

## ANEXO

### Manual del Usuario “PGP”

#### Objetivo

Con PGP se protegerá la privacidad y autenticidad de los archivos enviados utilizando la opción de **Entrega de Información Vía Electrónica** a través de la página WEB de la Comisión Nacional de Seguros y Fianzas (CNSF). Con PGP también se puede firmar digitalmente los archivos, lo cual asegura su autenticidad.

La aplicación PGP tiene como objetivo encriptar cualquier tipo de documentación enviada a través del correo electrónico.

Para efectos del envío de información por parte de las Instituciones o Sociedades a la CNSF a través de Internet, se requiere de esta aplicación, ya que es primordial para las Instituciones y Sociedades el hecho de que su información no sea modificada o editada una vez que ha sido enviada a la CNSF, por lo que requerirán encriptarla con la aplicación PGP utilizando llaves públicas y privadas.

PGP esta basado en una tecnología de encriptación ampliamente aceptada conocida como criptografía de llave pública en donde dos llaves complementarias –un par de llaves – son usadas para mantener la seguridad de las comunicaciones. Para enviar a alguien un archivo privado por correo electrónico se debe tener primero una copia de la llave pública de esa persona para encriptar la información, la cual únicamente será descifrada usando la llave privada correspondiente.

A continuación se describe el funcionamiento de esta aplicación como herramienta de apoyo en el proceso de Entrega de Información Vía Electrónica a través de la página WEB de la CNSF.

## I. Como obtener el programa de instalación de PGP de Internet

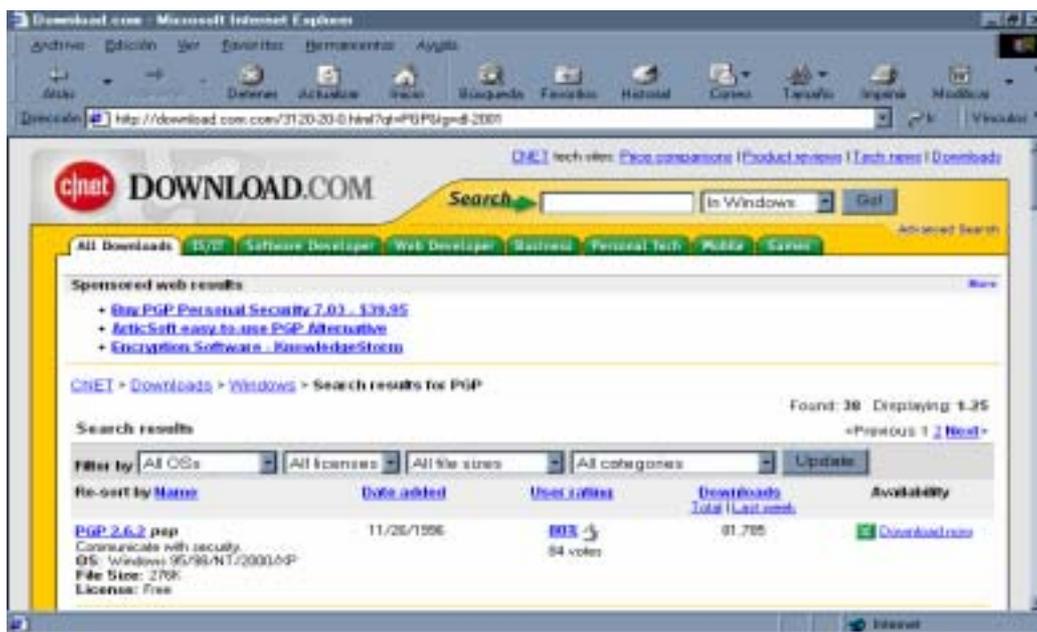
Como primer paso se debe tener acceso a internet y en el campo de **Dirección** teclear <http://www.download.com> , dar Enter y aparecerá la siguiente pantalla:



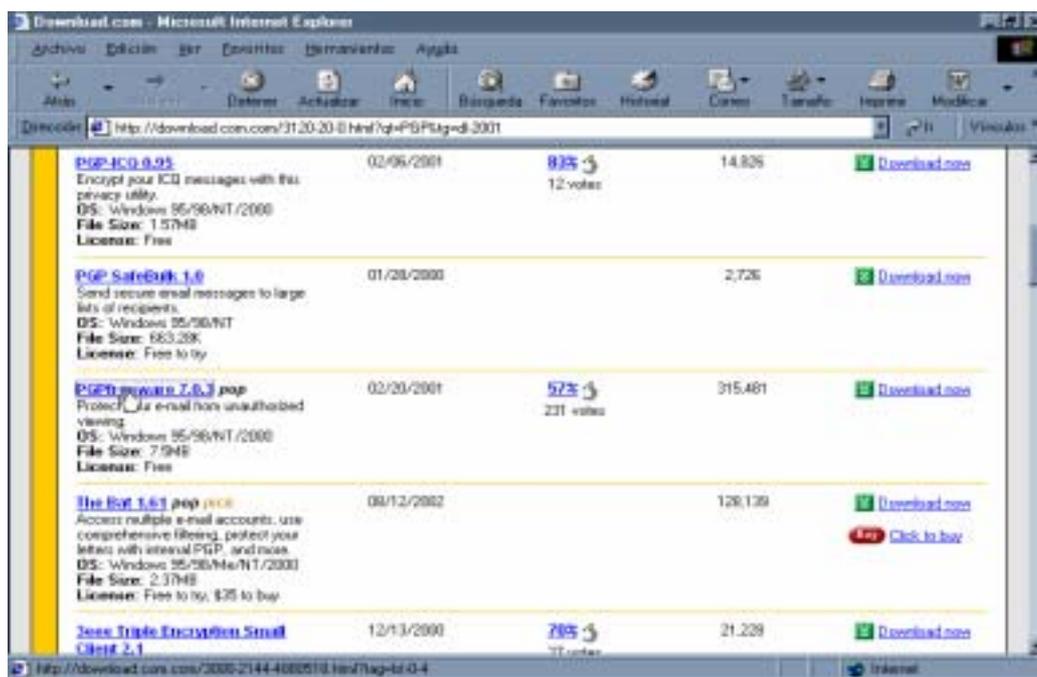
En el campo **Search** teclear las siglas PGP



Dar enter y aparecerá la siguiente pantalla:



Buscar y seleccionar el programa PGP freeware 7.0.3, dar Enter (Nota: Si se tiene la versión XP de Windows, se recomienda usar la versión 8)



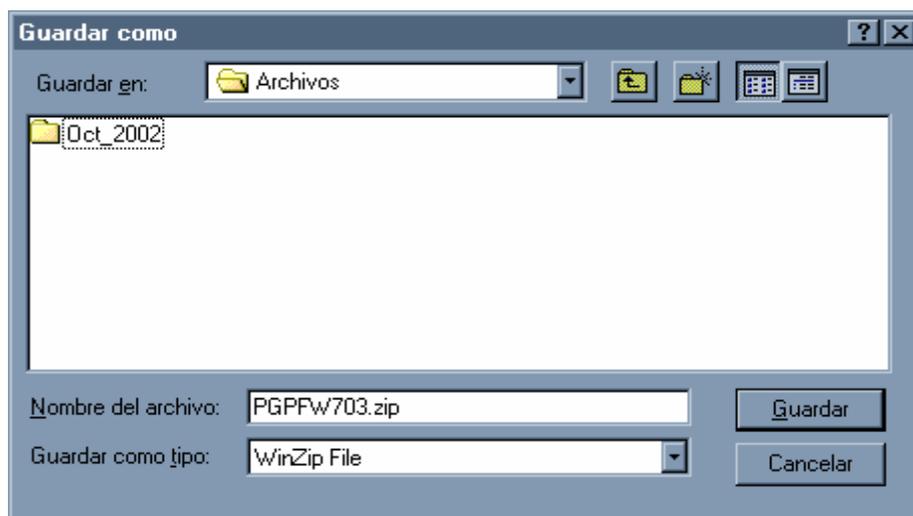
Entraremos a la siguiente pantalla en donde daremos inicio al proceso de descarga del software, dando click sobre las palabras "Download Now"



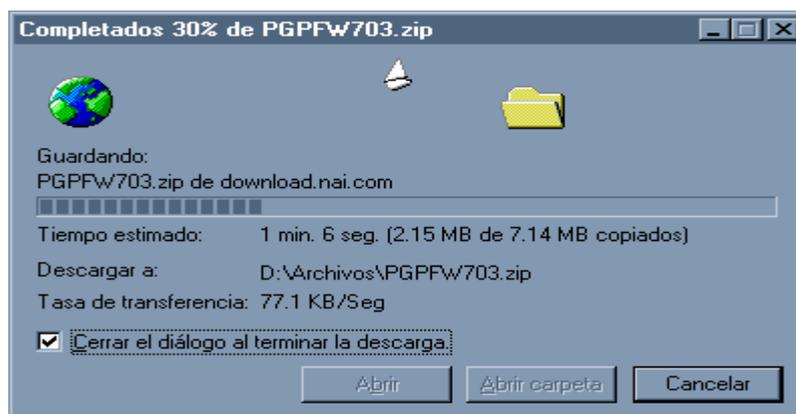
Aparecerán los siguientes mensajes



Por default nos indica que se guarde el archivo en disco, no cambiar esta opción y dar click en el botón **Aceptar**, nos mostrará el siguiente mensaje



Aquí indicaremos en qué carpeta de nuestra PC deseamos guardar el programa, posteriormente dar click en el botón  y aparecerá una pantalla indicando el avance de descarga



Al terminar la descarga se cerrará el cuadro de diálogo, siempre y cuando esté activado, en caso contrario dar click en el botón  que aparecerá en la parte inferior derecha y cerrar la conexión con Internet.



## II. Cómo instalar la aplicación PGP

Dependiendo del equipo de cómputo y la versión del sistema operativo, el programa lo instalará automáticamente al ejecutar la descompactación del archivo que se bajó de Internet.

