Guía de firma y cifrado de archivos utilizando PGP

Tipo de Documento:	Guía de uso
Fecha de Publicación:	16 / 6 / 2015
Clasificación:	Acceso Libre
Presentado a:	CSIRT Panamá
Autores:	Mario Góngora
Versión:	1.0
Estado:	Final

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
\| Autoridad Nacional para la Innovación Gubernamental
\| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
\| Tel: +507 520-CERT (2378) \| Fax: +507 517-9500 \| E-Mail: info@cert.pa \| Twitter: @CSIRTPanama

DECLARACIÓN DE PRIVACIDAD Y CLASIFICACIÓN DE LA INFORMACIÓN

En cumplimiento del Capítulo IV de la Ley número 6 del año 2002 acerca de "Información Confidencial y de Acceso Restringido", puede resultar en perjuicio del Estado Panameño el que las ideas, conceptos, planes, definiciones, descripciones de eventos e ideas generales contenidas en este documento sean conocidas por personas distintas a aquellas a quienes está dirigido.

El receptor de este documento acepta y está de acuerdo en: No publicar o revelar la información contenida en el presente documento de manera parcial o total a terceros, sin el permiso expreso del Centro Nacional de Respuesta a Incidentes (CSIRT Panamá).

Ninguna parte de este documento debe revelado, duplicado, usado, o publicado total o parcialmente, fuera de su organización sin la autorización escrita de Centro Nacional de Respuesta a Incidentes (CSIRT Panamá) y la respectiva de-clasificación del mismo. A su vez, el receptor del documento se compromete a regirse conforme a las leyes panameñas relativas a la protección de autoría intelectual y confidencialidad de la información, especialmente la Ley número 6 del año 2002.

Las medidas de protección y restricción de distribución establecidas en esta "Declaración de Privacidad y Clasificación de la Información" quedan sin efecto en caso de que este sea clasificado como de "Acceso Libre".

CONTROL DE VERSIÓN

PREPARADO POR: Mario Gongora

APROBADO POR: Silvia Batista

FECHA DE INICIO: 1/15/2015

ESTADO DEL DOCUMENTO: Final

HISTORIA DE CAMBIOS:

Fecha	Cambios	Autores	Versión
6/16/2015	Inicio de documentación.	M. Góngora	0.1
7/1/2015	Se ajusta el documento al formato estándar.	M. Góngora	0.2
2/3/2016	Se reestructura el documento. Se agregan nuevas secciones. Se redefine el alcance del documento.	M. Góngora	0.3
2/5/2016	Se completa el núcleo contextual del documento.	M. Góngora	0.4
2/24/2016	Se completa el documento. Nos movemos a la versión 1.0	M. Góngora	1.0

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
| Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

1 Tabla de Contenido

2 Sumario Ejecutivo 5
3 Objetivo 5
4 Alcance 5
5 Utilización de OpenPGP para la firma y cifrado de archivos 6
5.1 Creación de llaves 6
5.2 Listar llaves públicas disponibles en el sistema 8
5.3 Ver llaves privadas 9
5.4 Borrar llaves de los anillos 9
5.5 Ver huella de una llave 10
5.6 Exportar llaves 10
5.7 Importar llave 11
5.8 Cifrar mensajes 12
5.9 Descifrar Mensajes 14
5.10 Firmar mensajes 14
5.11 Verificar mensajes firmados 15
6 Conclusiones 16
7 Información de contacto: 16

2 Sumario Ejecutivo

CSIRT Panamá como parte de sus funciones, ha preparado una guía de utilización de un mecanismo de cifrado y firmado digital basado en la implementación del estándar OpenPGP definido en RFC4880. Este mecanismo permite cifrar y firmar la información que desee compartir con CSIRT Panamá; en caso tal que usted como parte interesada lo considere necesario. Cabe señalar que CSIRT Panamá recomienda la utilización de este mecanismo al momento de enviarnos información sensitiva relacionada a un incidente de seguridad.

