¿ Qué es GPG ?

Ver descripción aquí

GPG para usuarios windows

Existen varias aplicaciones bajo el sistema operativo Windows que permiten generar un par de claves gpg. Entre las más conocidas está Gnu4win y su módulo [Kleopatra]. La aplicación Gpg4win es un software de encriptación de libre distribución el cual permite el cifrado de ficheros y el envío de documentos a través del correo electrónico utilizando criptografía de clave pública para el cifrado de datos y firmas digitales.

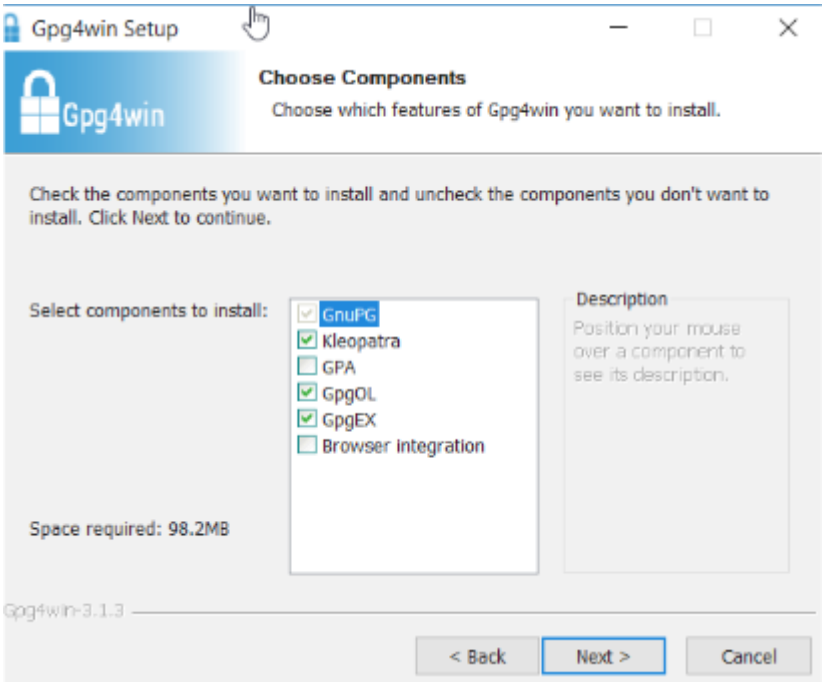
Soporta los estándares de criptografía OpenPGP y S/MIME (X.509).

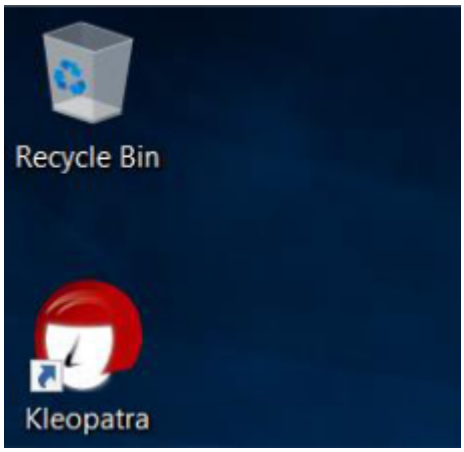
Gpg4win se compone varios módulos, entre ellos:

- GnuPG : la herramienta de cifrado básico
- Kleopatra : administrador de certificados para OpenPGP y X.509
- GPA : un administrador de certificados alternativa (GNU) para OpenPGP y X.509