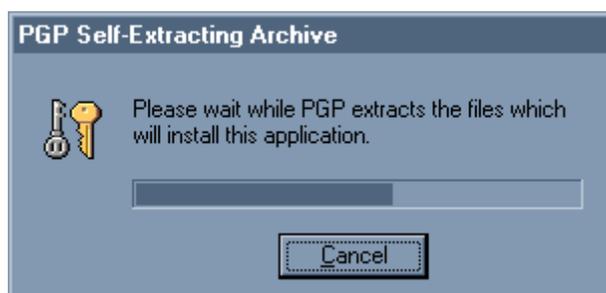
La primera vez que se crea una llave privada, el Administrador instala el producto PGP, el cual es de uso libre conforme a lo declarado por Integraciones Administrativas. Siguiendo los pasos de la instalación de PGP, la aplicación le pedirá ingresar una frase secreta o un "passphrase" para poder crear una llave privada, **el Administrador deberá crear la llave privada SIN ingresar una contraseña (passphrase) ni su confirmación.**

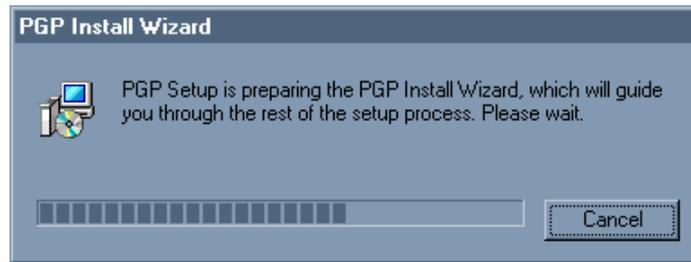
Procedimiento:

Localizar el archivo descargado PGP que lleva la extensión **.exe**

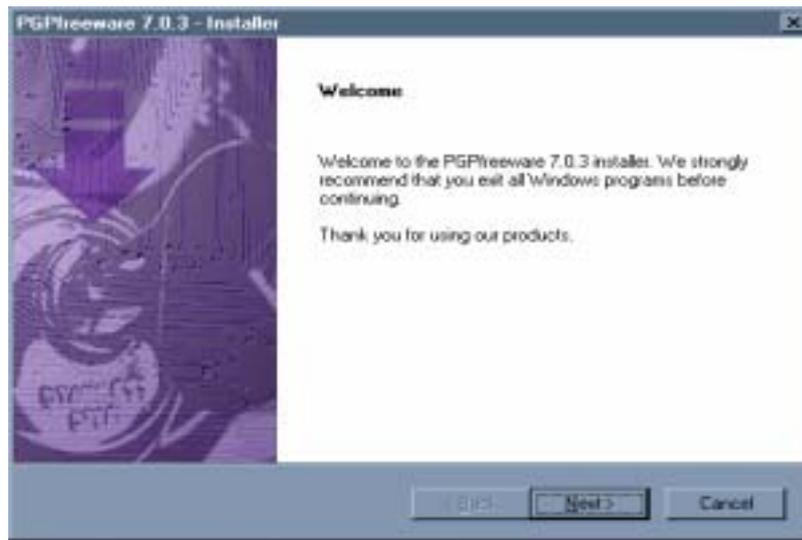


Dar doble click sobre el ejecutable  y aparecerá una secuencia de mensajes

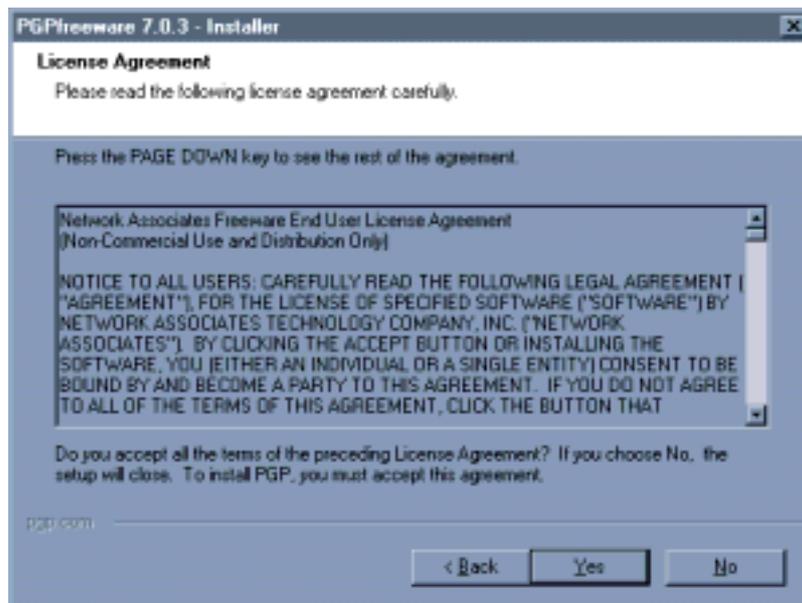


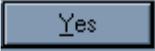


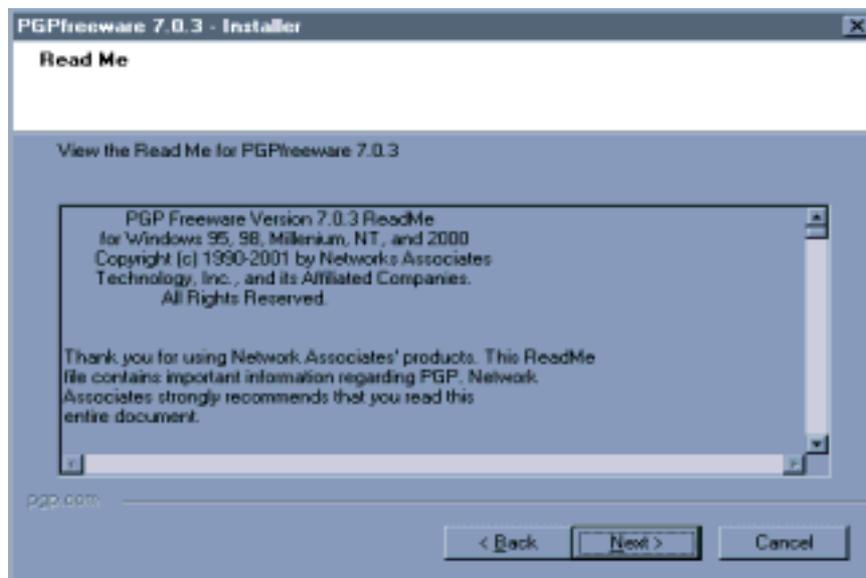
Al terminar la secuencia de mensajes aparecerá la pantalla de bienvenida



Dar click en el botón  y aparecerá un mensaje de Acuerdo de uso de Licencia

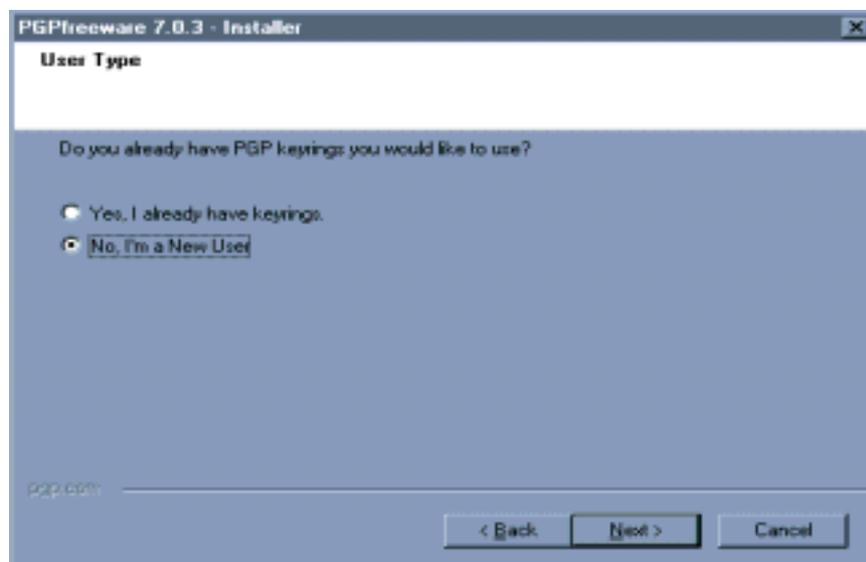


Dar click en el botón 

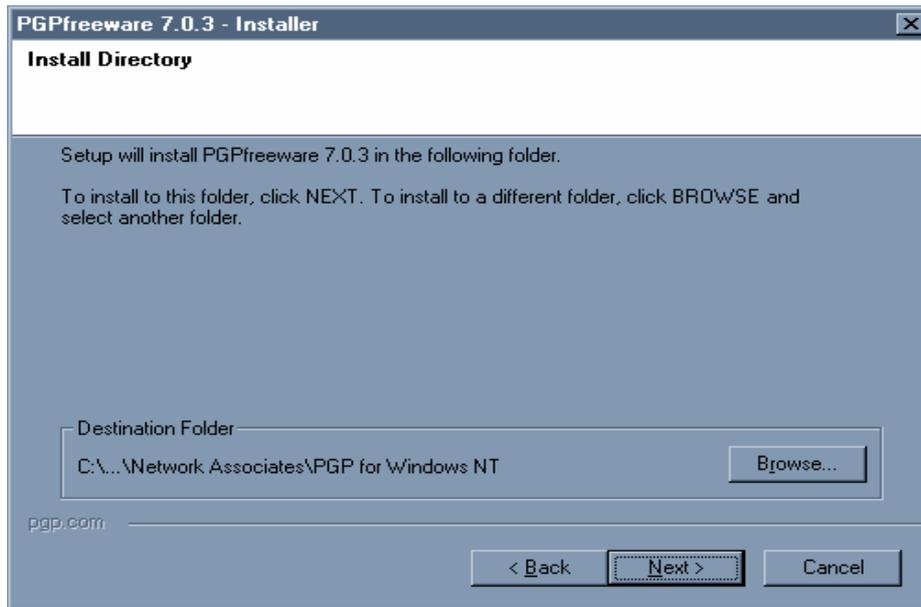


Dar click en el botón  y aparecerá la pantalla para seleccionar el Tipo de Usuario

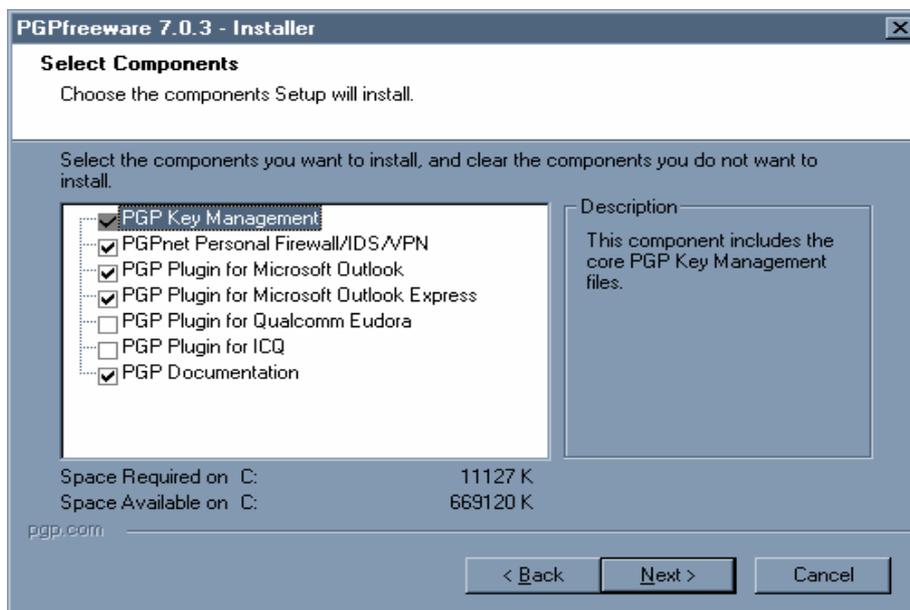
Por default aparecerá marcada la opción de  Yes, I already have keyrings., debemos seleccionar la opción  No, I'm a New User como se muestra en la siguiente pantalla



