

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

FRANCISCO JESÚS GARCÍA – UCEDA DÍAZ - ALBO

ÍNDICE

- INTRODUCCIÓN
- CryptoForge
- GP4Win
- Tr
- Conclusión

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.](#)



The screenshot shows the official website for CryptoForge. The browser address bar displays 'criptoforge.com.ar'. The website header includes navigation links: 'Inicio | Descargar | Seguridad | Comprar | Referencias | Preguntas | Ayuda'. The main content area features a central graphic of a document with a padlock and the text 'Proteja su información, donde sea que vaya'. To the right of this graphic are two prominent buttons: a blue 'Descargar' button and a green 'Comprar' button. Below the main graphic, there are two columns of text. The left column is titled 'Encriptación' and describes the program's capabilities. The right column is titled 'Características y Beneficios' and lists several key features. At the bottom of the page, there is a Windows taskbar with the Cortana search bar and the system clock showing 20:30 on 24/10/2019.

Inicio | Descargar | Seguridad | Comprar | Referencias | Preguntas | Ayuda

Encriptar

www.CryptoForge.com

Proteja su información, donde sea que vaya

Descargar

Comprar

Encriptación

CryptoForge™ es un programa de **encriptación** de datos para **seguridad profesional**. Permite **encriptar** archivos, carpetas, y mensajes confidenciales con hasta cuatro algoritmos de encriptación robustos. Una vez que los datos han sido encriptados o cifrados, pueden ser guardados en un medio inseguro como una unidad USB, o en la nube, o transmitidos por una red insegura (como Internet), y aún así permanecer secretos. Luego, los datos pueden ser descifrados a su formato original. CryptoForge es un conjunto de programas para encriptar datos, archivos, carpetas, unidades USB y de cualquier tipo, y email, que le añaden al Windows la más robusta encriptación disponible hoy día. Está diseñado para ocultar la complejidad de la tecnología para encriptar, y es realmente muy fácil de usar o de integrar en otros sistemas.

Descargar

► Más acerca de encriptación de datos

► ¿Es fácil encriptar archivos?

► ¿Es fácil encriptar carpetas?

Versión en inglés:

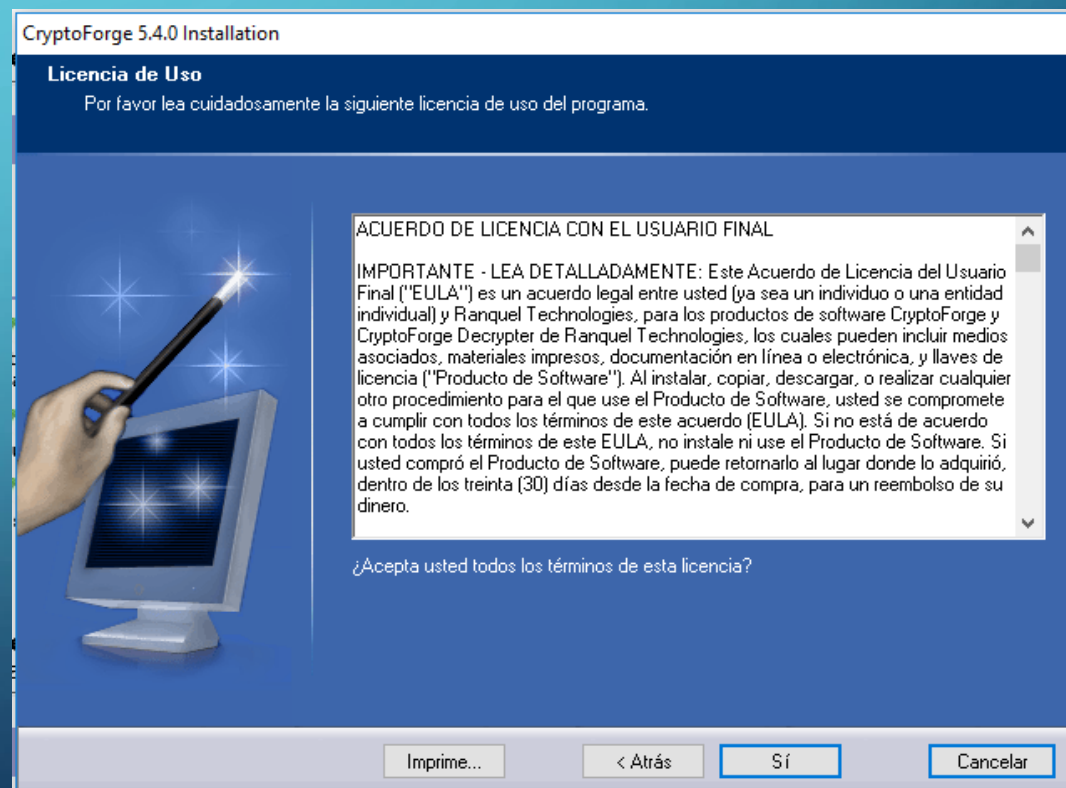
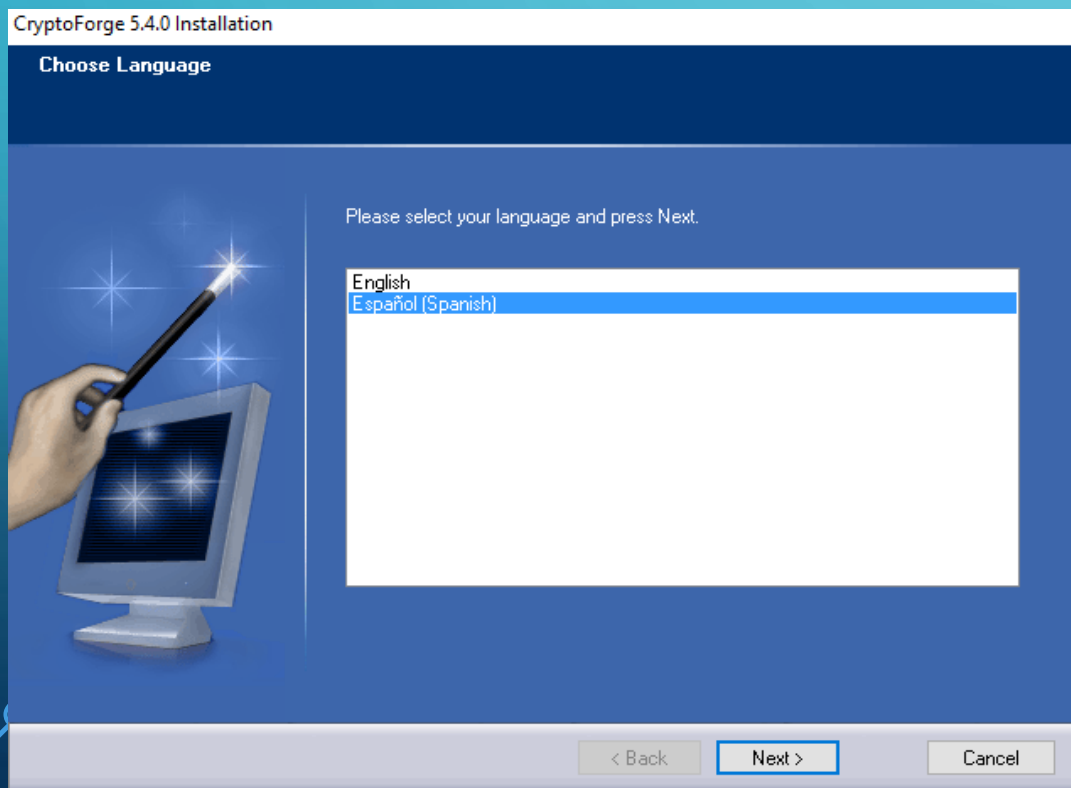
Características y Beneficios

Las características y beneficios del programa para encriptar CryptoForge incluyen:

- Rápido para **descargar**, simple de instalar, y muy **fácil de usar**.
- Basado en algoritmos para encriptar de dominio público - La robusta encriptación empleada por CryptoForge es la mejor disponible hoy día.
- Ataque por fuerza bruta impracticable - Con mil millones de ordenadores capaces de probar mil millones de contraseñas por segundo cada uno, y empleando un algoritmo con llave de apenas 168 bits, se necesitarían 10*10²⁴ años de trabajo para probar todas las contraseñas posibles (para comparar, la edad del universo se estima en 10*10⁹ años).
- Encriptación múltiple - Sus datos estarán seguros, aún sin el futuro uno de los algoritmos para encriptar fuese atacado con éxito.
- Destructor de archivos incorporado - Cumpliendo y excediendo las especificaciones DoD (Departamento de Defensa de EEUU).
- Potente compresión incorporada - Además de reforzar todavía más la seguridad criptográfica, la compresión reduce el espacio de almacenamiento requerido y los tiempos de transmisión en redes, haciendo sus sistemas más eficientes y ahorrando costos.

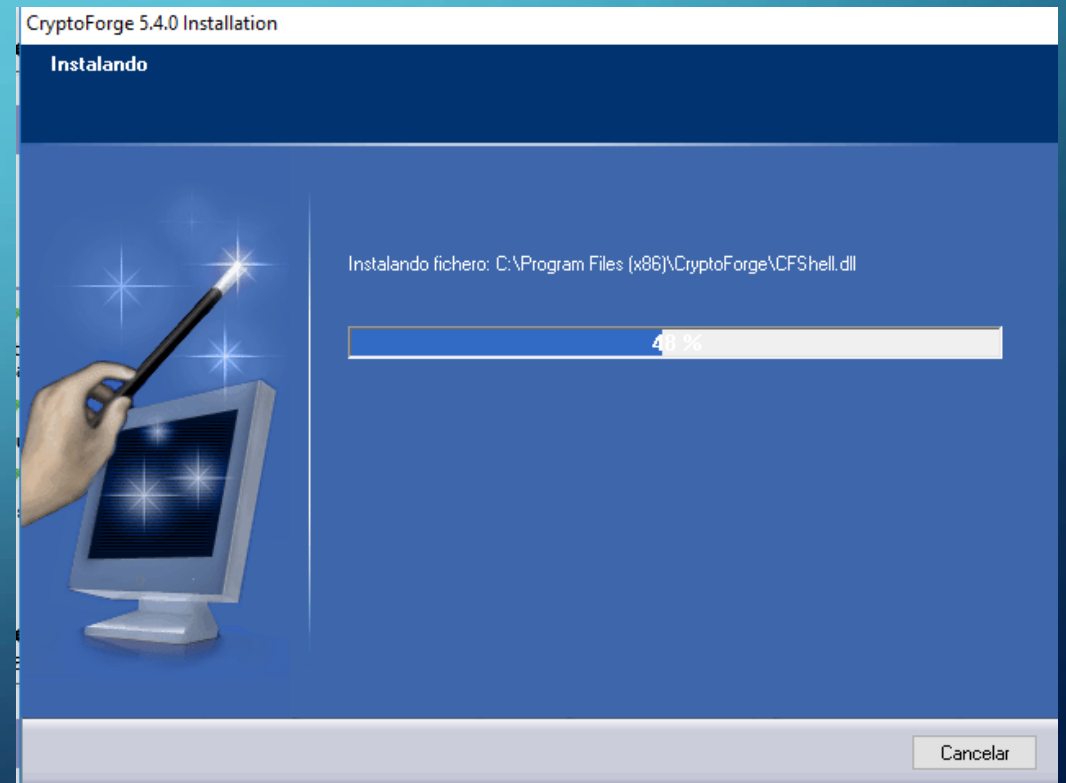
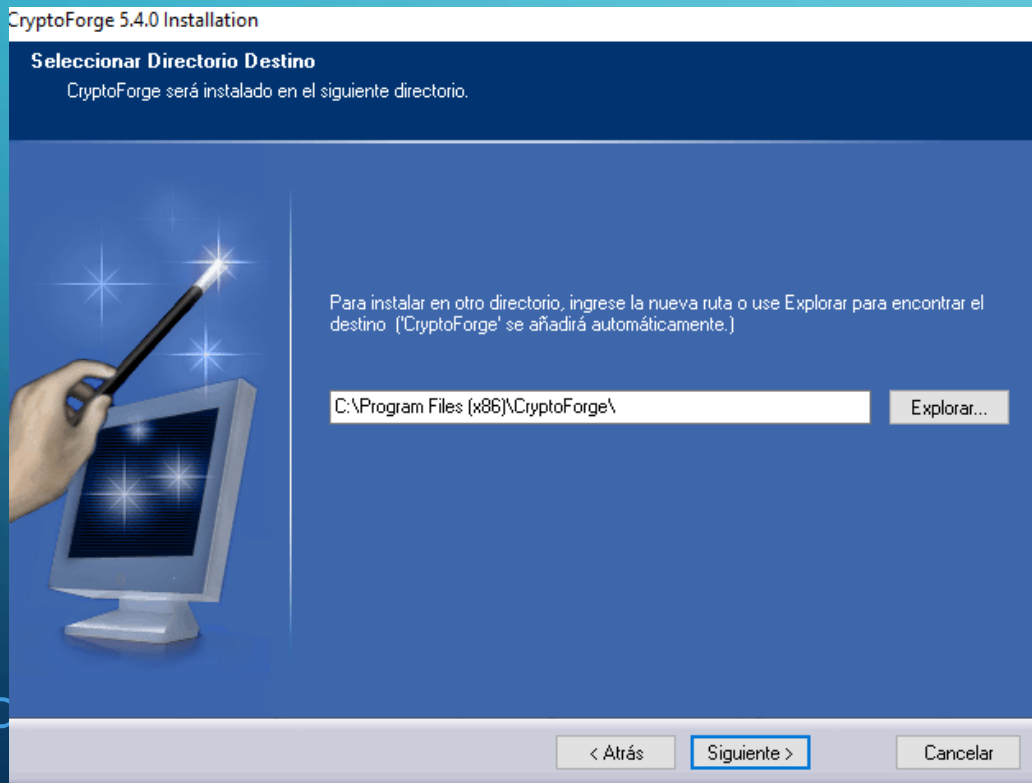
CRYPTOForge

