CIFRADO DE EMAILS CON PGP

¿QUÉ ES PGP?

PGP (acrónimo de “Pretty Good Privacy”) es un sistema de cifrado de correo que presenta las siguientes ventajas:

- **Mejora la seguridad**: tus correos se guardan cifrados.
- **Certifica su autenticidad**: tus correos se firman digitalmente.
- **Optimiza los recursos**: ahorra espacio, puesto que comprime los mensajes.

Te puede resultar especialmente útil, si gestionas un correo profesional en el que realizas comunicaciones confidenciales en las que quieras sumar un extra de seguridad.

¿CÓMO USAR PGP?

GENERACIÓN DE CLAVES CON MAILVELOPE

Para comenzar a usar el servicio es necesario generar un par de claves, una pública y otra privada.

Existen varias opciones, te sugerimos hacerlo a través de Mailvelope por su sencillez y compatibilidad.

Mailvelope es un plugin compatible tanto para Firefox como para Chrome, lo que te permitirá seguir esta guía independientemente del navegador o sistema operativo.

Una vez instalado el plugin, verás en la interfaz de tu navegador un nuevo icono, como se muestra a continuación:

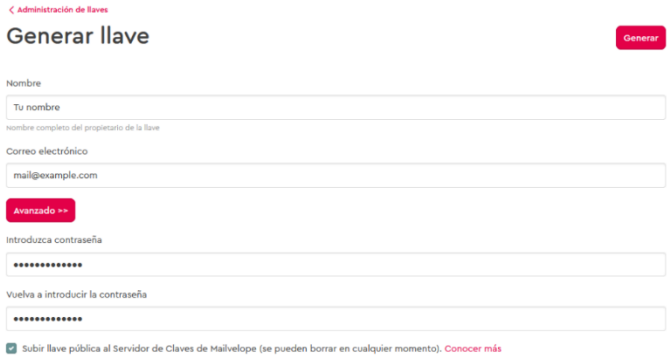
Cifrado de emails con Mailvelope

Pulsa ¡Iniciemos! para acceder a la configuración.

Configuración generar claves PGP

En las opciones de configuración accede a la opción Generar llave para comenzar, tal y como se muestra en la siguiente imagen:

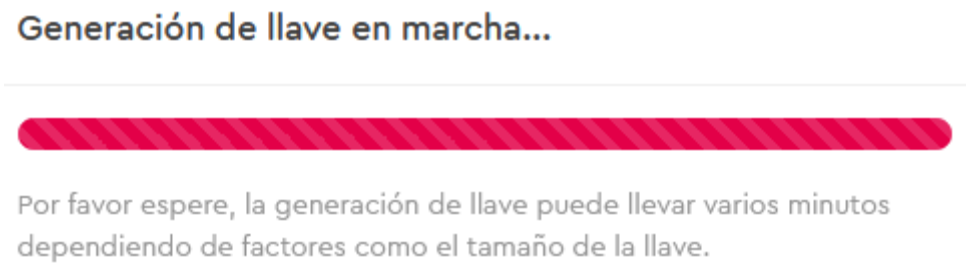
Genera una nueva clave cubriendo el formulario siguiente:



Generar llave

Si pulsas la opción Avanzado podrás modificar el tamaño en bits de la clave así como el algoritmo de cifrado. Es suficiente con que indiques 4096 bits.

Al finalizar con este formulario pulsa Generar.



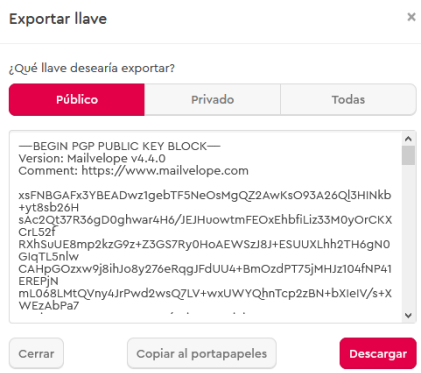
Proceso generación de llave

Hecho esto, ya dispondrás de todo lo necesario para importar tu clave pública en nuestro Panel de Control.

