CNSF

COMISIÓN NACIONAL
DE SEGUROS Y FIANZAS

Instructivo de Uso e Implementación de Medios de Identificación Electrónica.

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

Contenido

OBJETIVO

El presente documento (instructivo) tiene por objetivo apoyar al usuario en el proceso de generación de la firma electrónica, de documentos en formato PDF. Así como el proceso para la instalación del programa PGP, generación de llaves y cifrado de información.
Lo anterior con el objetivo de enviar a esta Comisión, información de manera segura y confiable, a través de Internet. Por parte de Instituciones de Seguros, Sociedades Mutualistas, Instituciones de Fianzas y Personas Supervisadas

Este instructivo, consta de dos apartados:

El primero, está elaborado para guiar al usuario en el proceso de: generación, implementación de firma electrónica para documentos en formato *.PDF, exportación e importación de esta. La cual es el sustituto de una firma autógrafa de las personas involucradas en el registro o elaboración de documentos que se envían a esta Comisión a través de los distintos sistemas, para los que sea requerido sean firmados por el responsable del documento, garantizando así la responsabilidad y autoría del responsable del documento.

El segundo apartado, nos apoya en el cifrado de la información, para su envío de manera segura, a través del **SISTEMA DE ENTREGA DE INFORMACIÓN VÍA ELECTRONICA (SEIVE)**, para lo cual la CNSF proporciona una herramienta llamada PGPUIv3, ésta es institucional y le permitirá de manera práctica, enviar la información de manera confidencial y segura.

FIRMA ELECTRÓNICA PARA DOCUMENTOS PDF

INTRODUCCIÓN

La finalidad del presente apartado es dar a conocer, el procedimiento para la generación de la firma electrónica y la firma de documentos en formato PDF (Portable Document Format).

Una firma electrónica es un sustituto de la firma autógrafa, pero de manera digital, que agiliza los procesos documentales en formatos digitales, como un medio de identificación, confiable y seguro, mediante el cual se permite certificar la identidad de una persona.

Como sustituto de la firma autógrafa, la firma electrónica, evita lo siguiente:

- Imprimir un documento
- Firmarlo manualmente
- Digitalizarlo, para su envío a través de medios electrónicos o magnéticos.

CREACIÓN DE DOCUMENTOS EN FORMATO PDF

Un documento en formato PDF (Portable Document Format o Documento en Formato Portátil), es un formato de almacenamiento, para documentos digitales independiente de plataformas de software o hardware. Algunas de sus características son las siguientes:

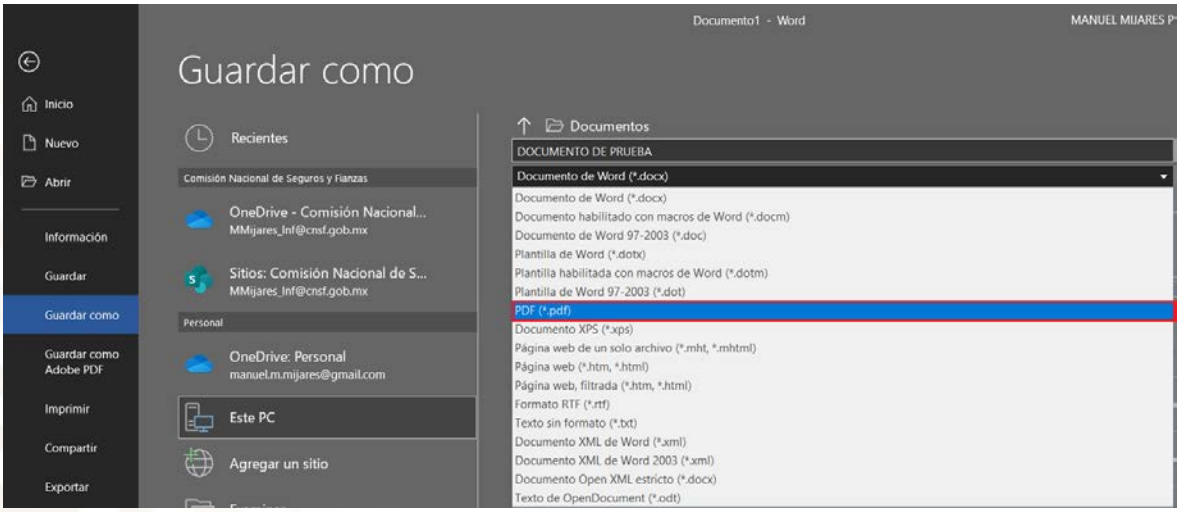
- Es multiplataforma, es decir, puede ser presentado en los principales sistemas operativos (GNU/Linux, OS X Mac, Unix, Windows), sin que se modifique el aspecto ni la estructura del documento original.
- Puede contener cualquier combinación de texto, elementos multimedia como vídeos o sonido, elementos de hipertexto como vínculos y marcadores, enlaces y miniaturas de páginas.
- Los PDF's no pierden el formato con el envío a otros usuarios, como sí sucede cuando se envían documentos de texto (se desordenan las páginas, se desorganizan los párrafos, etc.)
- Es uno de los formatos más extendidos en Internet para el intercambio de documentos. Por ello, es muy utilizado por empresas, gobiernos e instituciones educativas.
- **Puede cifrarse para proteger su contenido e incluso firmarlo digitalmente.**

- Un archivo PDF puede crearse desde varias aplicaciones exportando el archivo, como es el caso de los programas de OpenOffice.org y del paquete ofimático Microsoft Office (a partir de la versión 2007, si se actualiza a SP2).
- Puede generarse desde cualquier aplicación mediante la instalación de una "impresora virtual" en el sistema operativo, en caso de usar aplicaciones sin esa funcionalidad embebida.
- Los ficheros PDF son independientes del dispositivo, el mismo archivo puede imprimirse en una impresora de inyección de tinta o una filmadora. Para la optimización de la impresión se configuran las opciones apropiadas en la creación del fichero PDF.

Existen dos mecanismos para crear un documento en formato PDF:

1. A través de Microsoft Word (A partir de la versión de Office 2007 SP2). Una vez que el documento se encuentre elaborado en Word.

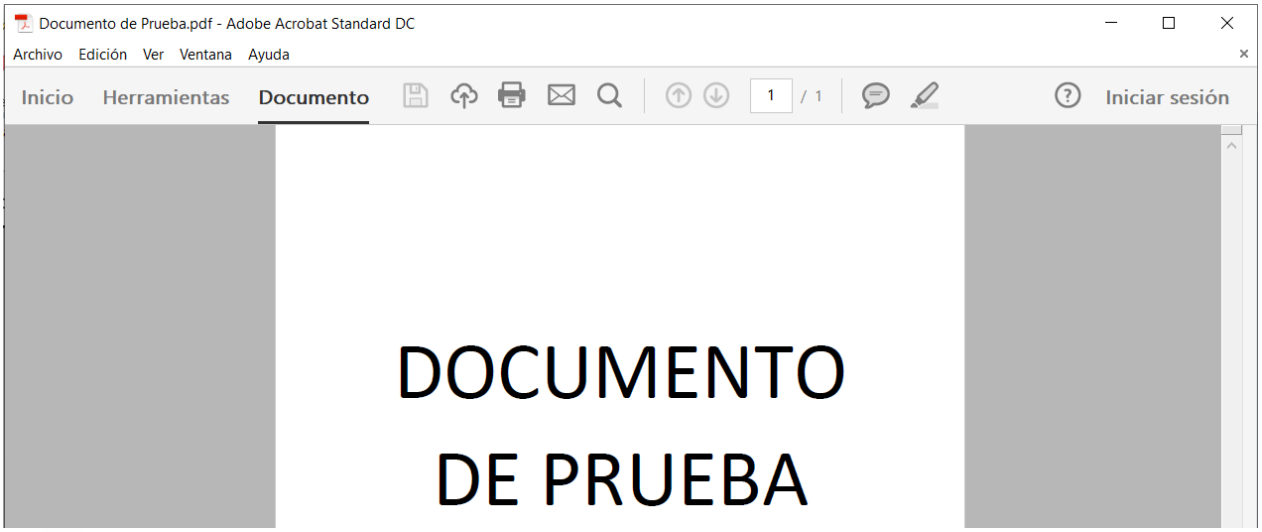
Mediante la opción de ***"Guardar Como"*** de Word



Seleccionar de la lista de ***"Tipo"*** el formato ***"PDF (*.PDF)"*** como se muestra en la imagen anterior.

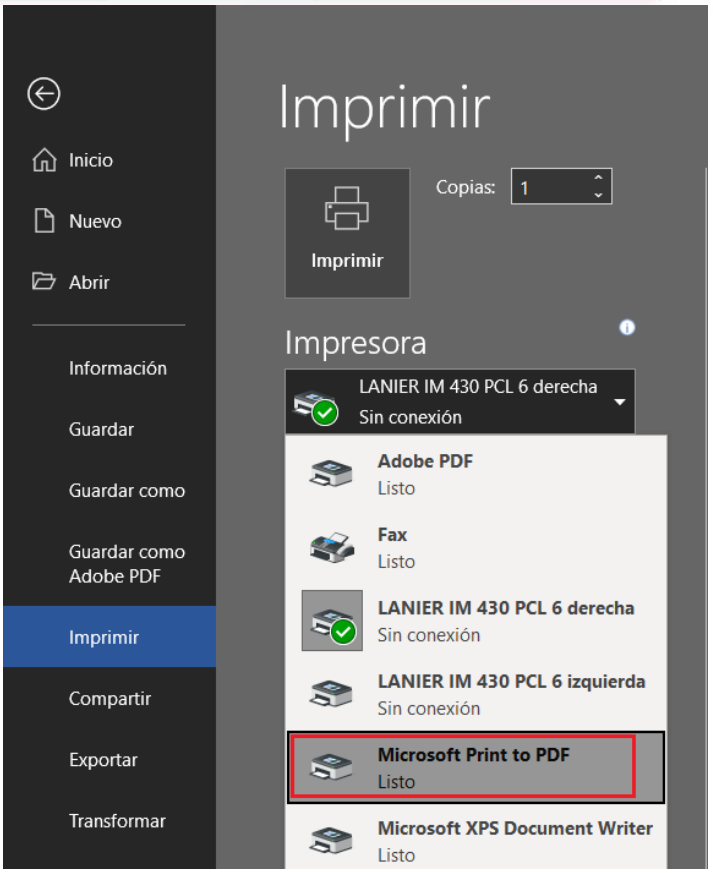
Una vez guardado el documento en formato PDF, este se mostrará en la aplicación para abrir archivos PDF que se tenga instalada, la cual puede ser Acrobat Reader o Acrobat Professional o Estándar, como se muestra en la siguiente imagen.