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



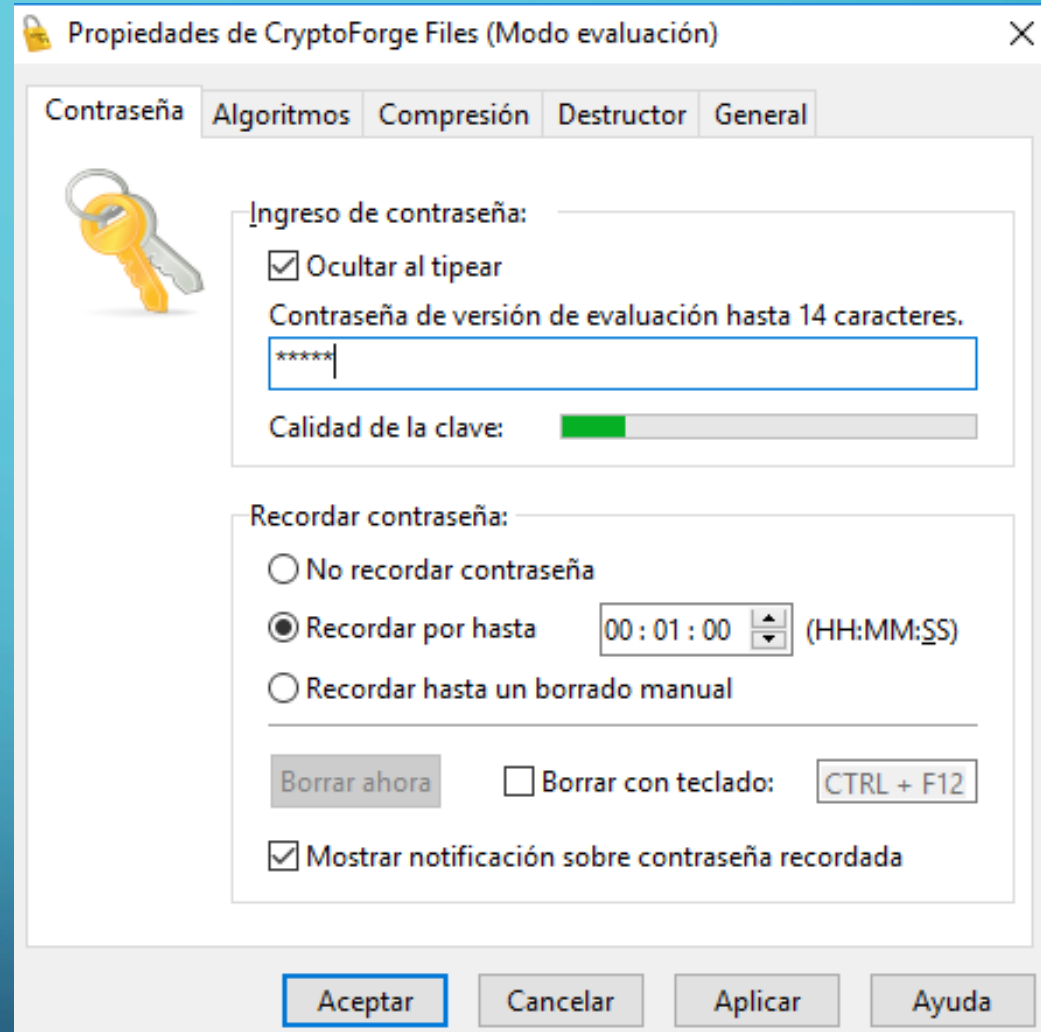
CRYPTOForge

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



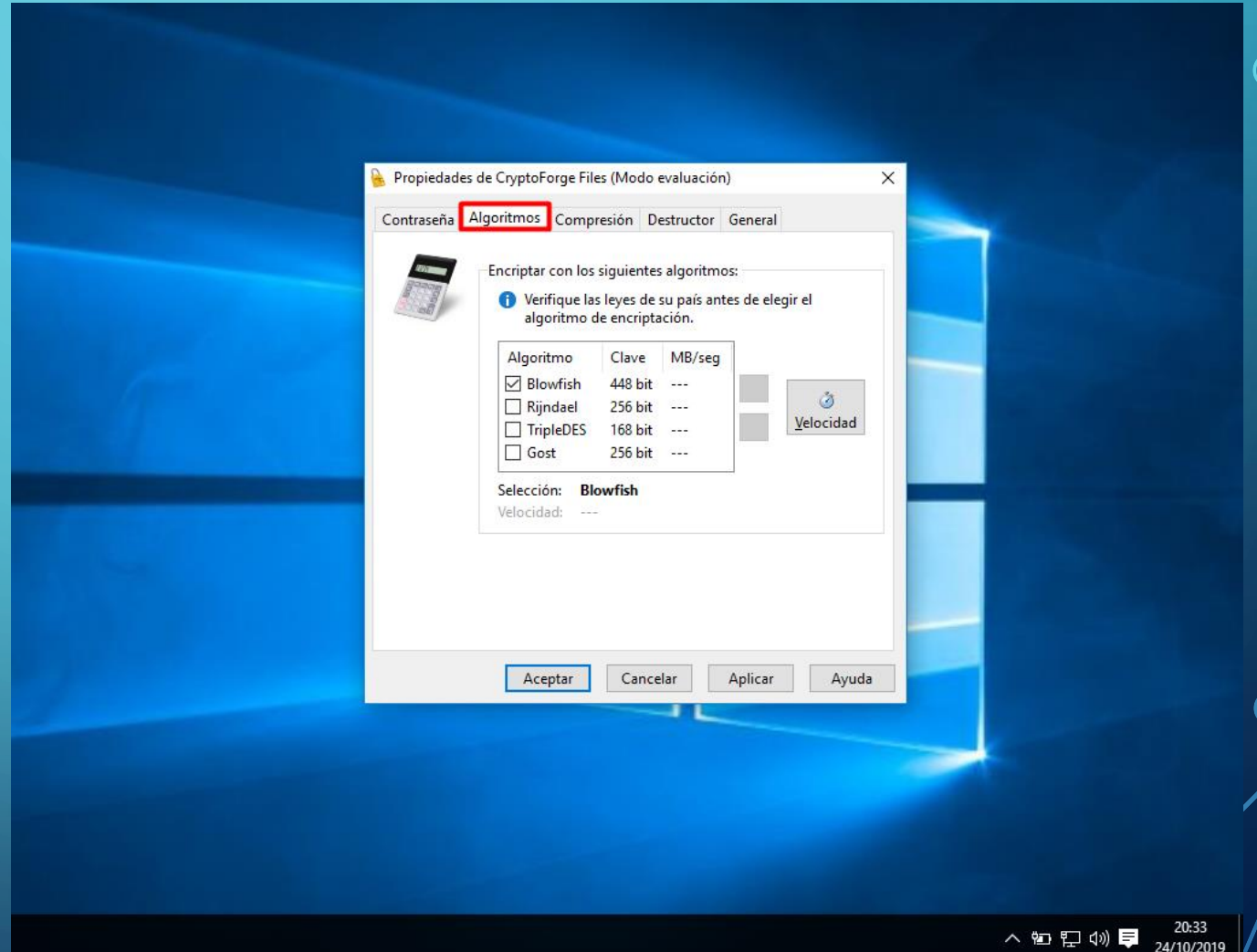
CRYPTOForge

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



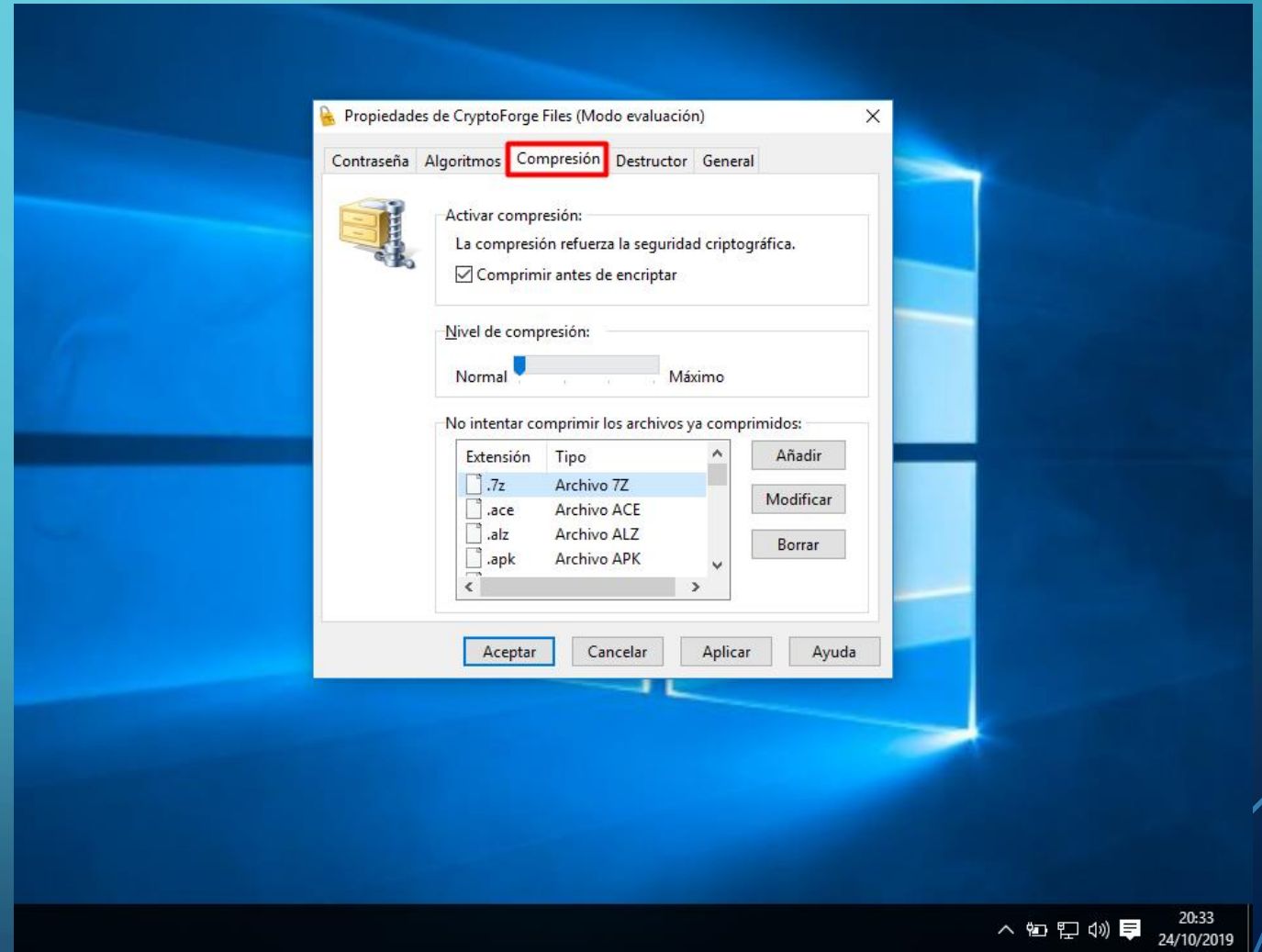
CRYPTOFORGE

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



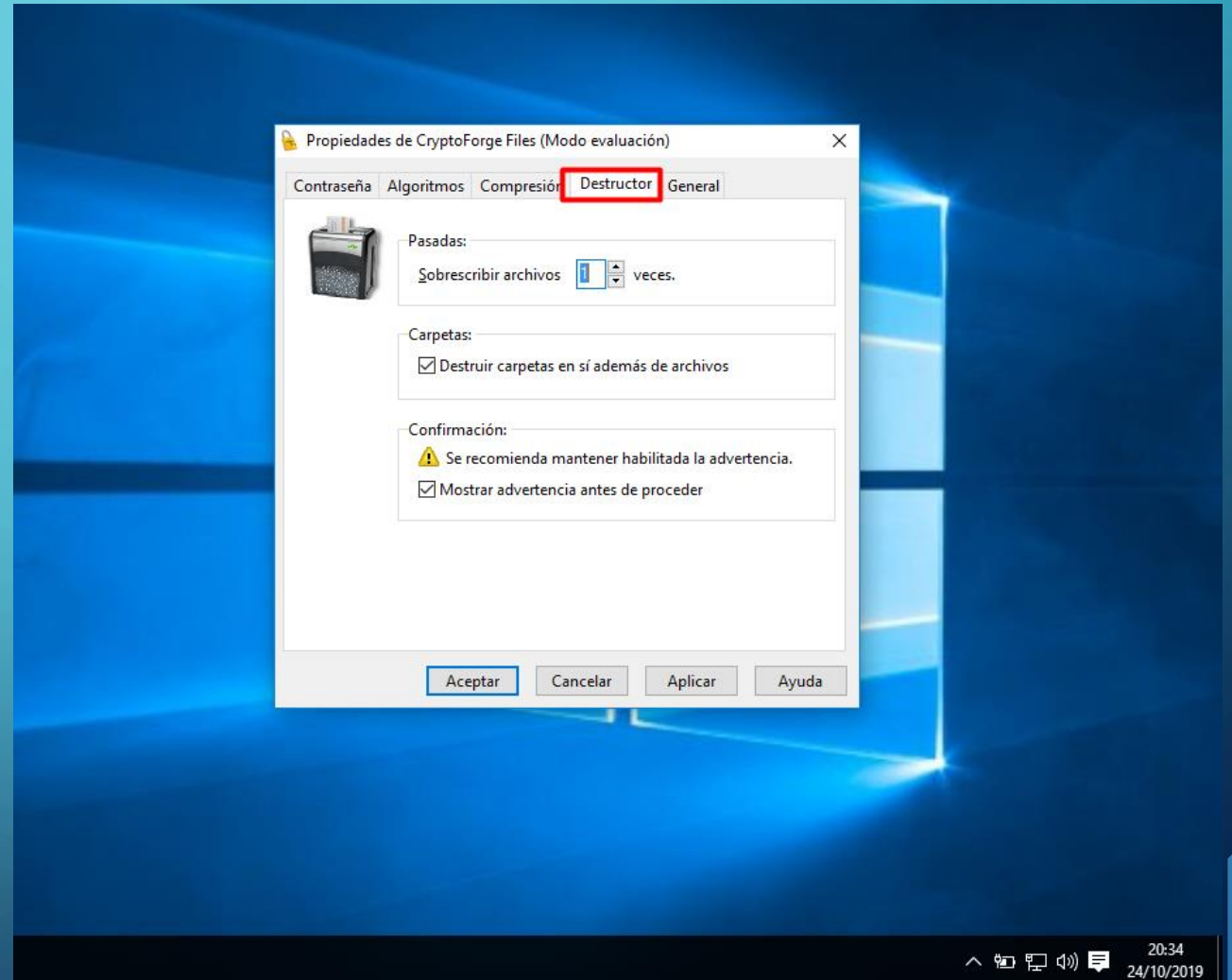
CRYPTOFORGE

- 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.