Instalación de GPG4win

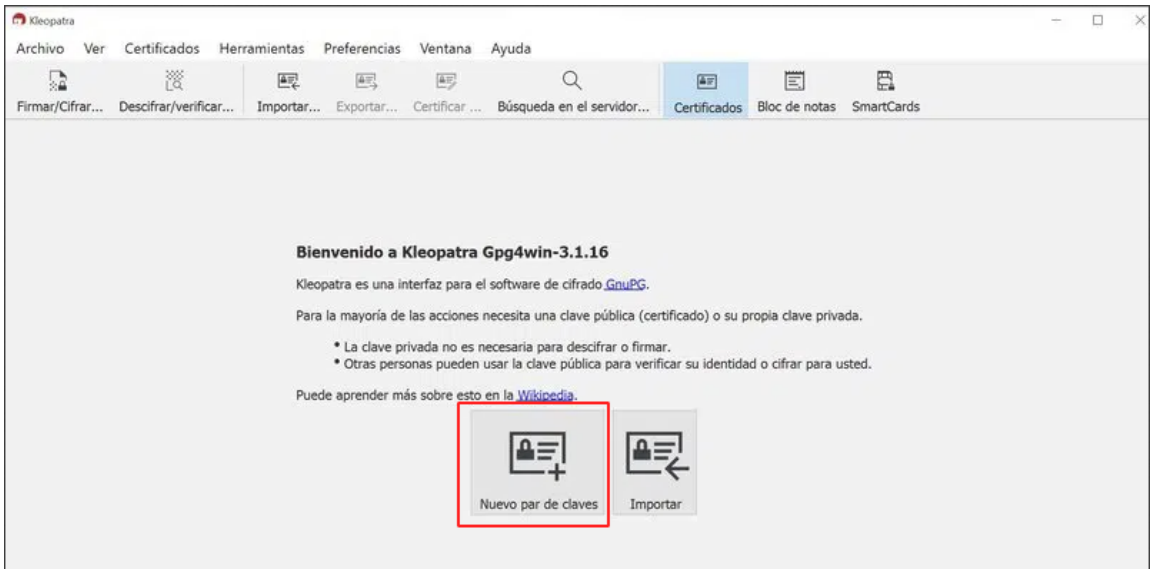
En la web del proyecto descargar la versión más reciente del software. Abrir el instalador y autorizar los cambios en caso necesario. Seguir los pasos indicados con el botón Siguiente.





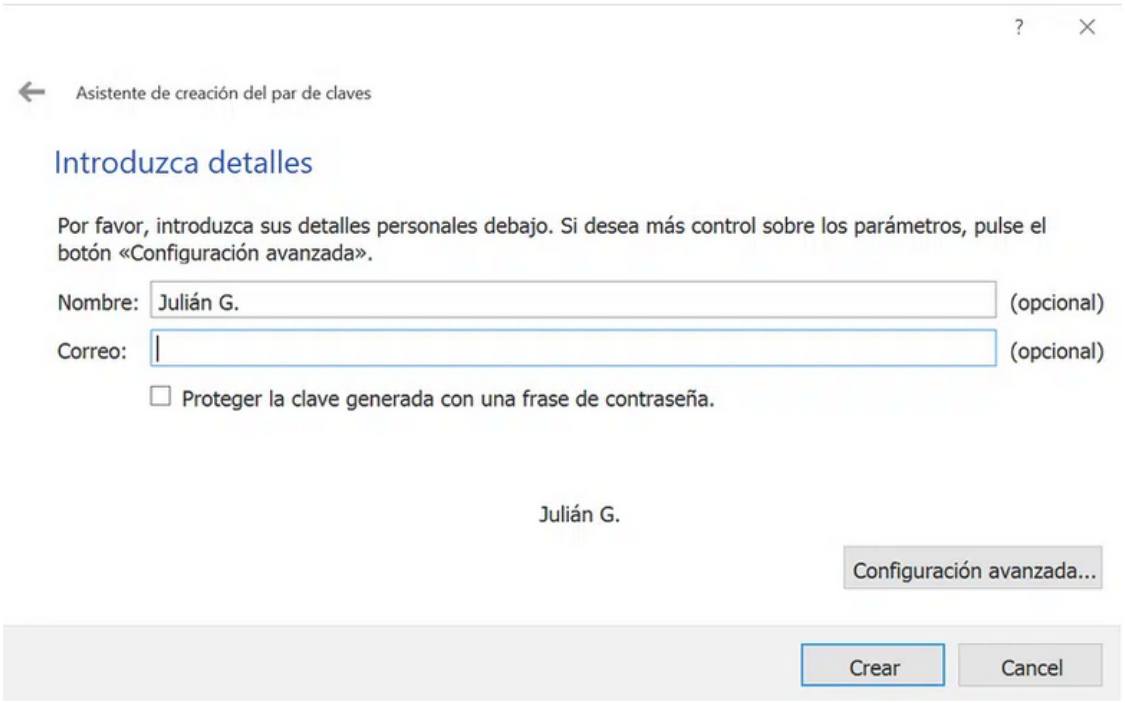
Generar una par de claves (pública y privada)

Una vez instalado Gpg4win vamos a utilizar el módulo **Kleopatra** para generar un nuevo par de claves gpg. Para ello desde la pestaña *Archivo* seleccionamos *Nuevo Certificado,* lo cual abrirá el asistente de generación de certificados.