Cabe mencionar que, si el documento se va a adjuntar a alguno de los sistemas de Registro de Documentos, se pueden utilizar las opciones de **"Optimizar para:"** y **"Tamaño mínimo (publicación en línea),** para reducir el tamaño del archivo.



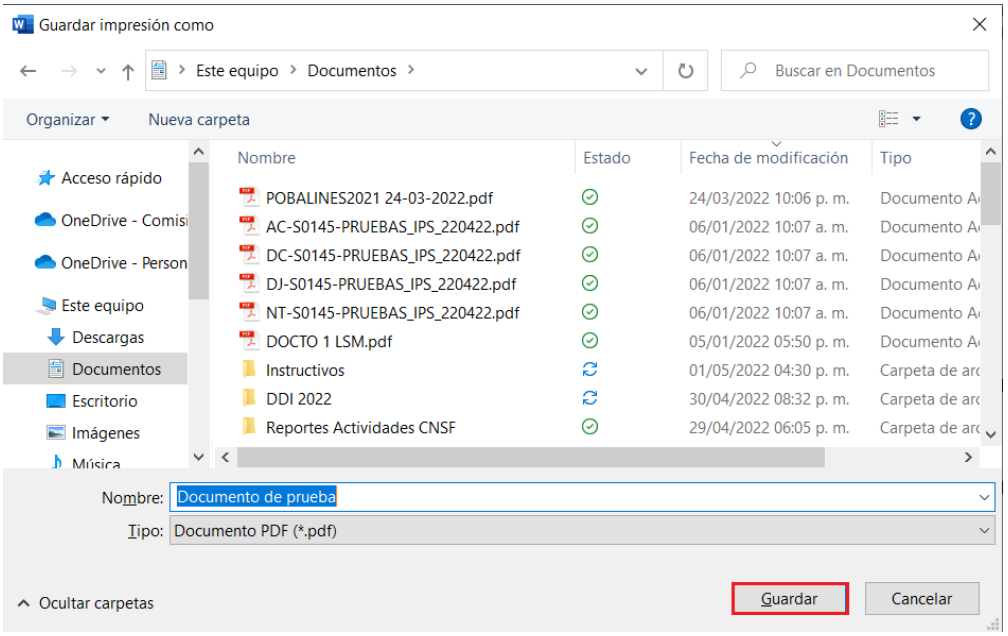
La segunda opción para generar un archivo en PDF, es a través de un programa que permita la impresión de documentos en este formato.

Únicamente se debe de instalar este programa, y desde el documento en Word que se desea convertir a PDF, seleccionar la opción de Imprimir



Seleccionar la impresora para documentos en formato *pdf.

Una vez seleccionada la impresora PDF y después de haber dado clic en “Imprimir” se mostrará la pantalla para seleccionar la ruta donde se desea guardar el documento y el nombre que se requiere.



Una vez guardado el documento este se encontrará disponible dentro de la ruta que se seleccionó al momento de guardarlo.

FIRMAS ELECTRÓNICAS VERSIONES ANTERIORES

Las firmas electrónicas que han sido creadas con las versiones:

- Acrobat Profesional 7.0
- Acrobat Pro 9.0
- Acrobat Estándar 9.0

Siguen siendo útiles para la firma de documentos, solo es necesario verificar la vigencia de la misma, que es de cinco años. Más adelante se indicará el proceso para importar y exportar la firma electrónica y como verificar la vigencia de la firma.

GENERACIÓN DE FIRMA ELECTRÓNICA

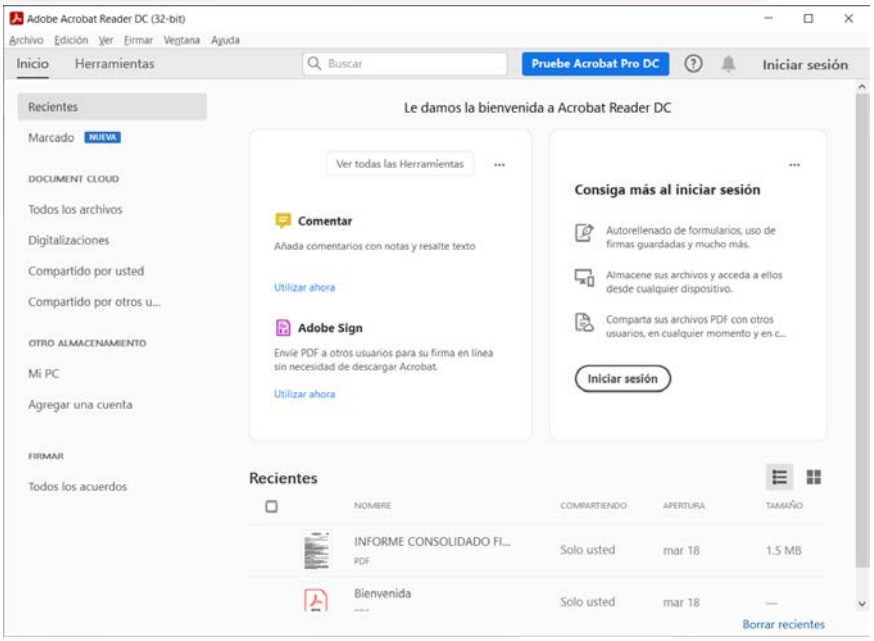
Dentro del presente apartado, se indicará el proceso para la generación de la firma electrónica a través del programa ***Adobe Acrobat Reader DC.***

La versiones de Adobe Acrobat Reader DC o Adobe Acrobat Estándar DC (Versión con licencia), son las versiones más recientes para la generación y edición de archivos PDF de Adobe, Acrobat Reader DC es gratuita y tiene la bondad de permitir al usuario, la generación y firma de documentos con una firma electrónica o certificado digital. En las versiones anteriores a la versión XI, la funcionalidad de generación y firma de documentos, solo estaba limitada a las versiones ***Adobe Acrobat Professional***, las cuales no son gratuitas y se debe de pagar por su licencia.

Para generar la firma electrónica a través de Adobe Reader DC, una vez instalado en el equipo el programa:

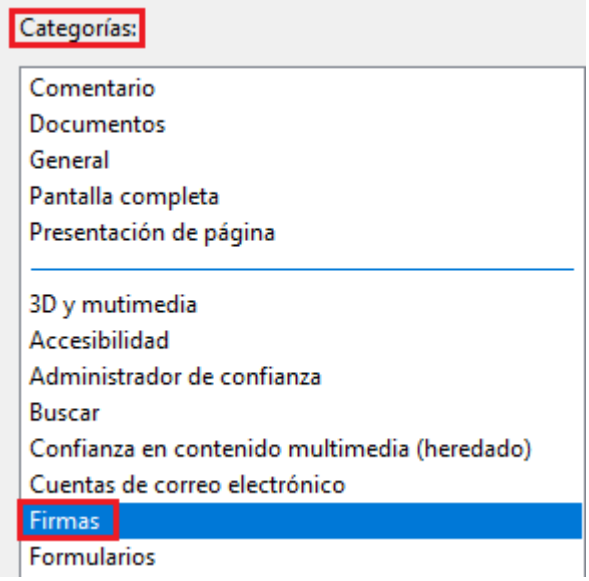
Al ingresar al programa y sin tener que abrir ningún archivo, se muestra la siguiente pantalla

Nota: Cualquier versión de Acrobat Reader superior a la XI, permite crear la firma electrónica y la firma de documentos sin ningún problema

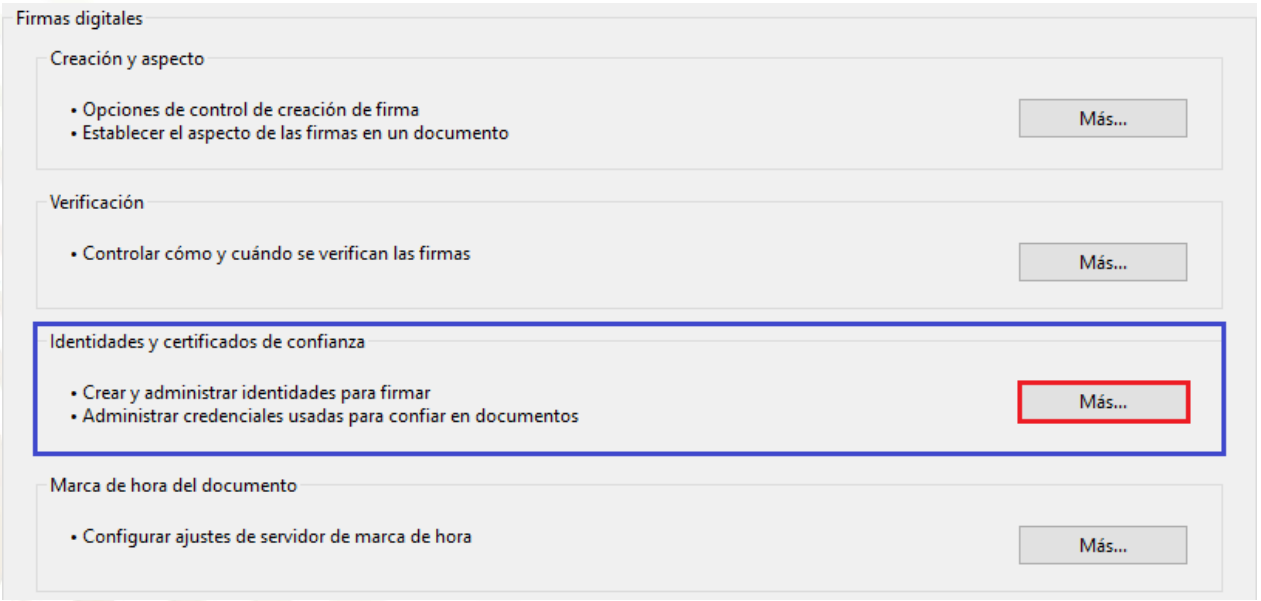


Seleccionar del menú ***"Edición"*** la opción de ***"Preferencias..."***

La acción anterior, mostrará la siguiente pantalla, donde se debe dar clic en la opción de ***"Firmas"***, de la lista de ***"Categorías"***