Este documento se compone de once subsecciones donde se explican las operaciones necesarias para establecer un envío seguro de los datos a compartir con nosotros. Estas subsecciones son: creación de llaves, listado de llaves públicas y privadas, borrar llaves, verificación de huella de una llave, exportación e importación de llaves, cifrado de archivos, firma digital en archivos y su posterior verificación.

Para mayor información acerca del funcionamiento de este mecanismo recomendamos la lectura de la documentación en el sitio del proyecto GnuPG: https://gnupg.org/documentation/guides.html

3 Objetivo

Proporcionar una guía que funcione como instructivo de uso de Pretty Good Privacy (PGP) para las personas que deseen enviarnos archivos cifrados o firmados digitalmente.

4 Alcance

Las instrucciones descritas en este documento aplican las implementaciones debidamente documentadas en: https://www.gnupg.org; el proyecto GPG4Win https://gpg4win.org (para sistemas Windows) contiene información para la instalación del programa en Windows.

Los usuarios de sistemas operativos basados en Microsoft Windows, deberán descargar la versión Gpg4win que se adecue a sus necesidades. El enlace para la descarga de este programa es: https://www.gpg4win.org/download.html

Para sistemas basados en GNU/Linux recomendamos verificar la documentación del sistema operativo para la instalación del paquete según sea el caso.

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

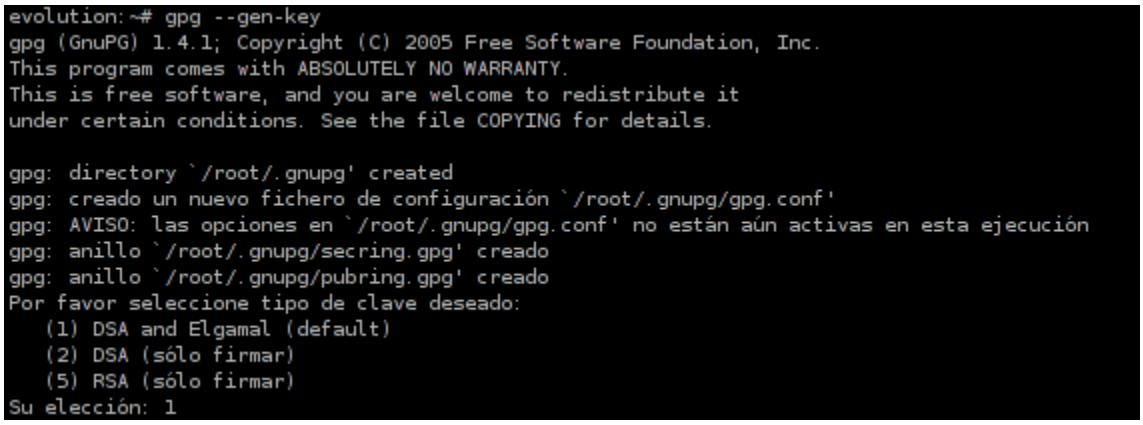
5 Utilización de OpenPGP para la firma y cifrado de archivos

5.1 Creación de llaves

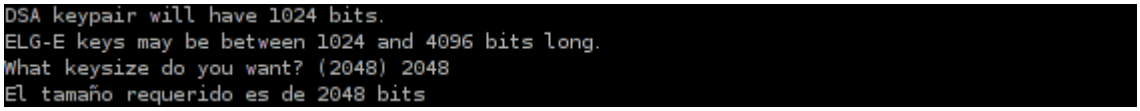
Abra una terminal y escriba:

- gpg --gen-key

Se le presentará varias opciones que ve a continuación. Dependerá de usted crear una sola llave para firmar y cifrar o una subllave para cifrar. Por ejemplo la opción 4 crea una llave solo para firmar, si desea cifrar tendrá que generar una subllave. Para manejo de esta guía nosotros utilizaremos la opción 1. (RSA and RSA).



Después se nos pregunta acerca del largo de la llave. El rango va desde 1024 a 4096 bits de largo. La opción por defecto es 2048. Recuerde lo siguiente: a mayor tamaño más segura es la llave, también a mayor tamaño más tiempo lleva el proceso de cifrado y descifrado.