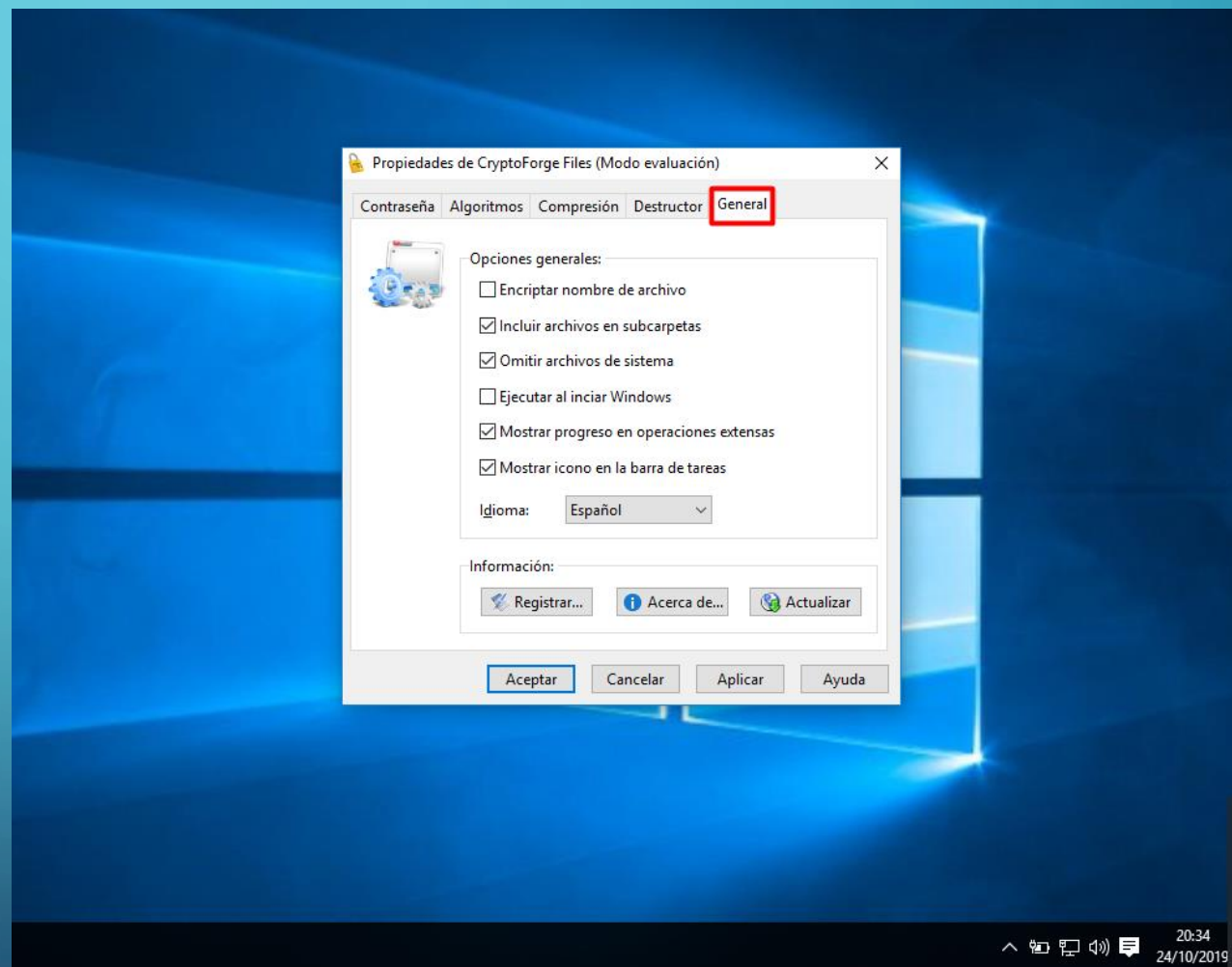
CRYPTOFORGE

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



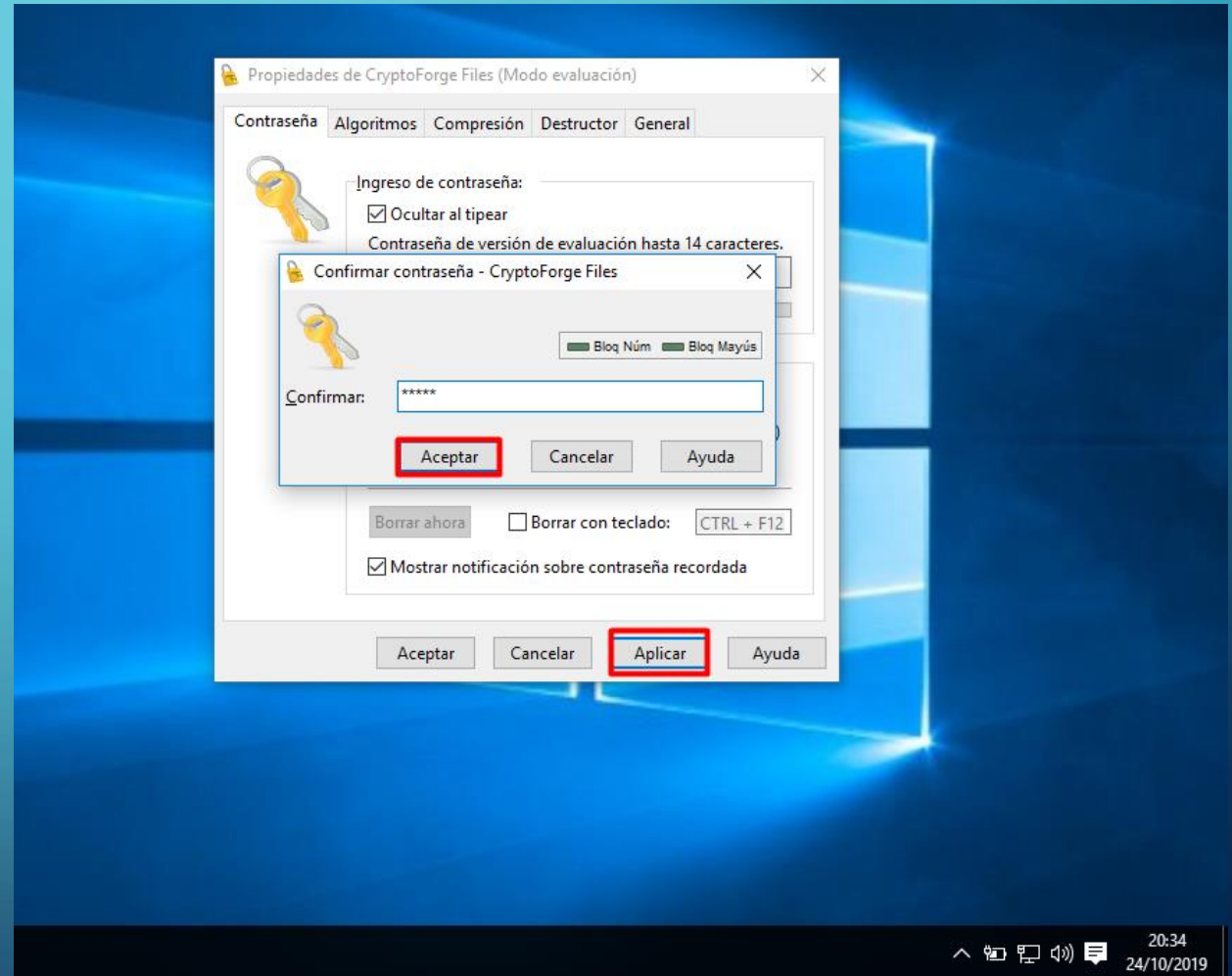
CRYPTOFORGE

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



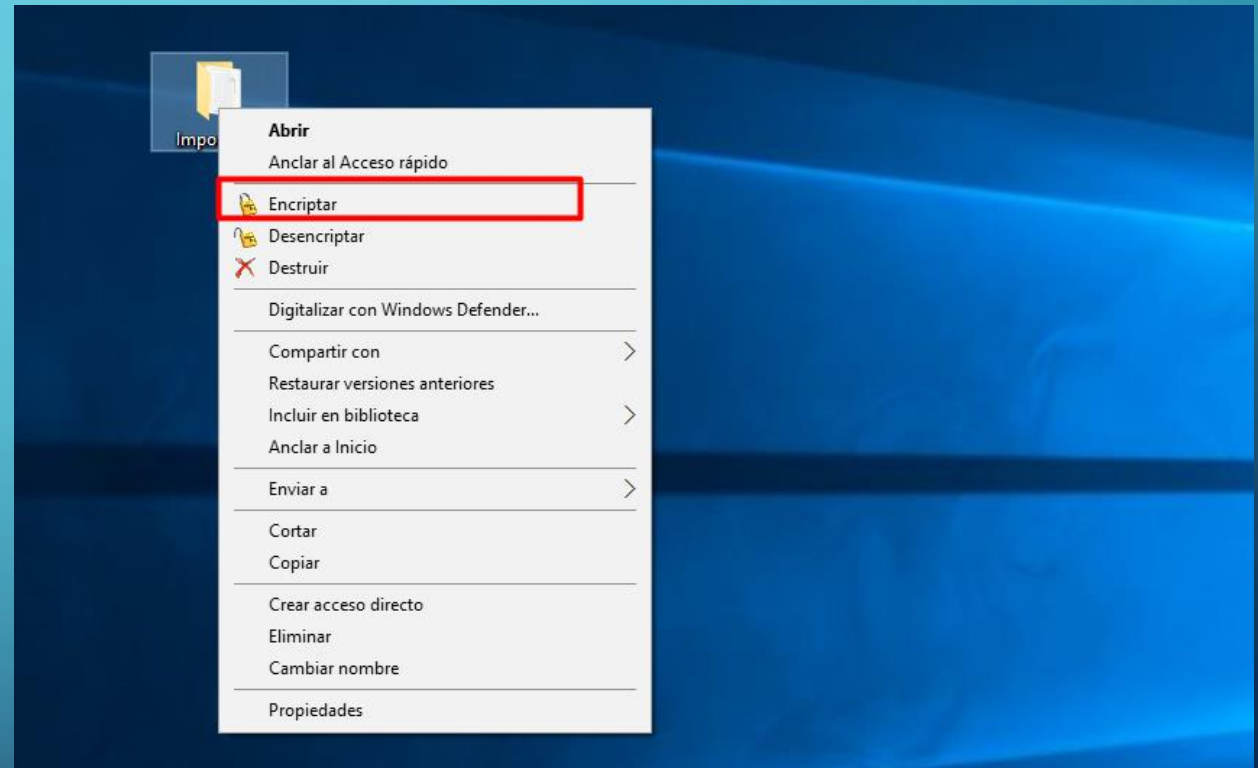
CRYPTOFORGE

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



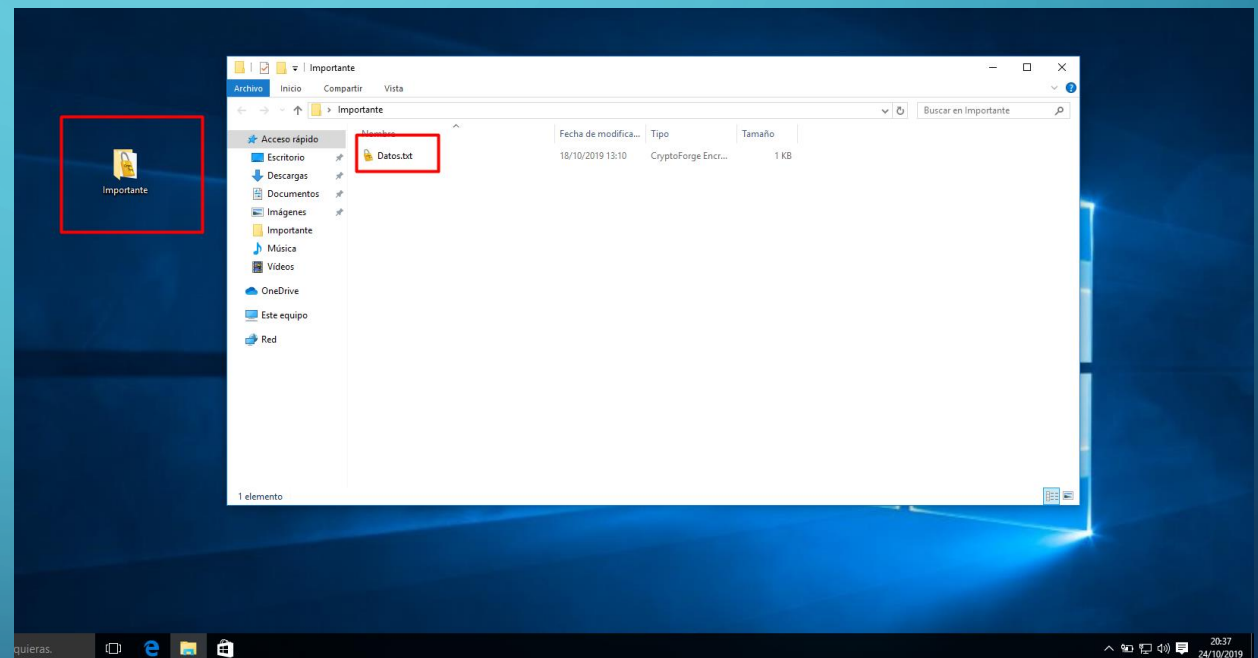
CRYPTOFORGE

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