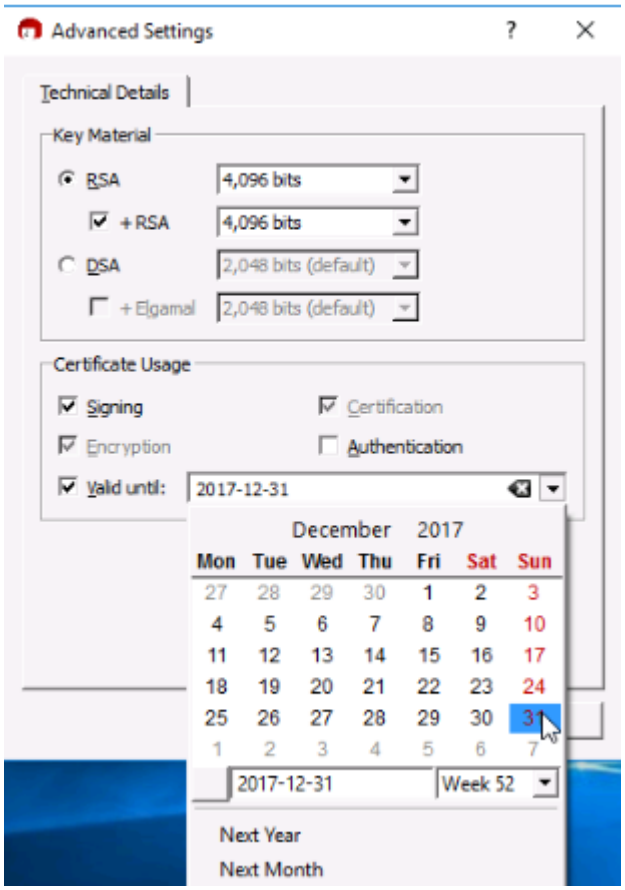


Pulsa en *Nuevo par de claves GPG*

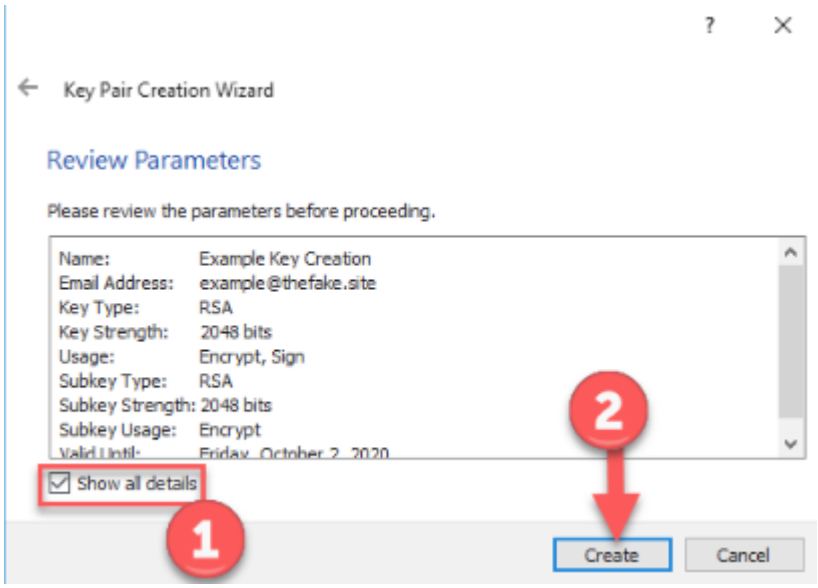
Introducir los datos requeridos



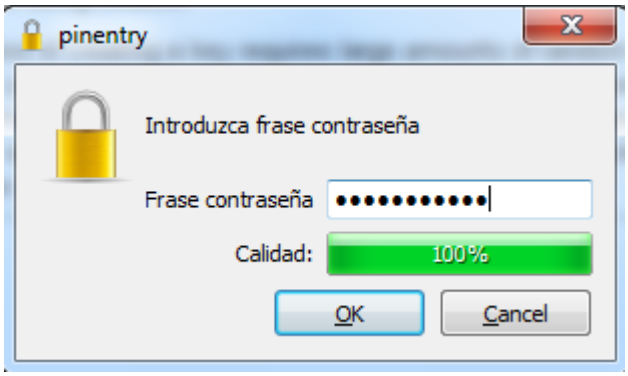
En la pestaña *Avanzadas* indicar una longitud de clave de 4096 bits y una fecha de caducidad en el desplegable inferior no superior a 2 años.



