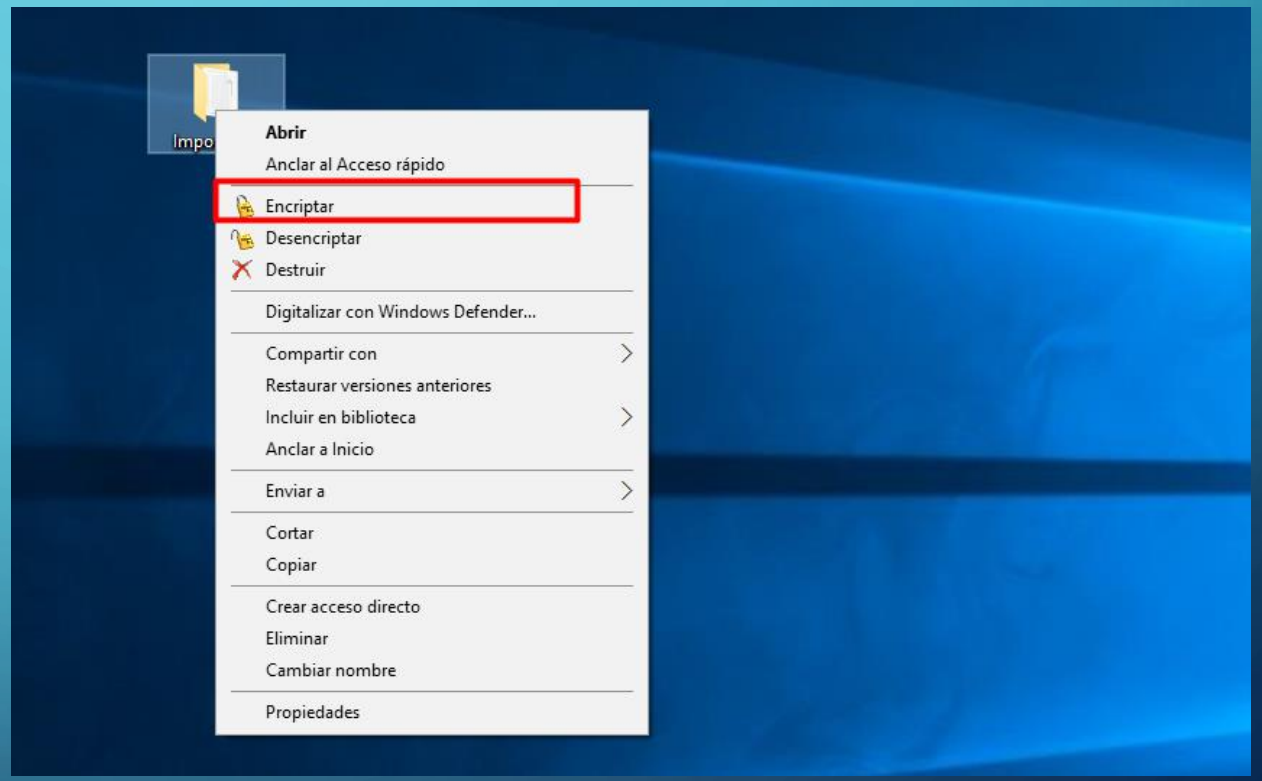
CRYPTOFORGE

- Si hemos realizado cambios simplemente con pulsar *Aplicar* e introducir la contraseña que pusimos al principio serviría.



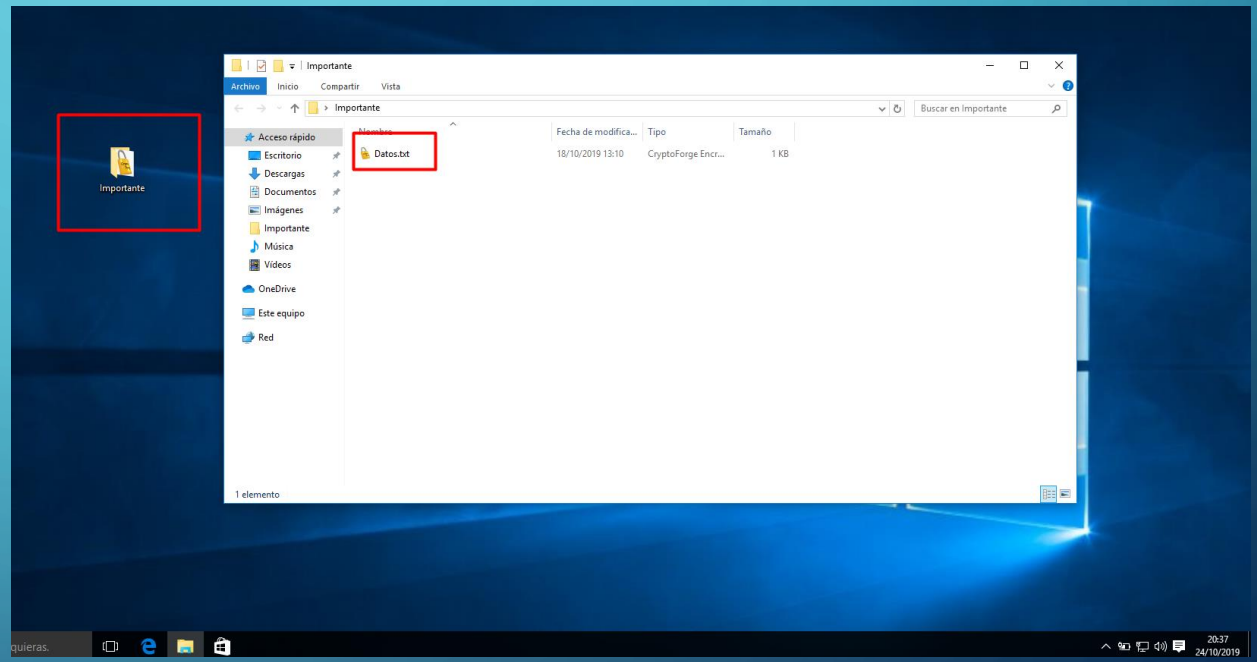
CRYPTOFORGE

- Para encriptar un archivo o carpeta pulsamos clic derecho en el y en *Encriptar.*



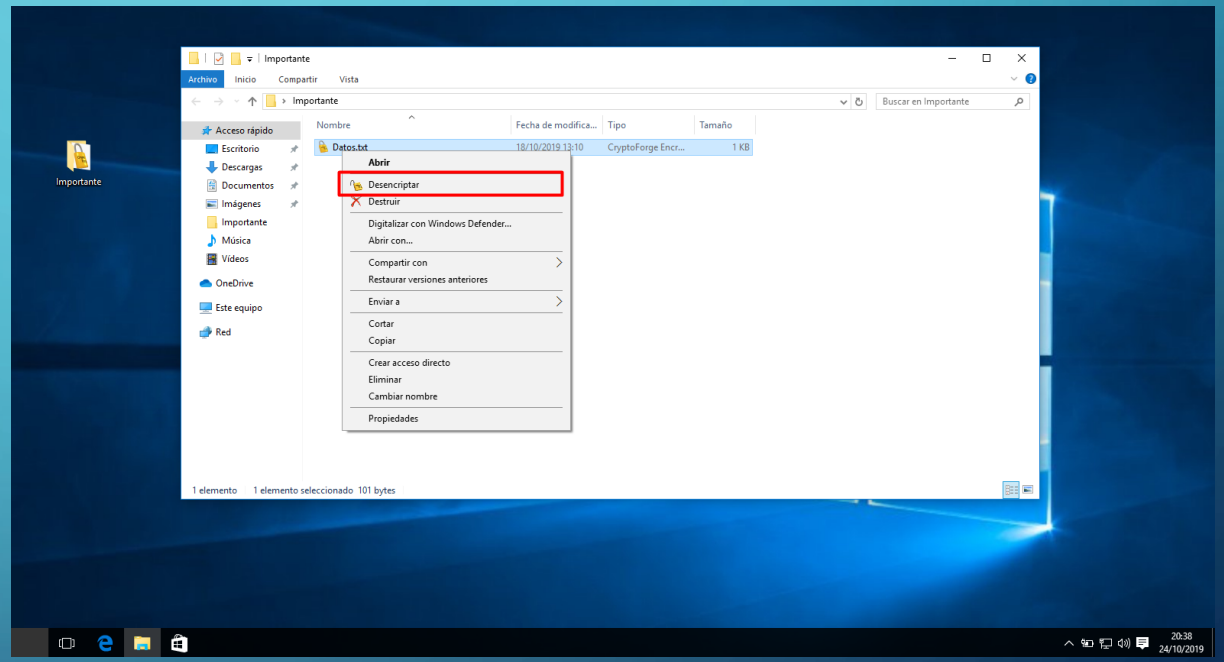
CRYPTOFORGE

- Vemos como se encripta el archivo dentro de la carpeta.



