

PROCEDIMIENTO DE USO DEL PROGRAMA DE ENCRIPCIÓN DE DATOS GPG4WIN

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.

La creación original de Gpg4win fue apoyado por la Oficina Federal para la Seguridad de la Información de Alemania. Sin embargo Gpg4win y todas las herramientas que se incluyen son de software libre y de código abierto, y es por lo general la opción no propietaria de la vida privada recomendada para los usuarios de Windows.

Legislación

La Ley Orgánica de Protección de Datos de Carácter Personal 03/2018 de 5 de diciembre (LOPD), tiene por objeto proteger y garantizar las libertades y los derechos fundamentales de las personas físicas, su honor e intimidad personal y familiar.

La LOPD establece unas obligaciones en relación a la protección de datos de carácter personal contenidos en ficheros automatizados y no automatizados (en papel) que poseen empresas y administraciones públicas, y que son tratados por éstas con diferentes finalidades.

Tras el análisis de impacto llevado a cabo por el IBESTAT, en ciertos tratamientos realizados por este, se ha identificado la necesidad de implementar salvaguardas que protejan la información gestionada de aquellas amenazas que, tras el pertinente análisis de riesgos, supongan un riesgo elevado para las diferentes dimensiones de la seguridad. Entre dichas salvaguardas y en relación con la presente instrucción, destaca la implementación de políticas de cifrado de la información con objeto de garantizar la confidencialidad de la misma.

La **criptografía asimétrica** (en inglés *asymmetric key cryptography*), también llamada **criptografía de clave pública** (en inglés *public key cryptography*) o **criptografía de dos claves**¹ (en inglés *two-key cryptography*), es el método [criptográfico](#) que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Llave o clave es lo mismo. Existiendo por tanto: **llave o clave** privada y **llave o clave** pública.

Si una persona que emite un mensaje a un destinatario, usa la llave pública de este último para cifrarlo; una vez cifrado, solo la clave privada del destinatario podrá descifrar el mensaje, ya que es el único que debería conocerla. Por tanto se logra la *confidencialidad* del envío del mensaje, *es extremadamente difícil que lo descifre alguien salvo*

¹ https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

el destinatario. Cualquiera, usando la llave pública del destinatario, puede cifrarle mensajes; los que serán descifrados por el destinatario usando su clave privada.

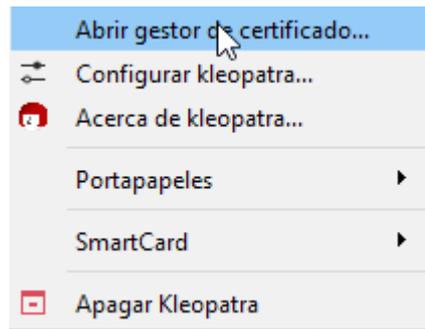
Si el propietario del par de claves usa su clave privada para cifrar un mensaje, cualquiera puede descifrarlo utilizando la clave pública del primero. En este caso se consigue la *identificación y autenticación* del remitente, ya que se sabe que solo pudo haber sido él quien empleó su clave privada (salvo que un tercero la haya obtenido). Esta idea es el fundamento de la [firma digital](#), donde jurídicamente existe la presunción de que el firmante es efectivamente el dueño de la clave privada.

Los 'sistemas de cifrado de clave pública' o 'sistemas de cifrado asimétricos' se inventaron con el fin de evitar por completo el problema del intercambio de claves de los [sistemas de cifrado simétricos](#). Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, cada uno debe conseguir la llave pública del otro y cuidar cada uno su llave privada. Es más, esas mismas claves públicas pueden ser usadas por cualquiera que desee comunicarse con alguno de ellos siempre que se utilice correctamente la llave pública de cada uno.