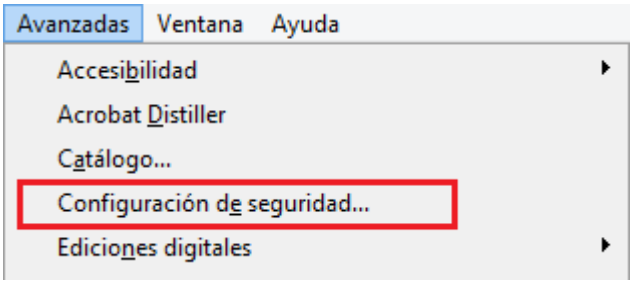


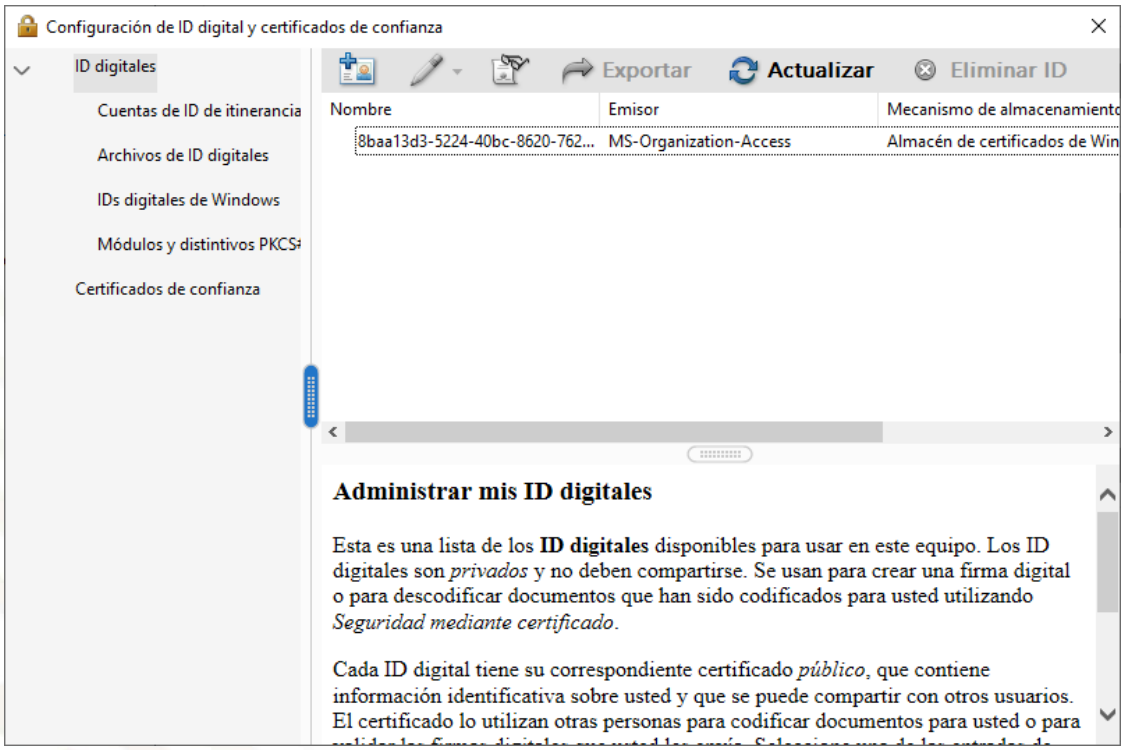
La opción de ***"Firmas"*** contiene las opciones que se muestran en la siguiente pantalla, donde se debe dar clic en la opción de ***"Más..."*** del apartado ***"Identidades y certificados de confianza"***



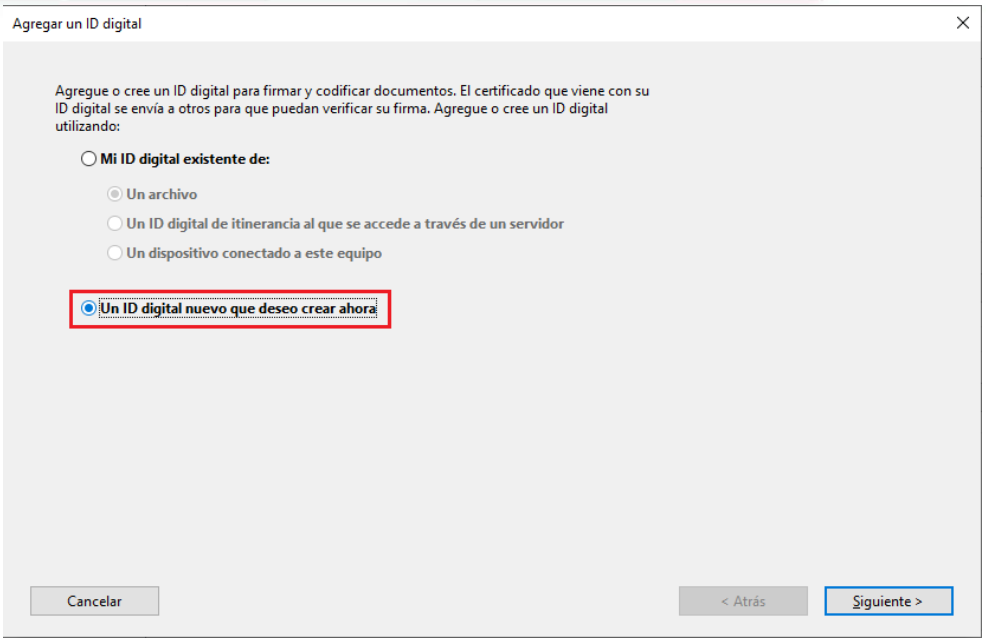
Lo anterior mostrará la siguiente imagen, donde por configuración de instalación se muestra la siguiente pantalla

En caso de tener alguna versión de Acrobat Profesional, el procedimiento es similar, con la salvedad de que para acceder a la generación de la firma es a través del menú de **"Avanzadas"** opción **"Configuración de Seguridad"**

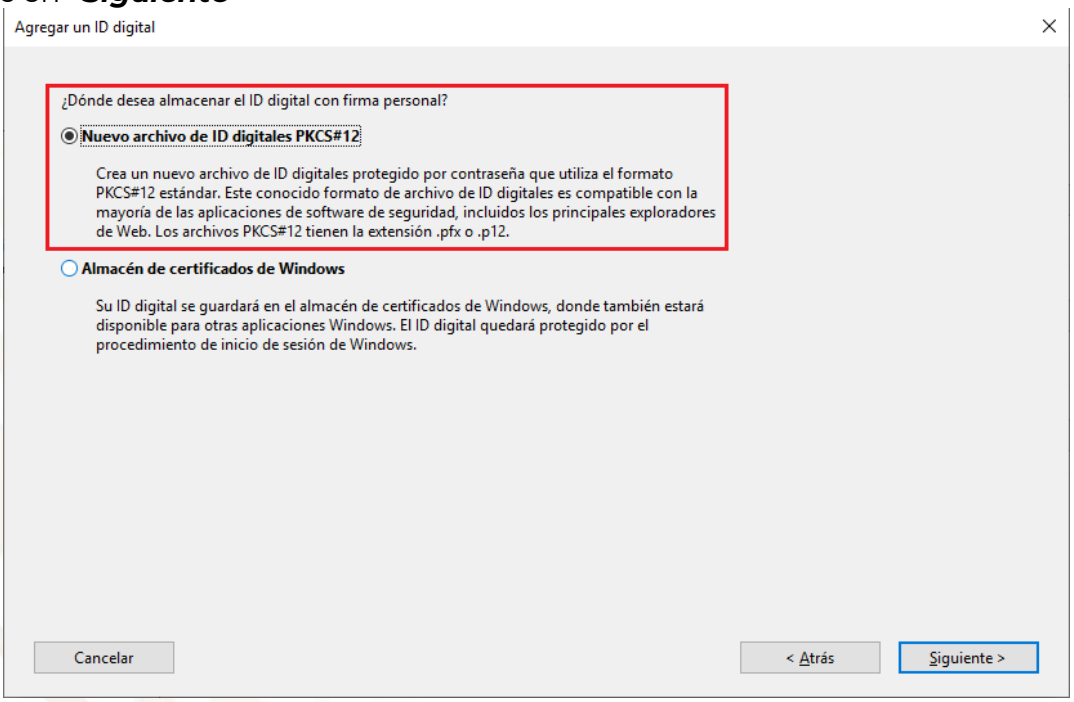




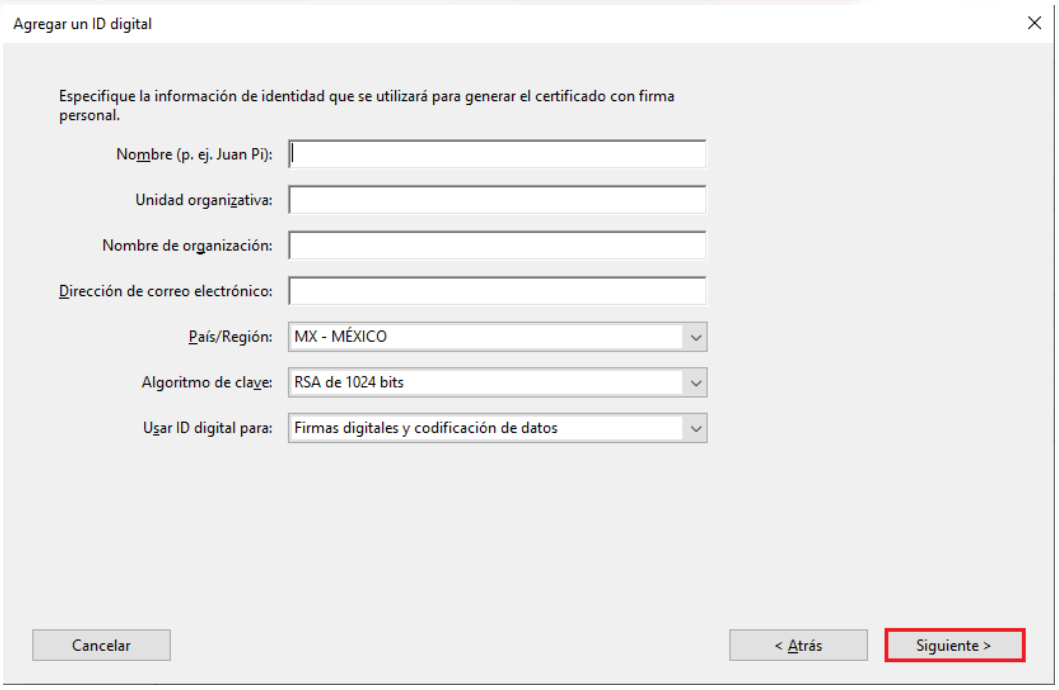
Donde se debe dar clic en la en el botón de ***"Agregar un Id digital"***  . Lo que mostrará la siguiente pantalla. Donde se debe seleccionar la opción de ***"Un ID digital nuevo que deseo crear ahora"*** y dar clic en ***"Siguiente"***



La acción anterior mostrará la siguiente pantalla, donde se debe seleccionar la opción de ***"Nuevo archivo de ID digitales PKCS#12".*** Una vez seleccionada la opción, dar clic en ***"Siguiente"***



Lo anterior mostrará la siguiente pantalla donde se deben de llenar los siguientes campos