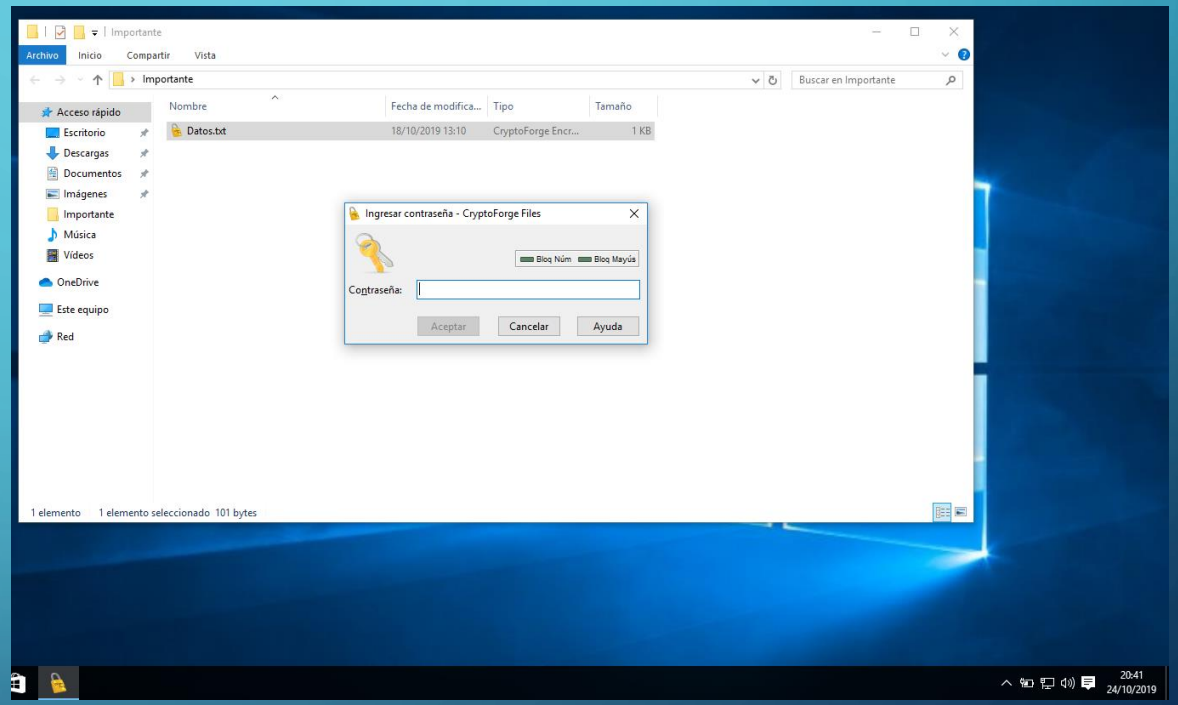
CRYPTOFORGE

- Si lo queremos desencriptar simplemente pulsamos otra vez clic derecho y *Desencriptar.*



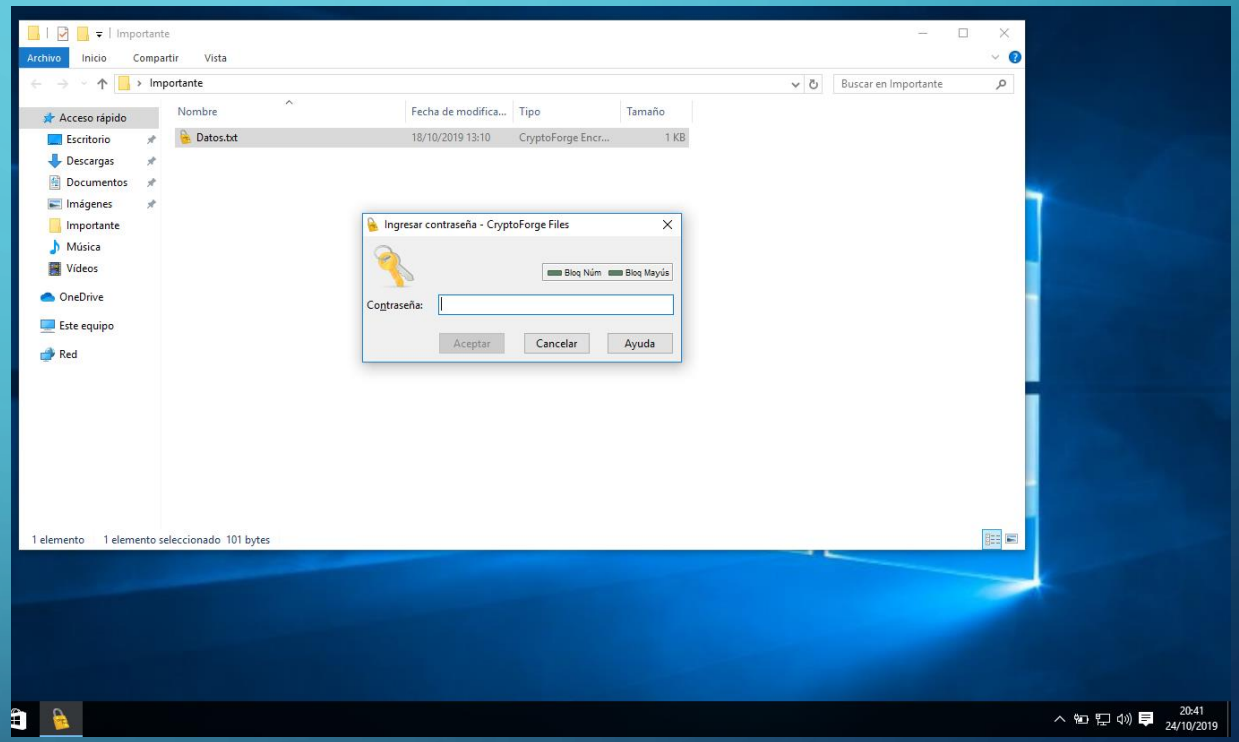
CRYPTOFORGE

- Nos pedirá la contraseña para desencriptarlo.



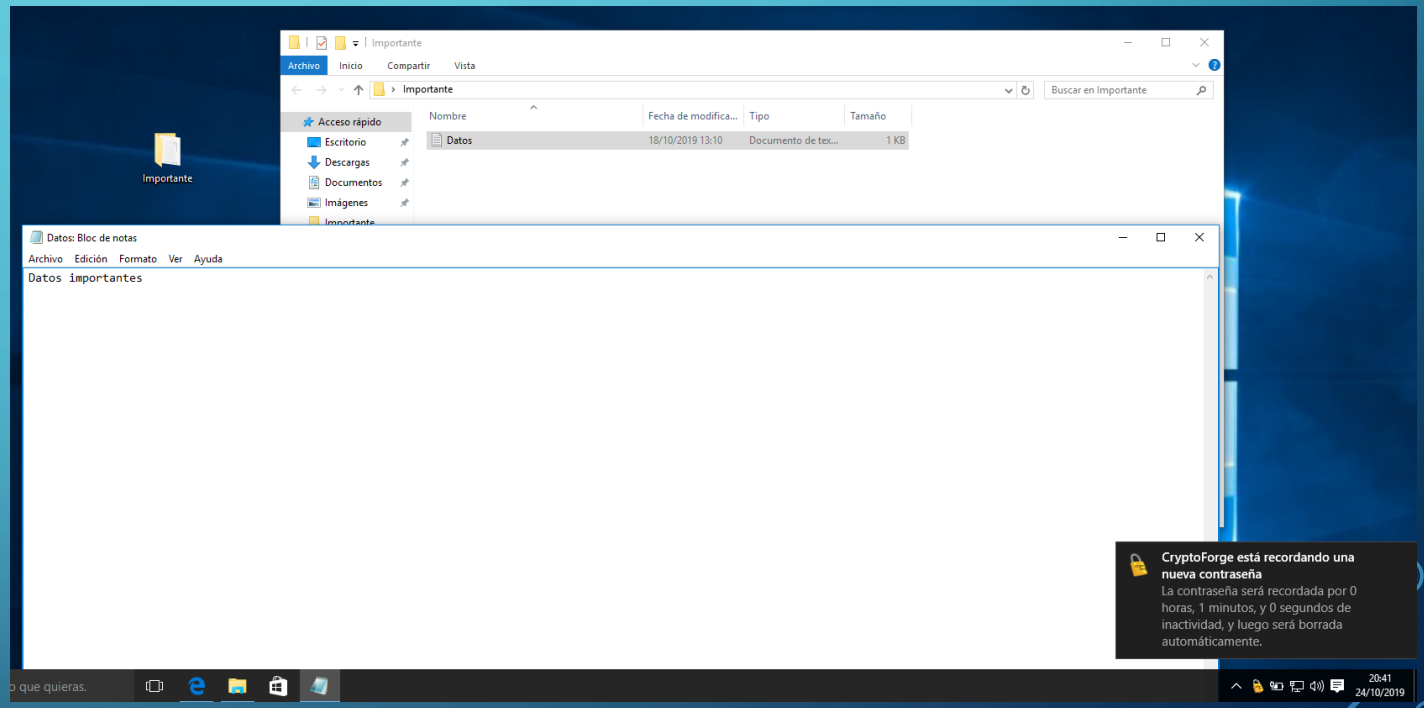
CRYPTOFORGE

- Nos pedirá la contraseña para desencriptarlo.



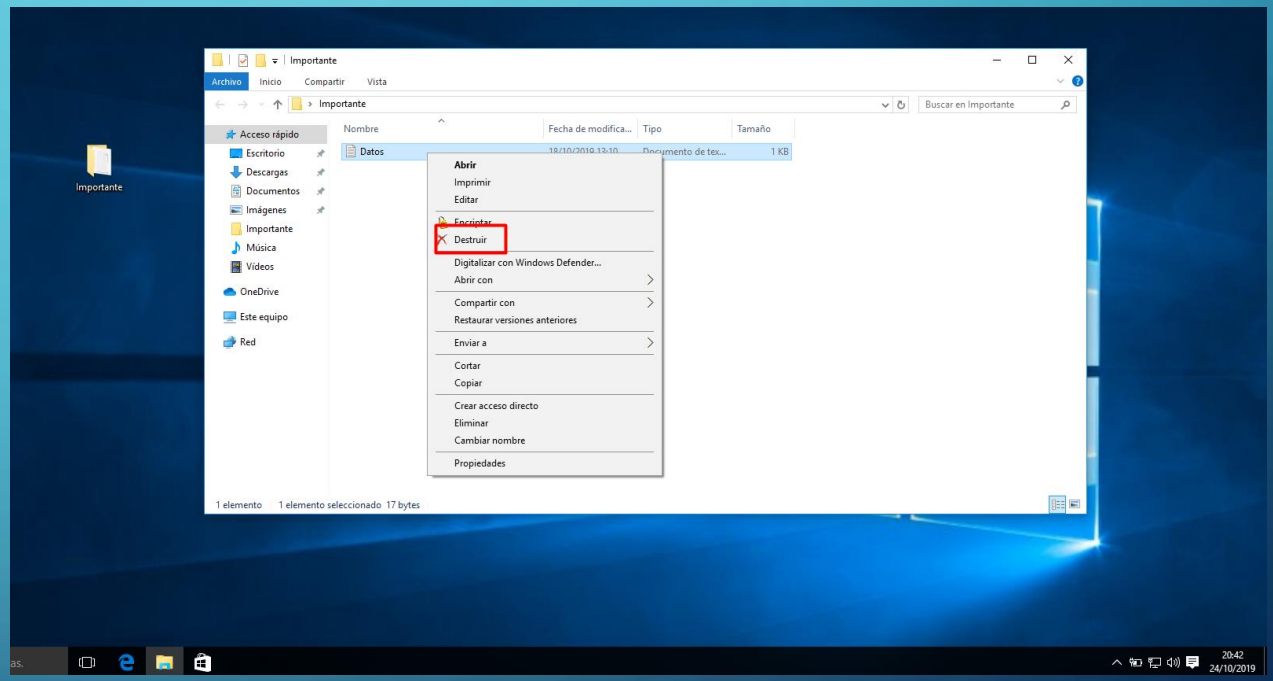
CRYPTOFORGE

- Ya tendremos el archivo totalmente desencriptado y podremos acceder a el.