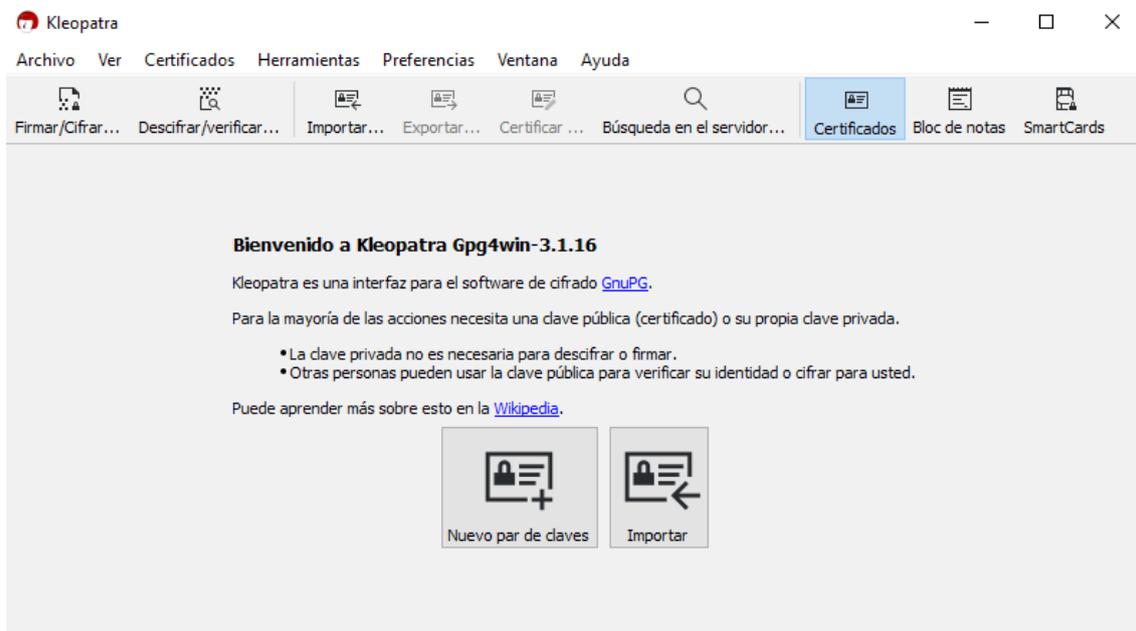
Creación y envío de llave publica en Gpg4win

Una vez instalado y reiniciado el sistema, podemos ir a la barra de tareas de Windows (donde se encuentra el reloj del sistema) y le damos al icono que simboliza una cabeza roja. Este icono nos permite abrir la herramienta Kleopatra para la gestión de los certificados y para encriptar/desencriptar los ficheros.

Le damos al botón derecho sobre este icono y nos muestra la ventana siguiente:



Seleccionamos la opción de abrir el gestor de certificado.



Al abrir el programa encontramos dos principales opciones, la de generar un nuevo par de claves (que nos permite generar la clave publica que podremos compartir y la clave privada que contiene la contraseña que nos permitirá desencriptar los ficheros que nos envíen con la pública).

Y la opción de Importar, que nos permite importar a nuestro repositorio las claves públicas de otras personas/entidades, para poder realizar la tarea de encriptar los ficheros que les tenemos que enviar con la seguridad necesaria.

Al seleccionar la opción de generar un nuevo par de claves, se abrirá un asistente para poder crear nuestra clave pública que utilizaremos para encriptar ficheros que vayan destinados a nosotros, nos pedirá el nombre que queremos que salga, nuestra dirección de correo electrónico y después le podremos asignar una clave privada que solo conoceremos nosotros en principio y nos servirá para abrir y desencriptar el fichero que nos envíen.

Asistente de creación del par de claves

Introduzca detalles

Por favor, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, pulse el botón «Configuración avanzada».

Nombre: (opcional)

Correo: (opcional)

Proteger la clave generada con una frase de contraseña.

Usuario <Usuario@CAIB.ES>

[Configuración avanzada...](#)

Una vez creada la llave pública que compartiremos saldrá en el listado de "Certificados", lo mejor es exportar la llave pública y enviarla a quien nos va a encriptar datos ya que al realizar el proceso indicara que lo haga con nuestros datos y solo nosotros podremos visualizar el contenido con nuestra clave.

Kleopatra

Archivo Ver Certificados Herramientas Preferencias Ventana Ayuda

Firmar/Cifrar... Descifrar/verificar... Importar... Exportar... Certificar... Búsqueda en el servidor... Certificados Bloc de notas SmartCards

Buscar... <Alt+Q> Todos los certificados

Nombre	Correo	ID de los usuarios	Válido desde	Válido hasta
IBESTAT (Institut d'Estadística de les Illes Balears)	info@ibestat.caib.es	certificado	11/07/2012	

Nos colocamos encima de la clave que queremos exportar y con el botón derecho le damos a exportar, nos creara un fichero con extensión ASC, y es el que tenemos que enviar para que nos puedan encriptar con nuestra clave, si esa persona recibe esa llave pública nuestra, lo importara en su juego de llaves y cuando tenga que encriptar algo para nosotros lo hará con esa clave pública.