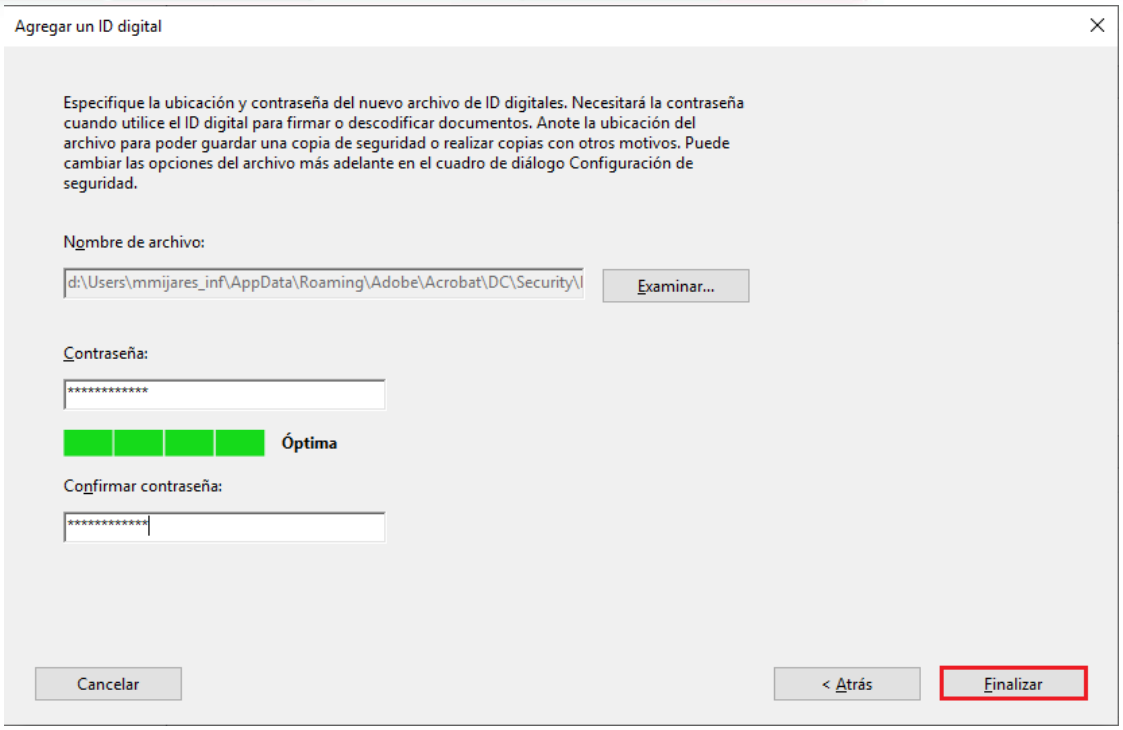


- **Nombre:** El nombre del signatario que está generando la firma electrónica (Obligatorio).
- **Unidad organizativa:** Se refiere al área, dirección o puesto del signatario (NO Obligatorio).
- **Nombre de organización:** Empresa a la cual pertenece el signatario o por la cual firmará los documentos (NO Obligatorio).
- **Dirección de correo electrónico:** Es la dirección de correo electrónico del signatario, la cual sirve para recibir notificaciones (Obligatorio).
- **País/Región:** Seleccionar **México**
- **Algoritmo de clave: Utilizar en RSA de 1024 bits NO SELECCIONAR RSA DE 2048 BITS.**
- **Usar ID digital para: Dejar en Firmas digitales y codificación de datos.**

IMPORTANTE: LOS CAMPOS DE ESCRITURA, DEBEN SER SIN ACENTOS O CARACTERES ESPECIALES (SOLO @ PARA LA DIRECCION DE CORREO)

Una vez llenados y seleccionados los campos requeridos, dar clic en ***"Siguiente"***

Lo que mostrará la siguiente pantalla.



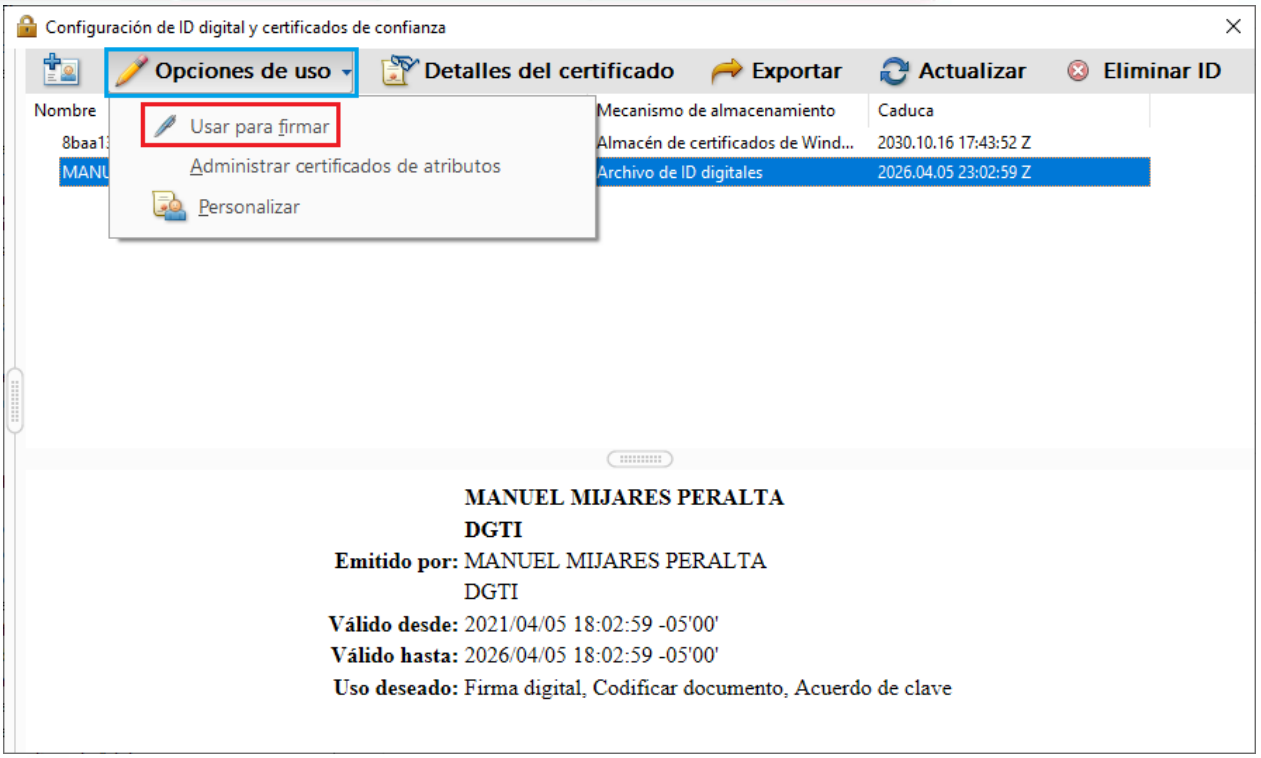
Dónde:

- **Nombre del archivo:** Es el nombre del archivo y la ruta donde se guardará la firma electrónica, la cual es el almacén de certificados de Acrobat Reader dentro del equipo, el nombre del archivo corresponde al nombre escrito en la pantalla anterior. **Sí se está generando la firma en un equipo distinto al equipo en donde se van a firmar los documentos, es necesario seleccionar un destino distinto a través del botón de *"Examinar..."* y guardar el archivo de la firma en una carpeta diferente al almacén de certificados**
- **Contraseña:** Esta debe ser al menos de 8 caracteres (Acepta números y caracteres especiales), El nivel de complejidad, se verá en reflejado en el indicador como aquí se muestra, la cual debe ser como mínimo **alta** y deberá confirmarse la contraseña.

NOTA: SE RECOMIENDA GUARDAR LA CONTRASEÑA, EN UN LUGAR SEGURO, PUES SI SE LLEGA A EXTRAVIAR U OLVIDAR, SE DEBE GENERAR UNA NUEVA FIRMA.

Una vez realizado lo anterior, dar clic en el botón ***"Finalizar"*** para continuar.

Al dar clic en ***"Finalizar"***, el sistema regresará a la pantalla de **Configuración de ID digital y certificados de confianza**.



Donde, en la opción de ***"Opciones de uso"*** seleccionar la opción de ***"Usar para firmar"***

Con esto se ha generado la firma electrónica y esta ha sido establecida para firmar documentos.

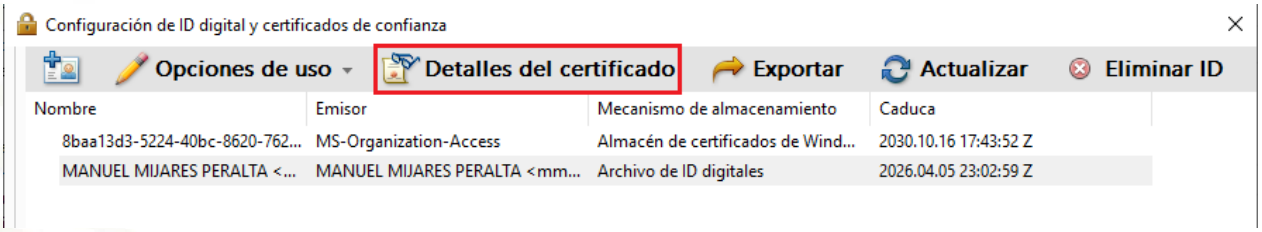
ARCHIVO *.p7c Y DETALLES DE LA FIRMA

Conforme a lo establecido en las disposiciones de la Circular Única de Seguros y Fianzas, los signatarios de documentos y signatarios involucrados en el "Sistema de Registro de Documentos" deberán entregar a esta Comisión:

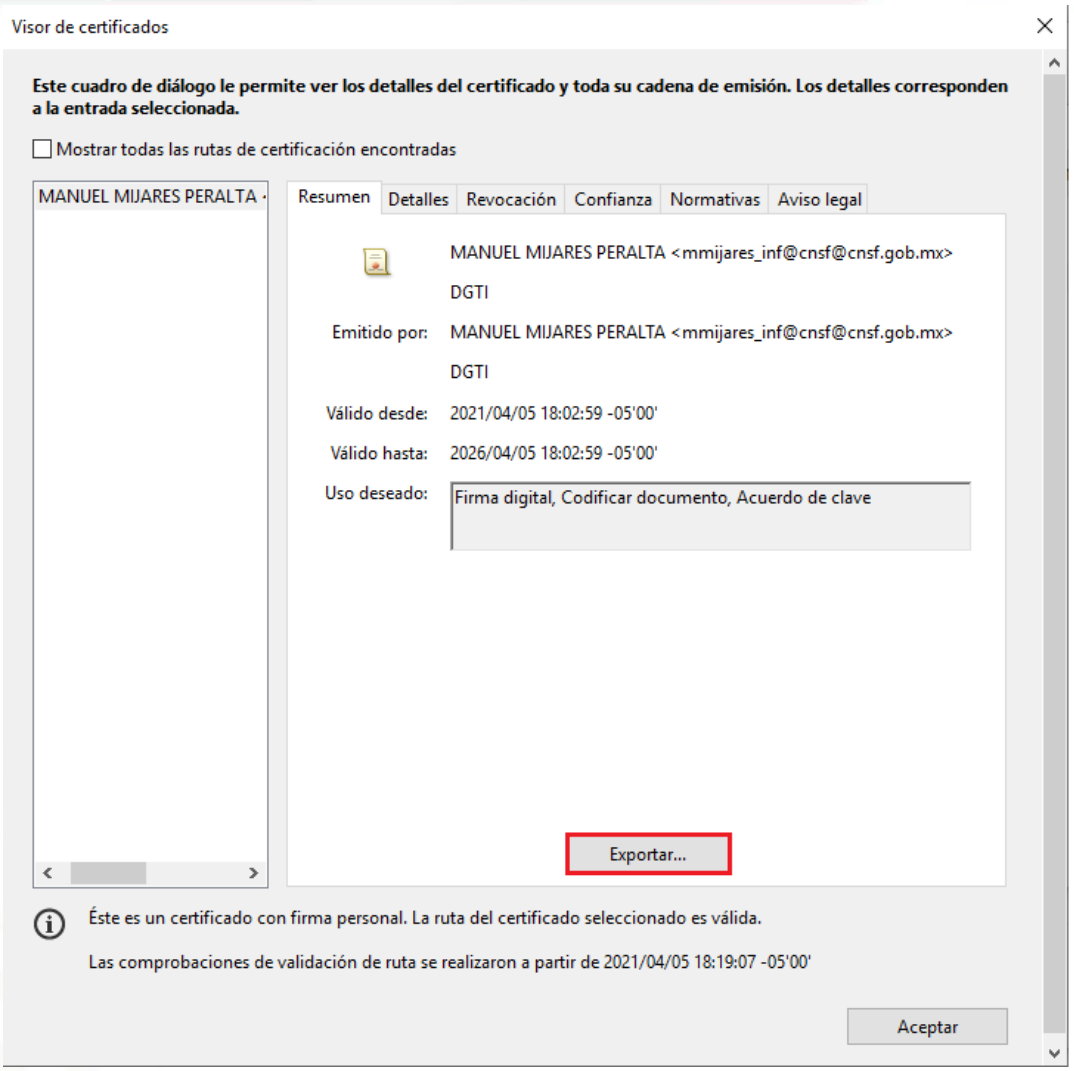
- La respectiva designación como signatario, por parte de la Institución de Seguros, Sociedad Mutualista o Institución de Fianzas.
- El formato correspondiente para la ***"Aceptación de Responsabilidad de los Signatarios de Documentos",*** con las características de la firma electrónica que se soliciten en dicho formato, este formato se encuentra dentro del Anexo 39.4.7-b de la Circular Única de Seguros y Fianzas.
- Obtener el archivo en formato ****.p7c*** (Que se encuentra dentro de la firma electrónica).

Para la obtener las características de la firma electrónica y el archivo en formato *.p7c se debe hacer lo siguiente:

Dentro de la ***"Configuración de ID digital y certificados de confianza",*** seleccionar la opción de ***"Detalles del certificado".***



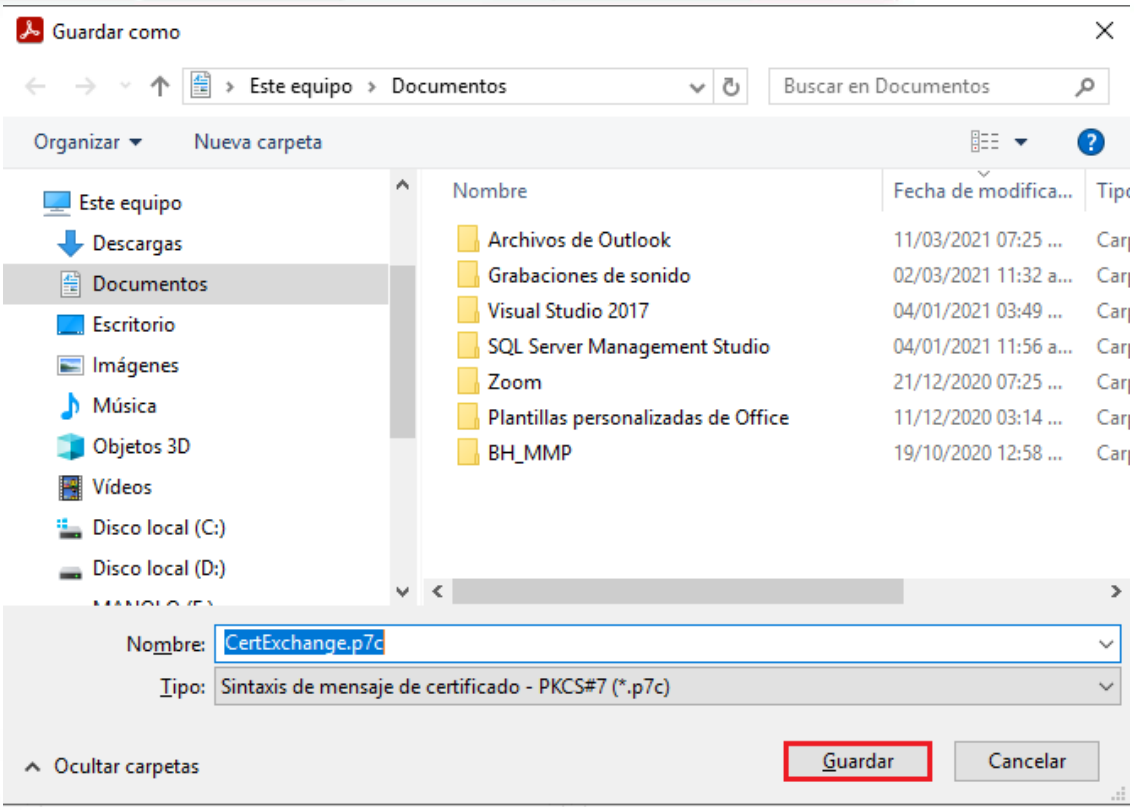
Al ingresar al ***"Visor de certificados"***, dar clic en el botón de **"Exportar..."**, para extraer el archivo con formato *.p7c.


Visor de certificados
Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.
Mostrar todas las rutas de certificación encontradas
MANUEL MIJARES PERALTA
Resumen
Detalles
Revocación
Confianza
Normativas
Aviso legal
MANUEL MIJARES PERALTA <mmijares_inf@cnsf.gob.mx>
DGTI
Emitido por:
MANUEL MIJARES PERALTA <mmijares_inf@cnsf.gob.mx>
DGTI
Válido desde:
2021/04/05 18:02:59 -05'00'
Válido hasta:
2026/04/05 18:02:59 -05'00'
Uso deseado:
Firma digital, Codificar documento, Acuerdo de clave
Exportar...
Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.
Las comprobaciones de validación de ruta se realizaron a partir de 2021/04/05 18:19:07 -05'00'
Aceptar

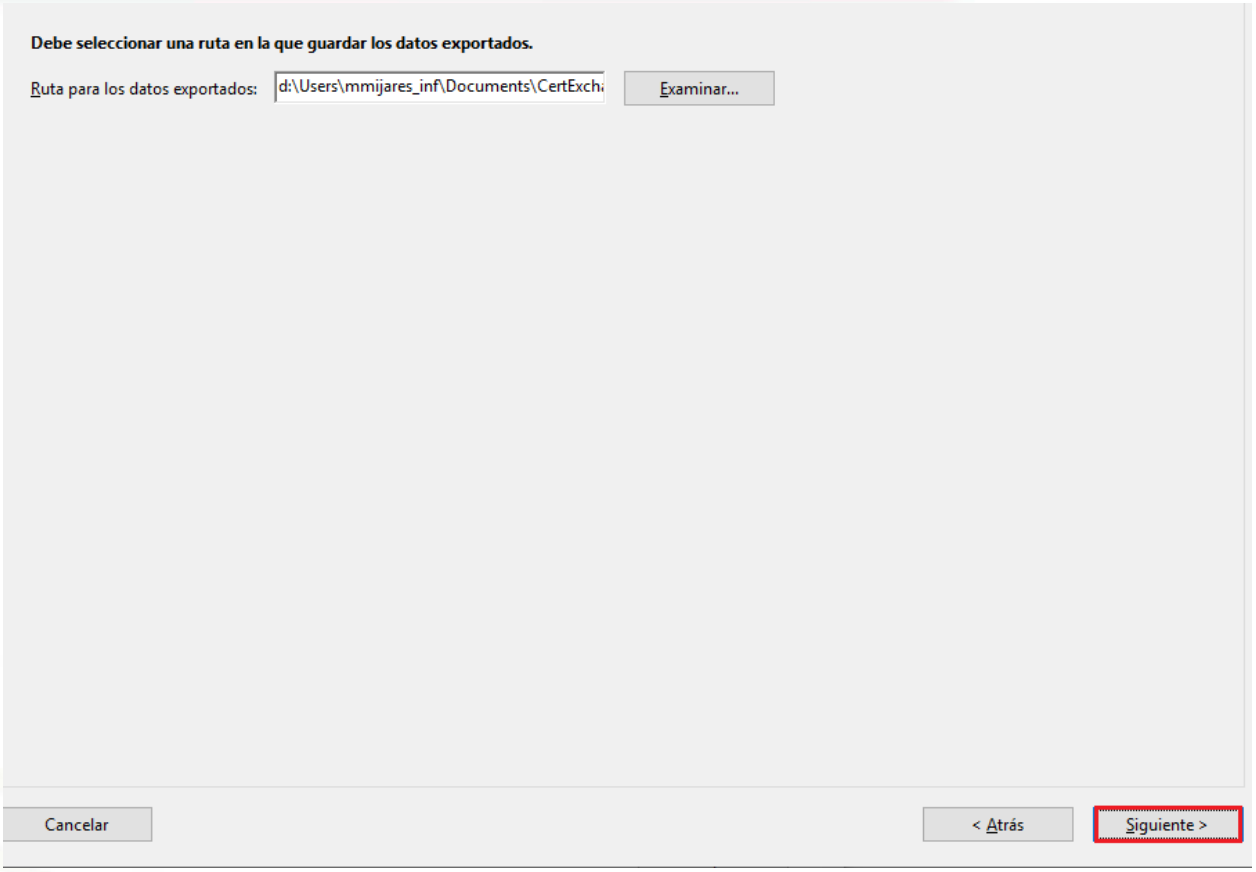
Lo anterior mostrará la siguiente pantalla, donde se deberán seleccionar las opciones de:

"Guardar los datos exportados en un archivo" y ***"Sintaxis de mensaje de certificado – PKCS#7".*** Como se muestra a continuación.