A continuación, podrás ver el listado de claves creadas.

Administración de llaves PGP

Pulsa sobre tu nueva clave, y a continuación en Exportar

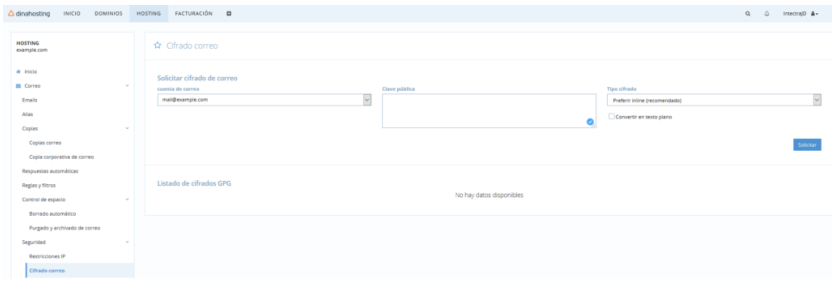


Exportar llave con Mailvelope

Selecciona todo el contenido de la clave pública para introducirla desde tu Panel de Control.

IMPORTACIÓN DE CLAVE PÚBLICA

Una vez generada la clave pública, es necesario que accedas a tu Panel de Control. En la pestaña Hosting, selecciona Cifrado Correo dentro de la sección Seguridad que encontrarás en la columna de la izquierda y sigue estos pasos:



Importación de Clave Pública PGP Panel dinahosting

- **Selecciona tu cuenta de correo** en el desplegable de la izquierda.
- **Pega la clave pública** que has generado en el apartado Clave pública, ten en cuenta que cada cuenta necesita una clave única.
- **Elige el tipo de cifrado** en el desplegable de la derecha

Con respecto al tipo de cifrado, puedes escoger entre las siguientes opciones, cuya funcionalidad variará en función de si activas, o no, la conversión en texto plano:

Con convertir en texto plano en NO

Tipo de cifrado	Resultado
Preferir inline	– Los mensajes en texto plano se cifran directamente. – Si el correo está en otro formato, se cifra con PGP/MIME.
Inline	– Los mensajes en texto plano se cifrarán. – El resto de correos quedan sin cifrar.
Mime	Todo el correo se cifra con PGP/MIME.

Con convertir en texto plano en SÍ

Tipo de cifrado	Resultado
Preferir inline	– Los mensajes en texto plano se cifrarán. – Si el correo está en otro formato, se intenta convertir. – Se cifra el correo convertido en texto plano y los correos no convertidos se cifran con PGP/MIME.
Inline	– Los mensajes en texto plano se cifrarán. – Si el correo está en otro formato, se intenta convertir. – Se cifra el correo convertido en texto plano, los que no hayan podido ser convertidos, no se cifran.
Mime	La combinación no es posible.

¿CÓMO USAR PGP EN WEBMAIL?

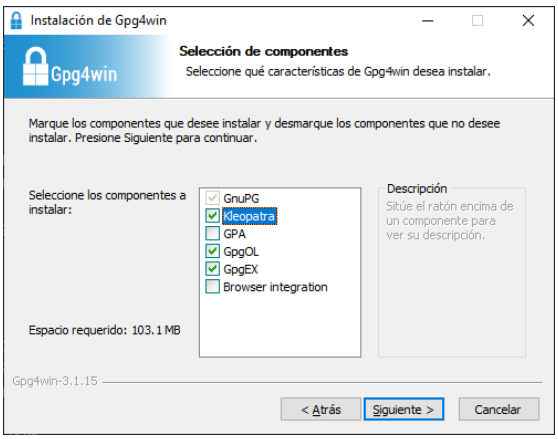
Simplemente agrega la URL de tu WebMail a Mailvelope. Para ello accede a tu correo a través de tu navegador preferido, en el que tienes instalado Mailvelope, y pulsa en Autorizar este dominio para que Mailvelope funcione sobre esta URL.

PGP en WebMail

Cada vez que quieras descifrar un correo, pulsa en el candado que verás encima del texto cifrado, e introduce la contraseña asociada a tu clave privada para poder visualizado.