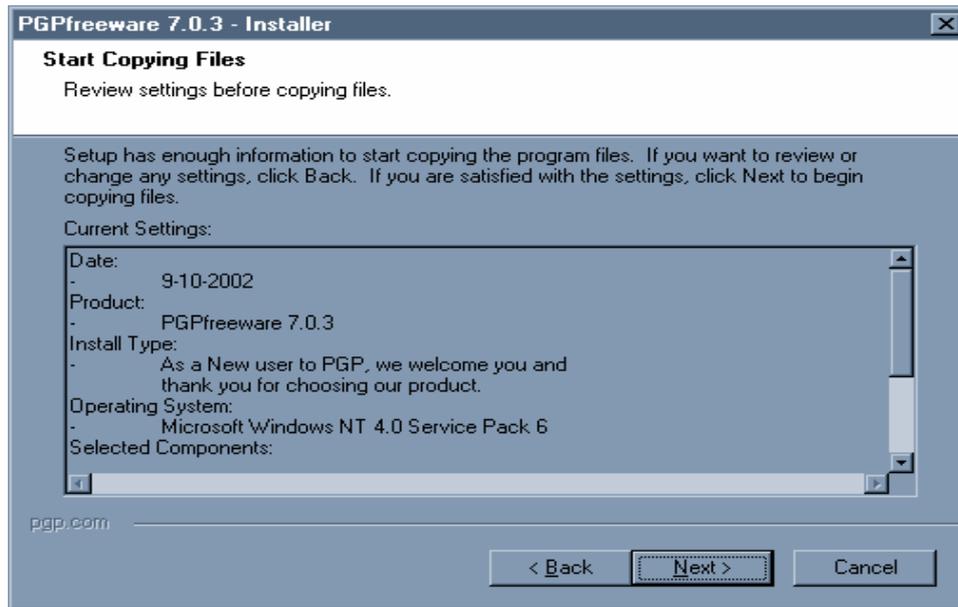
Dar click en el botón  para seleccionar el Fólдер Destino para la Instalación del Directorio



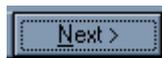
Si deseamos cambiar el Fólder Destino, pulsar el botón , si lo queremos dejar en la ruta marcada por default dar click en el botón  y aparecerá la ventana de Selección de Componentes



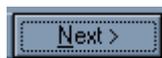
Dar click en el botón  y aparecerá la pantalla para comenzar a copiar los archivos



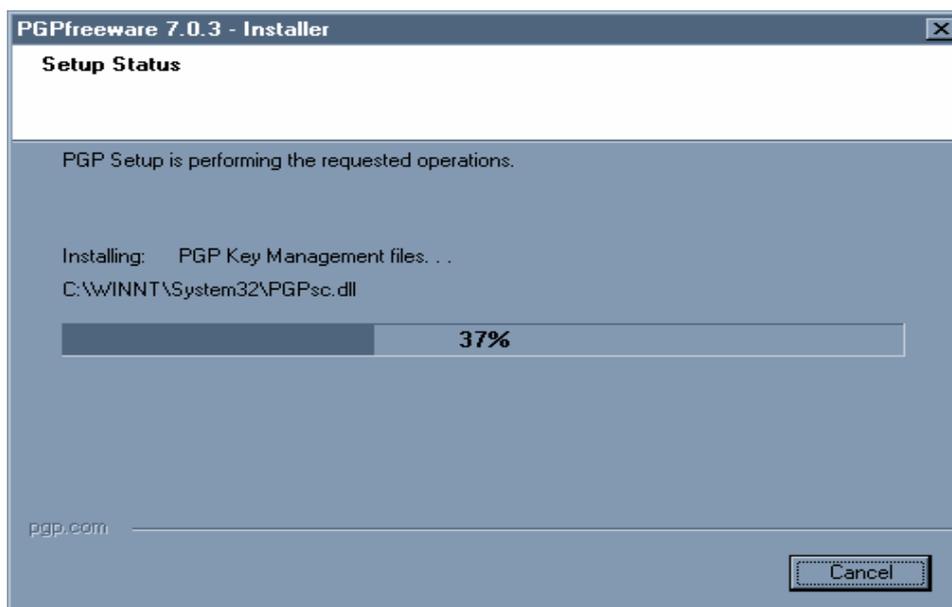
Dar click en el botón



Dar click en el botón

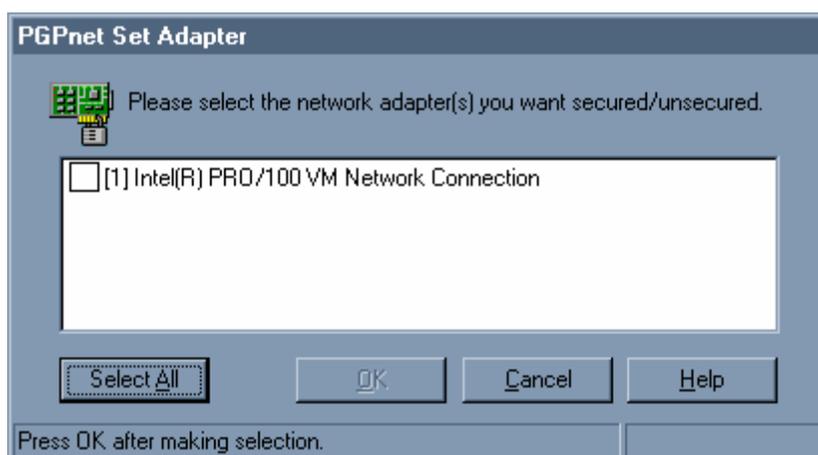


y aparecerá la pantalla que indica el avance de instalación

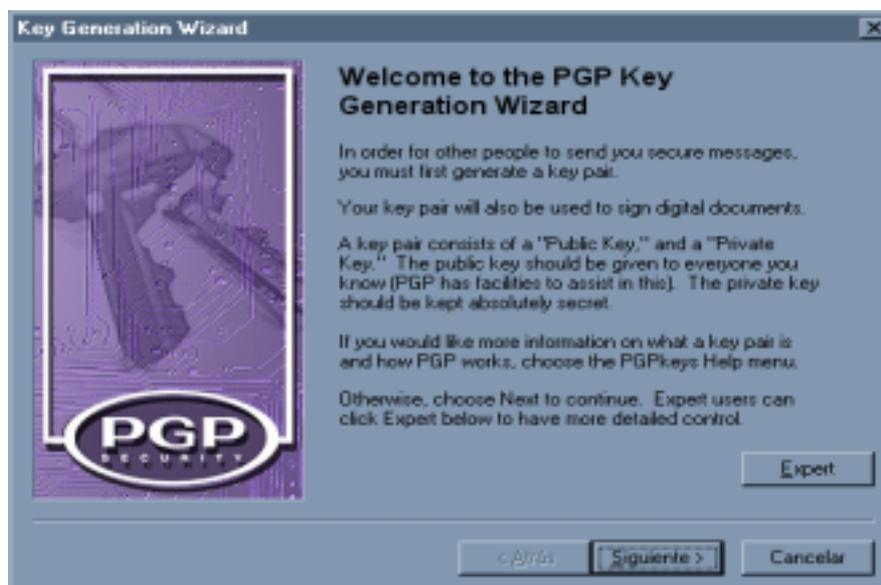


Al terminar la instalación se activará y pulsaremos el botón

Next >



Dar click en el botón **Select All** y se activará el botón **OK** y aparecerán una serie de mensajes, al terminar éstos aparecerá la siguiente pantalla, la cual nos permitirá crear la llave privada de la Institución o Sociedad, es recomendable que se cree en este momento, sin embargo, en caso de decidir hacerlo después, basta con que cancele el proceso pulsando el botón **Cancelar** y posteriormente accese a PGP, como se indica en este manual y realice los pasos que a continuación se indican,

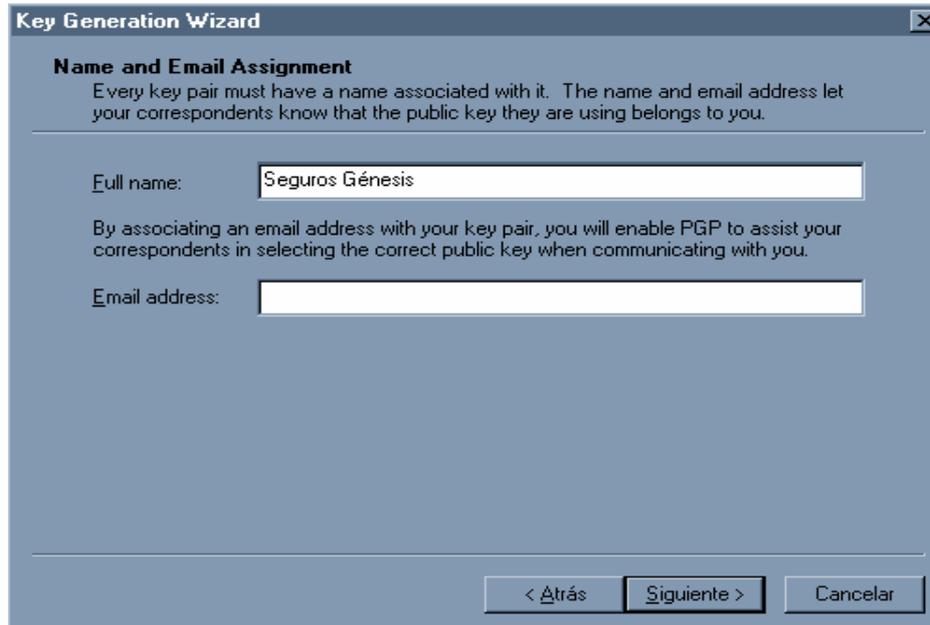


Pulsar el botón  y aparecerá la siguiente ventana

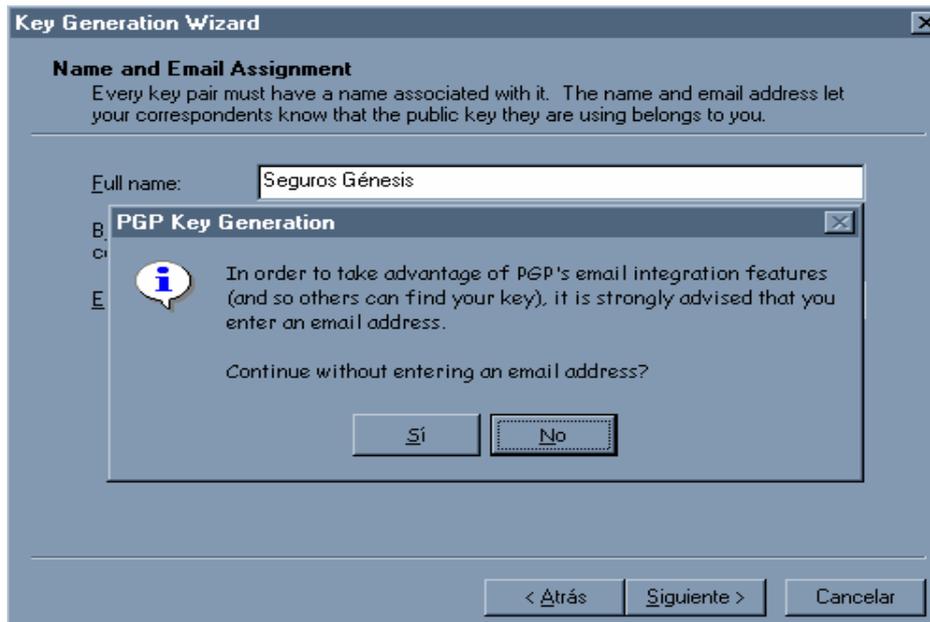
Asimismo, si usted decidió cancelar la creación de la llave privada al momento mismo de hacer la instalación, cuando decida hacerlo, deberá seguir los pasos que se indican a continuación