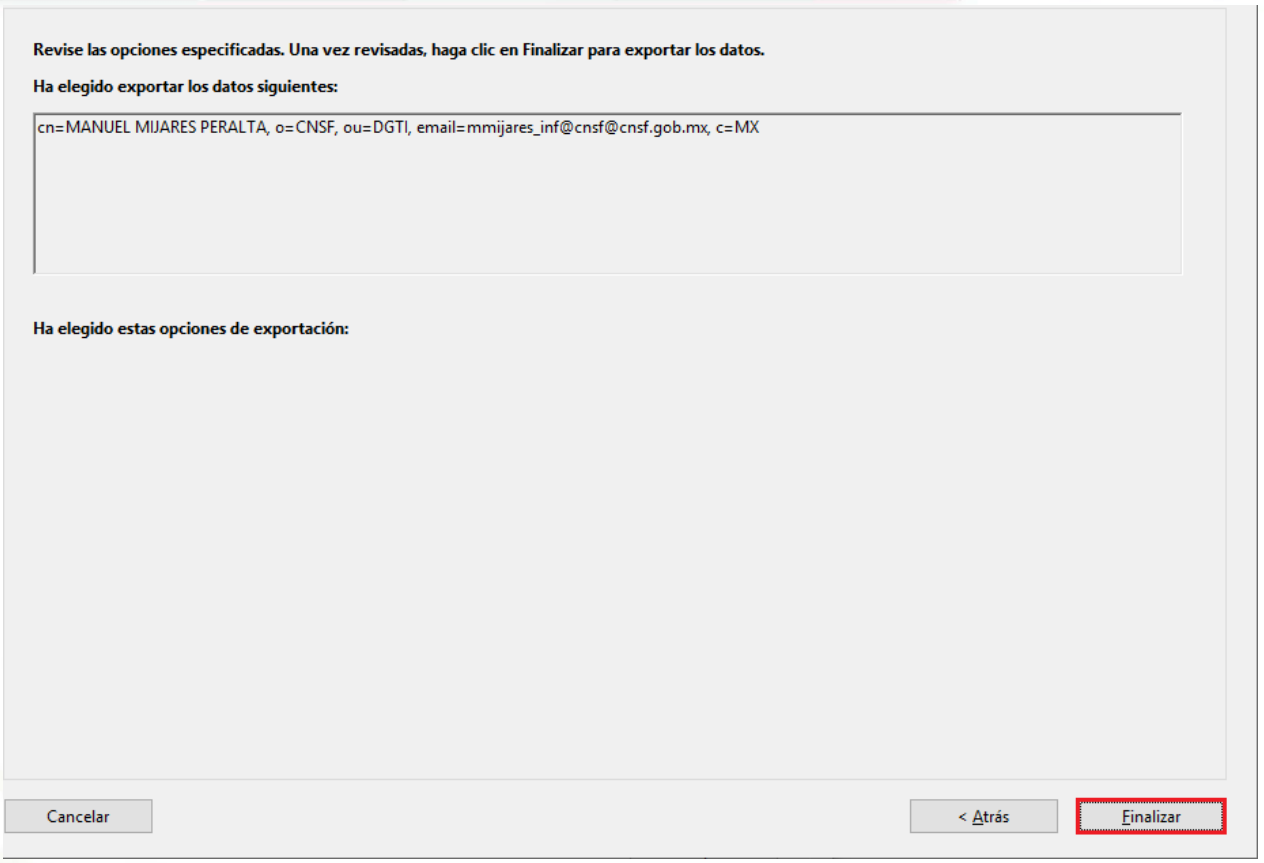
Realizado lo anterior dar clic en ***"Siguiente"*** para seleccionar la ruta o carpeta donde se guardará el archivo *.p7c.



Una vez seleccionada la ruta o carpeta de destino, donde se guardará el archivo *.p7c, dar clic en el botón de ***"Guardar"***, para regresar a la pantalla anterior. Si se requiere, puede cambiarse el nombre del archivo, para una mejor identificación.



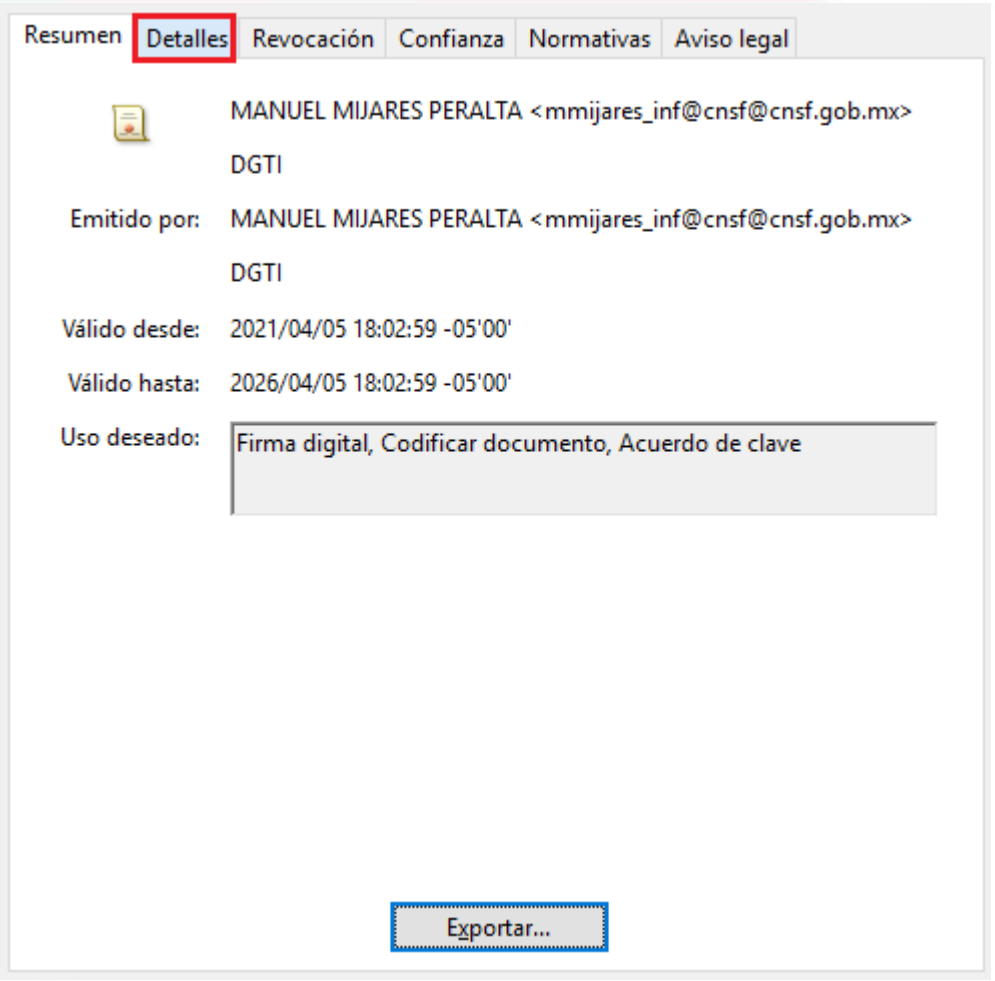
Una vez guardado el archivo *.p7c dar clic en **“Siguiente”** para continuar.



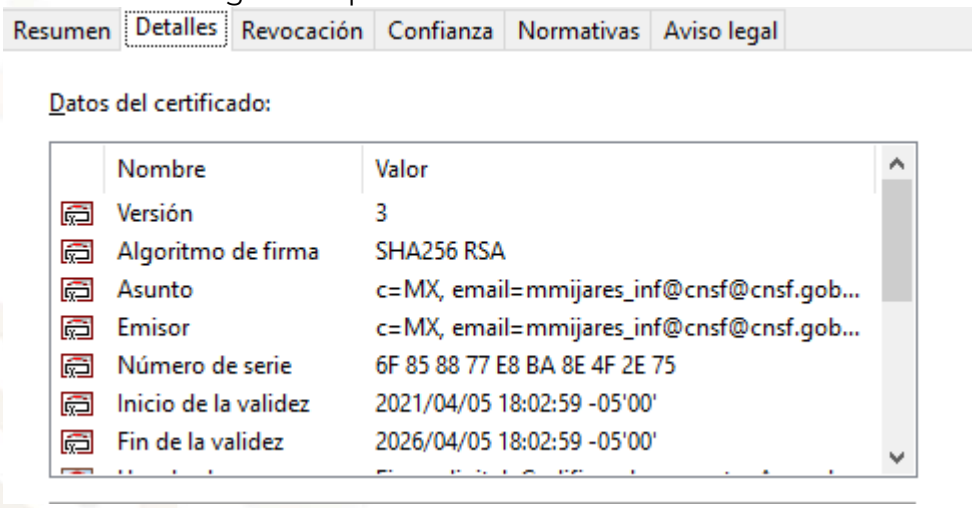
Para terminar y regresar a la pantalla del ***"Visor de certificados"*** dar clic en ***"Finalizar"***.

Adicionalmente al archivo *pc7, se deben extraer los datos que se solicitan, en el formato de aceptación del signatario que corresponda al Sistema de Registro de Documentos y sobre el cual será signatario.

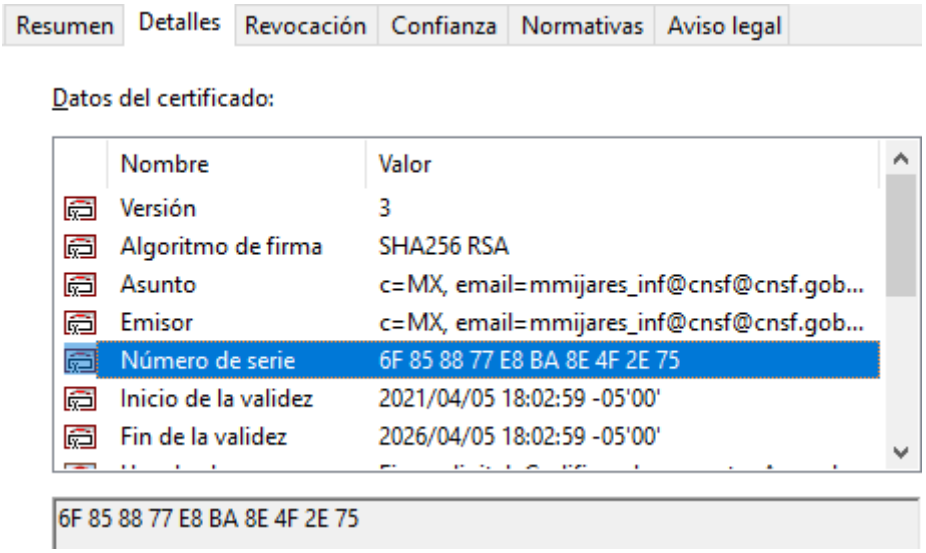
Dentro del "Visor de certificados", dar clic en la pestaña de ***"Detalles"***



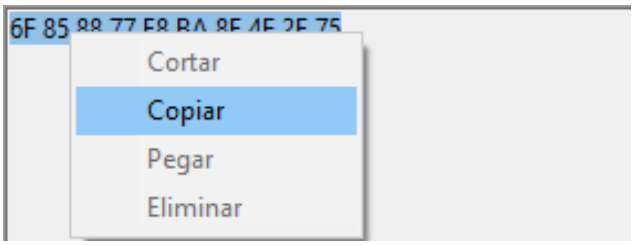
Lo anterior mostrará la siguiente pantalla.