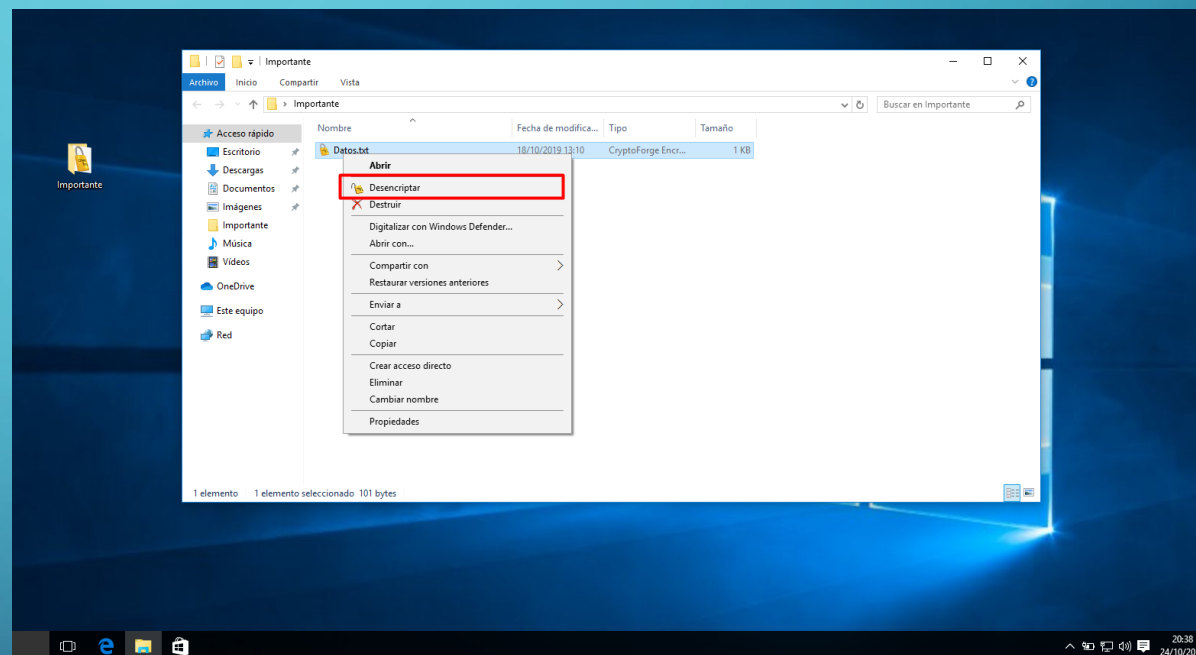
CRYPTOFORGE

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



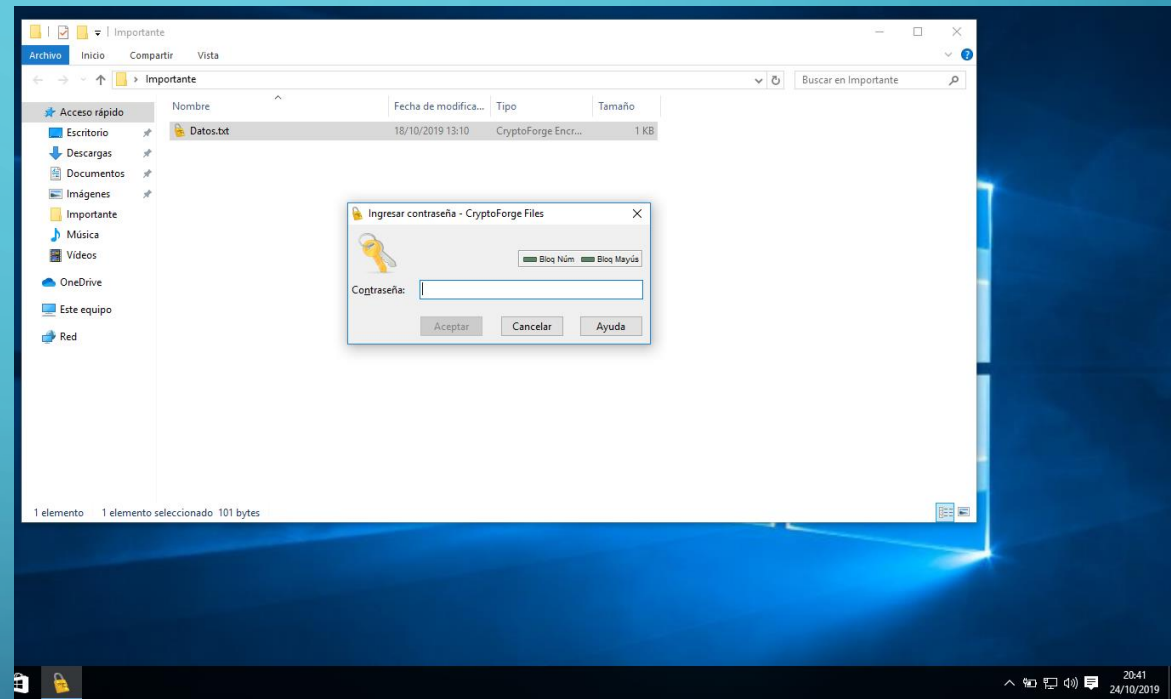
CRYPTOFORGE

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



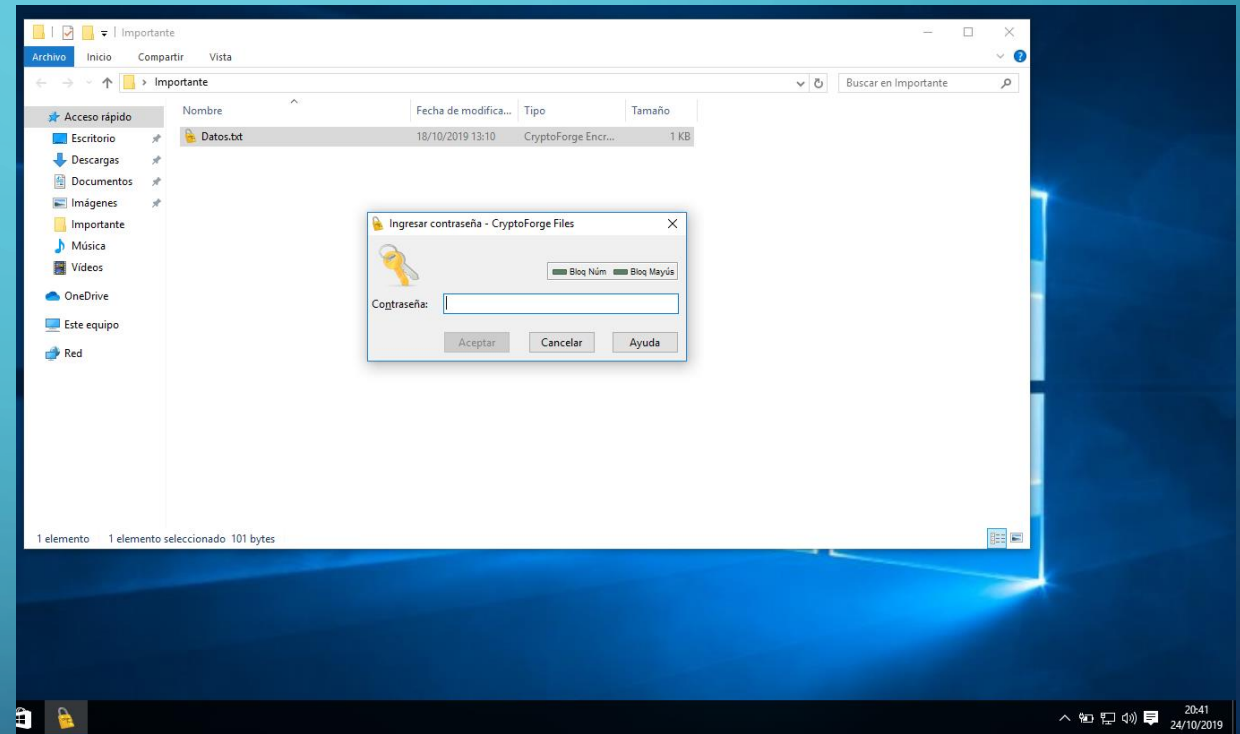
CRYPTOFORGE

- Nos pedirá la contraseña para descriptarlo.



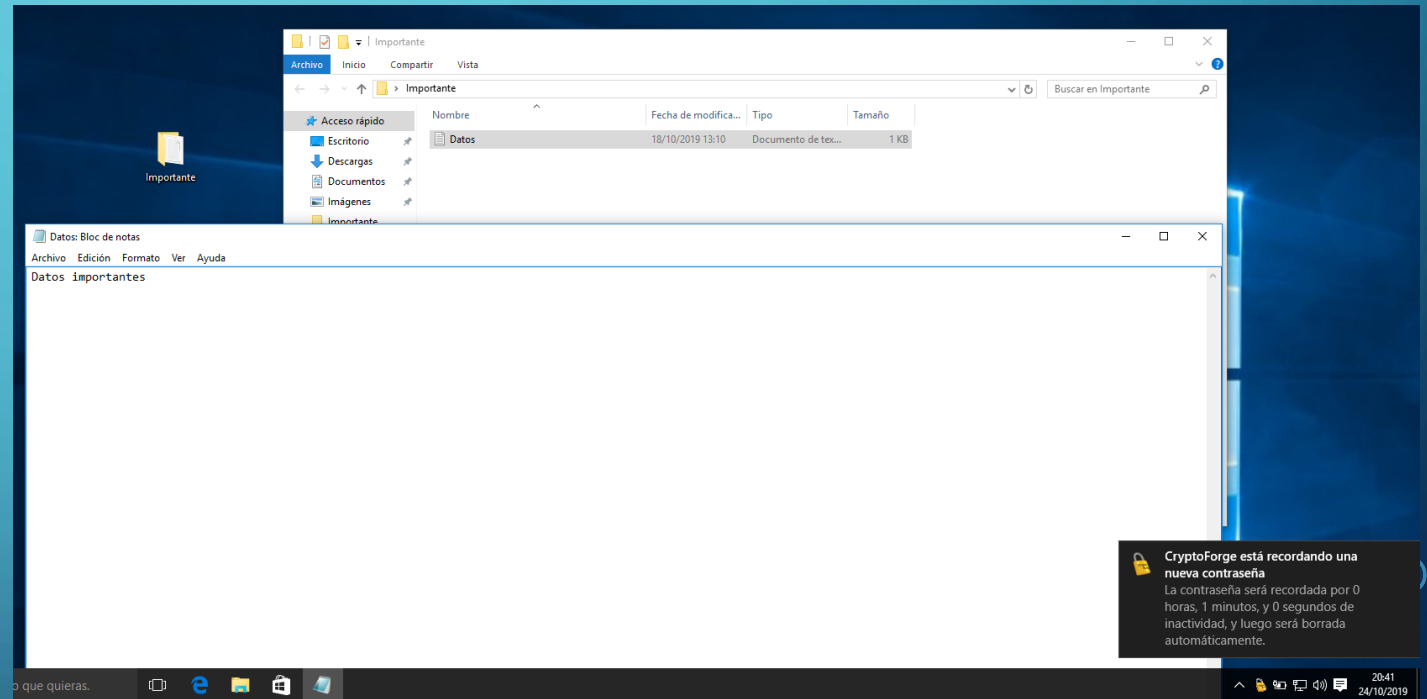
CRYPTOFORGE

- Nos pedirá la contraseña para descriptarlo.