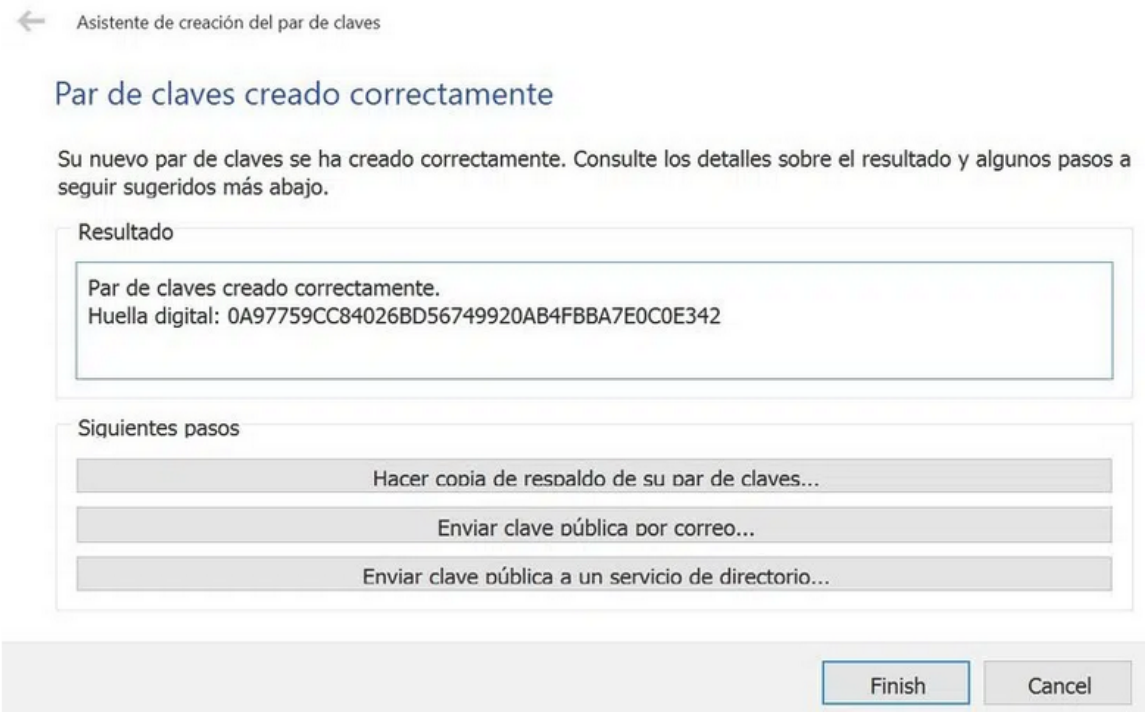
Confirmar los valores introducidos y generar las claves pulsando en *Crear*.



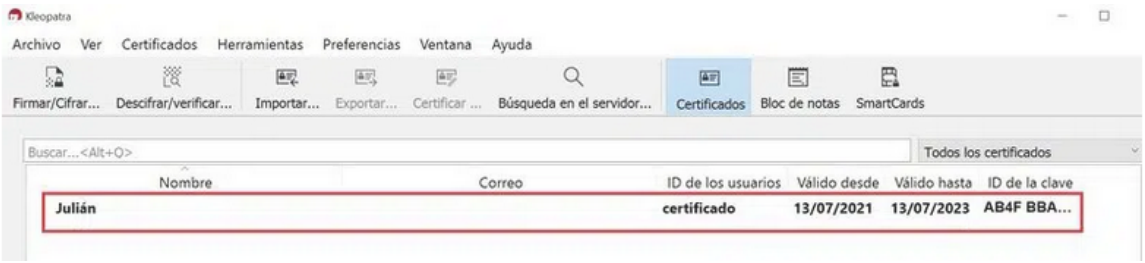
Introducir una contraseña que recuerde para su clave privada. Esta contraseña será la que deba usar para descrifrar los archivos que reciba cifrados con su clave pública.