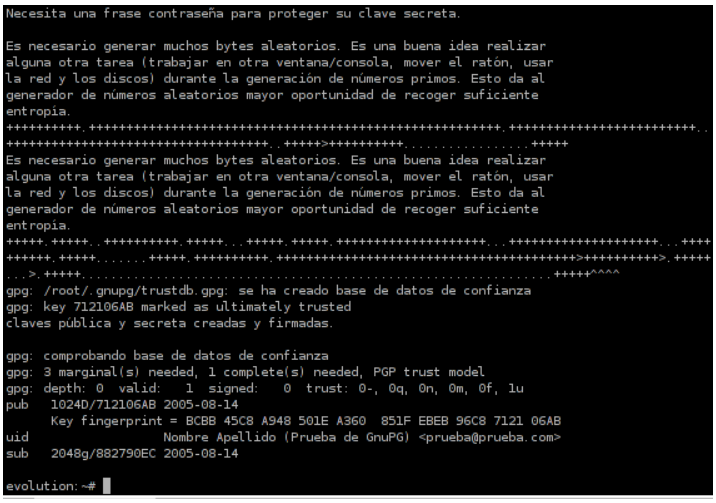
Luego, nos preguntará el tiempo de validez de la llave. La periodicidad se puede colocar de forma tal que nunca caduque; o que dure una cantidad fija de días, semanas, meses o años. Por defecto la opción es 0, lo cual significa que no tiene tiempo de caducidad.

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
| Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

```
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
       <n>  = la clave caduca en n días
       <n>w = la clave caduca en n semanas
       <n>m = la clave caduca en n meses
       <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
Key does not expire at all
Is this correct? (y/N) y
```

Después, se nos preguntará nuestro nombre y apellido, dirección de correo y un comentario para la llave que estamos creando. Una vez introducidos todos los datos nos muestra cual es nuestro ID de usuario. Esta identificación es creada a partir de los datos que hemos introducido anteriormente. Una vez confirmemos esta información comenzara el proceso final para la creación de las llaves.

Por último, se nos preguntará una contraseña (passphrase) para nuestra llave privada. Al introducir la contraseña no se podrá observar nada de lo que se escribe en la terminal. Después de introducirla nos vuelve a preguntar la contraseña y si coinciden comenzará la generación de las llaves. Cuando se produce el proceso de generación de llaves se recomienda generar actividad en el CPU de la máquina, es decir; mover el ratón, reproducir música o videos. Como se puede observar en la imagen a continuación: "*Es necesario generar muchos bytes aleatorios. Es una buena idea realizar alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar la red y los discos) durante la generación de números primos. Esto da al generador de números aleatorios mayor oportunidad de recoger suficiente entropía*". Cabe señalar que la explicación técnica de este mecanismo esta fuera del alcance de esta guía.



Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
| Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

5.2 Listar llaves públicas disponibles en el sistema

Luego de generar nuestras llaves (públicas) podemos verificar que fueron creadas de la siguiente forma:

```
evolution:~/.gnupg# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   1024D/712106AB 2005-08-14
uid                  Nombre Apellido (Prueba de GnuPG) <prueba@prueba.com>
sub   2048g/882790EC 2005-08-14

pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~/.gnupg#
```

De igual, forma con la instrucción "--list-keys" se pueden realizar búsquedas de las llaves utilizando distintos parámetros de búsqueda. Por ejemplo: Nombre, KeyID y correo electrónico asociado a la llave.

```
evolution:~# gpg --list-keys Nombre2
pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~# gpg --list-keys Apellido2
pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~# gpg --list-keys prueba2@prueba2.com
pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~# gpg --list-keys 0x3960CFFB
pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~# gpg --list-keys "Prueba 2 de GnuPG"
pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~# gpg --list-keys "Nombre"
pub   1024D/712106AB 2005-08-14
uid                  Nombre Apellido (Prueba de GnuPG) <prueba@prueba.com>
sub   2048g/882790EC 2005-08-14

pub   1024D/3960CFFB 2005-08-14
uid                  Nombre2 Apellido2 (Prueba 2 de GnuPG) <prueba2@prueba2.com>
sub   2048g/0C083FDC 2005-08-14

evolution:~#
```


Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
\| Autoridad Nacional para la Innovación Gubernamental
\| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
\| Tel: +507 520-CERT (2378) \| Fax: +507 517-9500 \| E-Mail: info@cert.pa \| Twitter: @CSIRTPanama

5.3 Ver llaves privadas

Para visualizar las llaves privadas que tenemos disponibles, podemos utilizar la instrucción "--list-secret-keys".

```
evolution:~# gpg --list-secret-keys
/root/.gnupg/secring.gpg
------------------------
sec   1024D/712106AB 2005-08-14
uid                  Nombre Apellido (Prueba de GnuPG) <prueba@prueba.com>
ssb   2048g/882790EC 2005-08-14

evolution:~#
```

5.4 Borrar llaves de los anillos

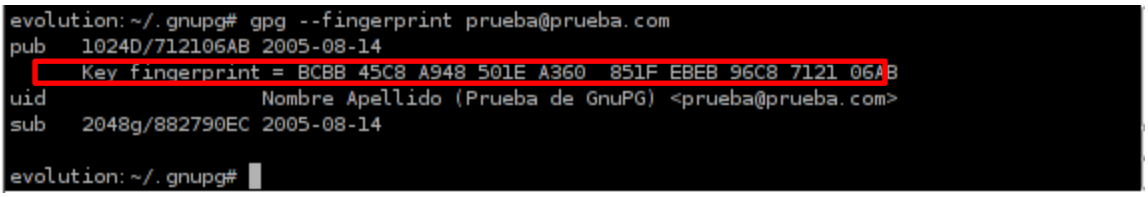
Se conoce como anillos a los archivos en los que están almacenados las llaves públicas y privadas. Generalmente estos archivos tienen como nombre: pubring.gpg y secring.gpg. Si se desea eliminar alguna llave primero se recomienda borrar la llave privada y luego la pública. Para eliminar la llave privada se debe ejecutar la instrucción: "*gpg --delete-secret-key KeyID*" y para eliminar la llave privada: "*gpg --delete-key KeyID*" en donde "KeyID" se entiende como el identificador de la llave.

```
evolution:~# gpg --delete-secret-keys Prueba4
gpg (GnuPG) 1.4.1; Copyright (C) 2005 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


sec  1024D/93A63FAC 2005-08-24 Nombre4 Apellido4 (Prueba4) <prueba4@prueba4.com>

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
evolution:~#
evolution:~# gpg --delete-keys Prueba4
gpg (GnuPG) 1.4.1; Copyright (C) 2005 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


pub  1024D/93A63FAC 2005-08-24 Nombre4 Apellido4 (Prueba4) <prueba4@prueba4.com>

Delete this key from the keyring? (y/N) y
```

5.5 Ver huella de una llave

Las llaves están identificadas por una huella (fingerprint). Esta huella es una secuencia alfanumérica que se utiliza para verificar la integridad de una llave.

La opción "*--fingerprint*" nos permite obtener la huella de una llave. La siguiente imagen ilustra este proceso.



5.6 Exportar llaves

Las llaves se pueden exportar a ficheros, con el fin de poder distribuirla con las personas con las que deseamos comunicarnos. Para exportar la llave pública se coloca:

- gpg --armor --output ficherodesalida --export KeyID

La siguiente imagen muestra esta operación.

También, es posible exportar nuestras llaves públicas a servidores de llaves alojados remotamente. De esta forma, nuestra llave pública puede ser descargada por cualquier persona que conozca nuestros datos, por ejemplo: correo electrónico.

El proceso es sencillo, solo basta con especificar el servidor de llaves donde deseamos subir nuestra llave y el identificador de llave "KeyID". Algunos servidores de llaves utilizados comúnmente son: pgp.mit.edu, pool.sks-keyservers.net y keys.gnupg.net

```
mgongora@csirt-desktop-mg:~$ gpg --keyserver pgp.mit.edu --send-key 3FC25F55
gpg: sending key 3FC25F55 to hkp server pgp.mit.edu
mgongora@csirt-desktop-mg:~$
```

5.7 Importar llave

Para importar nuestras llaves o las de un tercero solo basta con obtener el archivo de la llave pública (por ejemplo) que deseemos importar. Con dicho archivo solo basta con ejecutar en la terminal: "*gpg --import NombredeLlave.asc*", luego puede verificar ejecutando la opción "*--list-keys*" para mostrar las llaves públicas.