Desencriptar ficheros encriptados

Para desencriptar solo hay que ir al fichero en concreto, y le damos al botón derecho, luego a la opción de:

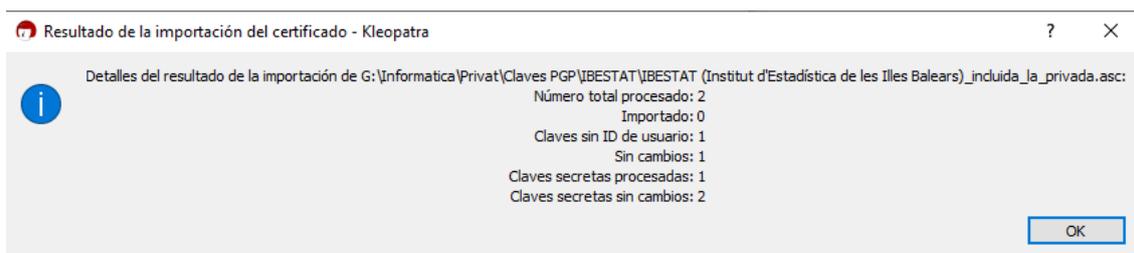


Entonces nos pedirá la clave privada asociada a ese fichero que será la que pusimos al principio al crear el par de llaves.

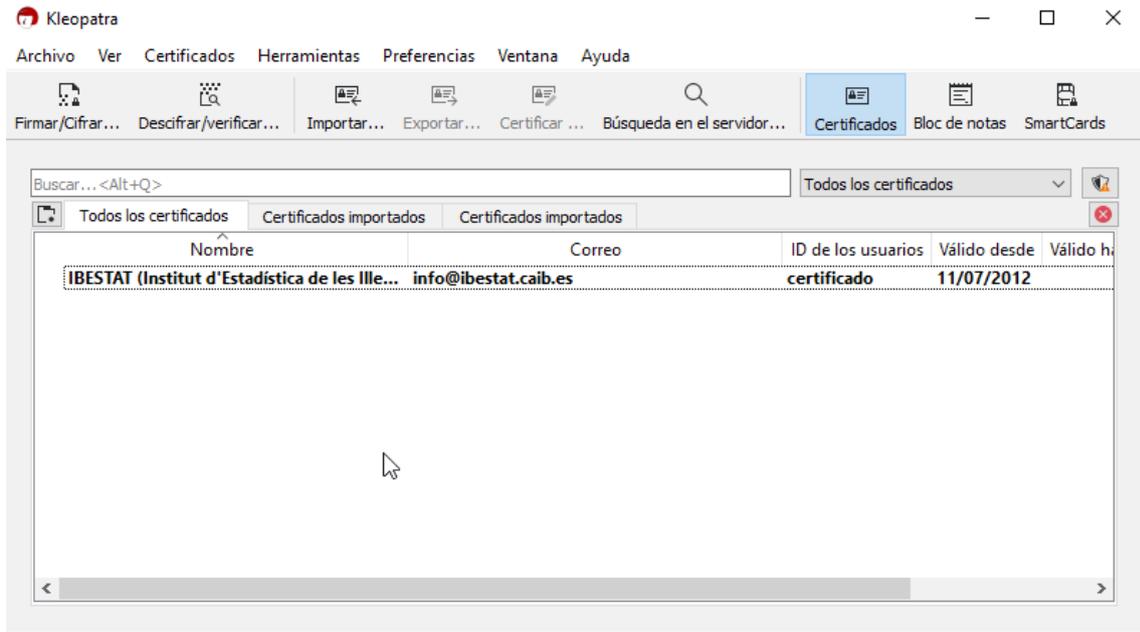
Encriptar datos con llaves públicas

Para poder enviar ficheros encriptados a alguien, debemos disponer de su llave pública para que solo él pueda desencriptar el contenido con la clave privada asociada.