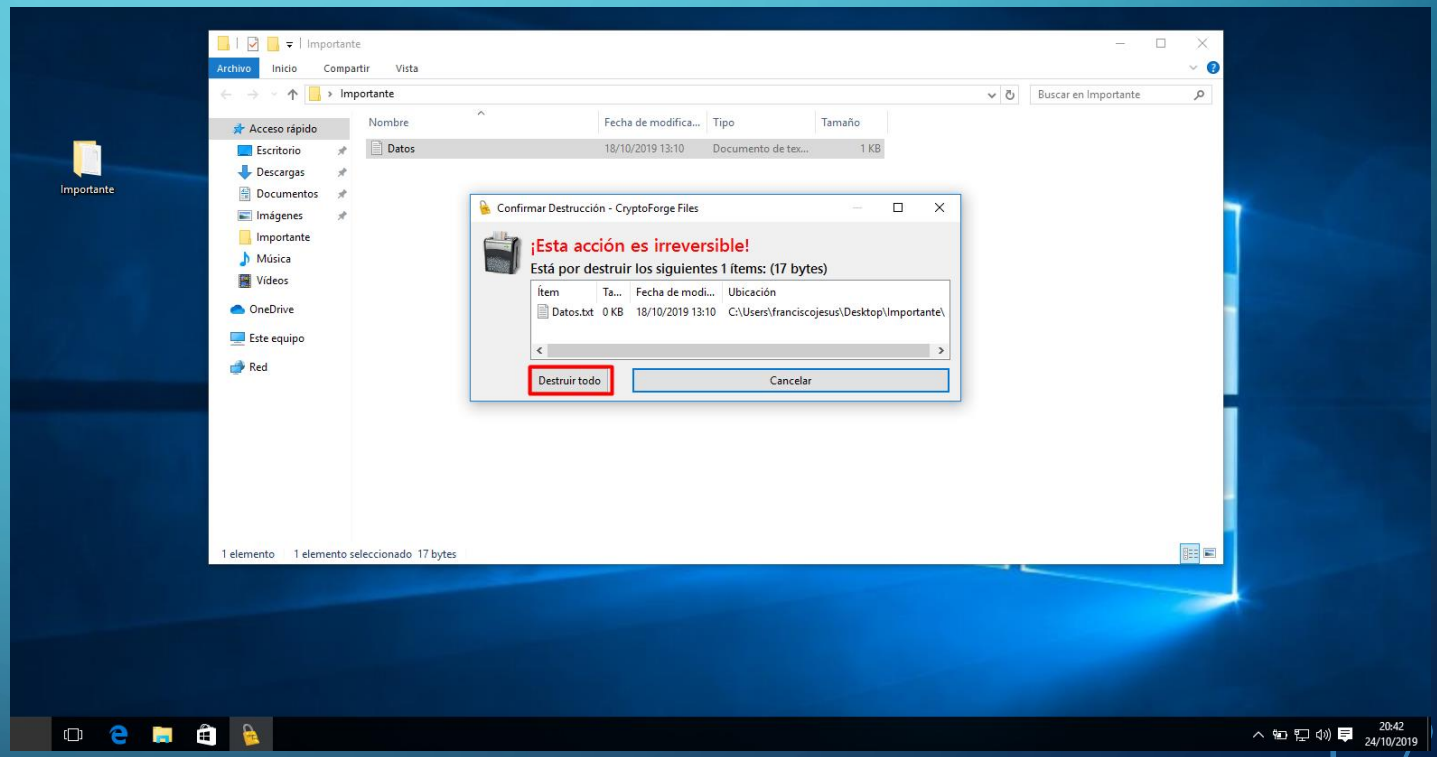
CRYPTOFORGE

- Si pulsamos clic derecho sobre el podremos destruirlo.



CRYPTOFORGE

- Nos mandará una advertencia, pulsamos en *Destruir Todo* y se borrará "permanentemente".

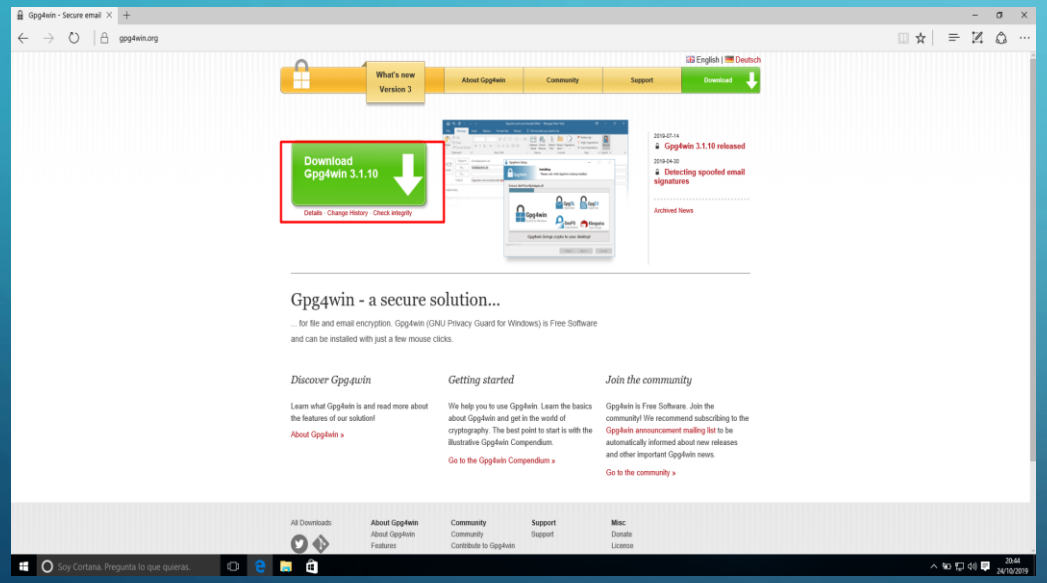


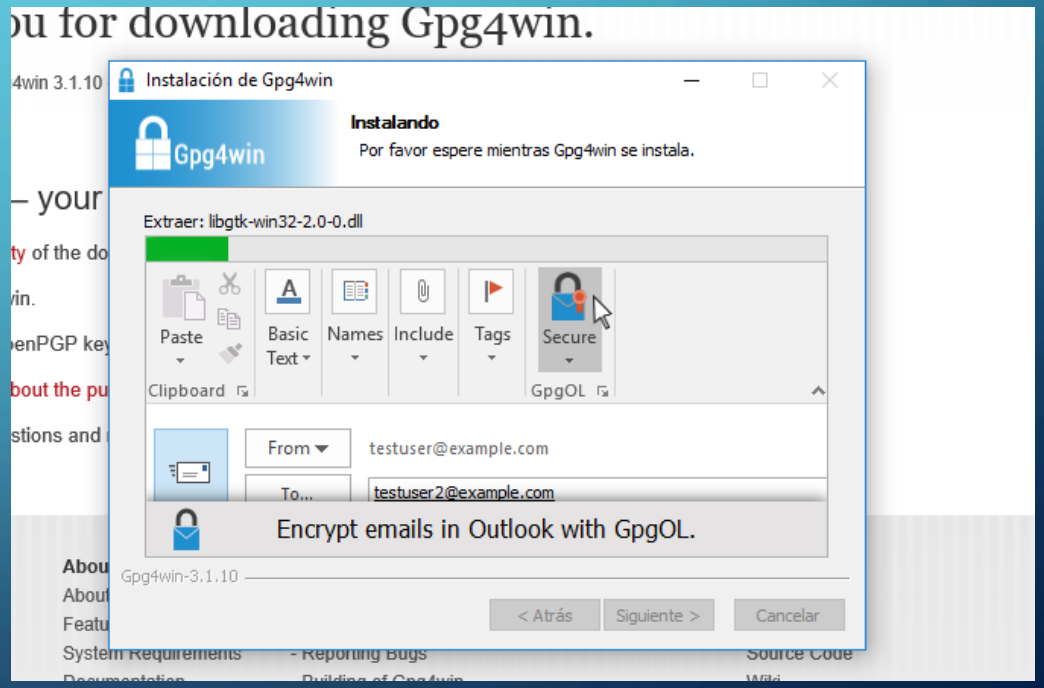
GP4WIN

- Gpg4win es un paquete de cifrado de correo electrónico y archivos para la mayoría de las versiones de Microsoft Windows que utiliza criptografía de clave pública GnuPG para el cifrado de datos y firmas digitales.