¿CÓMO HACER UN CIFRADO DE EMAILS PGP EN WINDOWS?

Para hacer un cifrado de emails PGP en Windows es necesario tener instalado un software que permita gestionar el encriptado, así como gestionar las distintas claves. Puedes usar **Gpg4win** (GNU Privacy Guard para Windows).



PGP en Windows

Dependiendo del gestor de correo que utilices selecciona los componentes:

- Si vas a utilizar Thunderbid necesitarás seleccionar el paquete Kleopatra durante la instalación.
- Si vas a utilizar Outlook necesitarás seleccionar el paquete GpgOL y Kleopatra durante la instalación.

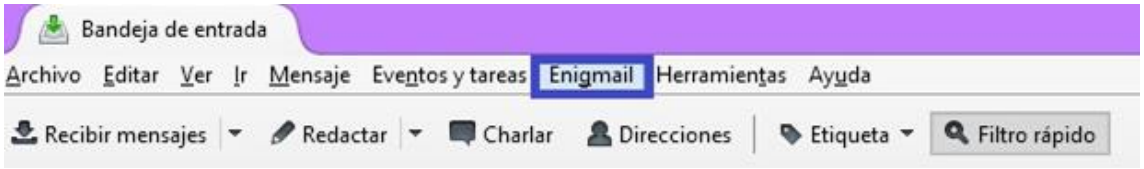
Otras alternativas de software podrían ser ppgp.sourceforge.net o instantcrypt.com

CIFRADO DE EMAILS PGP EN THUNDERBIRD CON ENIGMAIL

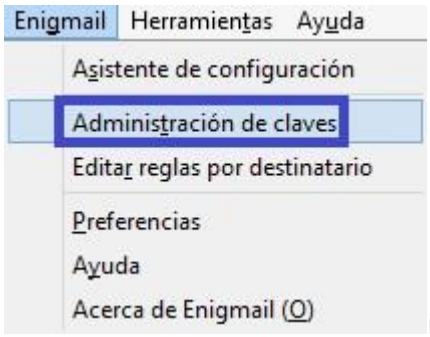
Puedes usar PGP en tu cliente Thunderbird usando el complemento EnigMail:

Para comenzar, instala la extensión Enigmail, que permite el cifrado y autenticación de mensajes mediante OpenPGP

Una vez instalado, accede a la nueva opción que aparece en el menú llamada Enigmail y pulsa sobre Administración de claves.



PGP en Thunderbird con EnigMail



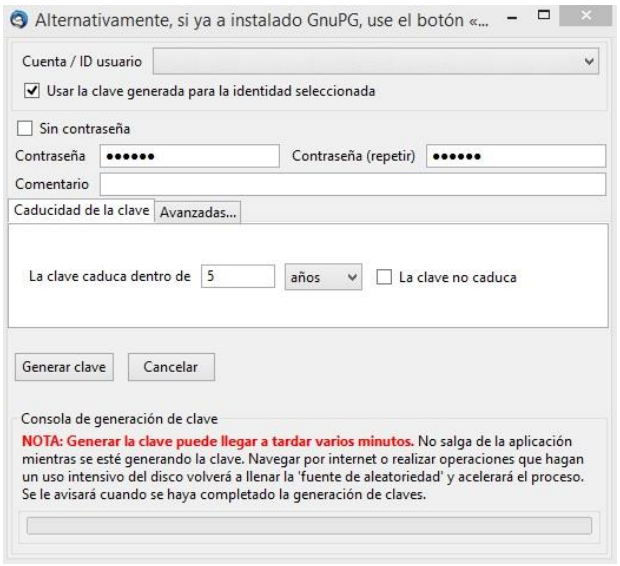
P

GP en Thunderbird con EnigMail

A continuación, selecciona la opción Generar y pulsa sobre Nuevo par de claves:

PGP en Thunderbird con EnigMail

Indica en que cuenta de correo deseas generar las claves desde el desplegable Cuenta / ID usuario, y escribe una contraseña. Introduce una fecha de caducidad o bien selecciona que la clave no caduque:



PGP en Thunderbird con EnigMail

En la pestaña Avanzadas elige el tamaño que tendrá la clave, lo recomendable es usar RSA de 4096. Después de esto pulsa Generar clave.