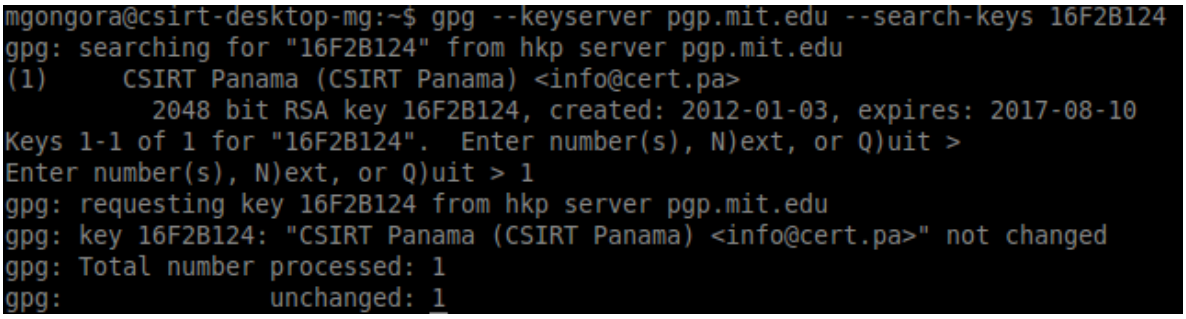
```
evolution:~/claves# gpg --import prueba-public-key.asc
gpg: directory `/root/.gnupg' created
gpg: creado un nuevo fichero de configuración `/root/.gnupg/gpg.conf'
gpg: AVISO: las opciones en `/root/.gnupg/gpg.conf' no están aún activas en esta ejecución
gpg: anillo `/root/.gnupg/secring.gpg' creado
gpg: anillo `/root/.gnupg/pubring.gpg' creado
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: key 712106AB: public key "Nombre Apellido (Prueba de GnuPG) <prueba@prueba.com>" imported
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
evolution:~/claves# gpg --import prueba-secret-key.asc
gpg: key 712106AB: secret key imported
gpg: key 712106AB: "Nombre Apellido (Prueba de GnuPG) <prueba@prueba.com>" 1 new signature
gpg: Cantidad total procesada: 1
gpg:               nuevas firmas: 1
gpg:      claves secretas leídas: 1
gpg:  claves secretas importadas: 1
evolution:~/claves# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   1024D/712106AB 2005-08-14
uid                  Nombre Apellido (Prueba de GnuPG) <prueba@prueba.com>
sub   2048g/882790EC 2005-08-14

evolution:~/claves#
```

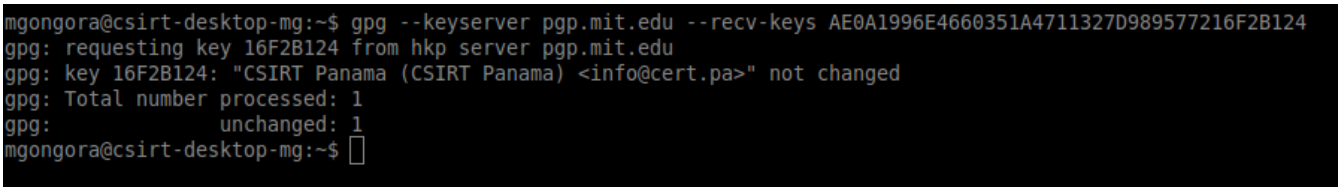

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
\| Autoridad Nacional para la Innovación Gubernamental
\| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
\| Tel: +507 520-CERT (2378) \| Fax: +507 517-9500 \| E-Mail: info@cert.pa \| Twitter: @CSIRTPanama

También es posible importar directamente desde un servidor de llave en caso tal se conozca algunos datos de la persona con la que deseemos entablar una comunicación.