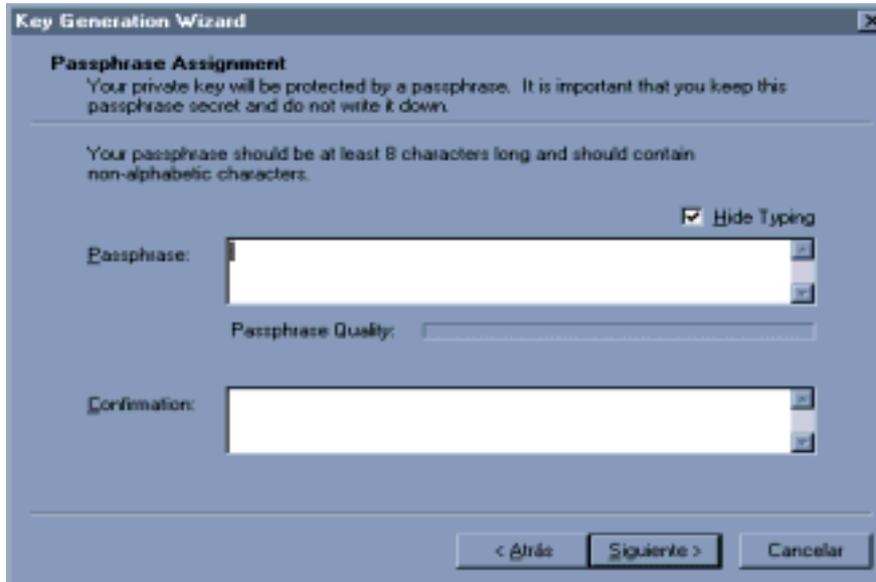
En el campo  teclaremos el nombre de la compañía



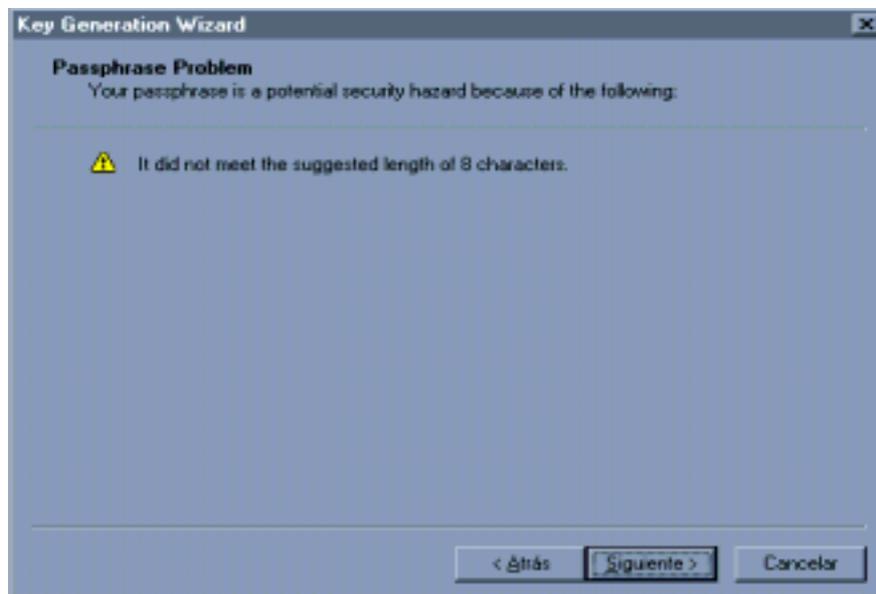
El campo  se dejará en blanco y al pulsar el botón



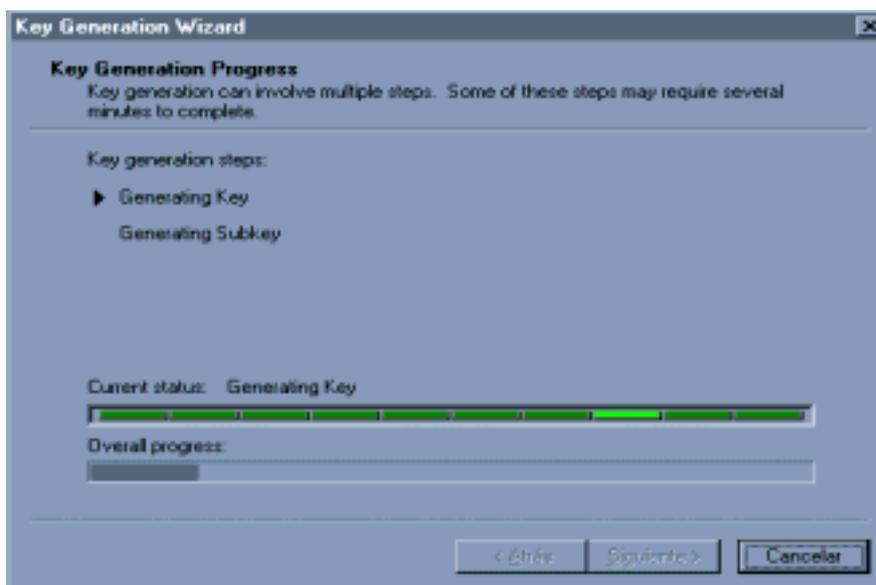
Aparecerá un mensaje preguntando si deseamos continuar sin haber teclado ninguna dirección de e-mail, pulsar el botón  y aparecerá la siguiente pantalla



En esta ventana **NO SE DEBE CAPTURAR EL “PASSPHRASE”**, dar click en el botón **Siguiente >**, aparecerá otra pantalla en la que indica que es necesario pulsar el “passphrase”, por favor **IGNÓRELA** y pulse el botón **Siguiente >**



Aparecerá una ventana indicando el proceso de instalación

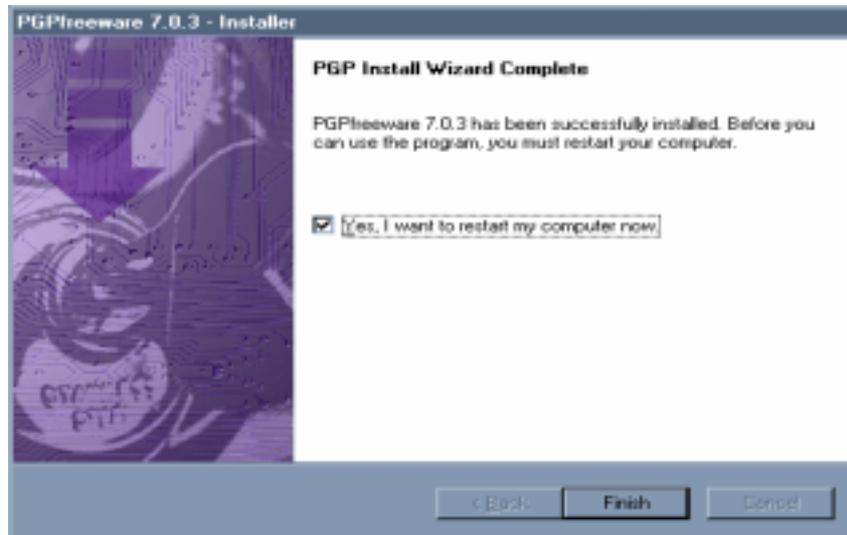


Al terminar el proceso aparecerá la siguiente pantalla



Pulsar el botón  y aparecerá un último mensaje, en el que se encuentra seleccionada por default la opción de reiniciar su PC

Si usted decidió crear su llave privada en un momento diferente al de la instalación, ya no se presentarán las pantallas de Wizard y tampoco le recomendará reiniciar su equipo, ya que esa recomendación sólo la hace después de haber instalado un software nuevo.



Se recomienda dejar activada la selección y pulsar el botón

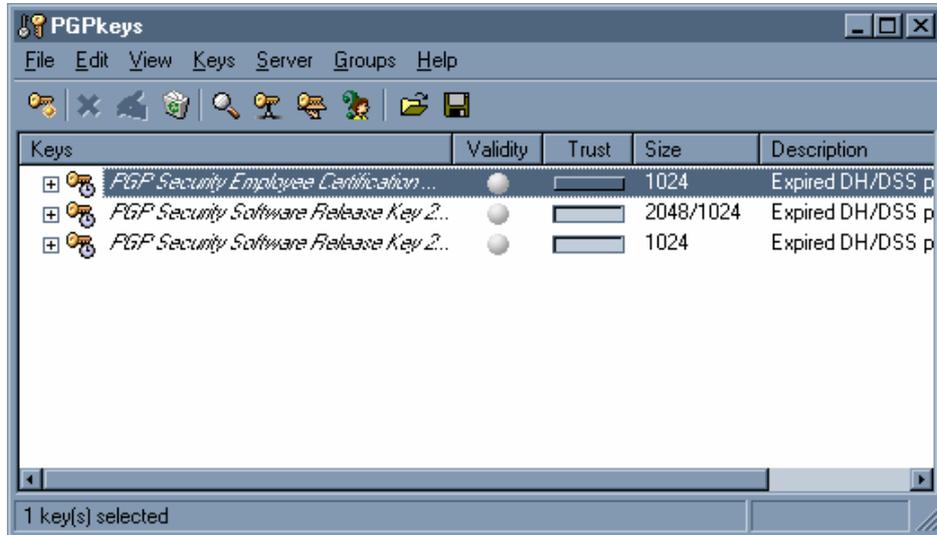


### III. Cómo acceder a PGP para crear una llave nueva

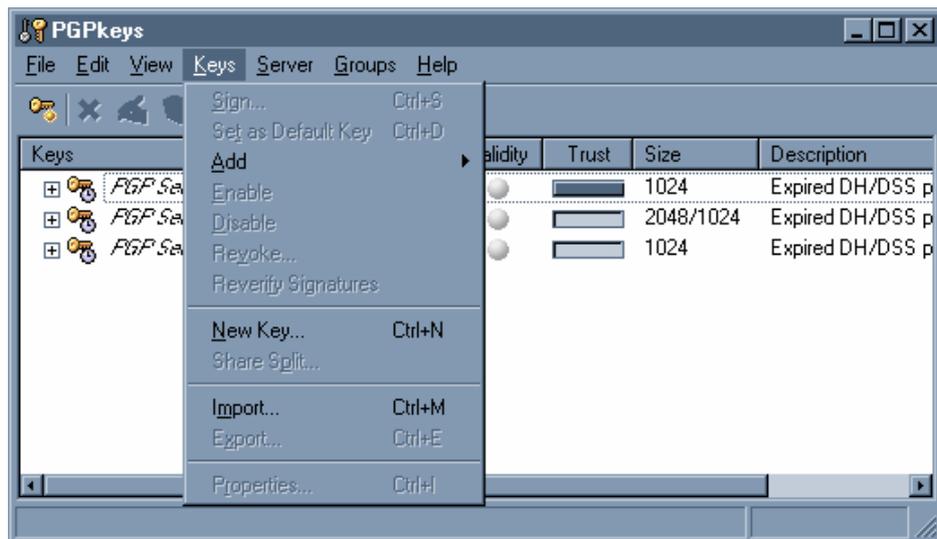
Para acceder a la aplicación, dar click en el botón  **Inicio** que se encuentra en la barra de tareas, seleccione del primer menú de opciones  **Programas**, en el segundo menú busque y seleccione  **PGP**, en el tercer menú busque y seleccione  **PGPkeys** como se muestra a continuación