GP4WIN

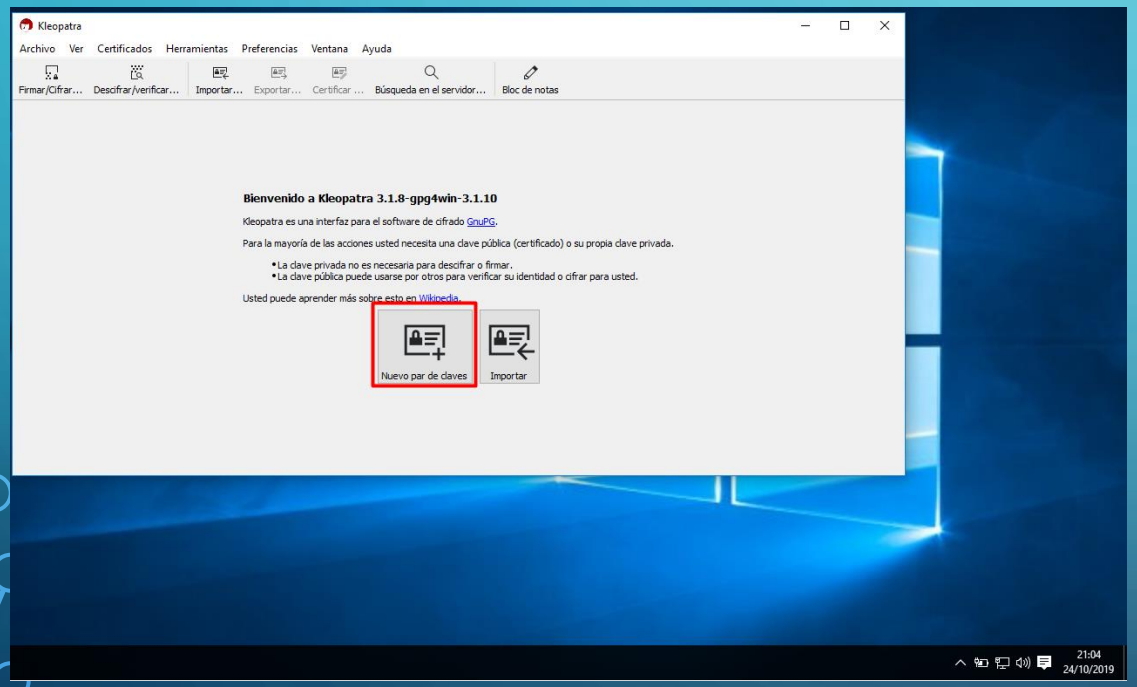
Para descargarlo simplemente vamos a su web. Link. Una vez descargado lo ejecutamos e instalamos.



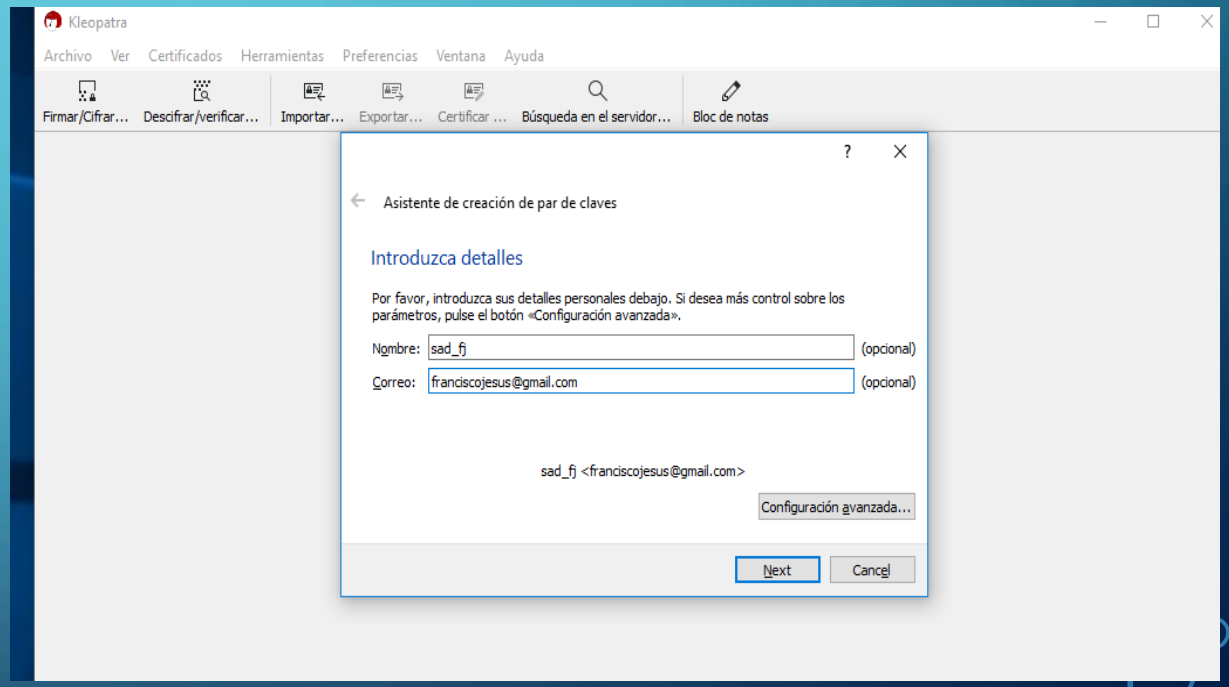


GP4WIN

Pulsamos en *Nuevo Par de Claves* para empezar a crear un par de claves.

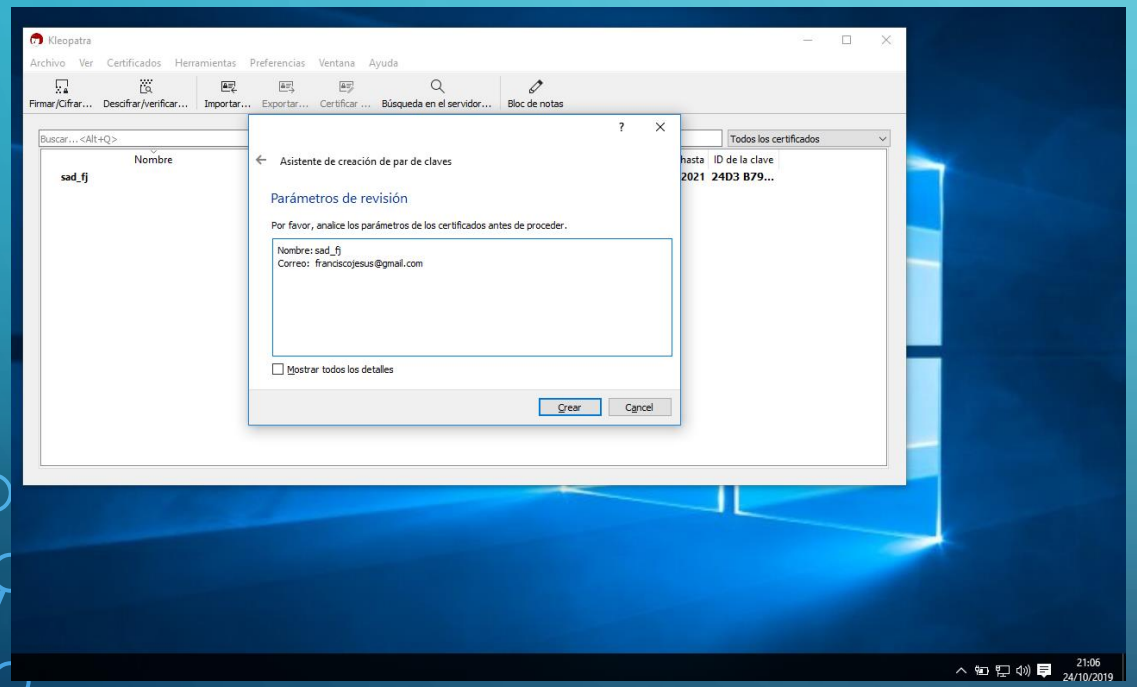


Le damos un nombre y correo.

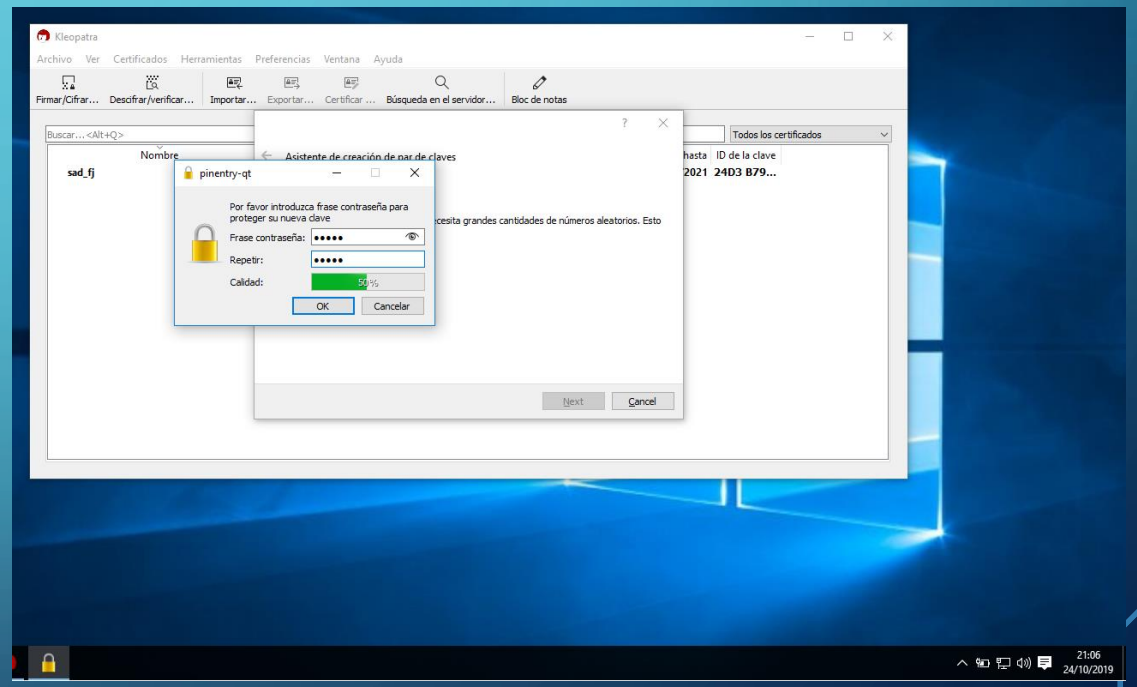


GP4WIN

Veremos un resumen, pulsamos en *Crear*.