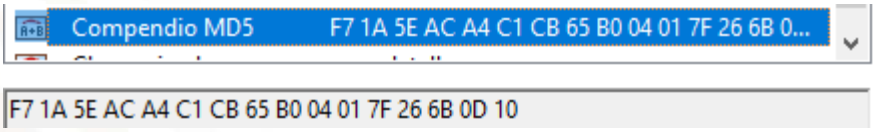
De donde se deben extraer los siguientes datos:
Número de Serie



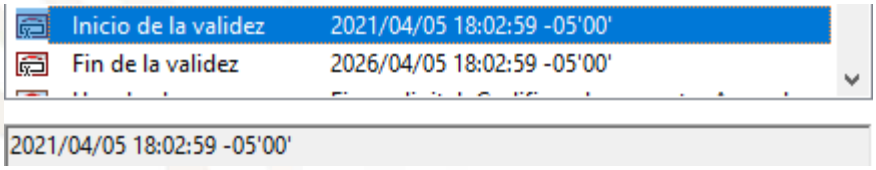
Nota: LOS DATOS PUEDEN SELECCIONARSE Y COPIARSE DEL PANEL INFERIOR DE LOS *"Datos del certificado"*.

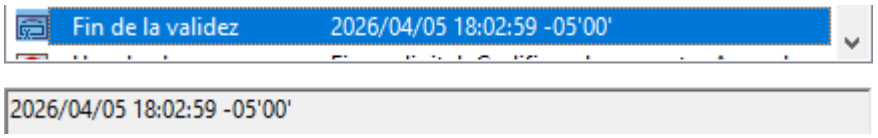


Cadena de validación (Compendio MD5, Finger Print, Huella Digital)

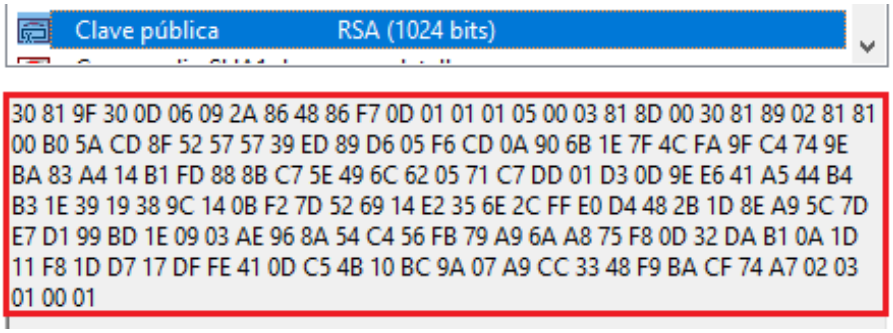


Vigencia: del_____al__ (Inicio de la validez y Fin de la Validez)

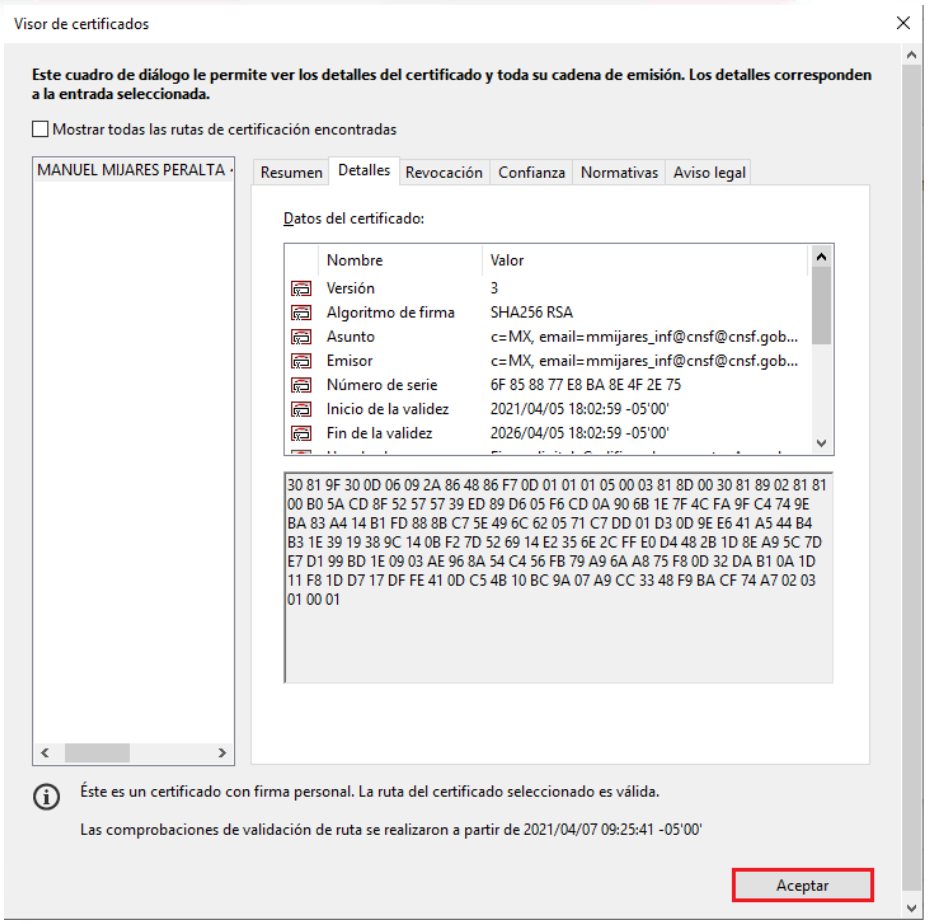




Llave pública (Clave pública)

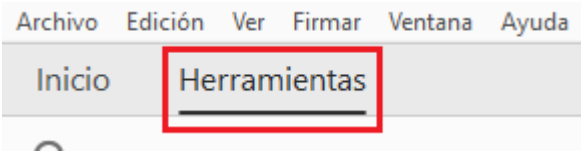


Una vez llenado el formato correspondiente como signatario responsable de alguno de los módulos del Sistema de Registro de Documentos (Anexo 39.4.7-b), dar clic en ***"Aceptar"*** para poder regresar a la pantalla de certificados y posteriormente, dar clic en cerrar para volver a la pantalla principal del programa.

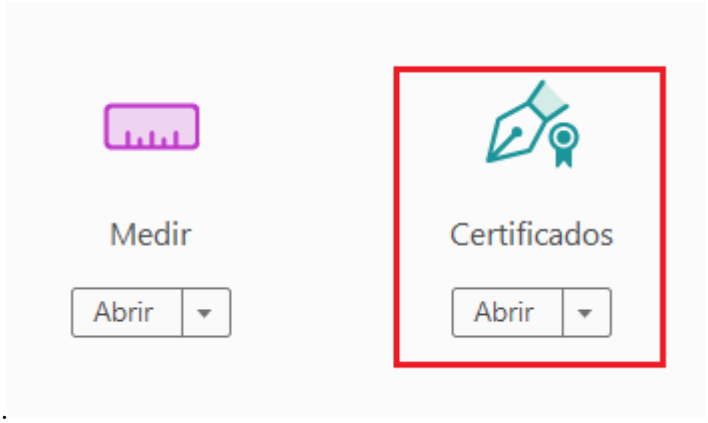

Visor de certificados
Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.
Mostrar todas las rutas de certificación encontradas
MANUEL MIJARES PERALTA
Resumen
Detalles
Revocación
Confianza
Normativas
Aviso legal
Datos del certificado:
Nombre
Valor
Versión
3
Algoritmo de firma
SHA256 RSA
Asunto
c=MX, email=mmijares_inf@cnsf@cnsf.gob...
Emisor
c=MX, email=mmijares_inf@cnsf@cnsf.gob...
Número de serie
6F 85 88 77 E8 BA 8E 4F 2E 75
Inicio de la validez
2021/04/05 18:02:59 -05'00'
Fin de la validez
2026/04/05 18:02:59 -05'00'
30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81 89 02 81 81 00 B0 5A CD 8F 52 57 57 39 ED 89 D6 05 F6 CD 0A 90 6B 1E 7F 4C FA 9F C4 74 9E BA 83 A4 14 B1 FD 88 8B C7 5E 49 6C 62 05 71 C7 DD 01 D3 0D 9E E6 41 A5 44 B4 B3 1E 39 19 38 9C 14 0B F2 7D 52 69 14 E2 35 6E 2C FF E0 D4 48 2B 1D 8E A9 5C 7D E7 D1 99 BD 1E 09 03 AE 96 8A 54 C4 56 FB 79 A9 6A A8 75 F8 0D 32 DA B1 0A 1D 11 F8 1D D7 17 DF FE 41 0D C5 4B 10 BC 9A 07 A9 CC 33 48 F9 BA CF 74 A7 02 03 01 00 01
Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.
Las comprobaciones de validación de ruta se realizaron a partir de 2021/04/07 09:25:41 -05'00'
Aceptar

FIRMADO DE DOCUMENTOS PDF EN ACROBAT READER Y PROFESIONAL

Para firmar digitalmente un documento en formato PDF, una vez abierto el documento en el programa, dar clic en el botón de ***"Herramientas"*** ubicado en la esquina superior izquierda.