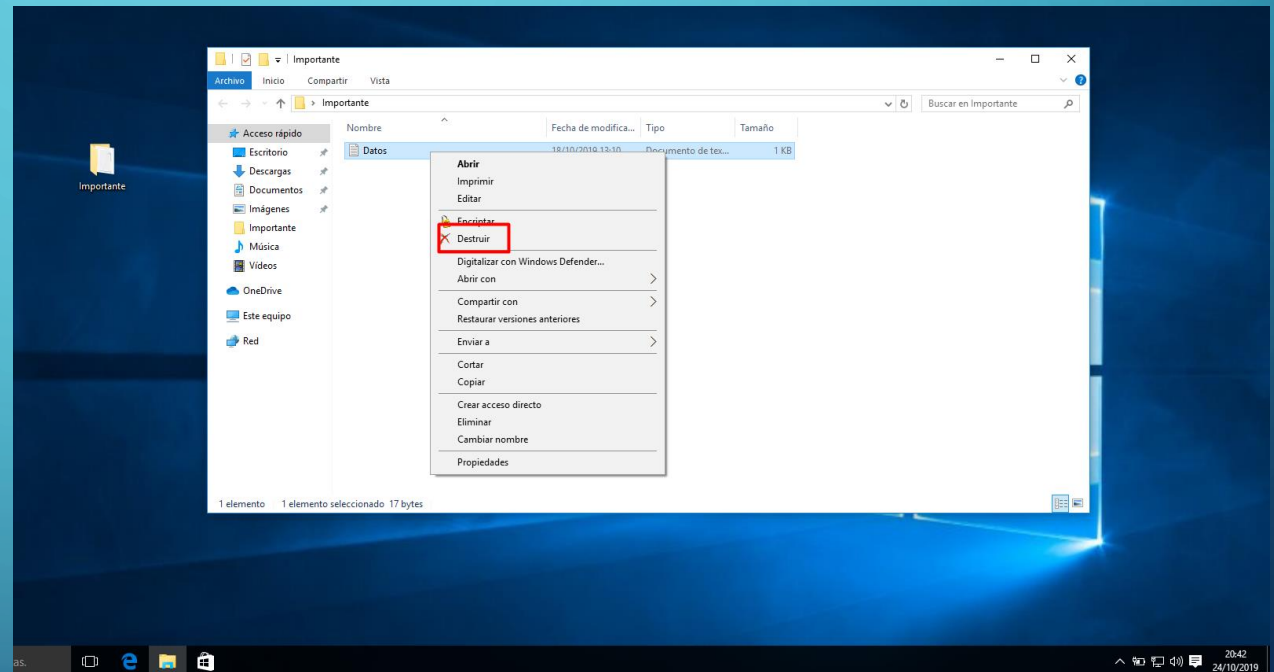
CRYPTOFORGE

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



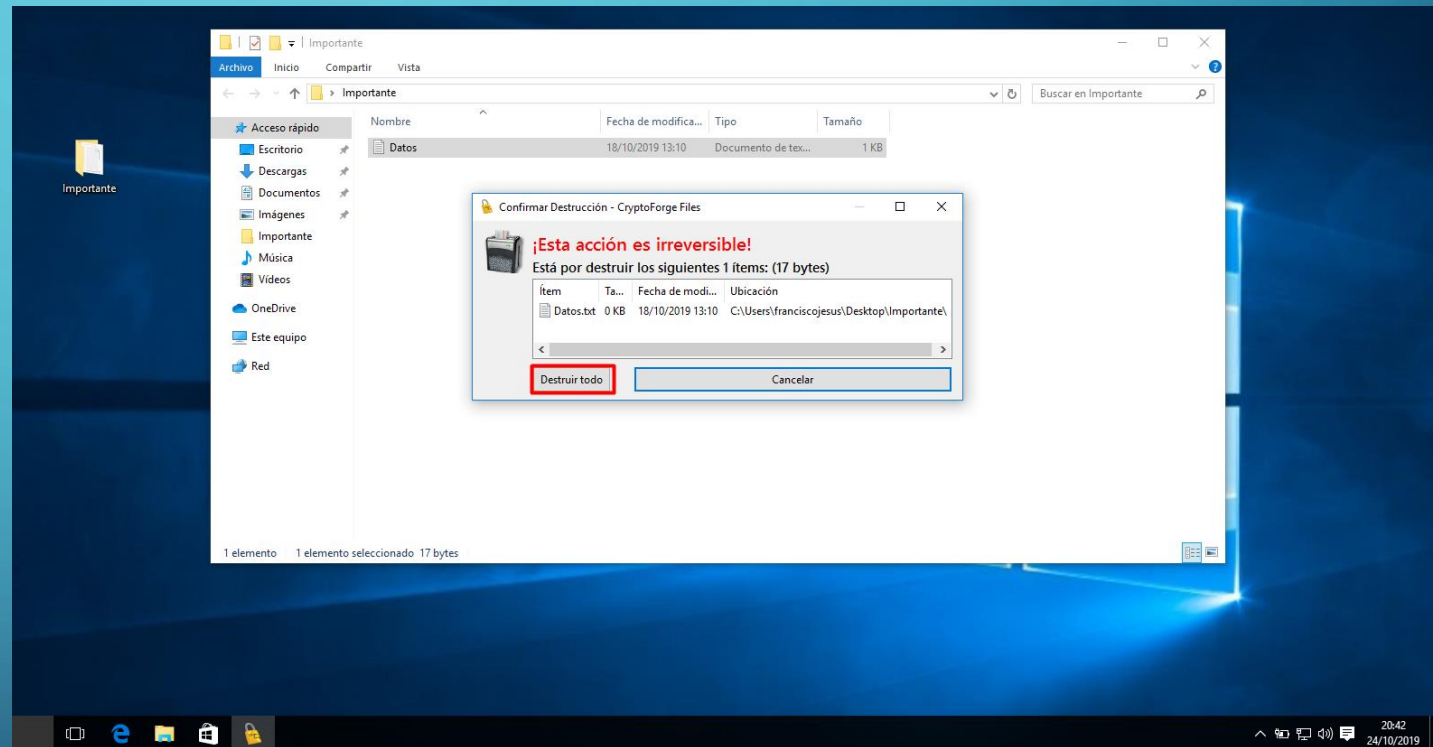
CRYPTOFORGE

- Si pulsamos clic derecho sobre el podremos destruirlo.



CRYPTOFORGE

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

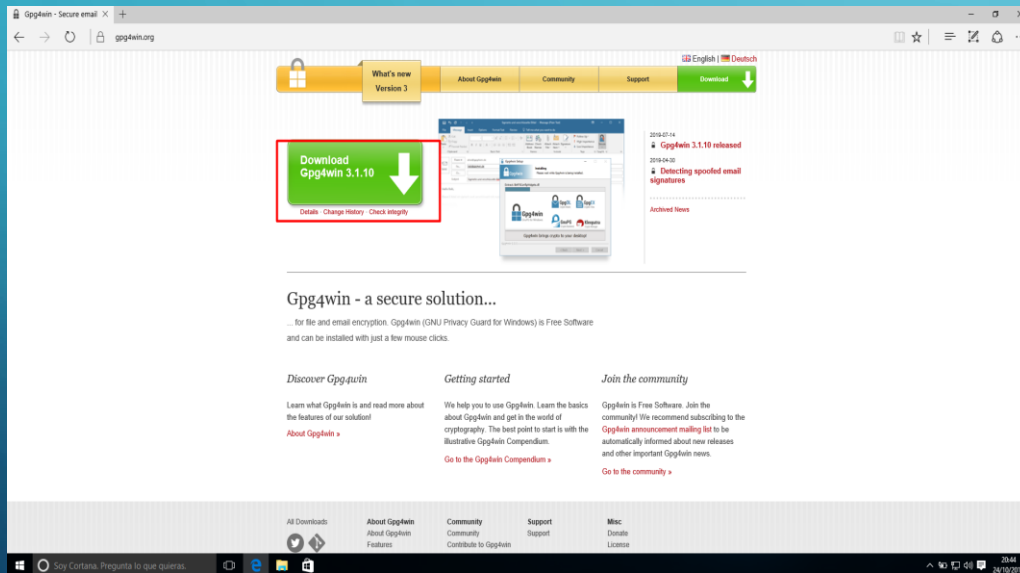


GP4WIN

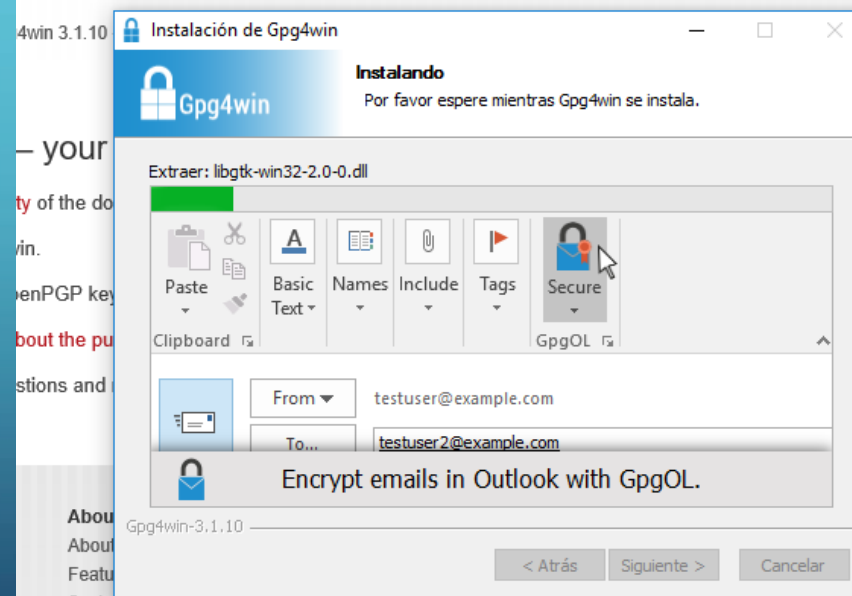
- Gpg4win es un paquete de cifrado de correo electrónico y archivos para la mayoría de las versiones de Microsoft Windows que utiliza criptografía de clave pública GnuPG para el cifrado de datos y firmas digitales.

GP4WIN

Para descargarlo simplemente vamos a su web. [Link](#). Una vez descargado lo ejecutamos e instalamos.



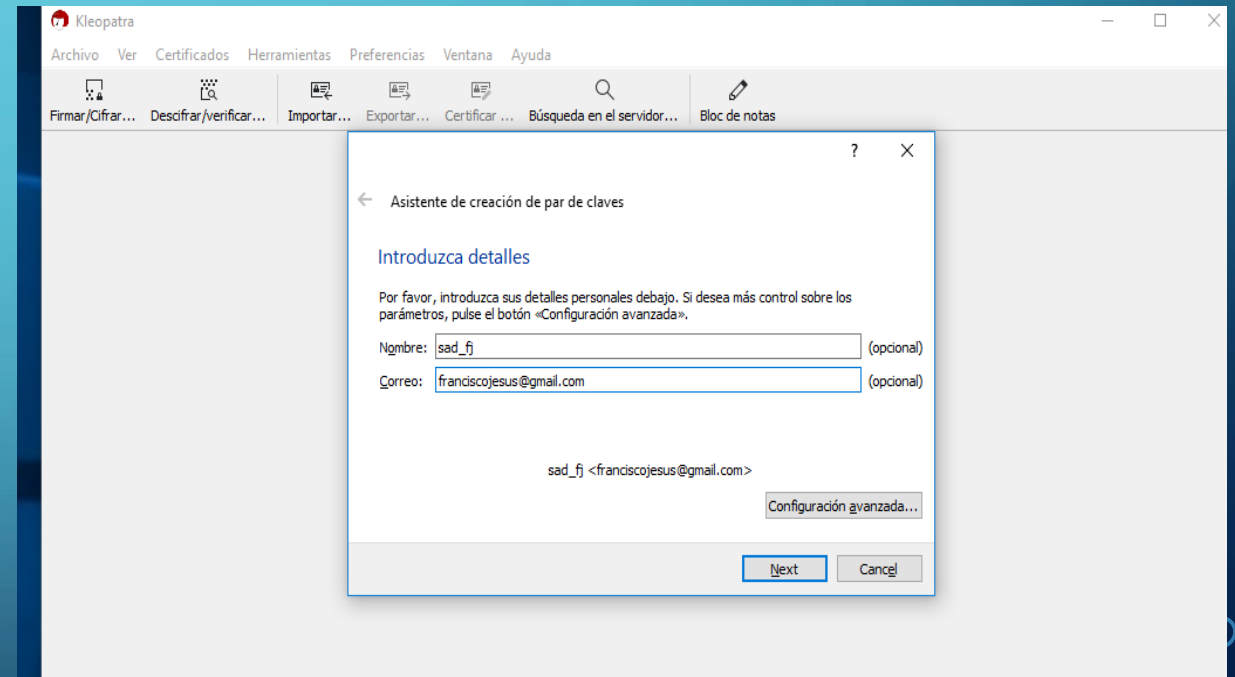
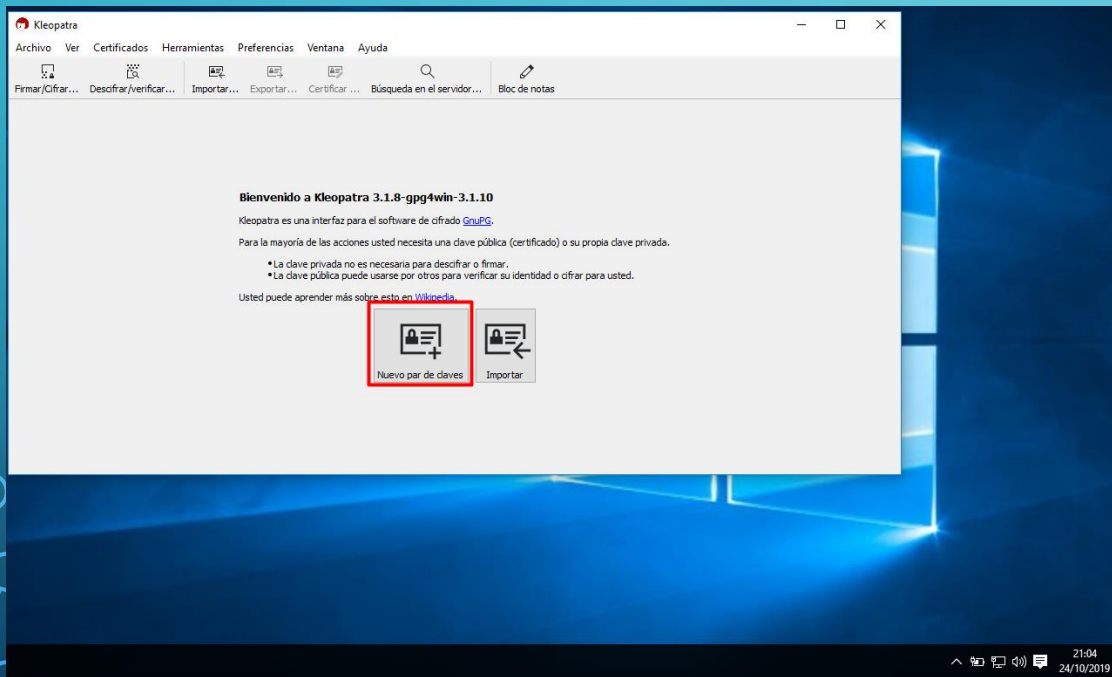
you for downloading Gpg4win.