Sólo debes aceptar la solicitud de confirmación de Enigmail, pulsando Generar clave.

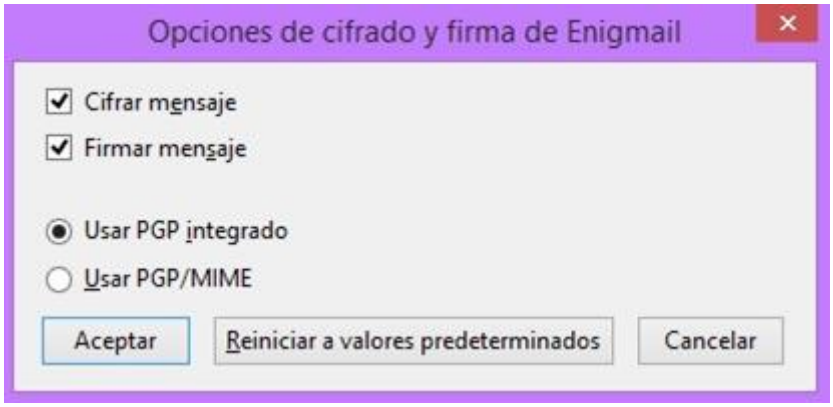
Ten en cuenta que las claves se generan utilizando la “entropía” que se genera en el ordenador (mover el ratón, poner música, etc.), por lo que tardarán en generarse dependiendo de las tareas que estés haciendo en ese momento en tu equipo.

Una vez haya terminado, tendrás la posibilidad de generar un certificado de revocación, por si pierdes las claves.

¿CÓMO USAR EL CIFRADO EN LOS CORREOS?

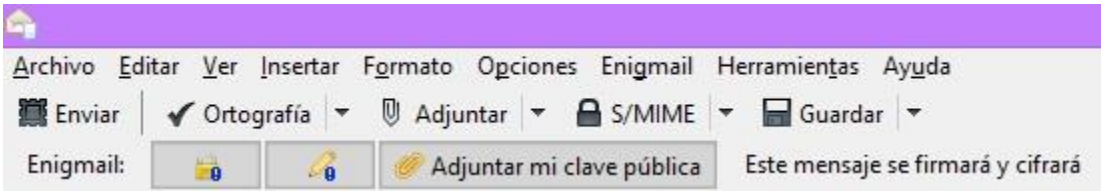
Una vez creadas las claves simplemente redacta un nuevo correo, accede al menú EnigMail (dentro de la ventana del correo que estás redactando). Elige Firmar mensaje y Cifrar mensaje.

Elige Usar PGP integrado o Usar PGP / MIME, en función del tipo de formato de correo que estés usando en la redacción de tu correo, y por último Aceptar:



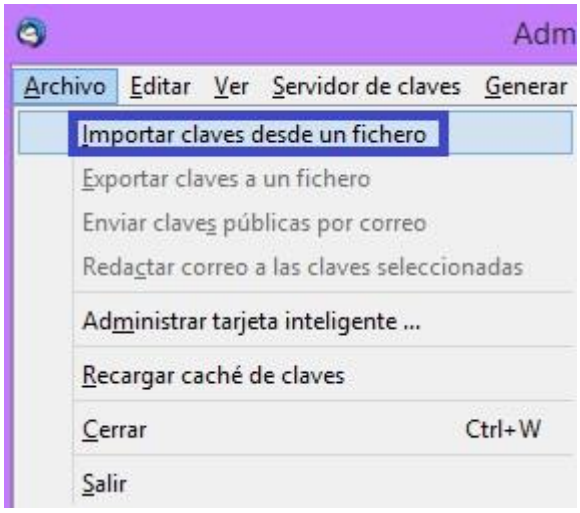
Usar cifrado PGP

Para poder descifrar el mensaje, el destinatario necesitará la clave pública con la que ha sido cifrado, por lo que la primera vez, adjunta la clave pública.