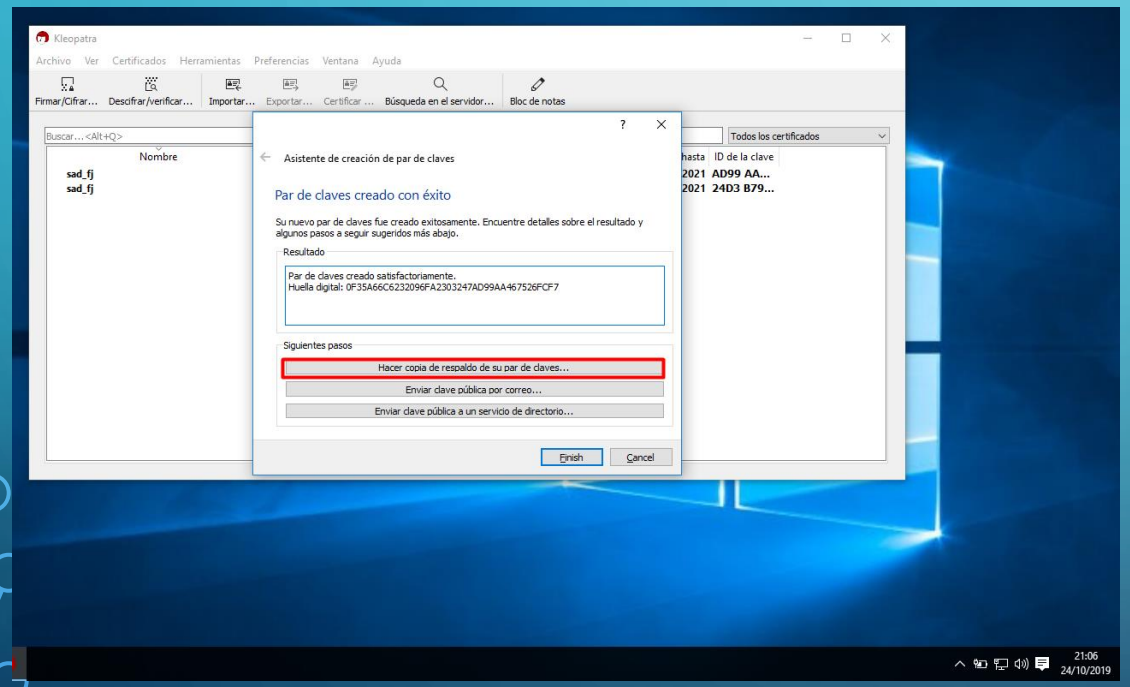


Nos pedirá una contraseña nueva para esas claves.

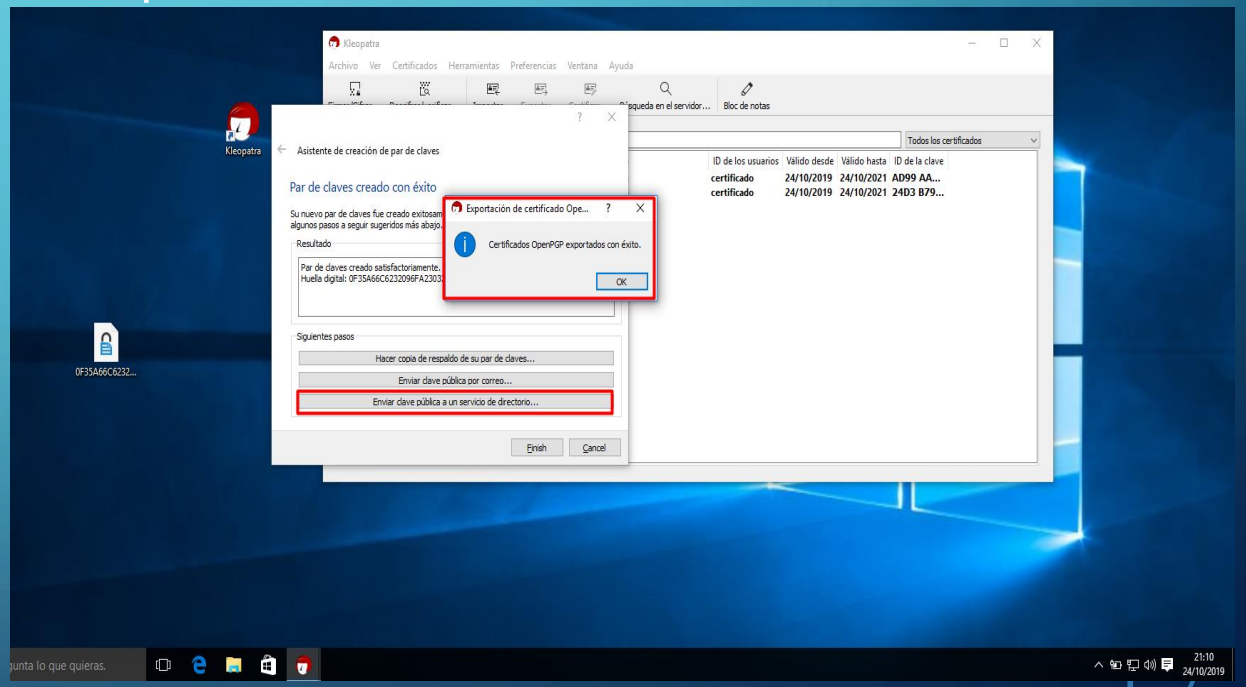


GP4WIN

Pulsamos en *Hacer copia* para guardar la clave secreta en un lugar seguro.

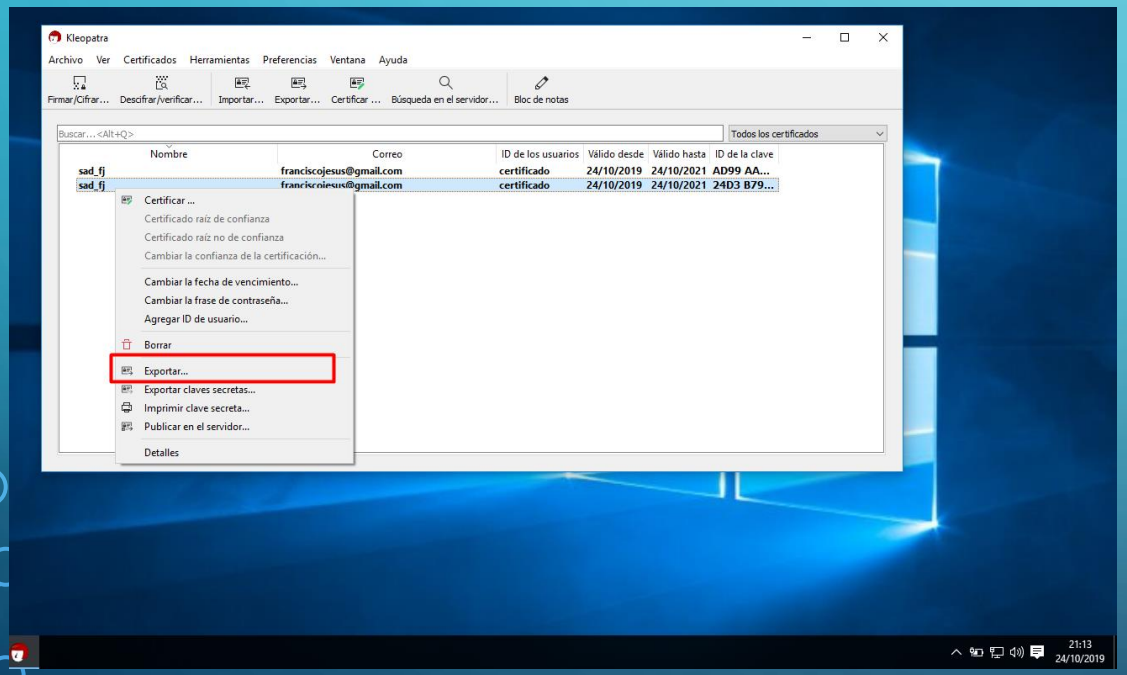


Escogeremos el lugar donde exportar la clave secreta y veremos como nos envía un mensaje que se exporta correctamente.

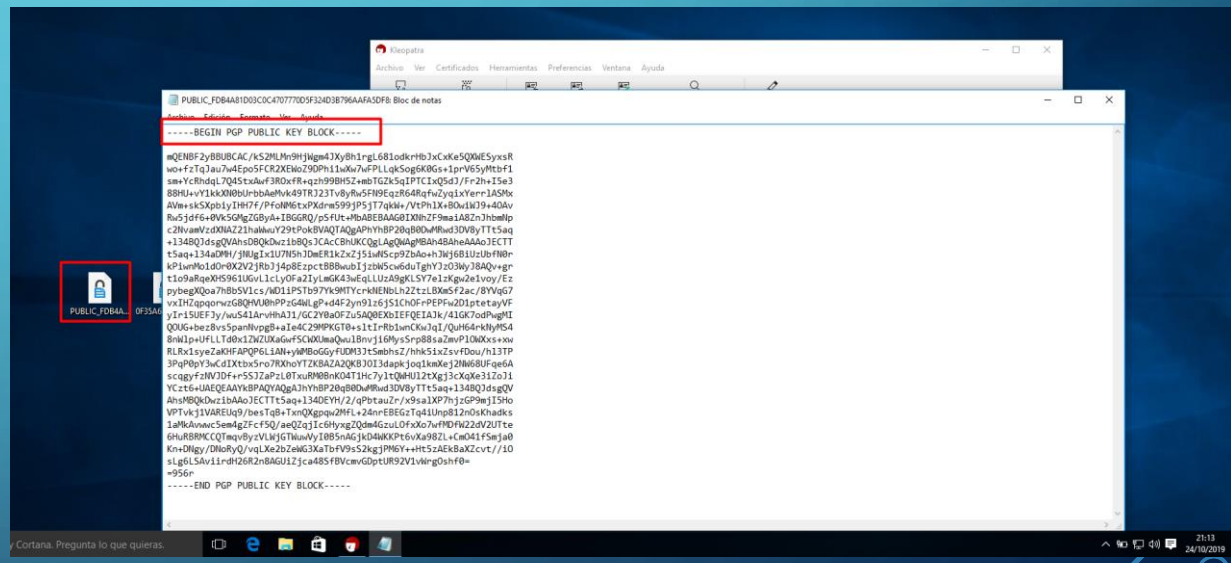


GP4WIN

Pulsamos *Exportar* para exportar la clave publica y así poder cifrar.