GP4WIN

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

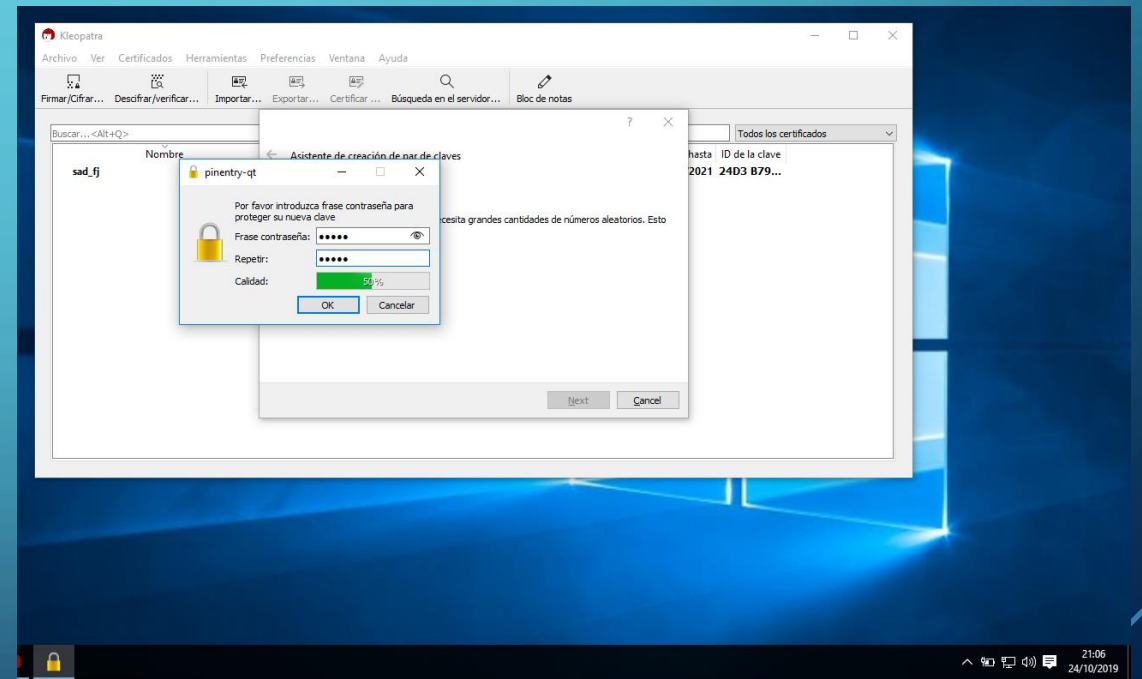
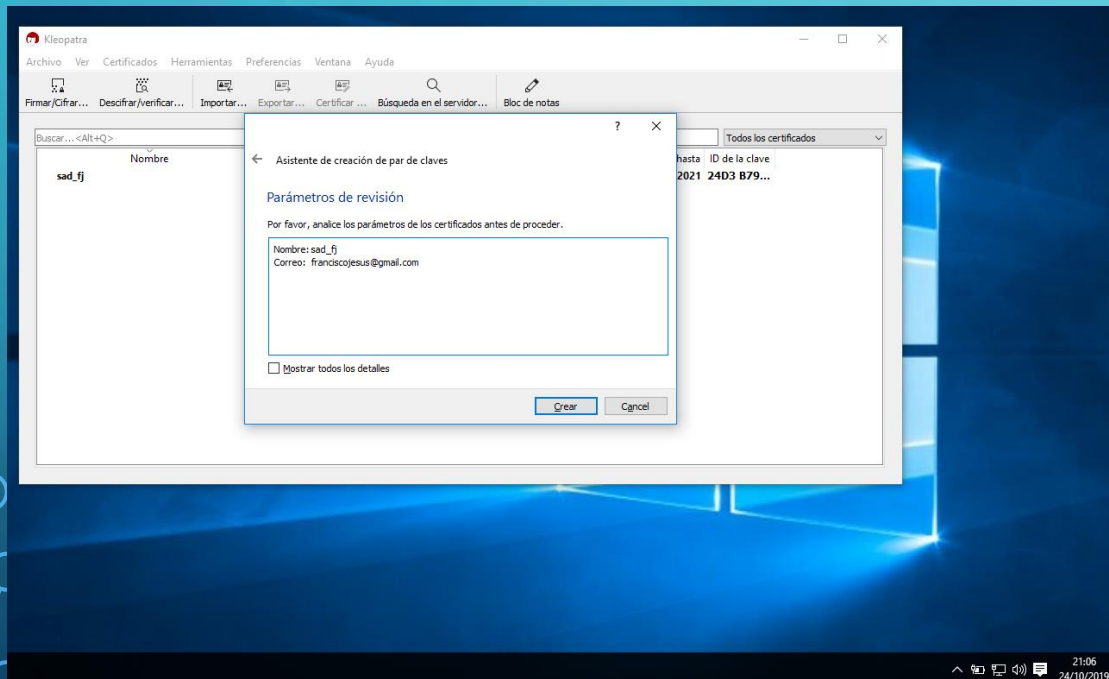
Le damos un nombre y correo.



GP4WIN

Veremos un resumen, pulsamos en *Crear*.

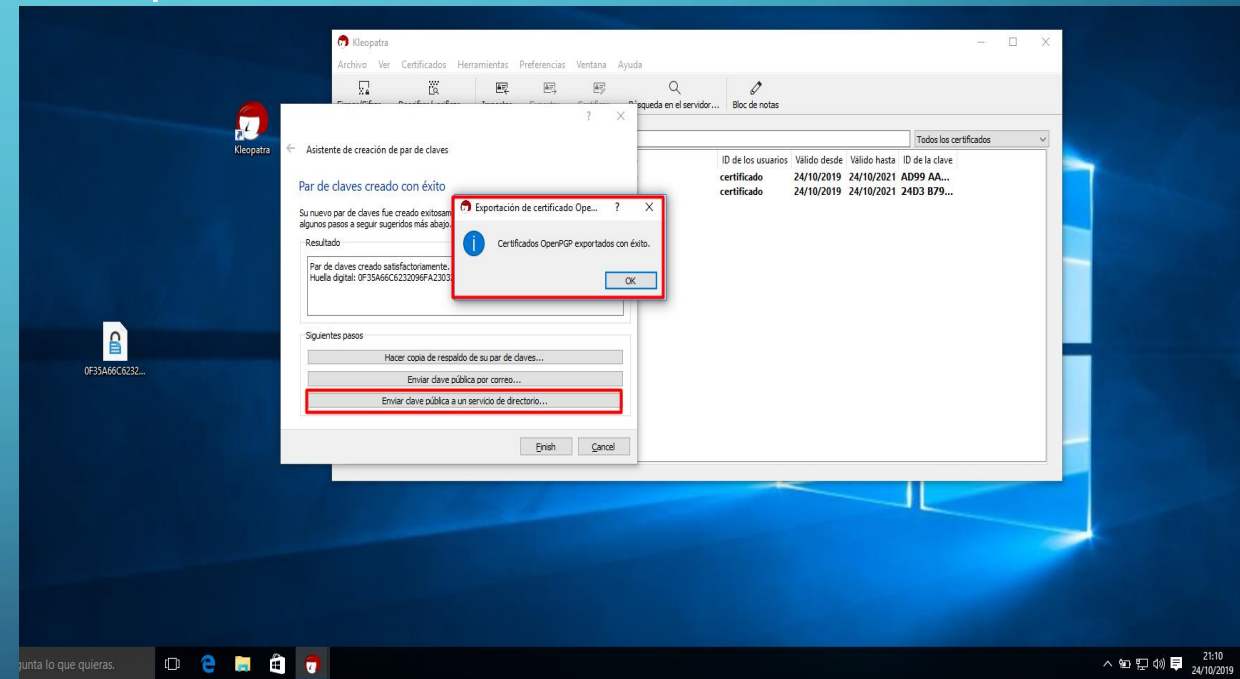
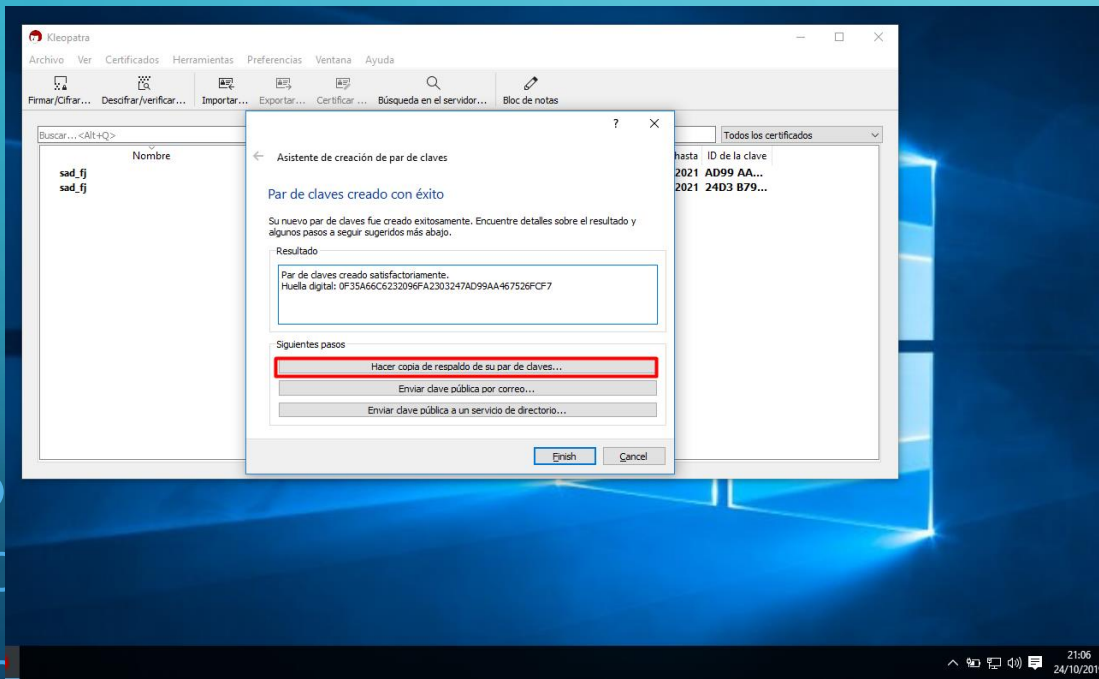
Nos pedirá una contraseña nueva para esas claves.



GP4WIN

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

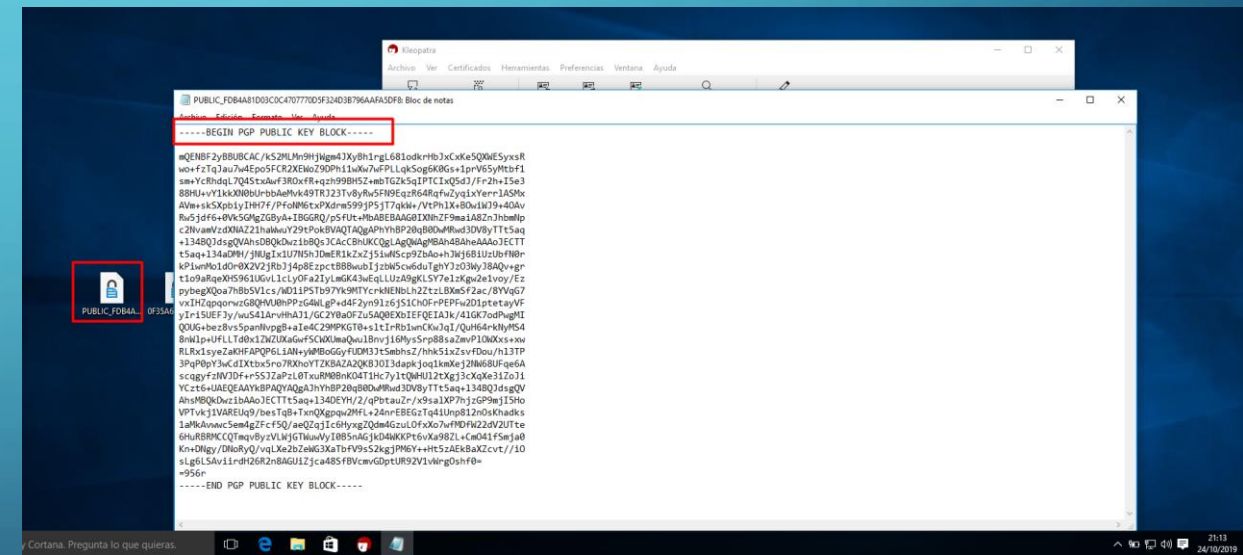
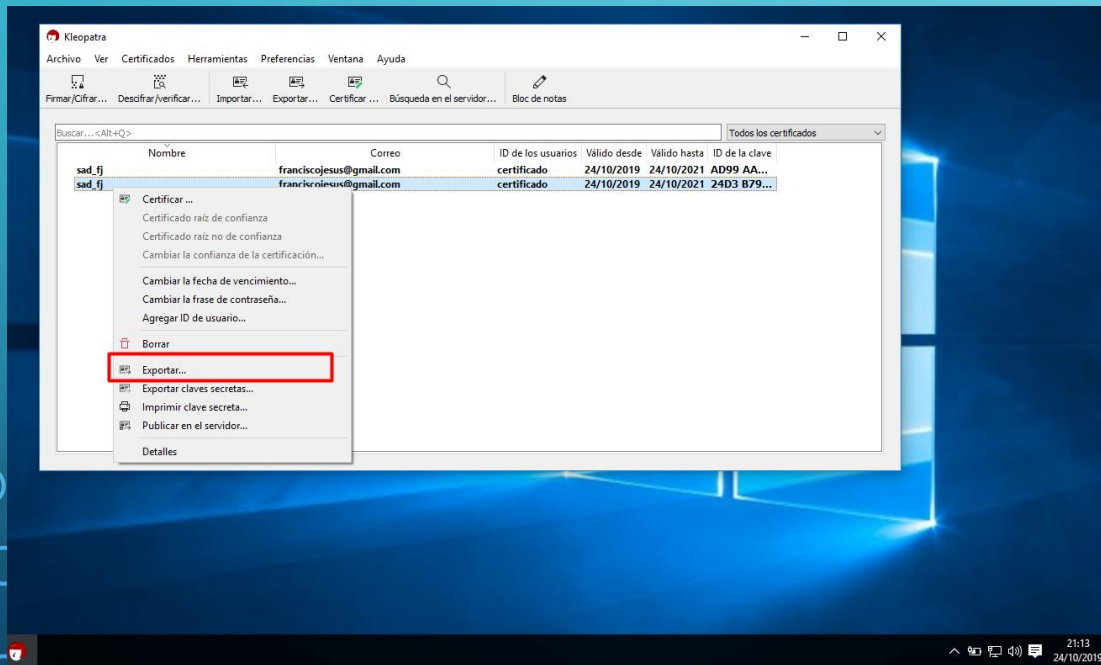
Escogeremos el lugar donde exportar la clave secreta y veremos como nos envía un mensaje que se exporta correctamente.