Cifrado de correo con PGP

Para enviar el correo encriptado necesitarás la clave pública de tu contacto. Puedes añadirla desde el Menú Enigmail en la sección Administración de claves. Una vez en ese apartado, accedemos a Archivo e Importar claves desde un fichero:



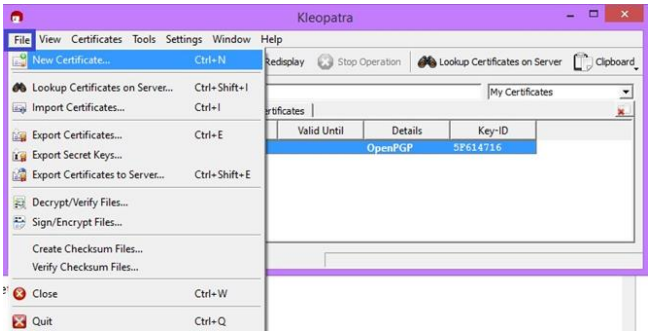
Importar claves desde un fichero

Una vez hecho esto, ya puedes enviar tu mensaje cifrado al destinatario cuya clave pública has importado.

PGP EN OUTLOOK

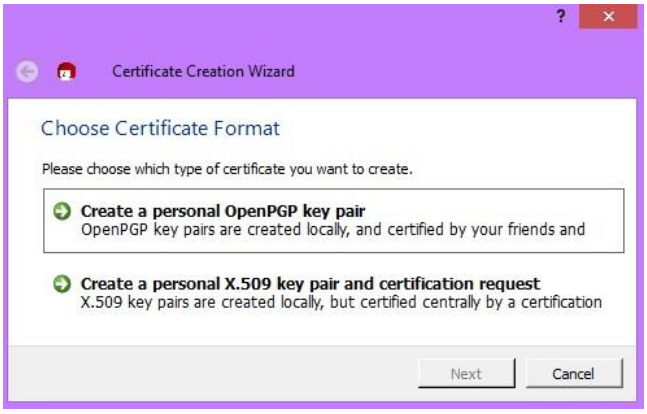
Al instalar el paquete GpgOL de GPG4win e iniciar Outlook, verás una nueva opción arriba a la derecha, con el mismo nombre. Tienes que pulsar en Start Certificate Manager General y a continuación se abrirá la aplicación Kleopatra.

Para generar las claves pulsa en la opción *File* (Archivo) y a continuación *New Certificate* (Nuevo certificado):



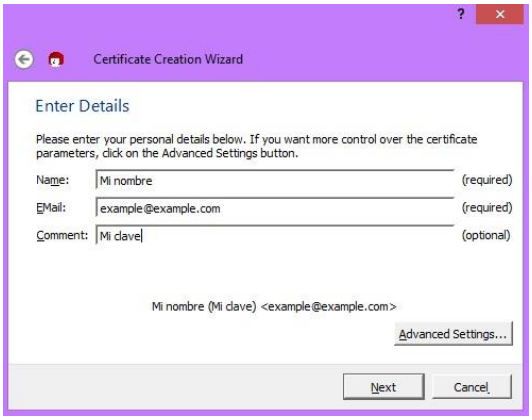
PGP en Outlook

Selecciona la primera opción y pulsa *Next o* siguiente:



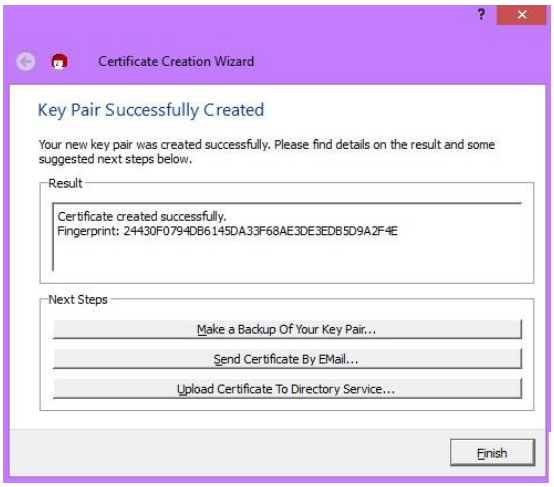
PGP en Outlook

Si pulsas en *Advanced Settings* (Opciones avanzadas) podrás modificar el nivel de cifrado por defecto.