- gpg --keyserver pgp.mit.edu --search-keys {correo electrónico, KeyID}
- gpg --keyserver pgp.mit.edu --recv-keys {huella}

Como puedo observar la opción "*--keyserver*" sirve para indicar el servidor de llaves que se desea utilizar para realizar la búsqueda de las llaves. La opción "*--search-keys*" puede tener como parámetro el correo electrónico o el KeyID de la llave. Otra forma más directa es utilizando la opción "*--recv-keys*" que recibe como parámetro la huella de la llave que deseamos importar. Las siguientes imágenes muestran este proceso.





5.8 Cifrar mensajes

Para cifrar archivos es necesario conocer la llave pública de la persona a quién vamos a enviar la comunicación. Por ejemplo si deseamos enviar un archivo cifrado a una persona debemos ejecutar las siguientes instrucciones en la terminal.

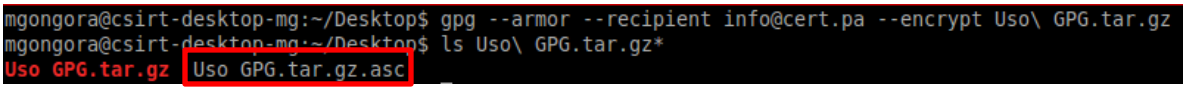
gpg --armor --recipient {Correo Electrónico, KeyID} --encrypt {nombredelarchivo}

Las opción "--recipient" puede tener como parámetro el correo electrónico de la persona de quien le vamos a enviar nuestro archivo cifrado o el KeyID. Y la opción "--encrypt" tiene como parámetro el nombre del archivo que se va a cifrar. La opción "—armor" permite convertir los archivos cifrados de cualquier tipo en ficheros de texto ASCII. Por ejemplo un

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

archivo binario como un programa puede cifrarse y convertirse en texto ASCII que se puede enviar como texto simple por correo electrónico.

En la siguiente imagen se muestra un ejemplo en donde se cifra un archivo con formato ".tar.gz" para CSIRT Panamá. El recuadro en rojo muestra el archivo que se genera luego del proceso de cifrado; noten la extensión "*.asc*". Este es el archivo que se debe enviar ya que se encuentra cifrado con nuestra llave pública.



Si abrimos el archivo Uso GPG.tar.gz.asc en un editor de texto, obtendremos lo que observamos a continuación. Solo la persona con la llave privada del mensaje cifrado podrá tener acceso al archivo que hemos cifrado.

Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
| Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

5.9 Descifrar Mensajes

Para descifrar un mensaje o archivo que nos enviado solo debemos ejecutar la siguiente instrucción en la terminal. Tomando en cuenta que la máquina donde estamos trabajando tiene las llaves necesarias para esta operación. La siguiente imagen muestra este proceso.

- gpg {nombredelarchivo.asc}

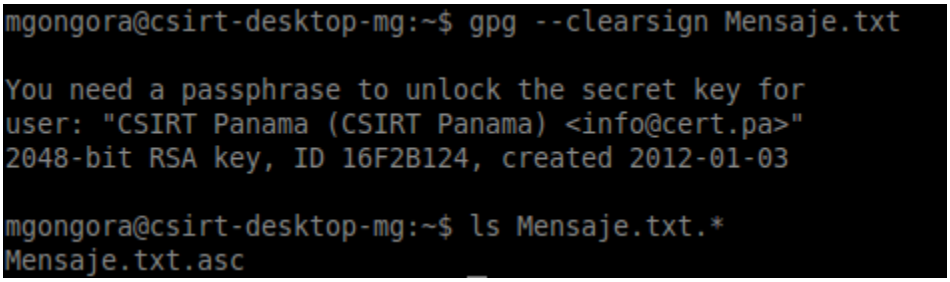
El recuadro en rojo muestra la salida de esta instrucción, se puede observar que el archivo ha sido descifrado utilizando nuestra llave privada.

5.10 Firmar mensajes

El proceso de firma de mensajes es utilizado con el fin de que el receptor pueda verificar la autenticidad del mensaje o archivo enviado.