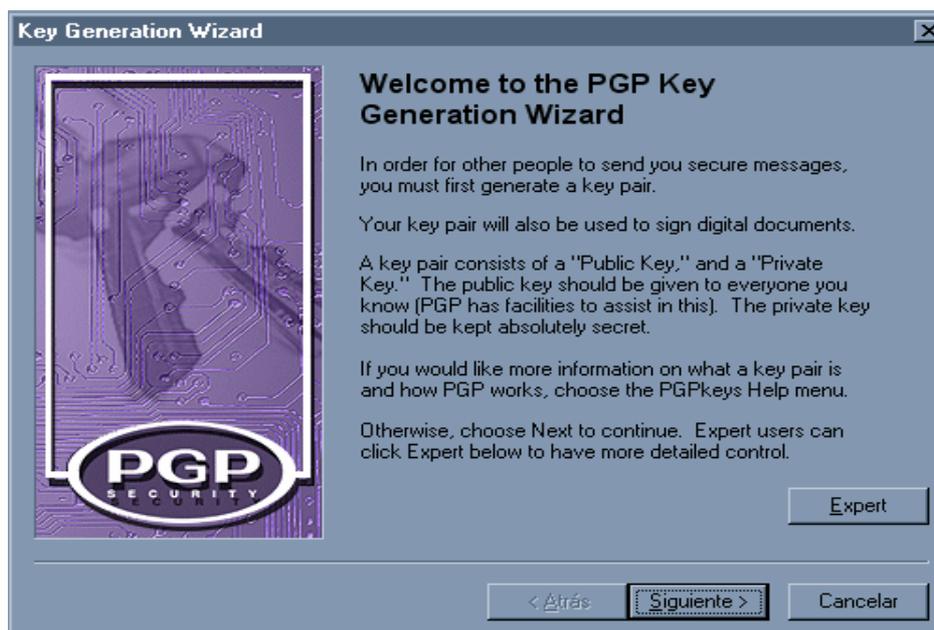
Al pulsar la opción  PGPkeys aparecerá la siguiente pantalla



Seleccionar el menú **Keys** y se desplegará un cuadro de opciones



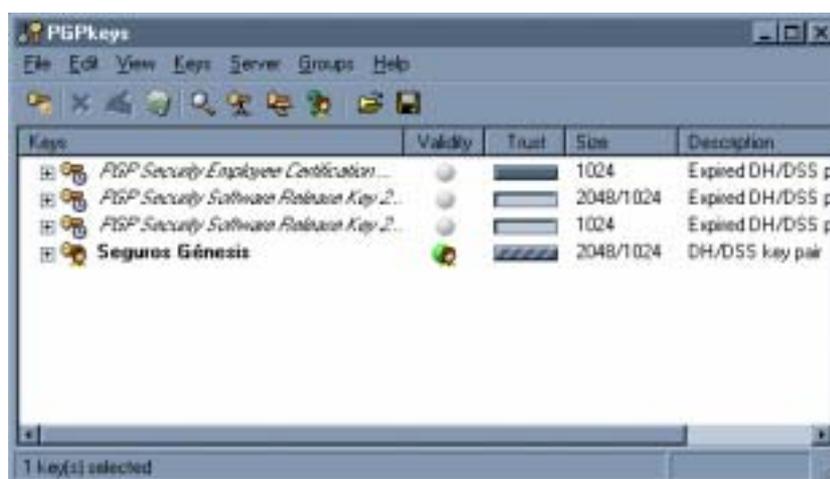
Seleccionar la opción **New Key...** y aparecerá la siguiente pantalla



Seguir los pasos descritos a partir de la página 12 de este manual.

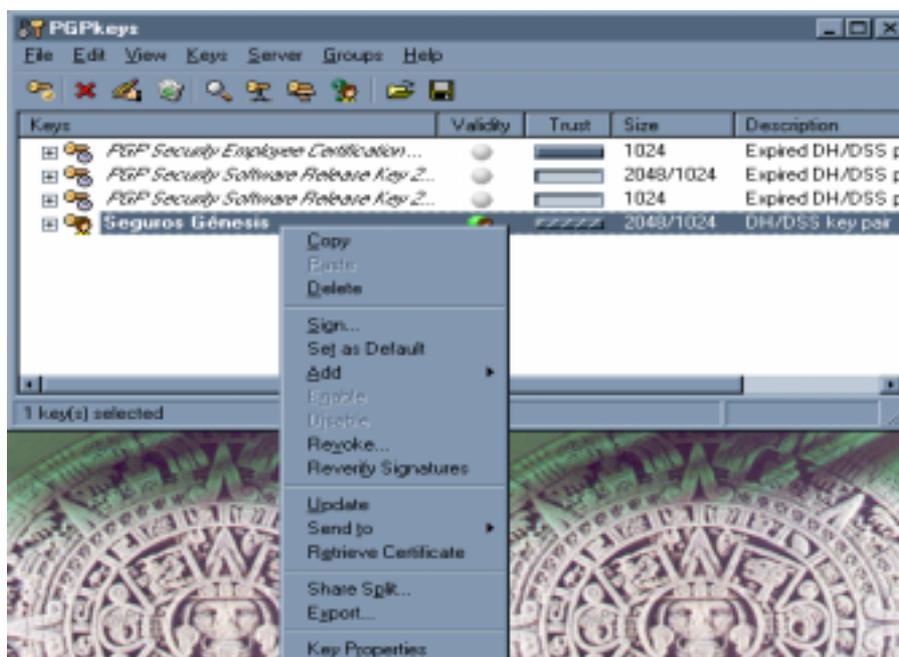
#### IV. Envío de la llave pública de la Institución o Sociedad a la CNSF

Accesar a la aplicación  PGP y seleccione , al pulsar esta opción aparecerá la siguiente pantalla

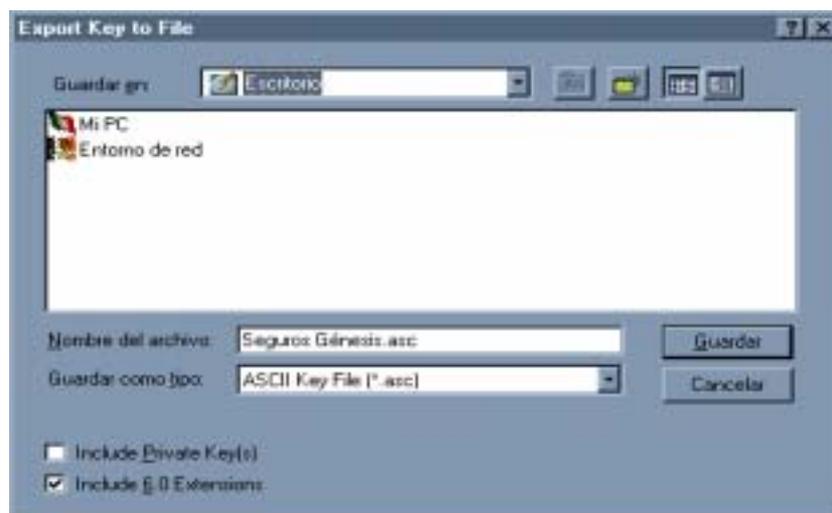


En esta pantalla aparecerá resaltada en **letras negritas** la llave de su institución o sociedad, la cual tiene que enviar a la CNSF para ser registrada.

Seleccionar la llave de la institución o sociedad y pulsar el botón derecho del mouse para que se despliegue un catálogo de opciones



Seleccionar la opción **Export...** y aparecerá la siguiente pantalla



En esta pantalla se deberá indicar en los campos **Guardar en:** y **Nombre del archivo:** el lugar en que se guardará el archivo y con qué nombre.

Es importante aclarar que el campo **Guardar como tipo:** e  **Include Private Key(s)** no deben ser modificados, es decir se quedarán con los datos que aparecen por default en la pantalla.

Para cerrar esta aplicación pulse el botón **Guardar**

Terminado el proceso deberá enviar a la dirección **admin\_entrega@cnsf.gob.mx** de e-mail la llave pública de su institución o sociedad.

## V. Importar la llave pública de la CNSF

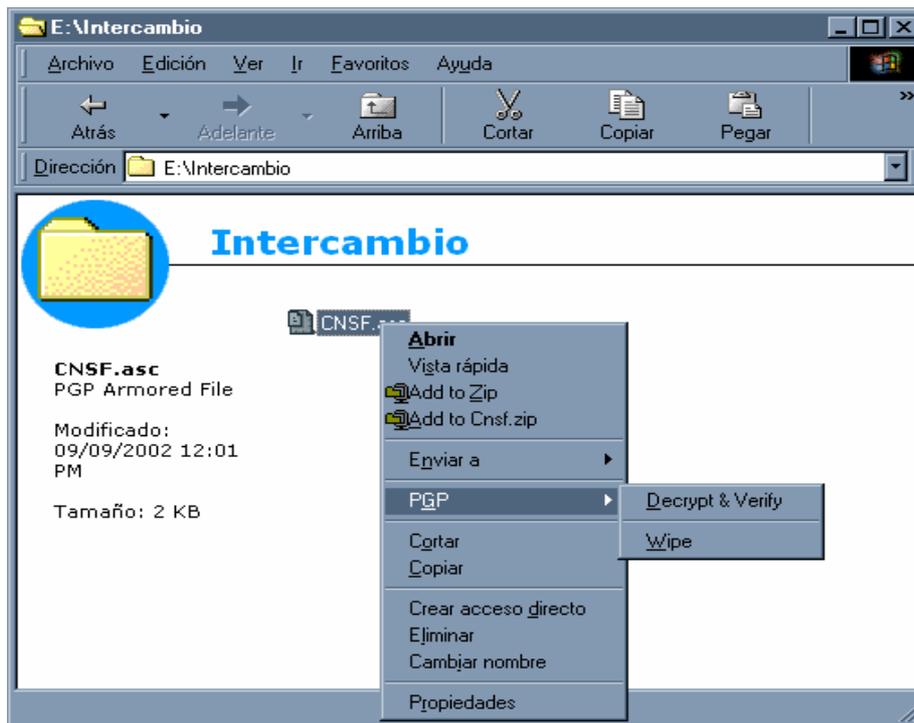
El Administrador de la Comisión Nacional de Seguros y Fianzas enviará al correo electrónico indicado por la Institución o Sociedad la llave pública.