Al pulsar **OK** verá que su par de claves pública/privadas se han generado correctamente

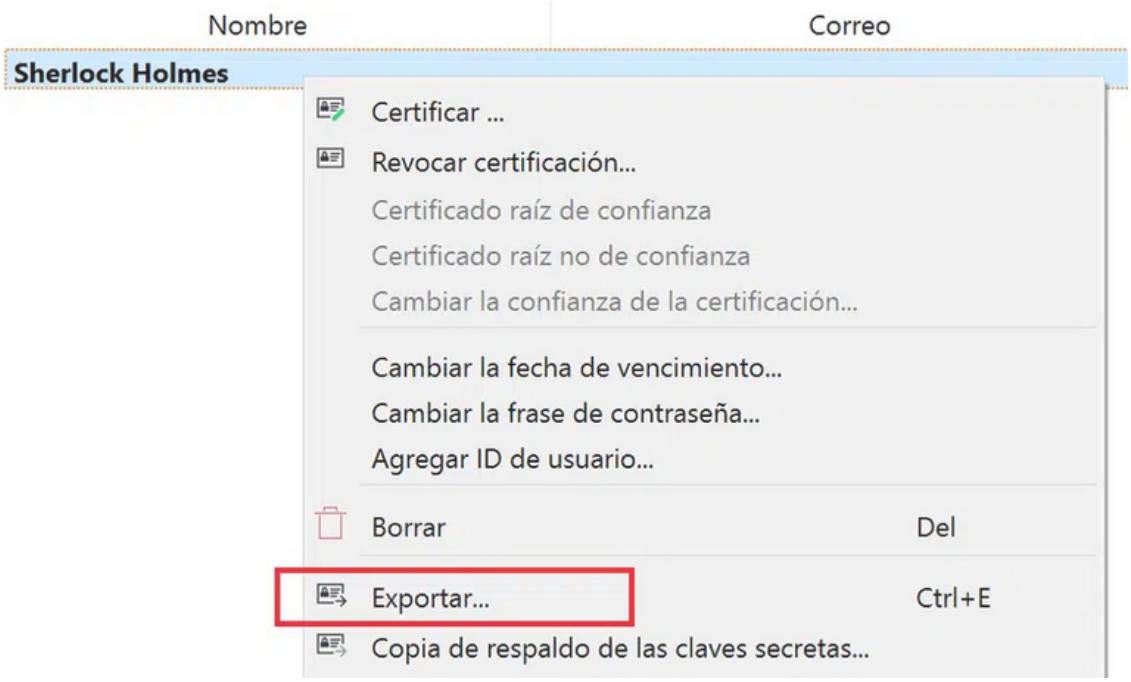


Se puede comprobar que se han creado con éxito el par de claves en la pestaña *Certificados*.



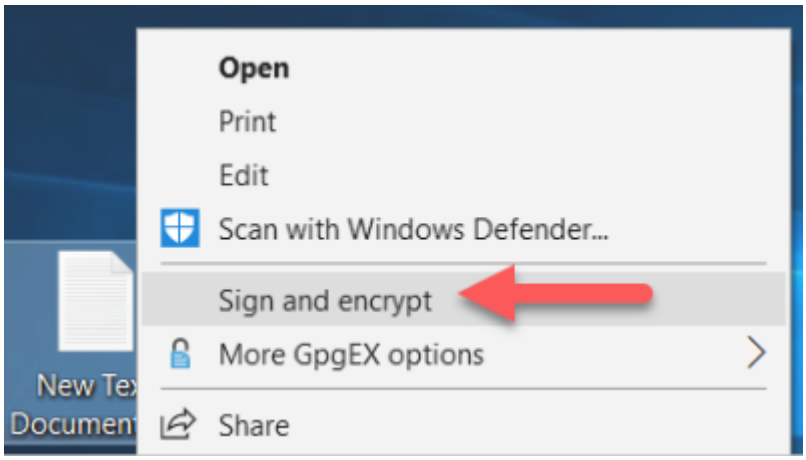
Exportar la clave pública

Al exportar la clave pública se genera un fichero de texto que por norma general se almacena con la extensión *.asc*, que es el que podrá distribuir por correo electrónico o bien publicar en un servidor de claves públicas como *REDIRIS* y donde cualquier persona la puede descargar.