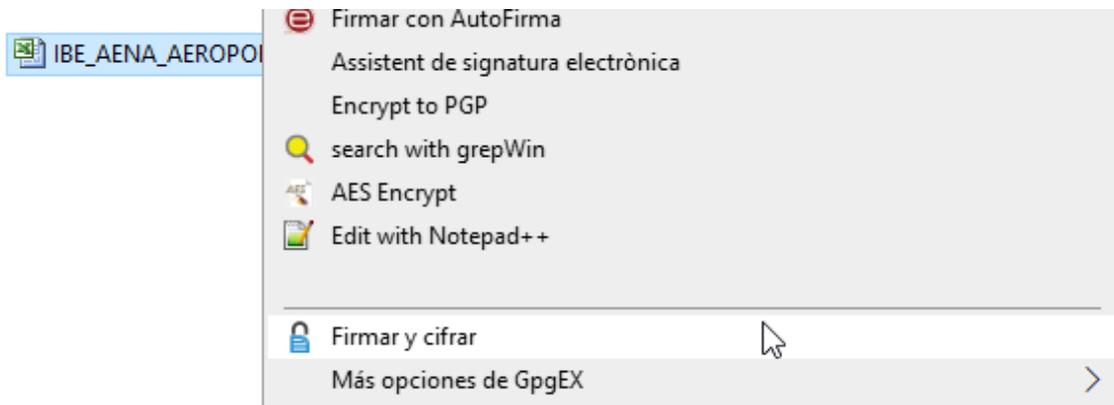
Para importar la llave pública de alguien procederemos a darle doble clic al fichero que nos envían con extensión ASC y acto seguido nos mostrara automáticamente la siguiente ventana:

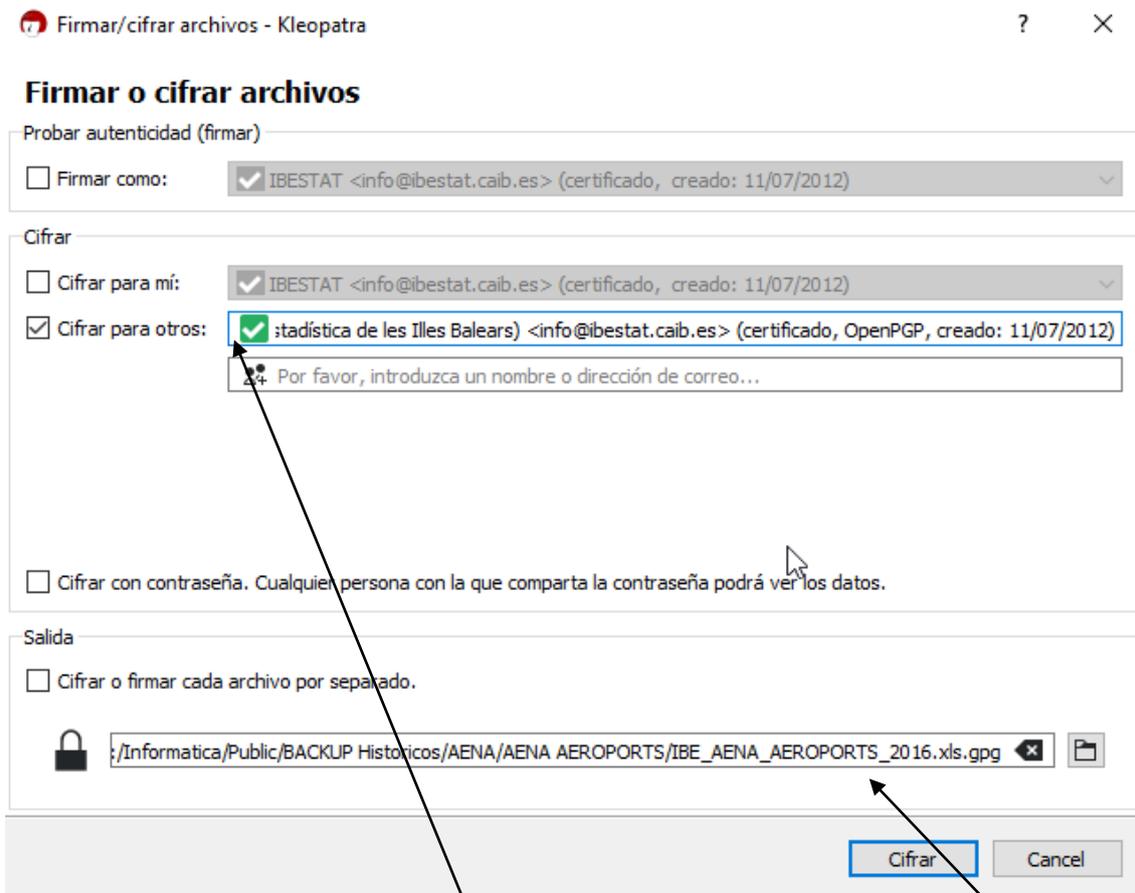


Al abrir la interface de Kleopatra, nos aparece ya el certificado (clave pública), que hemos importado y ya podemos utilizarla para encriptar los ficheros a enviar y que solo el destinatario con su clave privada podrá desencriptar.