Al recibir el Administrador de la Institución o Sociedad la llave pública de la CNSF deberá importarla para poder realizar la encriptación de sus archivos.

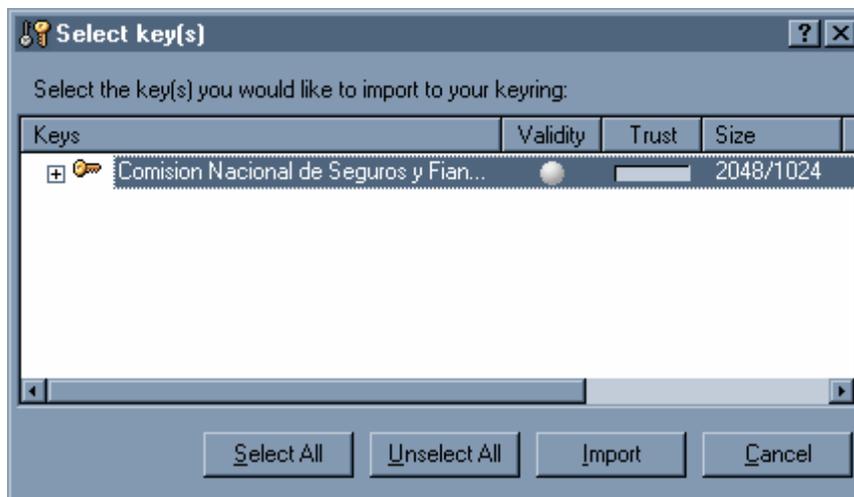
Como primer paso copiar la llave que ha sido enviada por la CNSF en una carpeta de nuestra elección



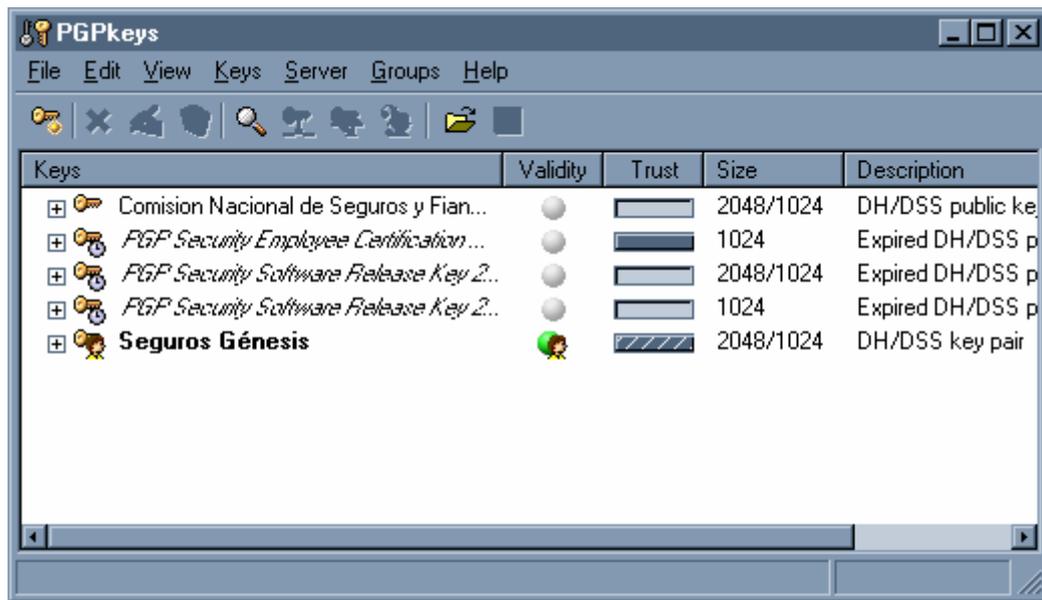
Sobre el archivo, dar click con el botón derecho del mouse y aparecerá un cuadro de diálogo en el cual elegiremos la opción **PGP** que a su vez mostrará otro cuadro de diálogo.



Dar click en la opción **Decrypt & Verify** y aparecerá la siguiente pantalla



Pulsar el botón **Import** y la llave pública de la CNSF aparecerá dentro de PGKeys



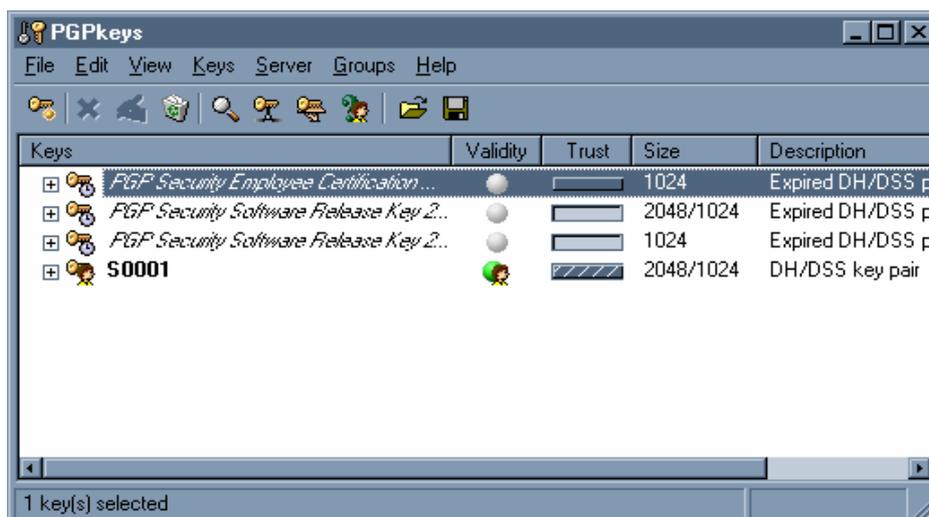
**NOTA**

- + Este icono aparecerá cuando se trate de una llave privada
- + Este icono aparecerá cuando se trate de una llave pública

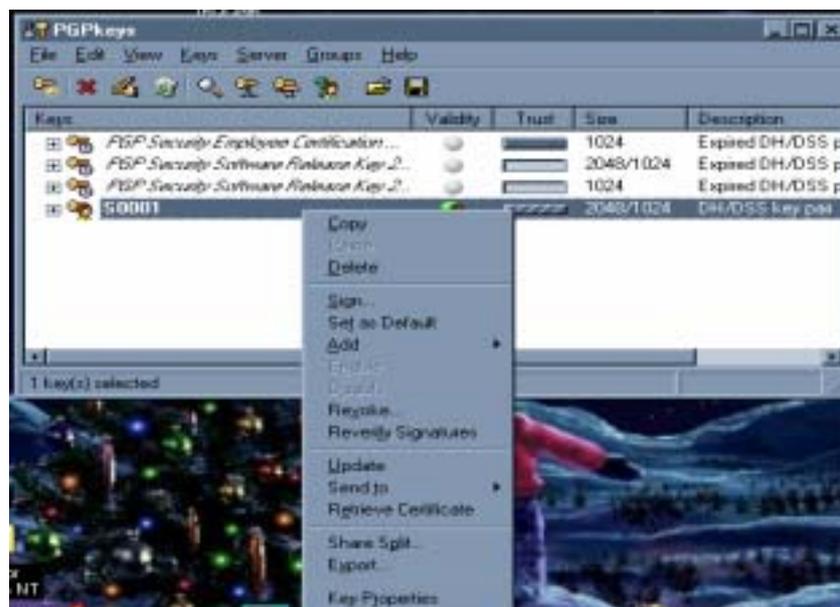
## VI. Envío de llave privada de la Institución o Sociedad a otra PC de la misma Institución o Sociedad

Pueden ser diversas personas las que requieran encriptar en su propia máquina con la misma llave privada de la Institución o Sociedad. Para poder cumplir esa funcionalidad, se debe instalar el PGP en dichos equipos e importar la llave pública de la CNSF y la privada de la Institución o Sociedad. Para esto último, primero deberá exportar la llave privada de la Institución o Sociedad, para lo cual deberá seguir las siguientes instrucciones.

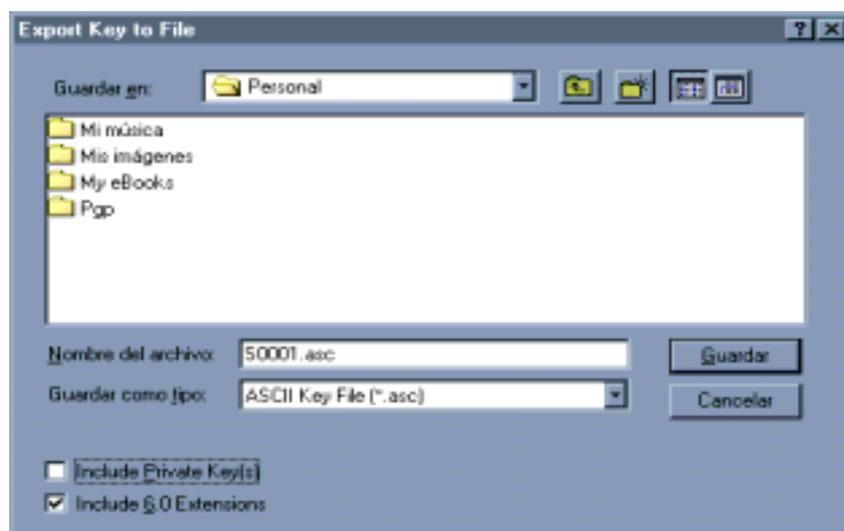
Como primer paso es necesario acceder la pantalla de  **PGPkeys** en la que ya aparece la llave privada.



En esta pantalla aparecerá resaltada en **letras negritas** la llave de su institución o sociedad, selecciónela y pulse el botón derecho del mouse para que se despliegue un catálogo de opciones



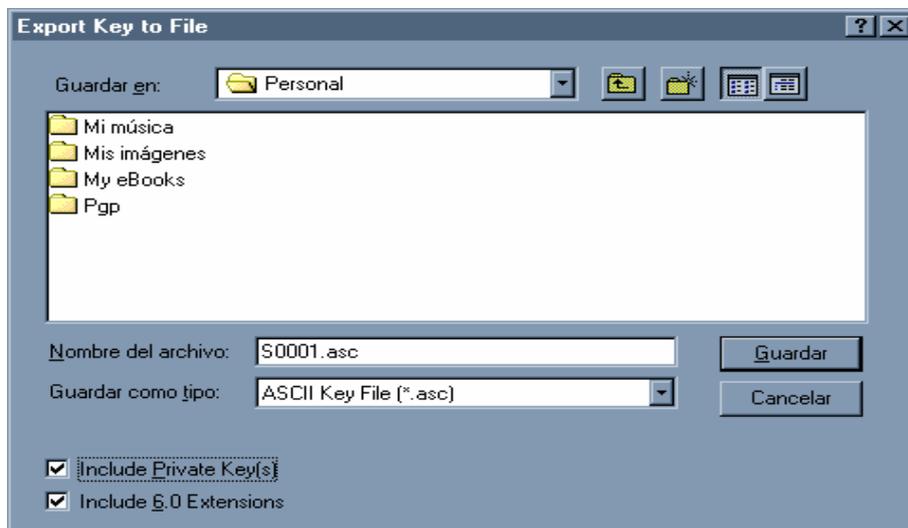
Seleccione la opción **Export...** y aparecerá la siguiente pantalla



En esta pantalla se deberá indicar en los campos **Guardar en:** y **Nombre del archivo:** el lugar en que se guardará el archivo y con qué nombre.