Obtendrá un fichero de este tipo:

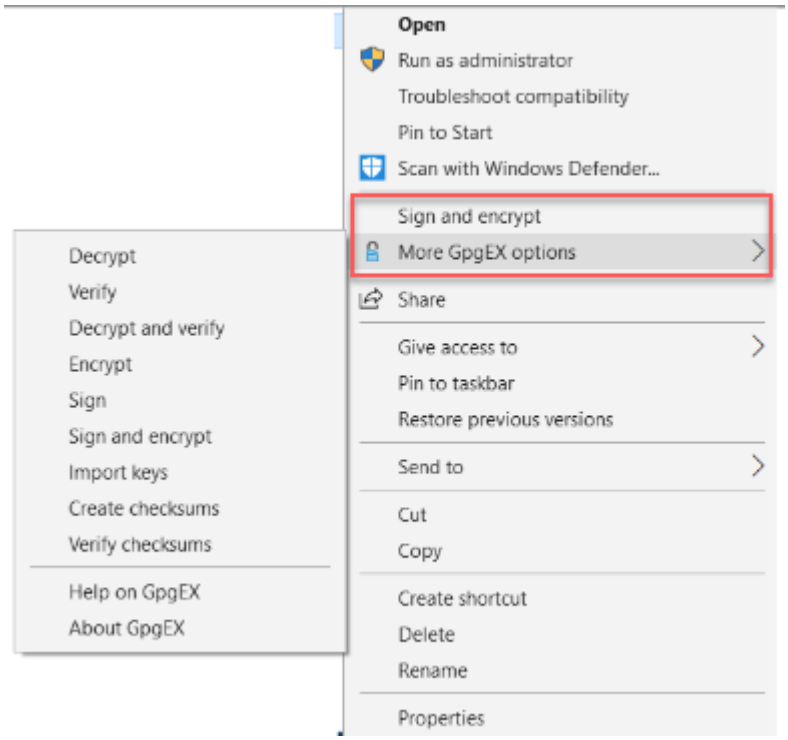
Cifrar ficheros con la clave pública.



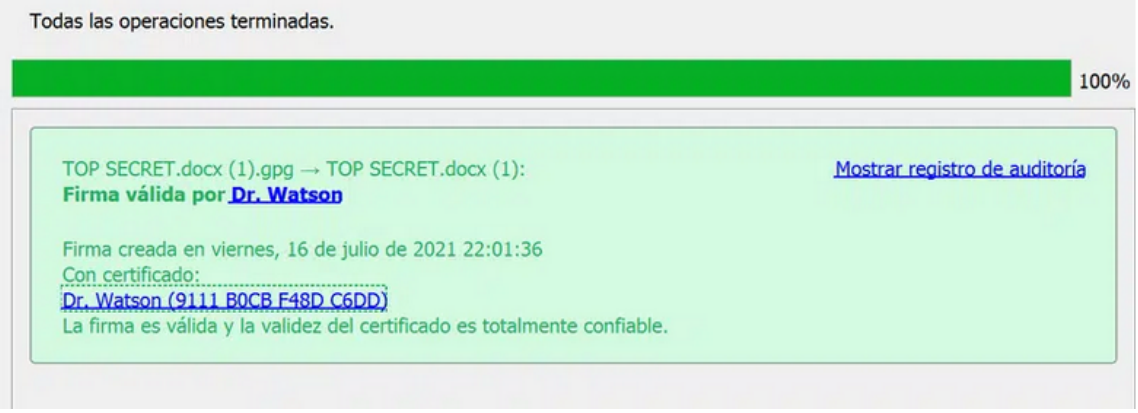
Descifrar ficheros con la clave privada

Sólo si un archivo *.gpg* ha sido cifrado con su clave pública y tiene la clave privada, así como su contraseña, podrá descifrar su contenido.

Se puede usar el menú contextual *Descifrar y verificar* para recuperar el fichero original pulsando con el segundo botón. También es posible realizar esto desde Kleopatra.



Una vez desencriptado este tendrá el mismo nombre sin la extensión gpg.



NOTA IMPORTANTE: Si cambia de ordenador o usa uno diferente asegurese de tener su par de claves a buen recaudo. Sin ellas no tendrá la posibilidad de descrifrar el contenido del archivo. Por ello recomendamos realizar un backup del par de claves GPG