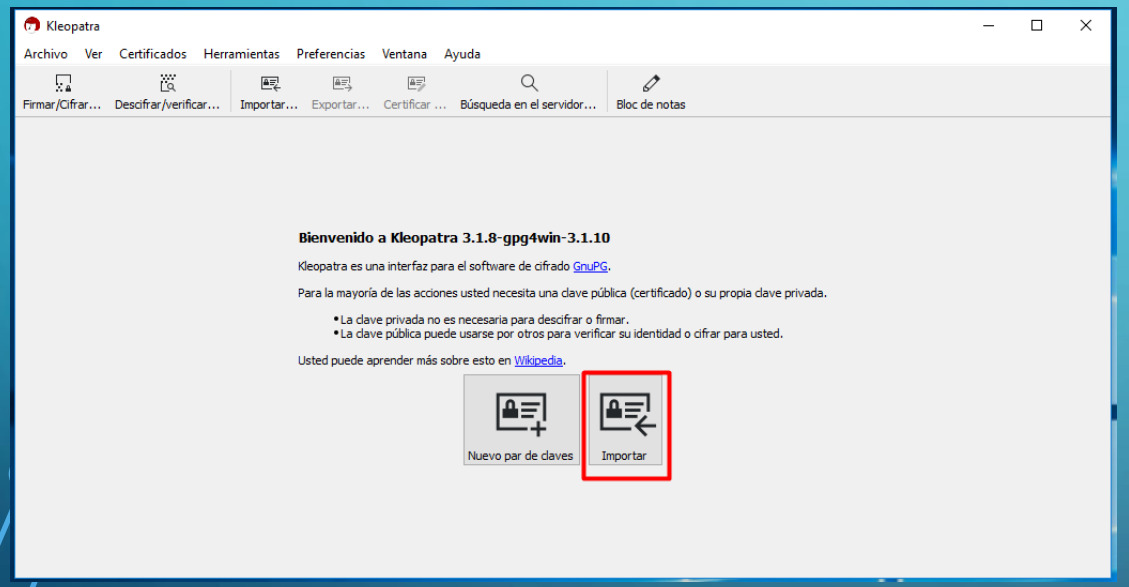


Vemos como exporta la clave publica.

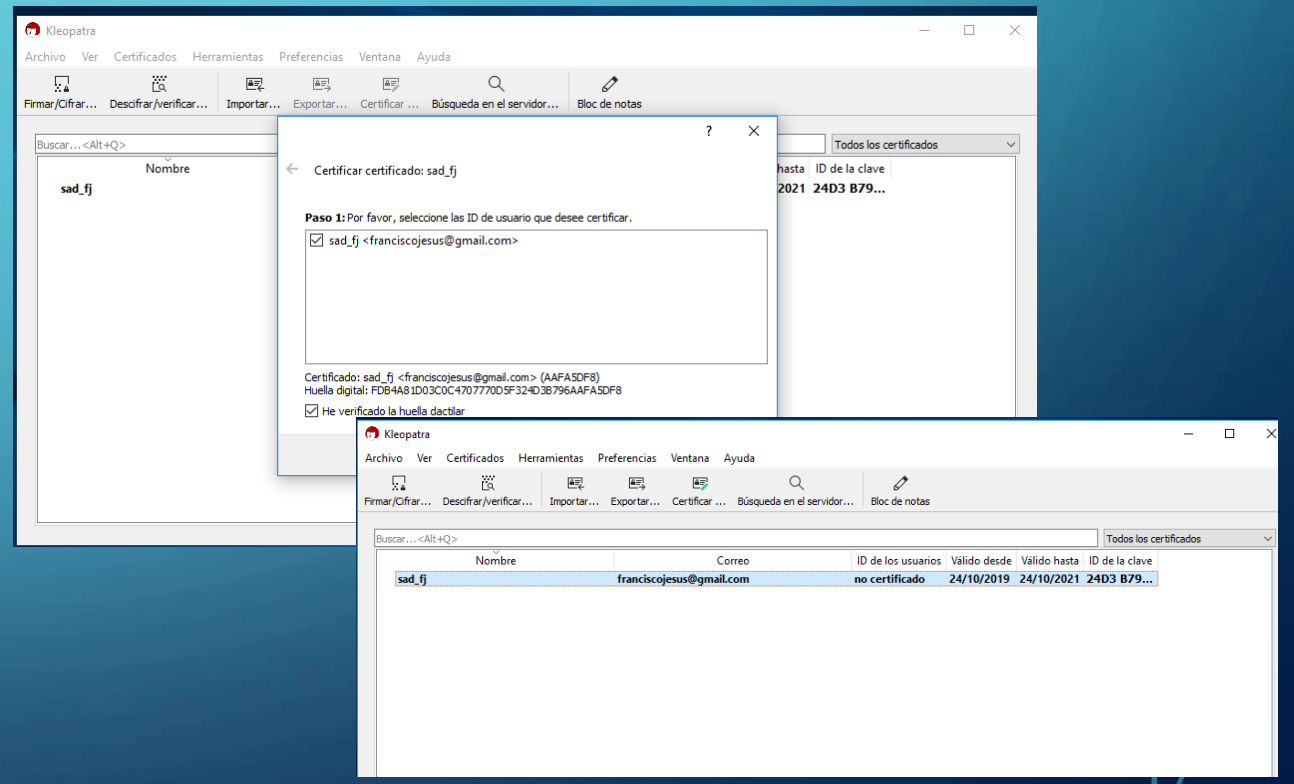


GP4WIN

Ahora en otro equipo con GP4Win instalado importamos la clave publica.

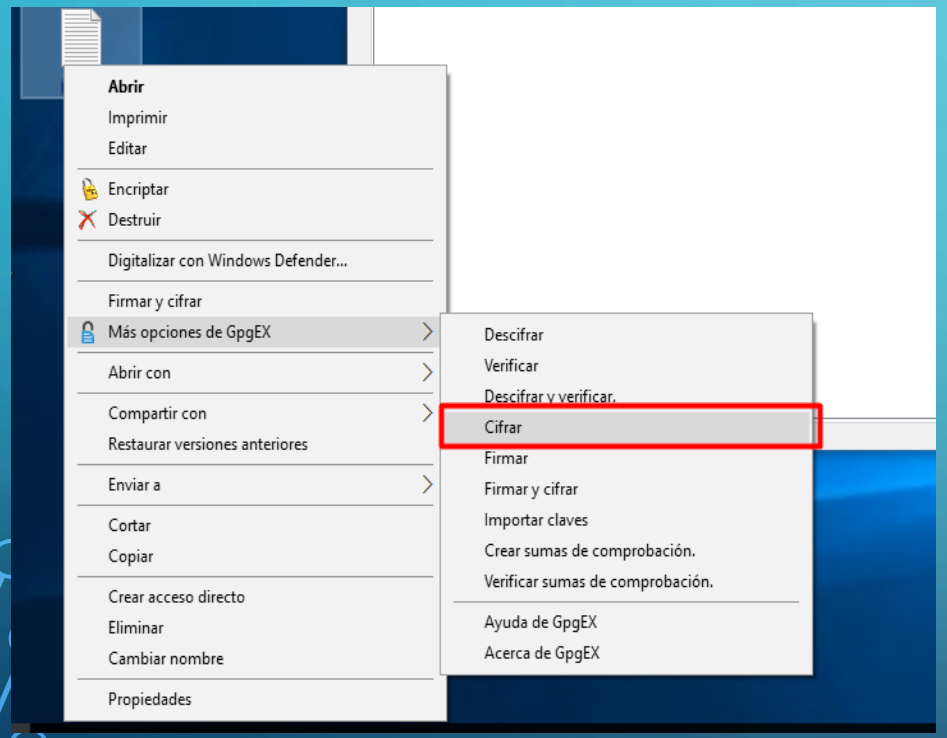


Importamos la clave publica.