PGP en Outlook

A continuación, pulsa *Next o* siguiente y *Create Key* (Crear clave). Se mostrará un aviso para indicar una contraseña, que deberás volver a introducir en el paso siguiente.

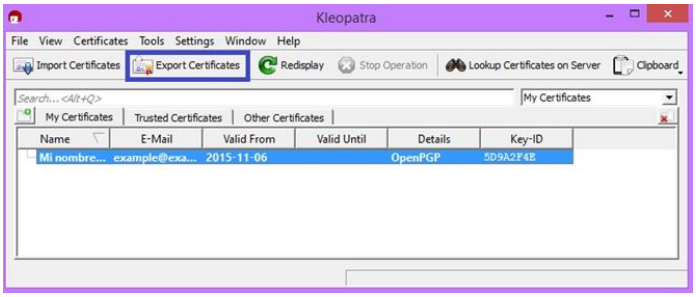


PGP en Outlook

Pulsa *Finish* para Finalizar.

De esta forma ya podrás enviar correos cifrados, ten en cuenta que deberás mandar tu clave pública a tu destinatario en el primer envío que realices.

Para ello tendrás que exportarla, y generar el fichero .ASC correspondiente y enviarla como fichero adjunto.

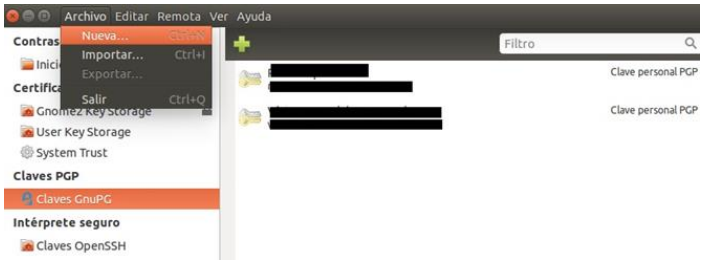


PGP en Outlook

Para poder leer los correos cifrados de tus contactos, deberán facilitarte previamente su clave pública, y tendrás que importarla desde la opción *Import Certificates*.

¿CÓMO REALIZAR EL CIFRADO DE EMAILS PGP EN LINUX CON SEAHORSE?

Puedes generar claves para cifrado de correo en Linux mediante Seahorse, una interfaz gráfica de GNOME que te permite trabajar con GnuPG.

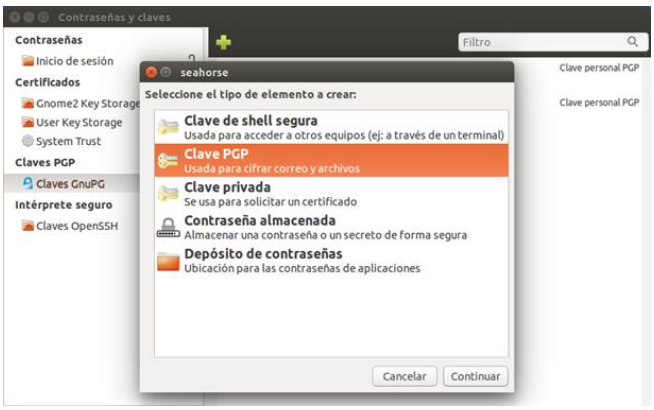


Usar PGP en Linux con Seahorse

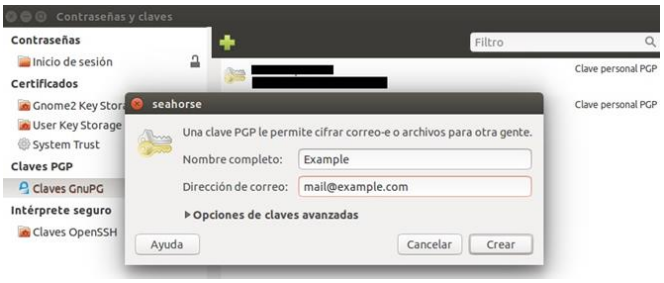
Abre la aplicación Seahorse y haz clic en Archivo y a continuación Nueva

Aquí verás una nueva ventana, con varias opciones de clave.