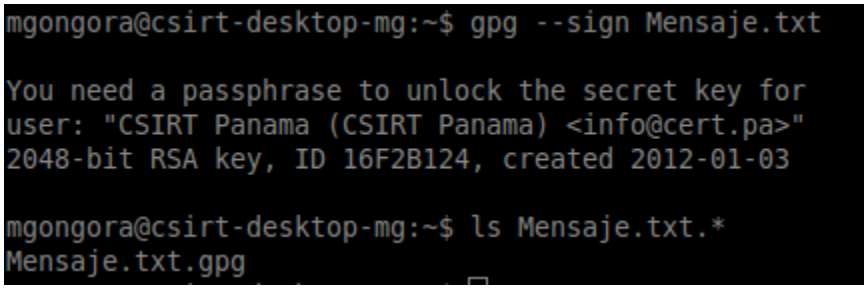
Existen varios métodos para firmar un archivo:

- gpg --clearsign {nombredelarchivo}: esta opción crea un archivo de salida de texto con extensión "*.asc*", que envuelve el texto firmado con una armadura ASCII como se puede ver a continuación.



Centro Nacional de Respuesta a Incidentes - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

- gpg --sign {nombredelarchivo}: esta opción crea un archivo de salida en binario con extensión "*.gpg*". Para validar la firma y ver el contenido tendríamos que descifrarlo con la opción "*--decrypt*".



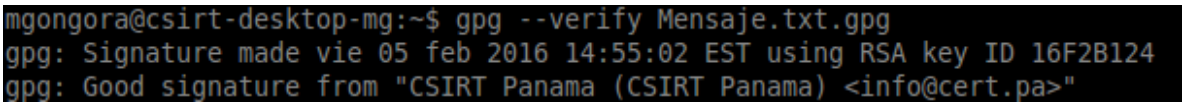
5.11 Verificar mensajes firmados

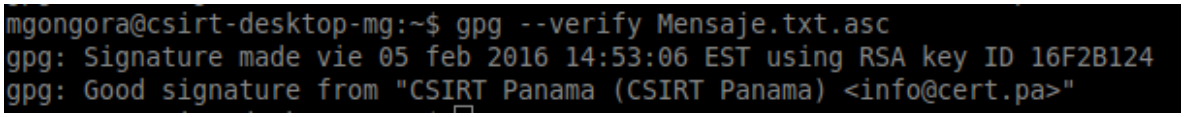
Si recibimos un mensaje firmado y deseamos verificar la autenticidad de la persona que lo está enviando, podemos corroborarlo colocando la siguiente instrucción en nuestra terminal.

gpg --verify {ArchivoFirmado}

El "*ArchivoFimado*" debe tener la extensión "*.asc*" o "*.gpg*", dependiendo de la forma con que la otra persona haya firmado el archivo.

Las siguientes imágenes muestran las salidas para ambos casos.





Centro Nacional de Respuesta a Incidentes - CSIRT Panamá
| Autoridad Nacional para la Innovación Gubernamental
| Vía Ricardo Arango y Calle 61 Obarrio, Edificio Sucre, Arias & Reyes – Nivel 300
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

6 Conclusiones

La utilización de mecanismos de cifrado nos permite, de manera segura; enviar documentación, mensajes de texto o cualquier tipo de archivo que consideremos sensitivos al momento de comunicarnos con otra persona a través del Internet. Esto lo podemos lograr utilizando PGP, que sigue el estándar OpenPGP; para el cifrado y el descifrado de datos. De esta forma, agregamos una capa adicional de confidencialidad a nuestros mensajes.

La guía que hemos preparado está orientada a personas dentro de nuestra comunidad y fuera de ella, que requieran enviarnos documentación cifrada al momento de reportar un incidente de seguridad de la información.

7 Información de contacto:

CSIRT PANAMA
Computer Security Incident Response Team
Autoridad Nacional para la Innovación Gubernamental
E-Mail: info@cert.pa
Phone: +507 520-CERT (2378)
Web: https://cert.pa
Twitter: @CSIRTPanama
Facebook: http://www.facebook.com/CSIRTPanama
Key ID: 16F2B124