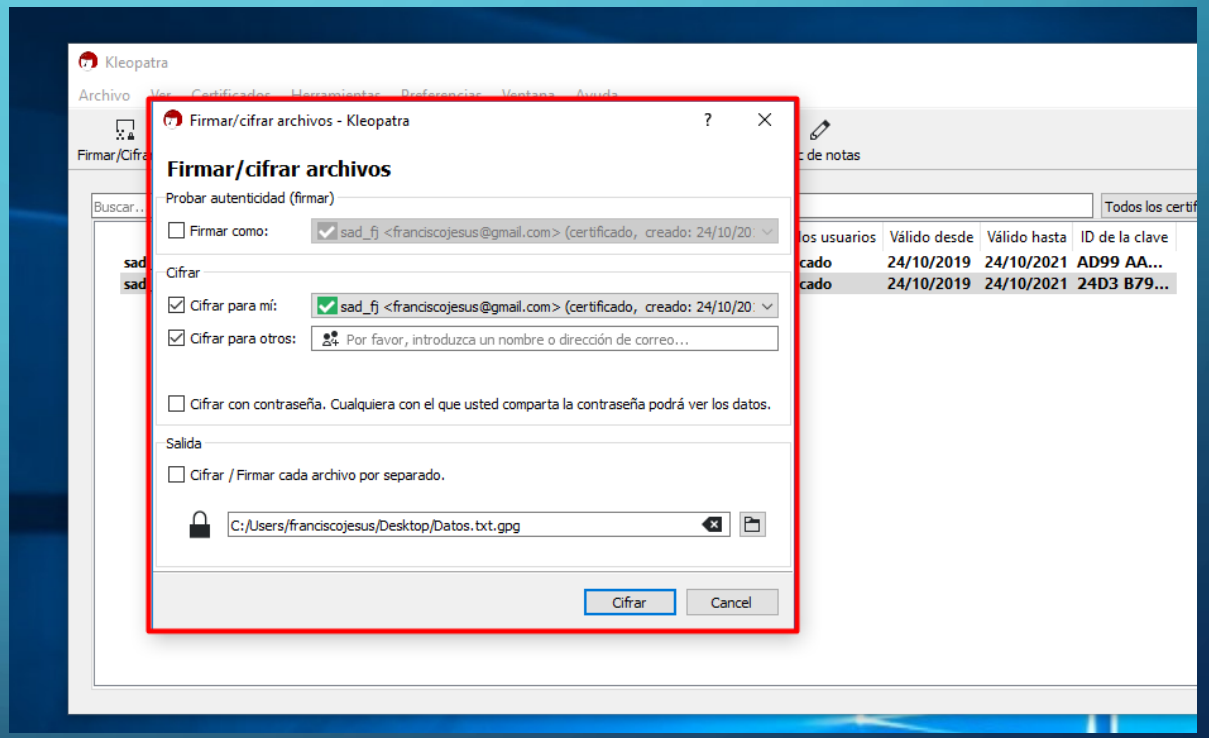


GP4WIN

Una vez realizado esto podemos cifrar el archivo.

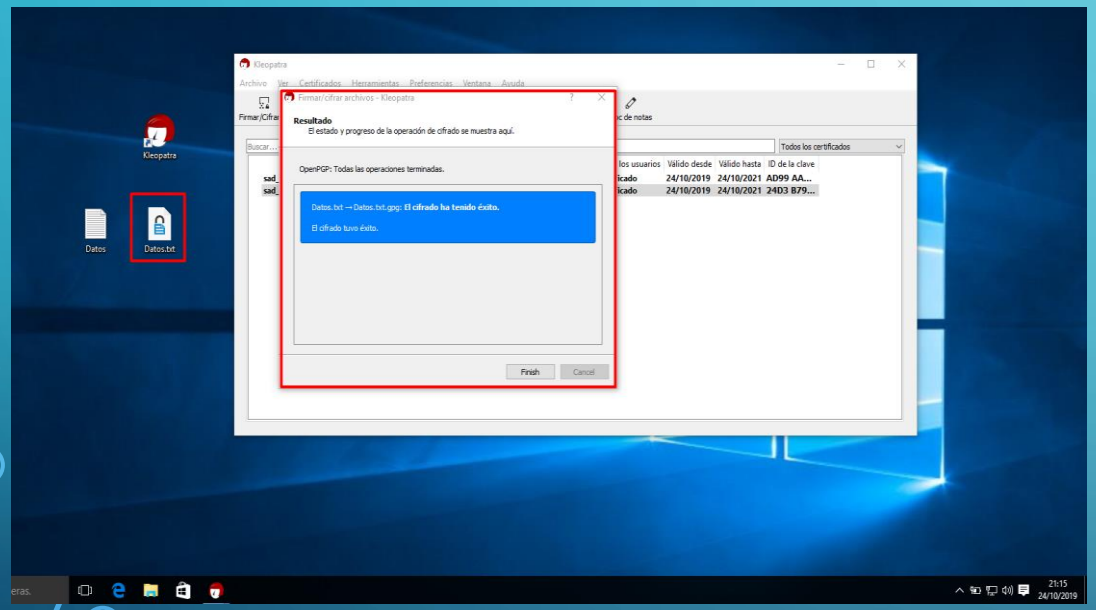


Pulsamos en *Cifrar.*

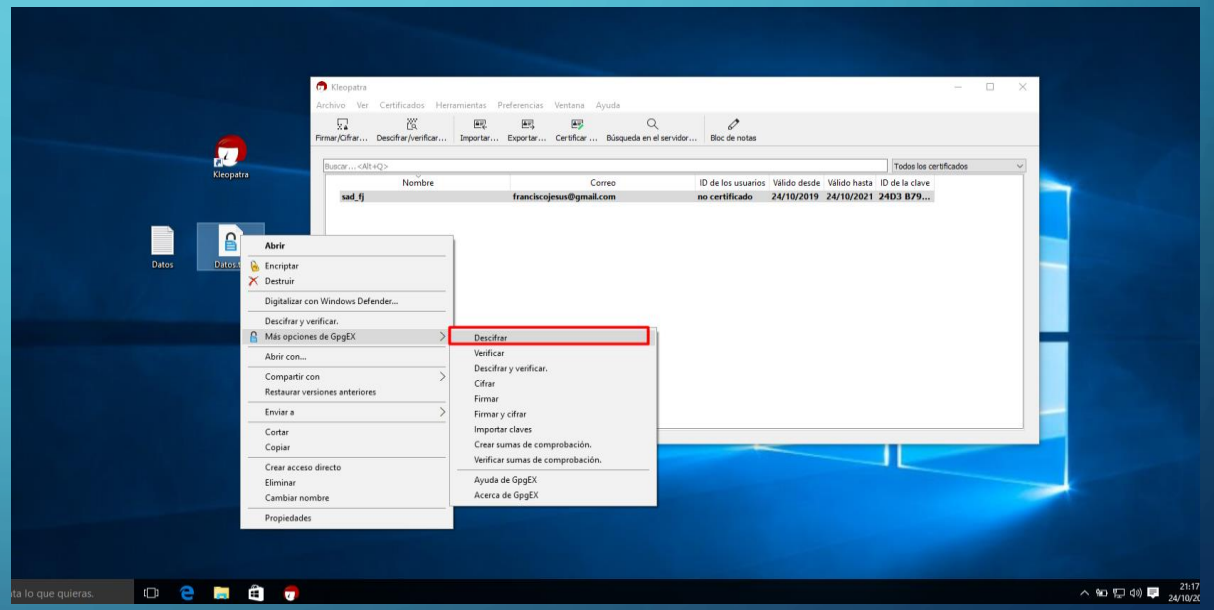


GP4WIN

Vemos como se cifra.

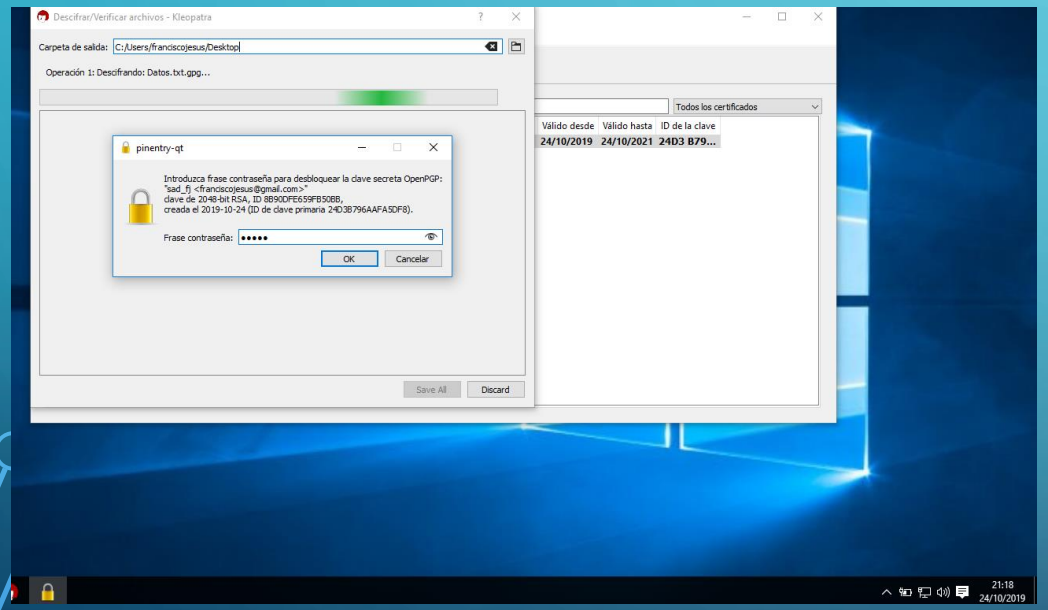


Ahora enviaremos la el archivo cifrado al equipo donde hemos creado el par de clave y descifraremos el archivo.

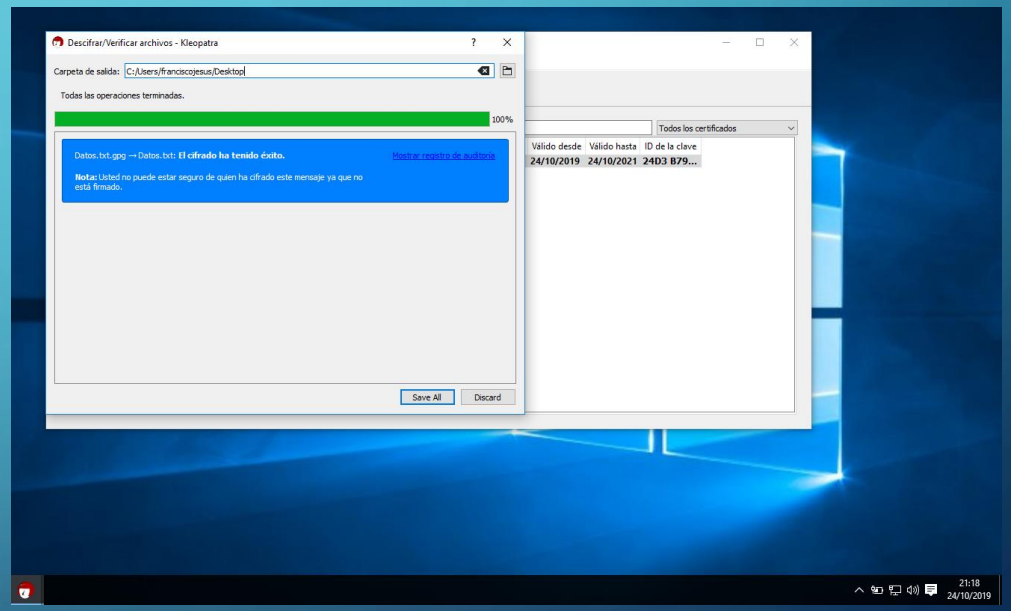


GP4WIN

Nos pedirá la contraseña ya que el equipo en el que generamos las claves tiene de por si la claves secreta para poder descifrarlo.