Es importante aclarar que el campo **Guardar como tipo:** no debe ser modificado, es decir se quedará con los datos que aparecen por default en la pantalla.

**Y ACTIVAR** el campo  **Include Private Key(s)** como se muestra en la siguiente pantalla

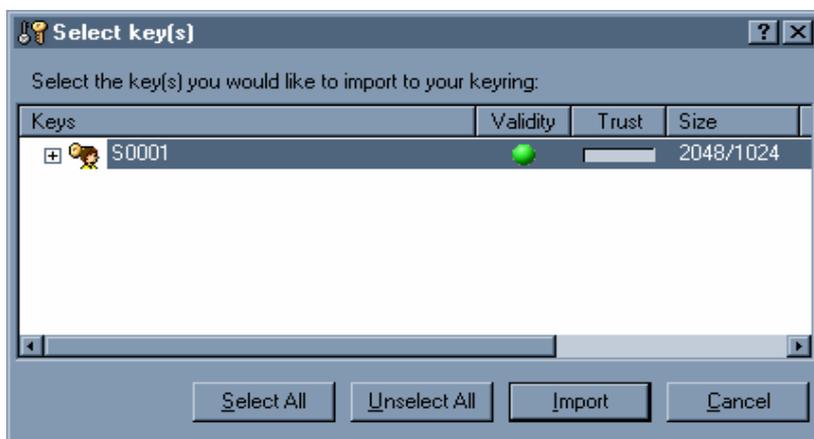


**ya que precisamente, esta alternativa marca la diferencia para que se exporte como llave privada o pública**

Para cerrar esta aplicación pulse el botón **Guardar**

El archivo que se generó, deberá copiarse en la computadora a la que deseamos importar la llave privada de la Institución o Sociedad.

Una vez que se haya instalado PGP sin haber creado ninguna llave privada, deberá seleccionar desde el explorador de Windows el archivo (dar doble click) en el que exportó la llave privada y aparecerá la siguiente pantalla

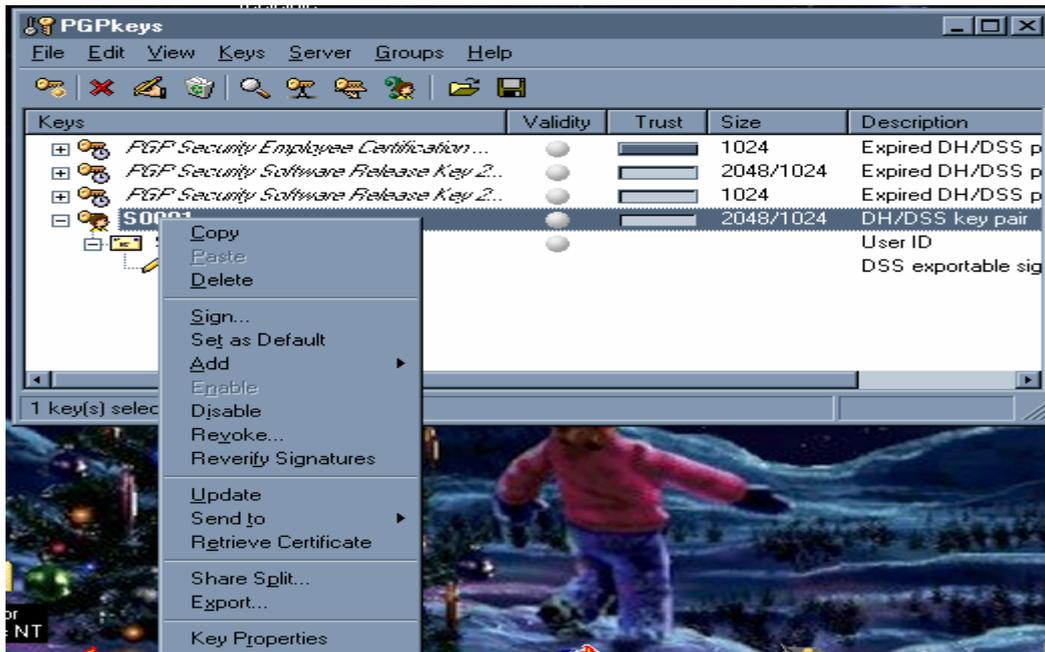


Pulse el botón  y aparecerá el siguiente cuadro de información

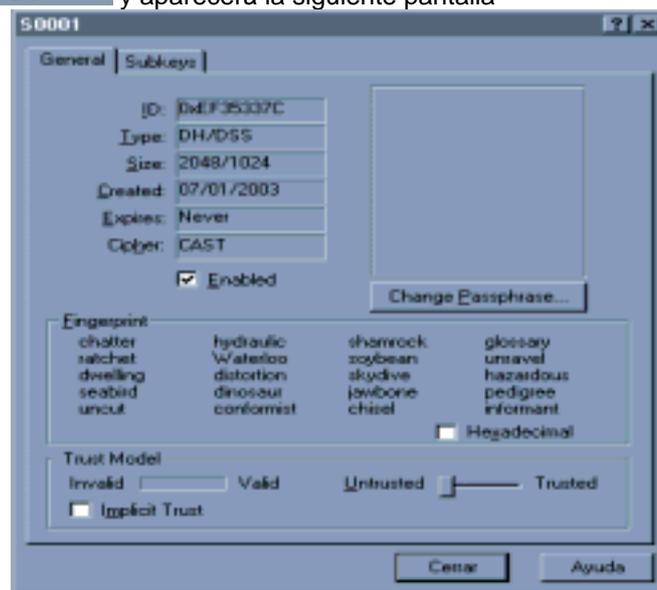


Pulse el botón 

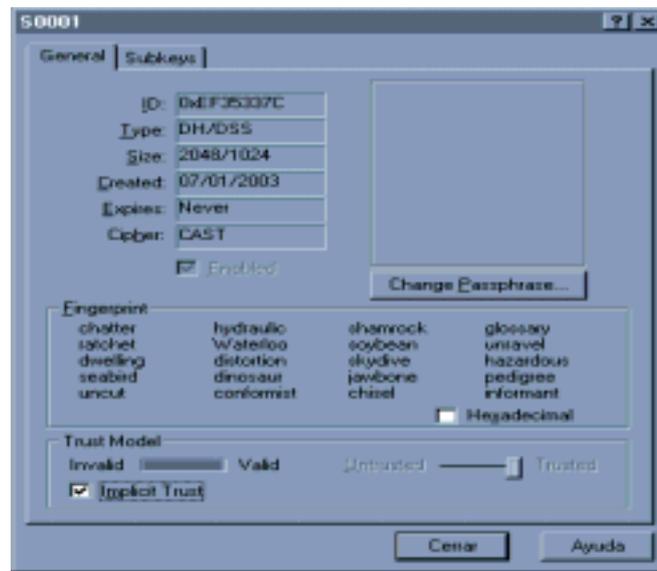
Para confirmar como llave privada la que acabamos de importar, deberá ingresar nuevamente a la pantalla de  dar click con el botón derecho del mouse sobre la llave de nuestra compañía y aparecerá la siguiente pantalla



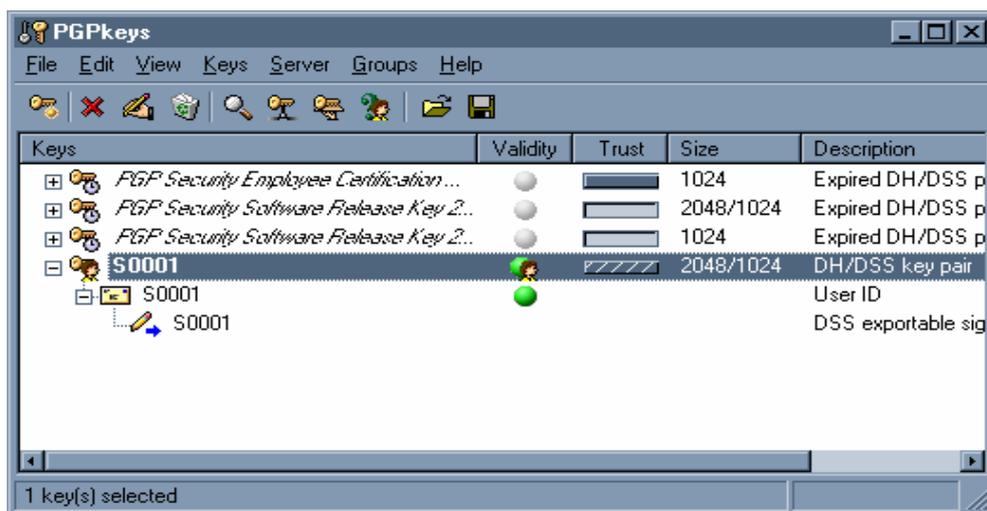
Pulse la opción **Key Properties** y aparecerá la siguiente pantalla



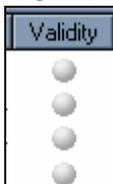
En esta pantalla seleccionaremos la opción  **Implicit Trust**



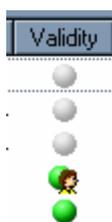
Para terminar pulse el botón  y aparecerá la siguiente pantalla



**NOTA:**



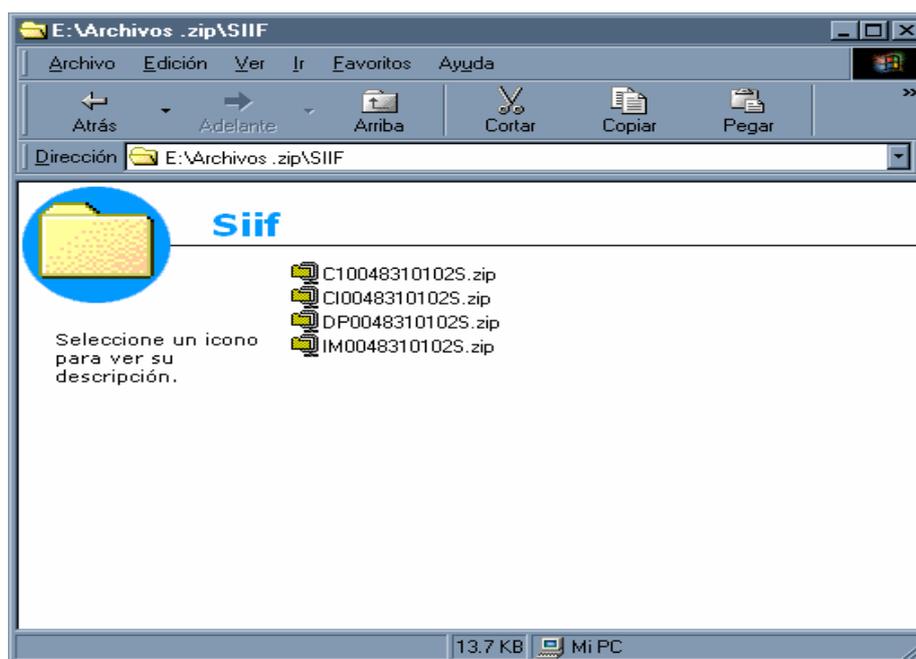
Esta columna aparecerá con círculos grises antes de reconocer la llave privada