Selecciona la opción Clave PGP y pulsa Continuar:



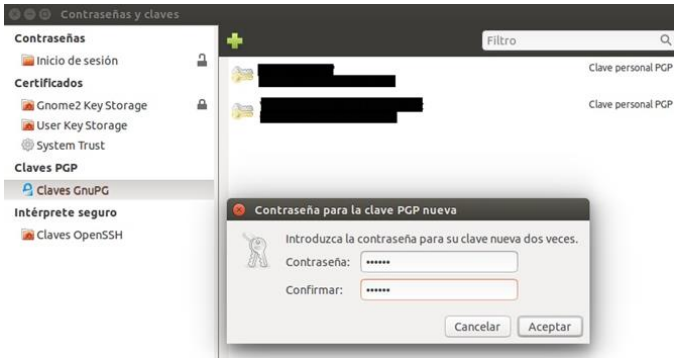
Usar PGP en Linux



Usar PGP en Linux

Introduce tu nombre de correo electrónico y clica en Crear.

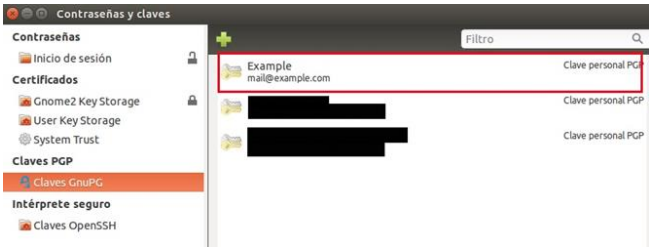
Introduce y confirma la contraseña seleccionada para la clave privada y pulsa en Aceptar.



Usar PGP en Linux

En unos minutos se mostrará la nueva clave generada.

Es un proceso que puede demorarse dependiendo de las tareas que estés realizando en el equipo. Para agilizarlo, puedes hacer tareas simples como navegar, escuchar música, etc, con el fin de generar entropía para la generación de la clave.



Usar PGP en Linux

Una vez hecho esto, puedes usar tu programa favorito para cifrar tus correos.

CIFRADO DE EMAILS PGP EN MAC OS X

Para usar PGP en Mac puedes descargarte GPG Suite, de GPG Tools.

Una vez hemos descargado la Suite de aplicaciones, realiza la instalación del aplicación.

Usar PGP en Mac OS X

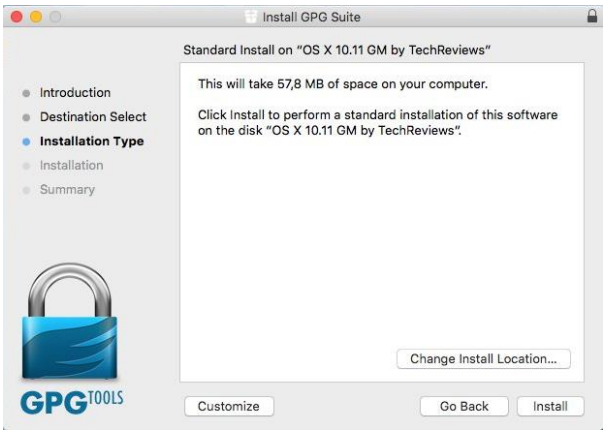
Seleccionamos *Install* una vez abierto el instalador:

En el siguiente paso, se indican los distintos paquetes que incluye la suite, selecciona GPGMail y GPG Keychain, el resto de paquetes son necesarios para el funcionamiento de estos dos.

Pulsamos en *Continue*.