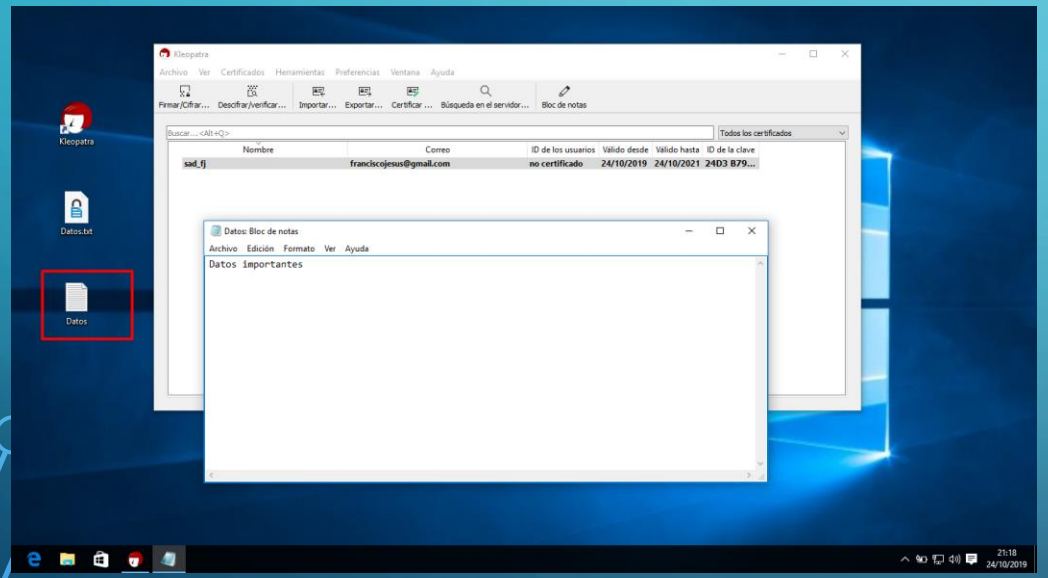


Vemos como se descifra correctamente.

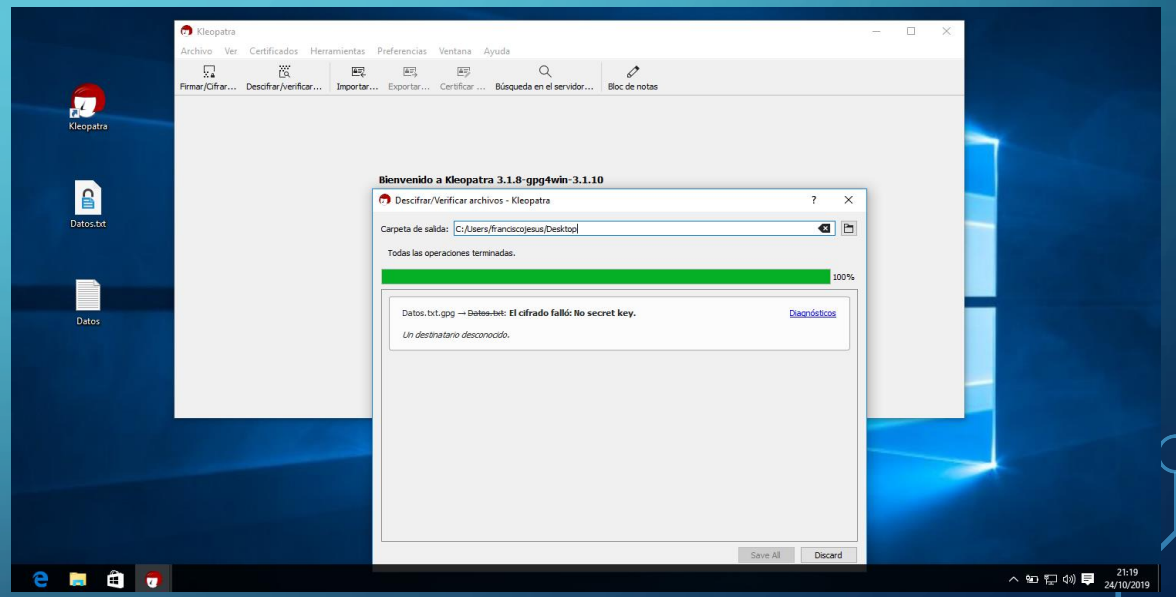


GP4WIN

Vemos como se descifra y podemos ver correctamente su contenido.

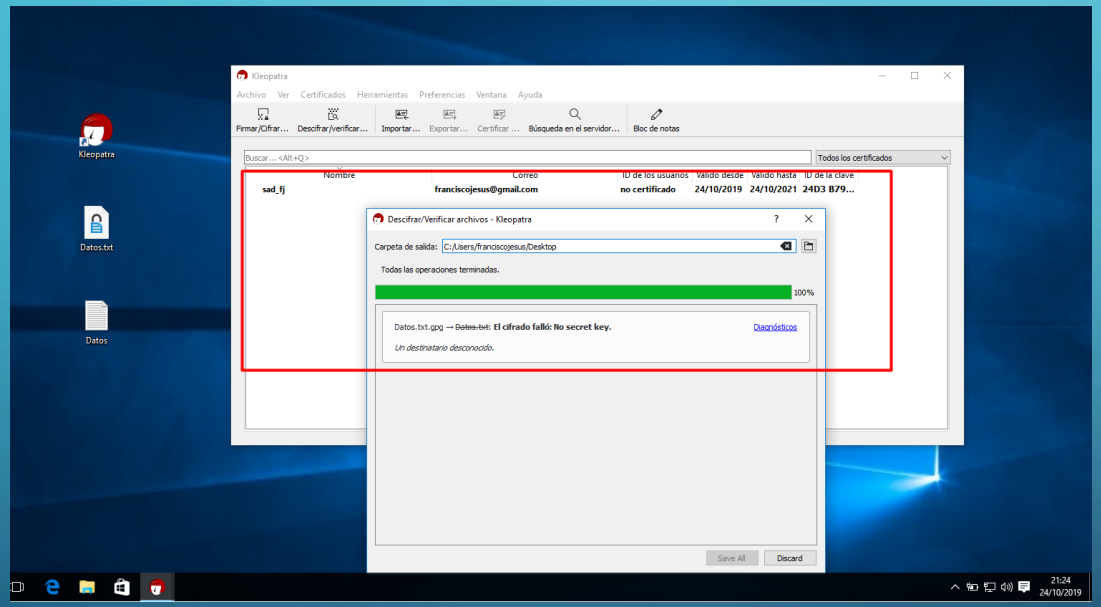


Si llevamos el archivo cifrado a otro equipo no podemos visualizar el contenido.



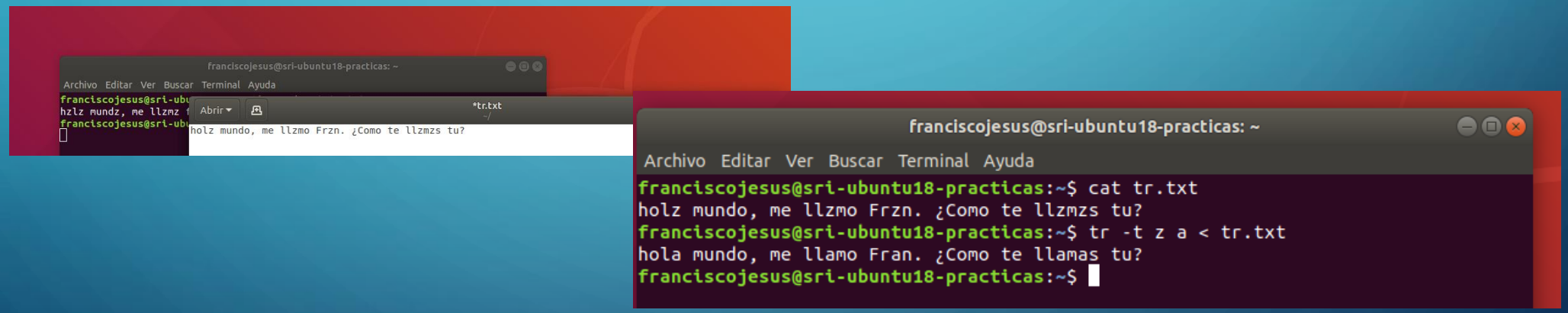
GP4WIN

Si intentamos descifrarlo con la clave publica tampoco podremos.



TR

Traduce su entrada standard sustituyendo cada carácter del primer argumento por el que se encuentra en la misma posición en el segundo argumento. Su uso es muy fácil, crearemos un archivo con una frase sustituyendo la A por la Z. Después, aplicaremos el comando tr para descifrarlo.



CONCLUSIÓN

- La práctica ha sido sencilla y muy entretenida, he podido aprender aún más sobre los cifrados y la clave secreta y pública además de saber usarlo ahora mucho mejor. Una práctica esencial para poder mandar archivos cifrados y que nadie lo intercepte y lo pueda leer.