GP4WIN

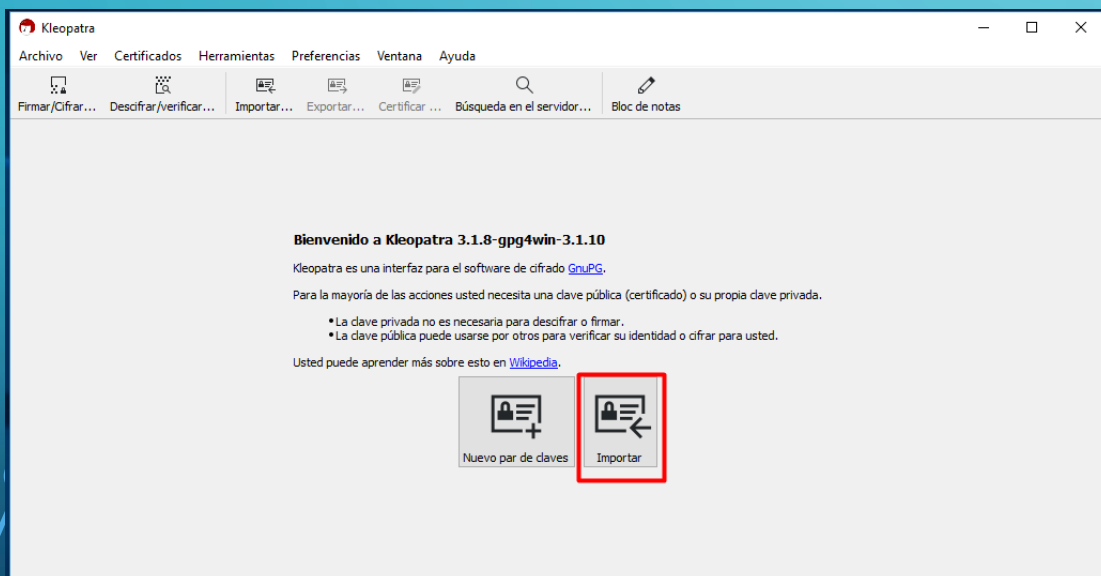
Pulsamos *Exportar* para exportar la clave publica y así poder cifrar.

Vemos como exporta la clave publica.

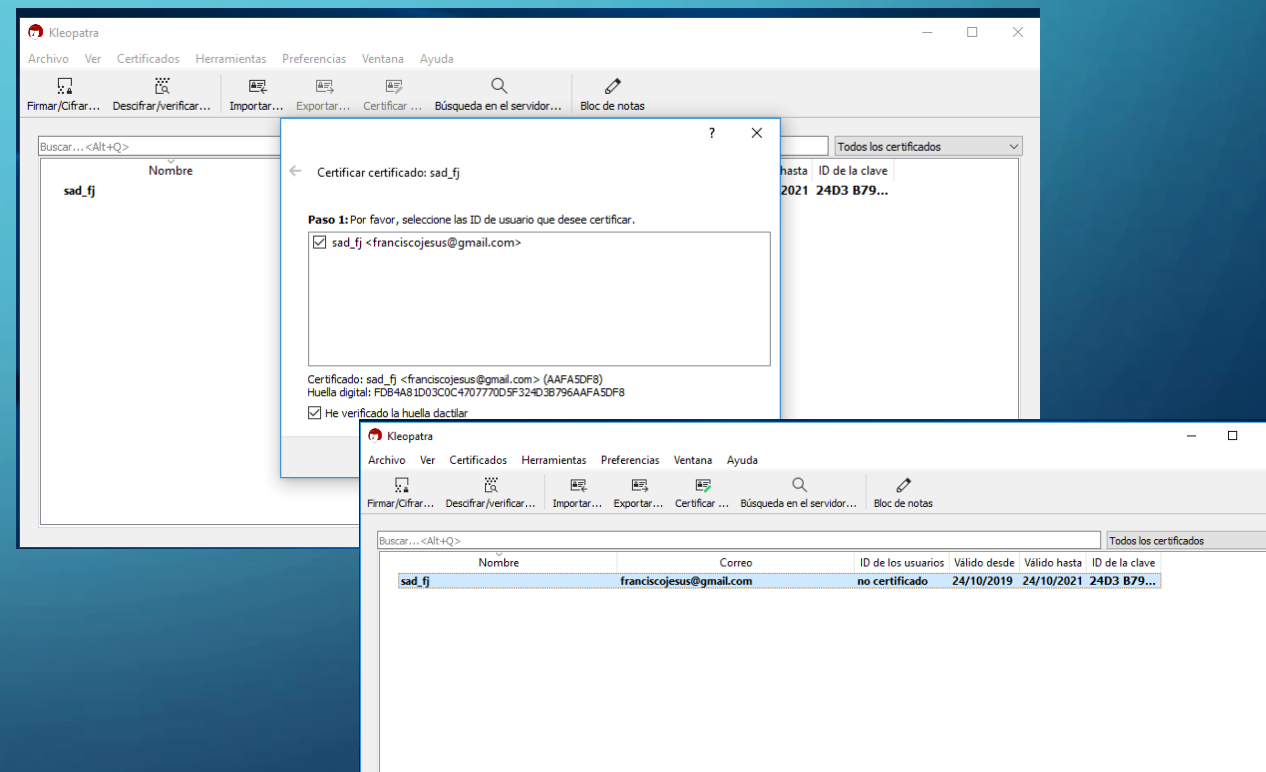


GP4WIN

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

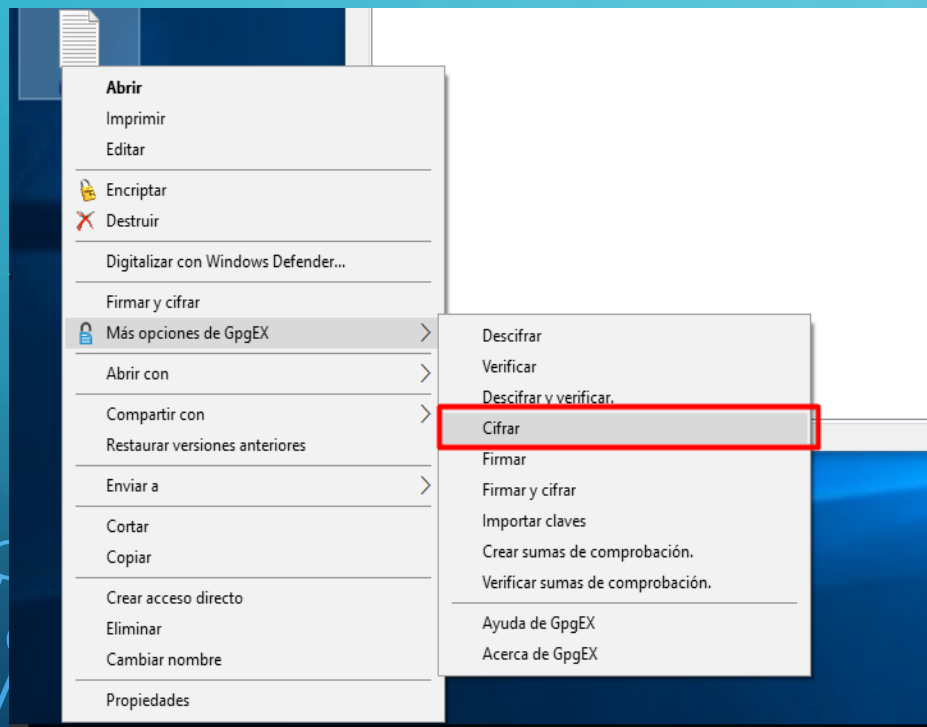


Importamos la clave publica.

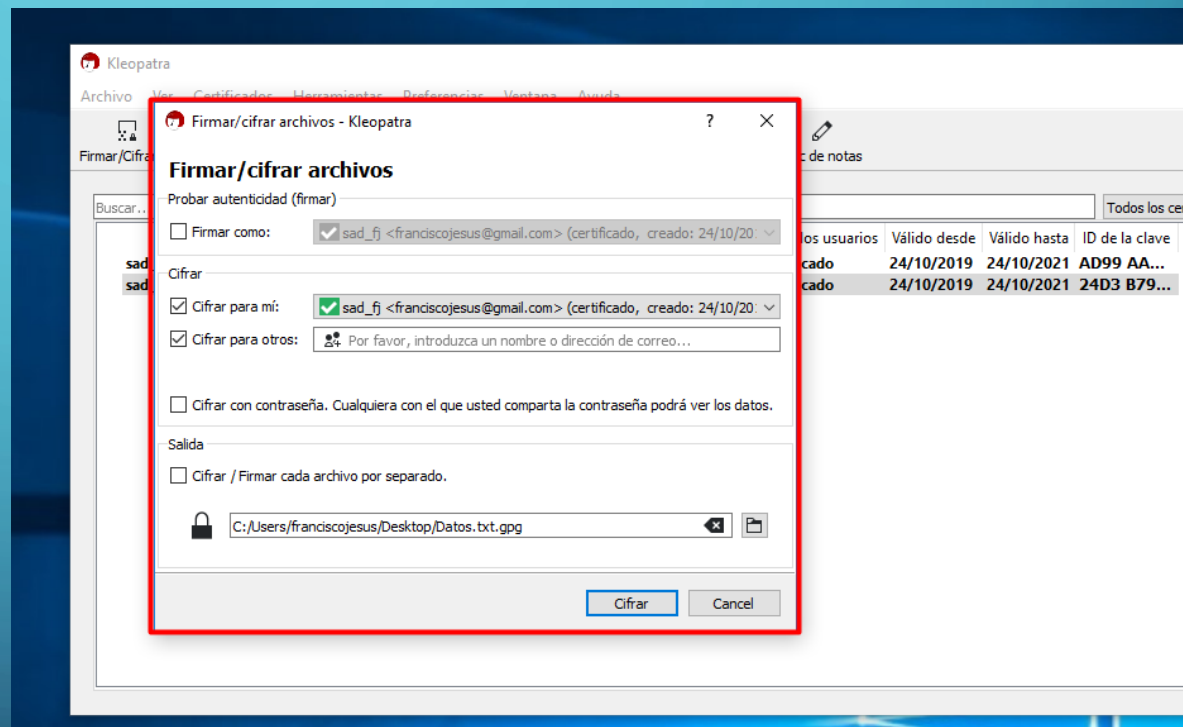


GP4WIN

Una vez realizado esto podemos cifrar el archivo.

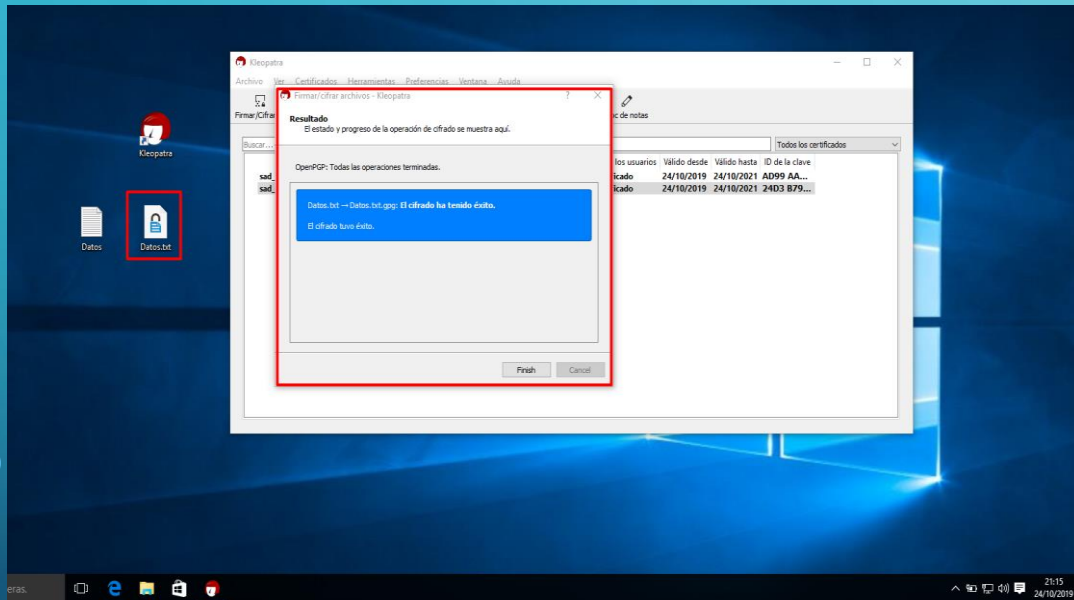


Pulsamos en *Cifrar*.