El proceso para encriptar es más sencillo, simplemente nos colocamos encima del fichero a encriptar y pulsamos el botón derecho, al aparecer el menú contextual seleccionaremos

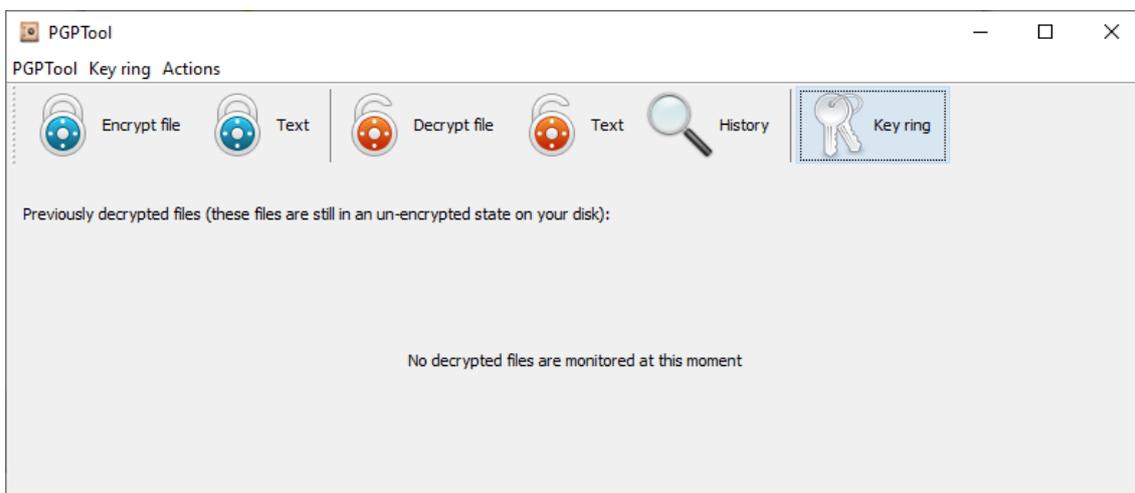




Hemos de indicar la clave pública del destinatario, y posteriormente indicarle el directorio de salida donde se ubicara el fichero encriptado.

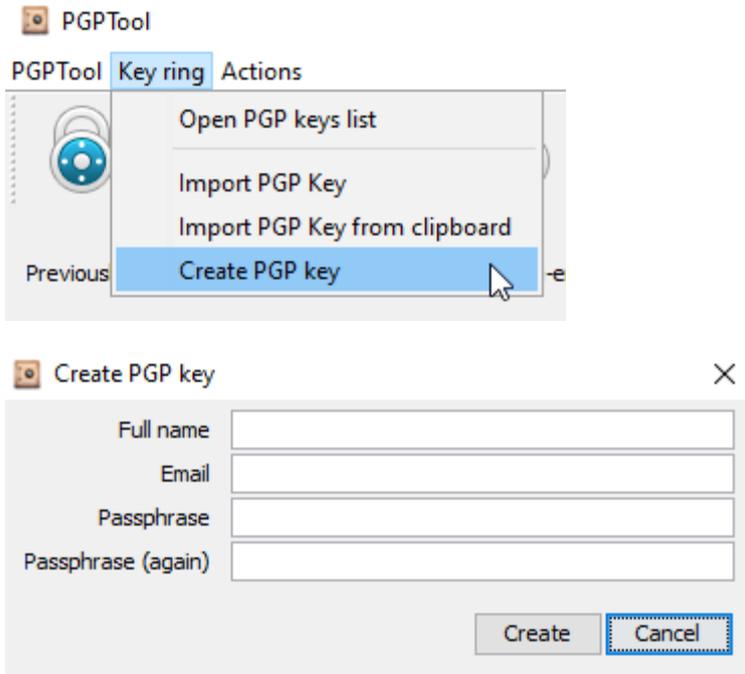
PGPtool

Existe una alternativa al programa GPG4WIN, y es una herramienta llamada PGPtool, su funcionamiento es muy similar al anterior, pero es más liviano y sencillo de utilizar.



Este programa requiere tener instalado en el sistema el JAVA RUNTIME ENVIRONMENT +18, para funcionar.

Para crear desde este programa la clave pública y privada, se realiza a través del correspondiente menú:



La pagina para su descarga e instrucciones de uso se encuentra disponible en:

<https://pgptool.github.io>