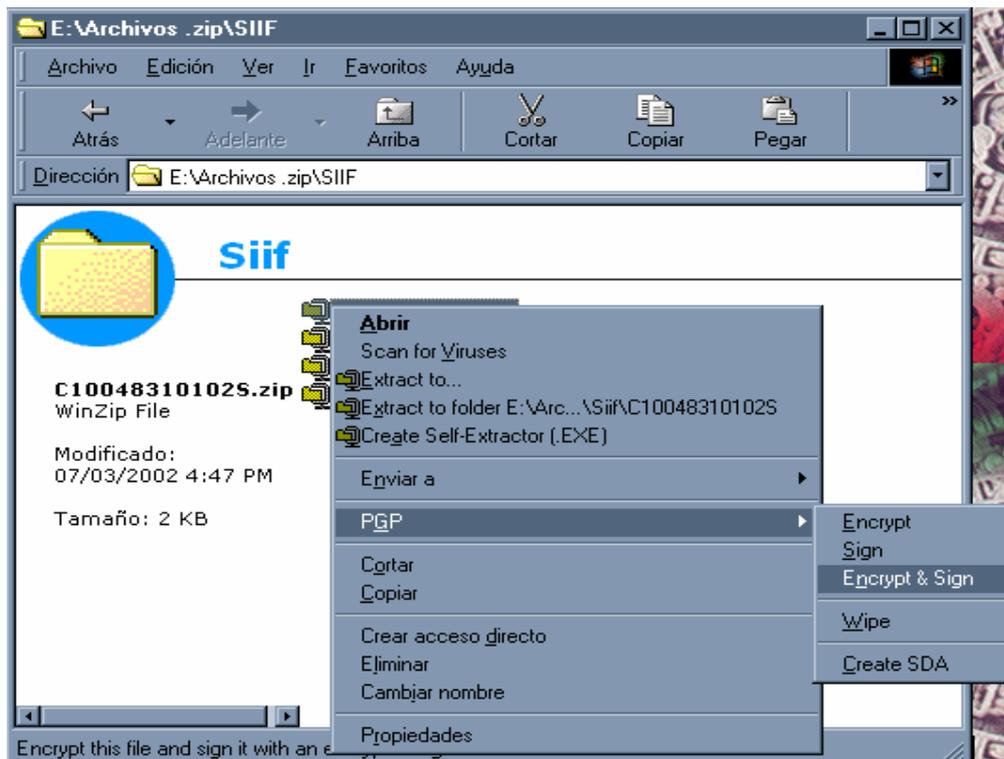
Esta columna aparecerá con círculos grises y verdes después de reconocer la llave privada

## VII. Encriptación de archivos

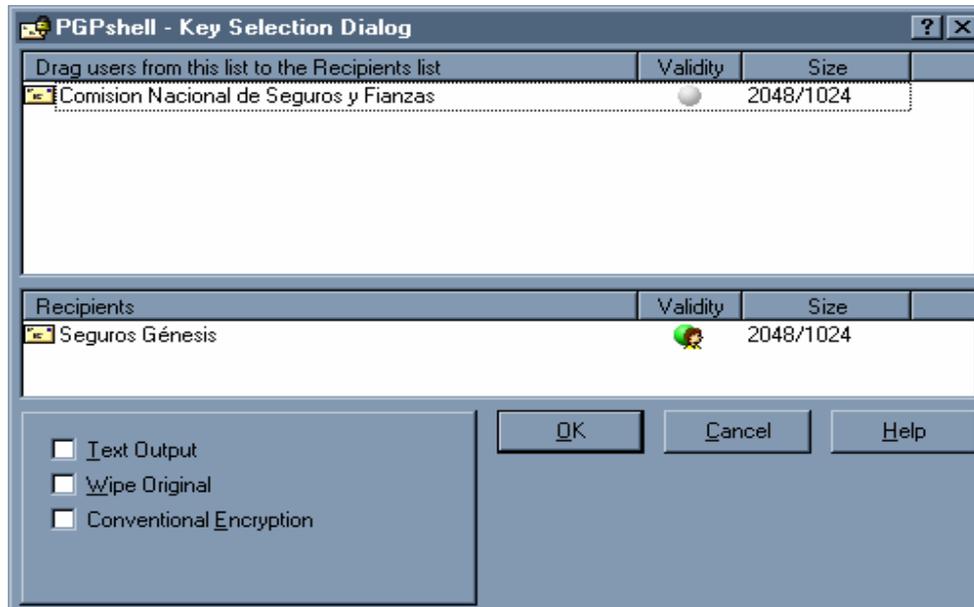
Para encriptar sus archivos y poder realizar el Envío de Entrega de Información Vía Electrónica por Internet a la CNSF, primero debe realizar la generación de el (los) archivo(s) (SIIF, VAR, OPERACIONES RELEVANTES, ETC.) y copiarlos en una carpeta que pueda localizar con facilidad.



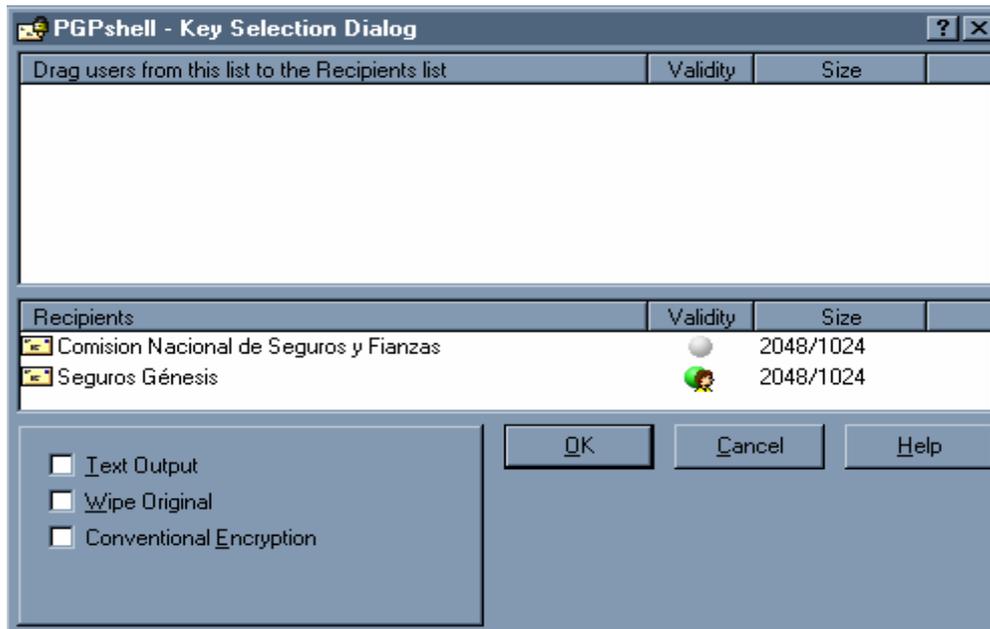
Seleccione uno a uno los archivos dando click con el botón derecho del mouse donde aparecerá un cuadro de diálogo en el cual seleccionaremos la opción **PGP** apareciendo un segundo cuadro de diálogo en el que seleccionará, la opción **Encrypt & Sign** como se muestra a continuación



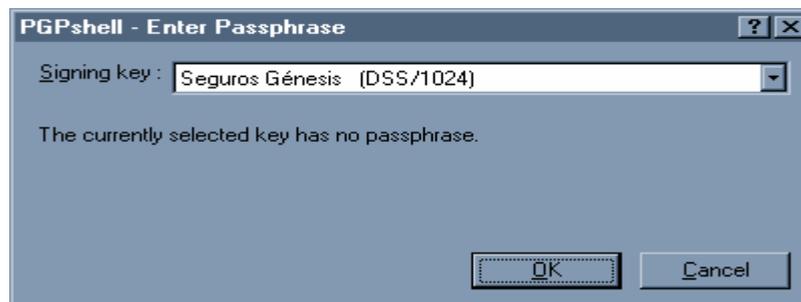
Aparecerá la siguiente pantalla



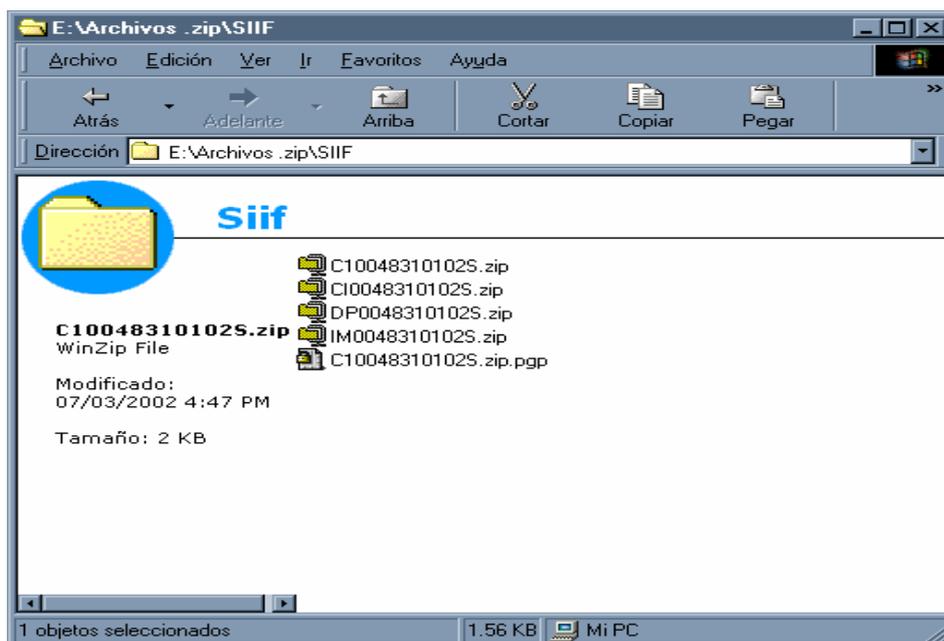
De la sección **Drag users from this list to the Recipients list** donde aparece la llave de la Comisión, seleccionarla con el botón derecho del mouse y arrastrarla hasta la sección **Recipients**



Pulsar el botón  y aparecerá el siguiente mensaje



Pulsar el botón  y aparecerá nuestro archivo encriptado y firmado con la llave privada de la Institución o Sociedad.



La etiqueta del archivo encriptado debe ser el nombre del archivo original y el programa de encriptación agregará la extensión PGP. Ejemplo:  C10048310102S.zip.pgp .

Deberá seguir los pasos anteriormente descritos para cada uno de los archivos que desee encriptar, o bien, seleccionar un bloque y encriptarlos siguiendo los mismos pasos antes descritos.

Después de encriptar y firmar electrónicamente los archivos, deberá enviarlos a la CNSF a través de la página WEB, para esto refiérase al **Manual del Usuario para la Entrega de Información Vía Electrónica**.