Usar PGP en Mac OS X

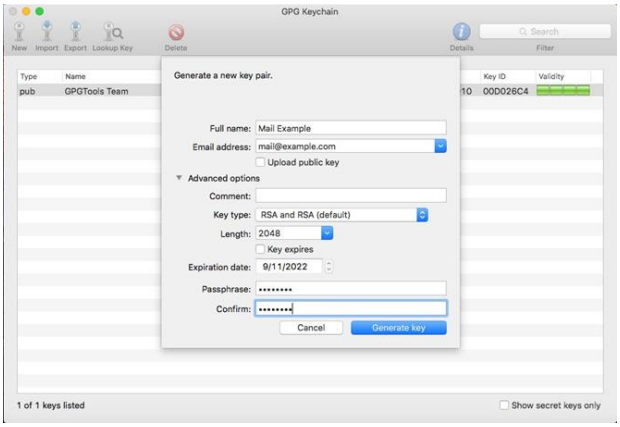
En el siguiente paso podrás modificar la carpeta de instalación si es necesario y a continuación pulsa Instalar.



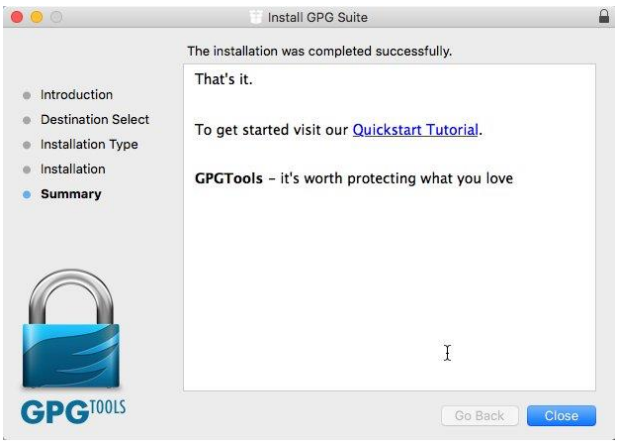
Usar PGP en Mac OS X

Durante el proceso de instalación se abrirá la aplicación GPG Keychain por vez primera, se te solicitará generar tu clave pública y privada para poder utilizarla con la aplicación Mail.

Simplemente cubre los campos que se solicitan, prestando especial atención al apartado *Email address*, donde deberás de indicar la cuenta de correo sobre la que vas a hacer uso de PGP, así como la *Passphrase* o contraseña de la clave, esta será necesaria para encriptar o desencriptar un correo con tus claves.



Usar PGP en Mac OS X

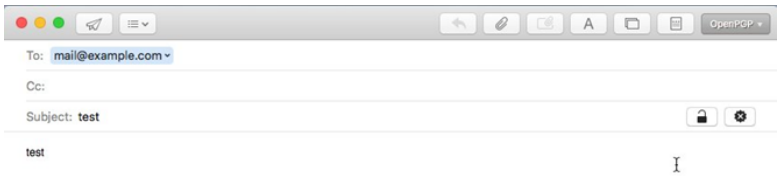


Usar PGP en Mac OS X

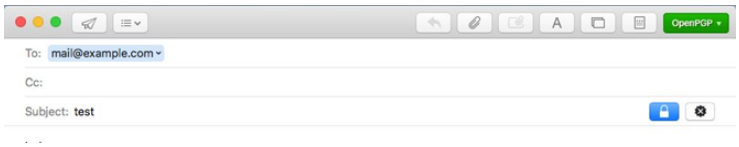
Una vez generada la clave, podemos cerrar GPG Keychain y el instalador de GPG Suite pulsando en *Close*.

Ahora accede a la aplicación Mail, y verás que cuando redactes un nuevo correo, ya tendrás nuevos iconos insertados por el plugin GPGMail. Cuando pulses sobre ellos, habilitarás la opción de cifrado, o de firma electrónica.

Aquí te mostramos el antes y el después de habilitar el cifrado de un correo:



Usar PGP en Mac OS X antes



Usar PGP en Mac OS X después

Verás que, tras pulsar sobre el candado, cambiará de color mostrándose en azul, y se hará visible en verde el botón OpenPGP de la parte superior.

Ten en cuenta que sólo las personas con las que compartas tu clave pública podrán leer tus correos.

Puedes exportar o importar nuevas claves desde la aplicación GPG Keychain. Ten presente que para poder enviar un correo cifrado necesitas la clave pública del destinatario.