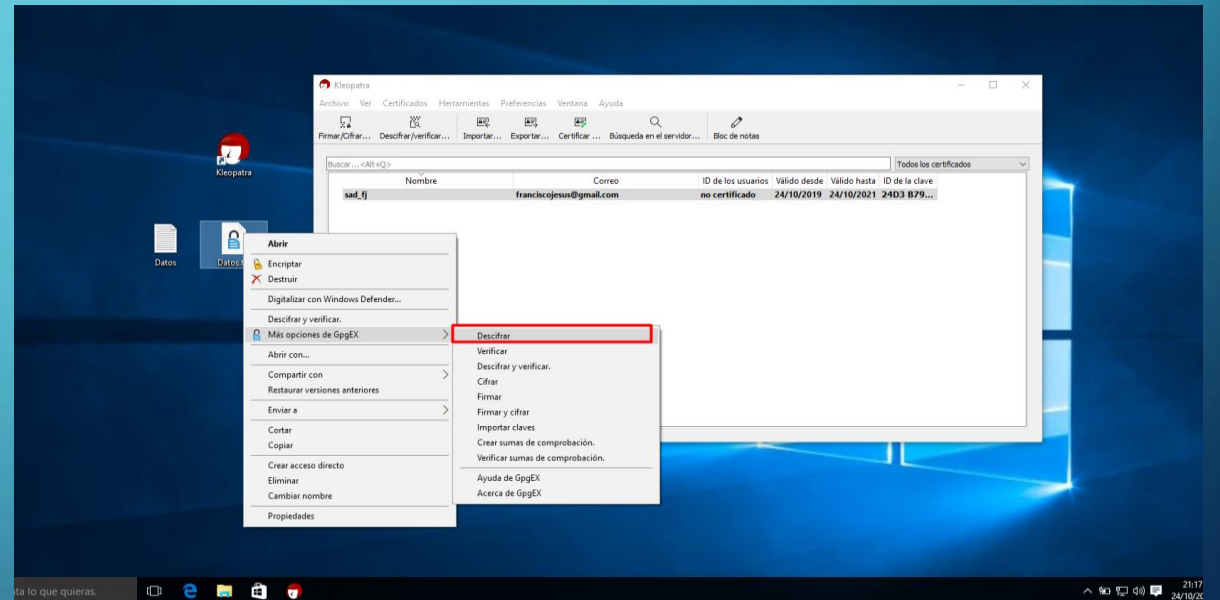


GP4WIN

Vemos como se cifra.

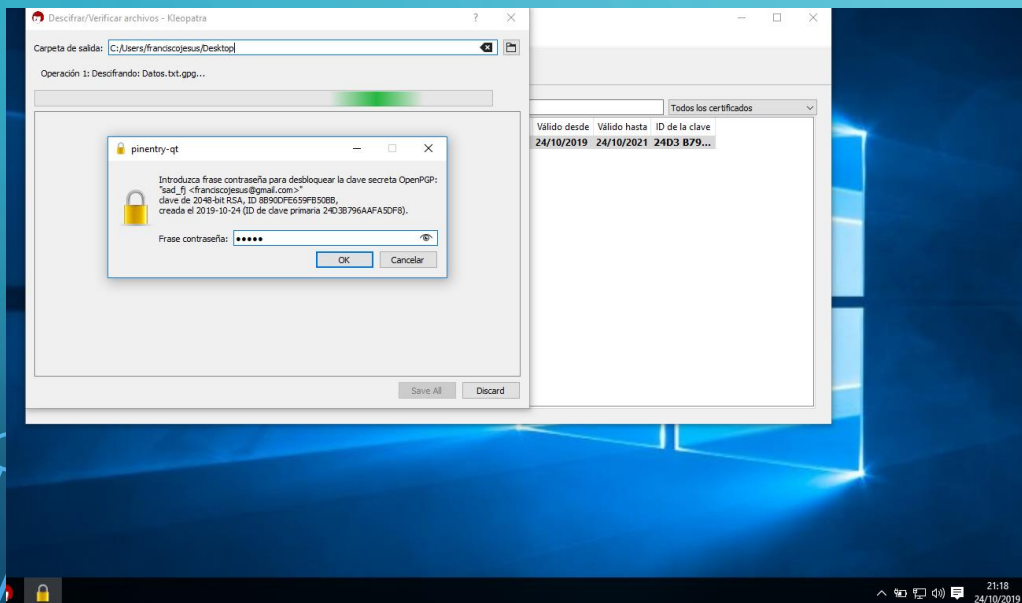


Ahora enviaremos la el archivo cifrado al equipo donde hemos creado el par de clave y descifraremos el archivo.

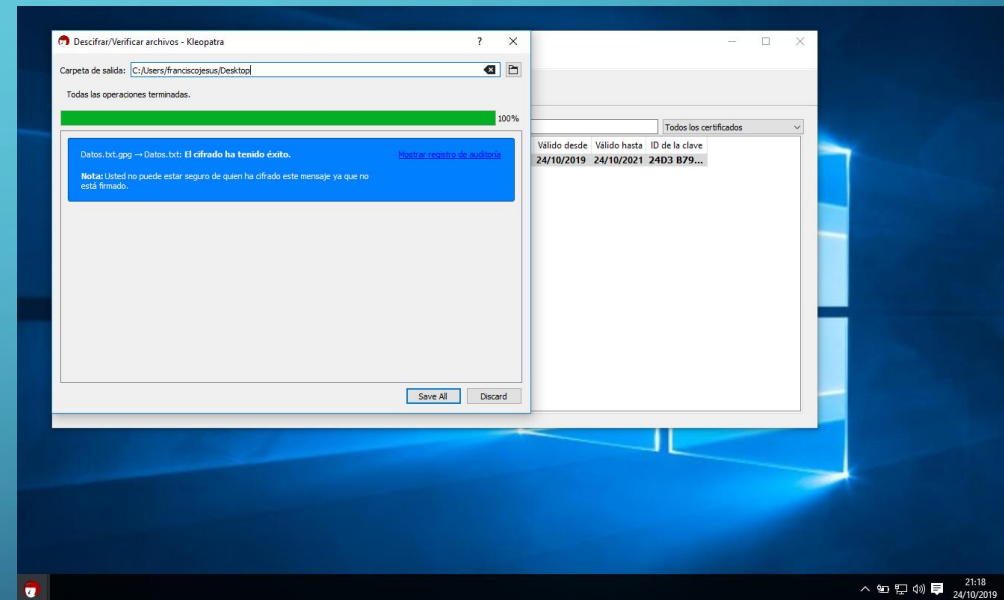


GP4WIN

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

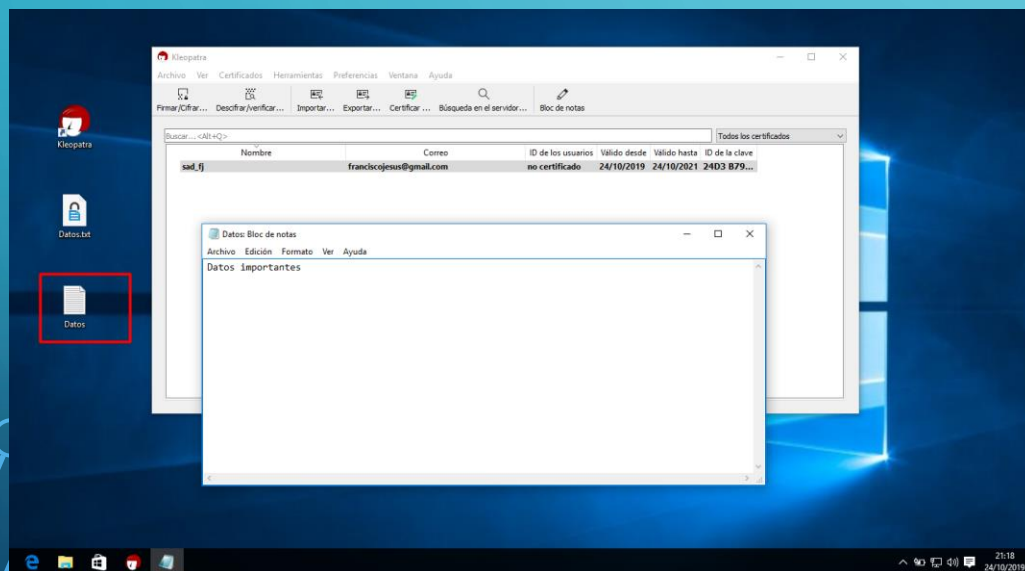


Vemos como se descifra correctamente.

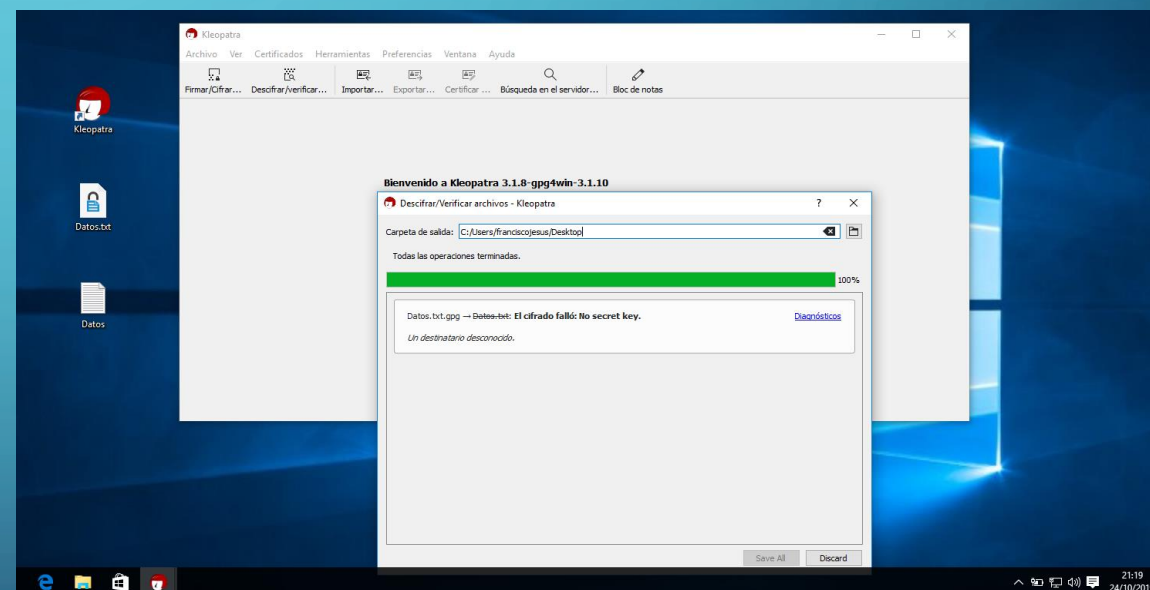


GP4WIN

Vemos como se descifra y podemos ver correctamente su contenido.

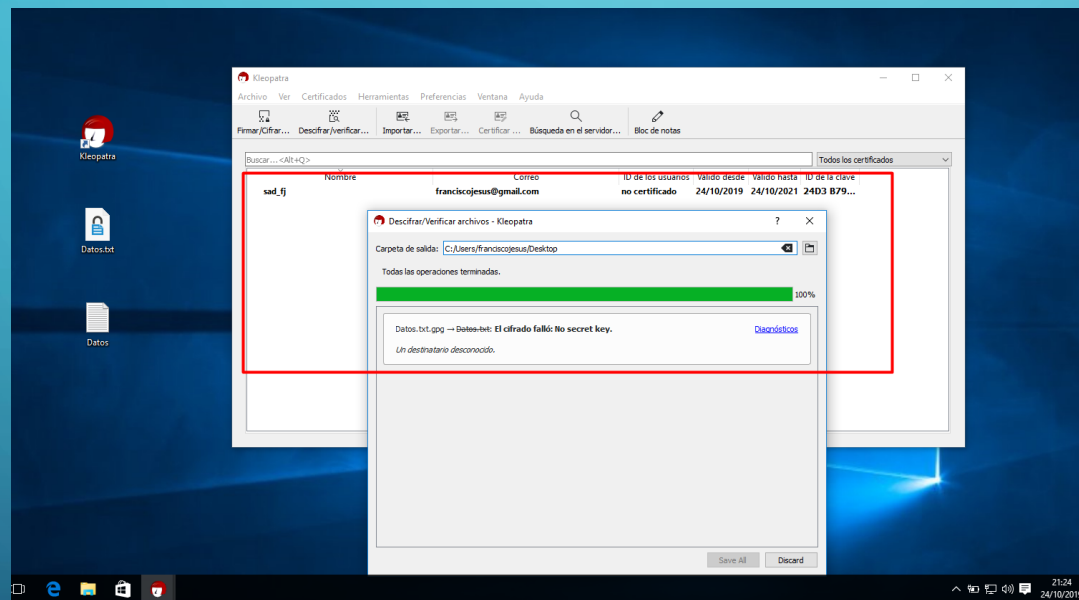


Si llevamos el archivo cifrado a otro equipo no podemos visualizar el contenido.



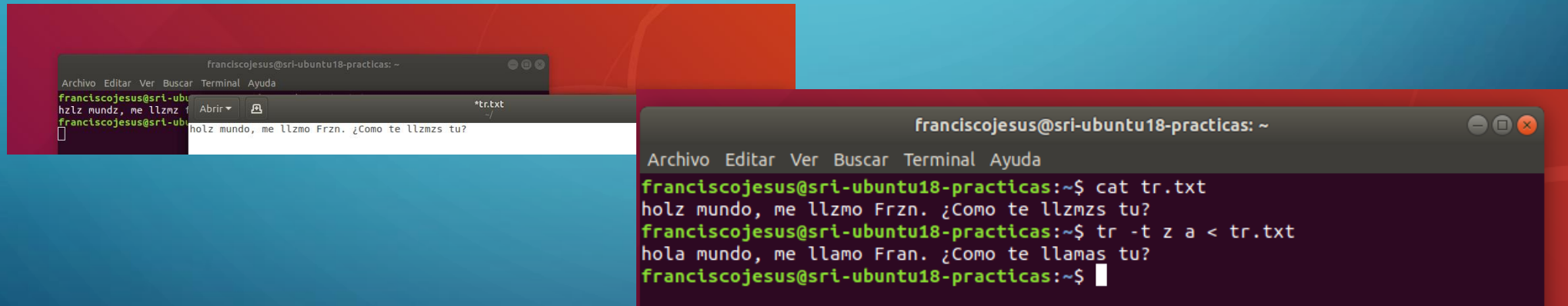
GP4WIN

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.



```
franciscojesus@sri-ubuntu18-practicas: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
franciscojesus@sri-ubuntu18-practicas:~$ cat tr.txt  
hzzz mundz, me llzmz Frzn. ¿Como te llzmzs tu?  
franciscojesus@sri-ubuntu18-practicas:~$ tr -t z a < tr.txt  
hola mundo, me llamo Fran. ¿Como te llamas tu?  
franciscojesus@sri-ubuntu18-practicas:~$
```

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.