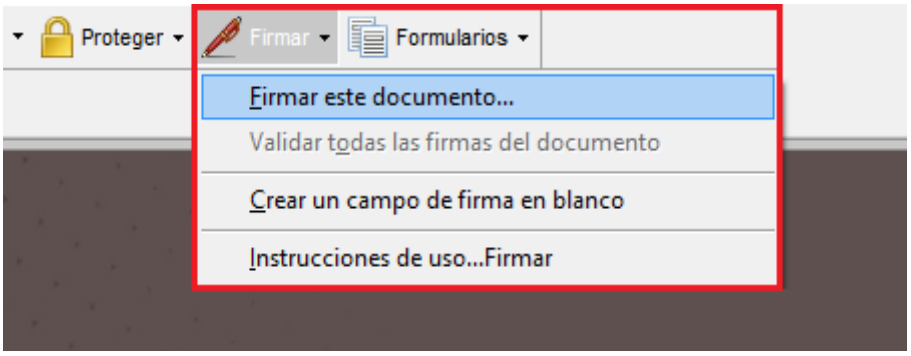
Seleccionar la opción de ***"Certificados"***



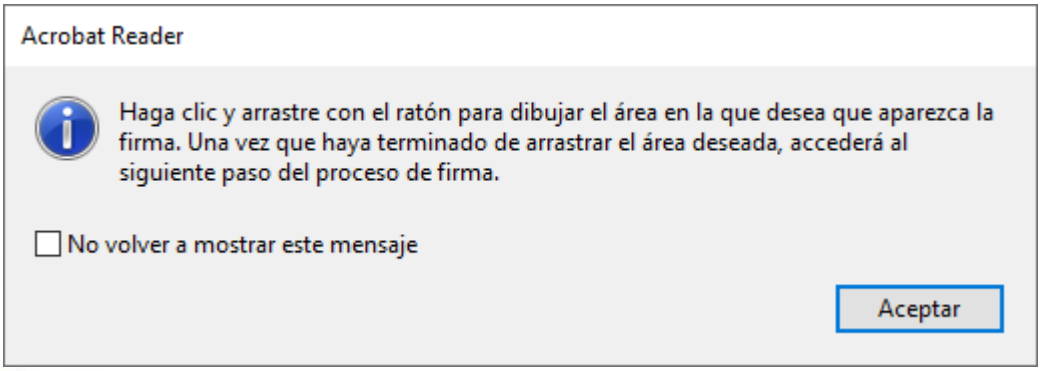
.

Seleccionar la opción de ***"Firmar con digitalmente"***.

En Acrobat Profesional existe la opción de “Firmar”, para seleccionar la opción de ***“Firmar este documento…”***



Para caso de ambos programas se mostrará el siguiente mensaje.

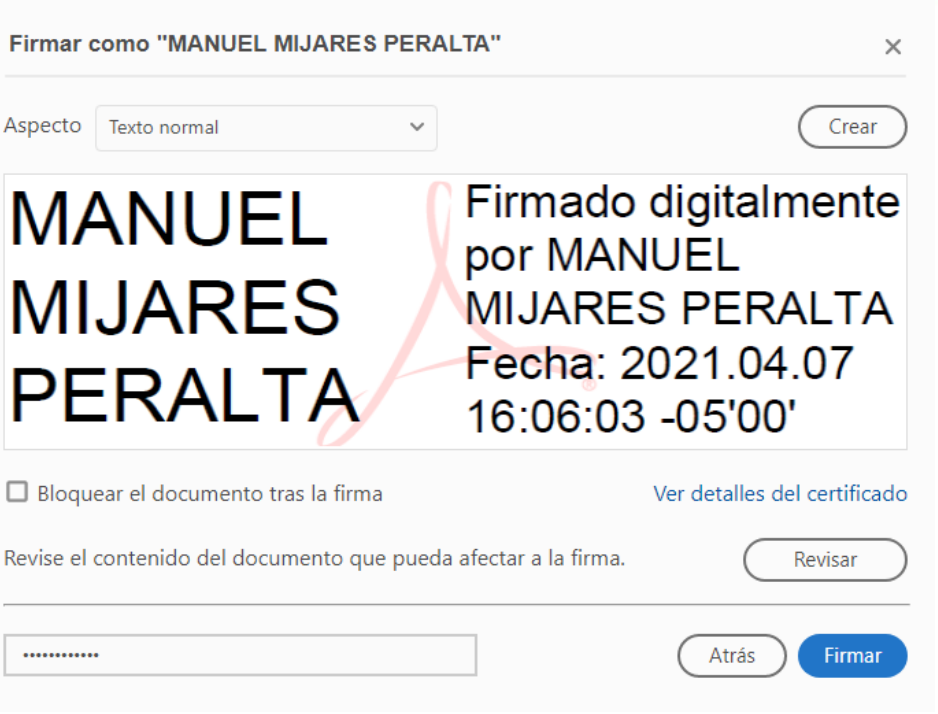


Donde, siguiendo las instrucciones del mensaje que se muestra:

Dar clic en el botón de ***“Arrastrar nuevo rectángulo de firma….”***

Dejando presionado el botón del ratón (Mouse) seleccionar el área y el tamaño que se desea para la firma.

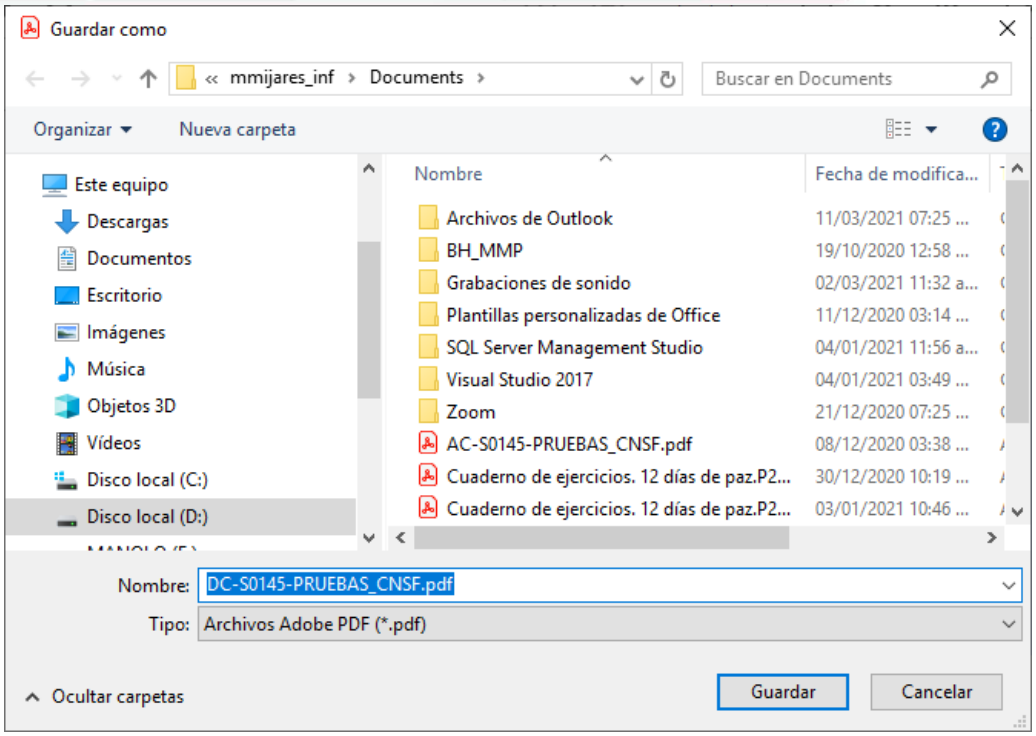
Seleccionar el ID o firma que se desea y dar clic en **“Continuar”**



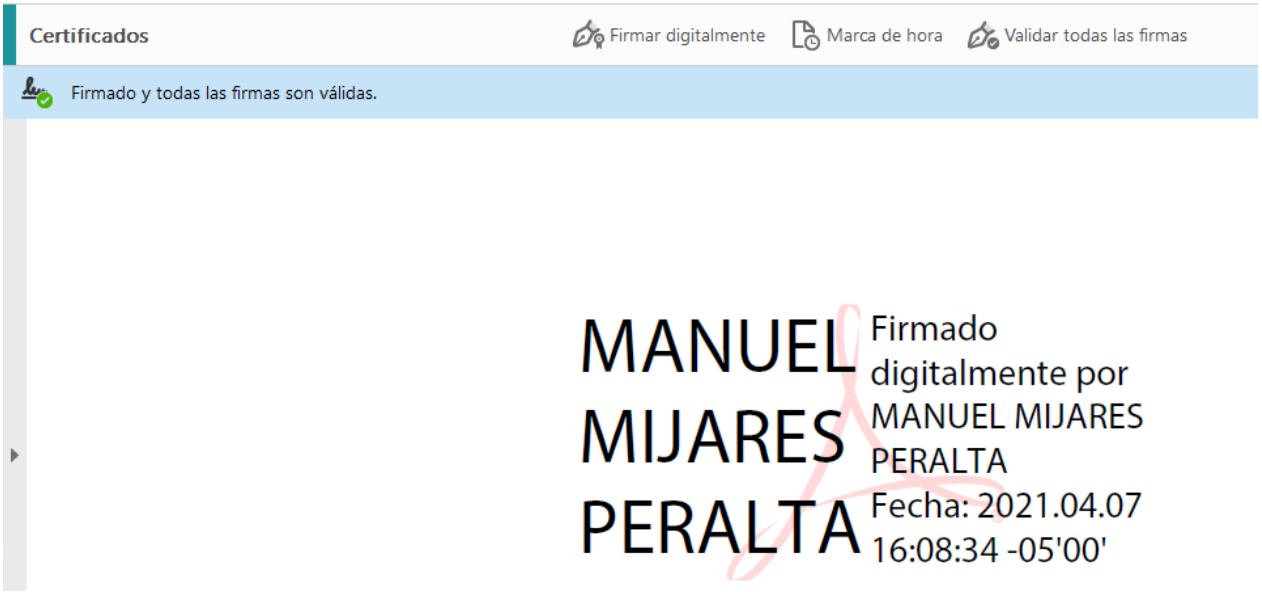
Donde:

- Se debe ingresar la contraseña de la firma electrónica.
- **NO se debe de bloquear el documento tras la firma.**

Si se desea, se puede guardar el archivo firmado, con otro nombre y/o en otra carpeta para conservar el documento original sin firmar. Dar clic en ***"Guardar"*** para terminar.


Guardar como
« mmijares_inf › Documents ›
Buscar en Documents
Organizar
Nueva carpeta
Este equipo
Descargas
Documentos
Escritorio
Imágenes
Música
Objetos 3D
Vídeos
Disco local (C:)
Disco local (D:)
Nombre
Fecha de modifica...
Archivos de Outlook 11/03/2021 07:25 ...
BH_MMP 19/10/2020 12:58 ...
Grabaciones de sonido 02/03/2021 11:32 a...
Plantillas personalizadas de Office 11/12/2020 03:14 ...
SQL Server Management Studio 04/01/2021 11:56 a...
Visual Studio 2017 04/01/2021 03:49 ...
Zoom 21/12/2020 07:25 ...
AC-S0145-PRUEBAS_CNSF.pdf 08/12/2020 03:38 ...
Cuaderno de ejercicios. 12 días de paz.P2... 30/12/2020 10:19 ...
Cuaderno de ejercicios. 12 días de paz.P2... 03/01/2021 10:46 ...
Nombre: DC-S0145-PRUEBAS_CNSF.pdf
Tipo: Archivos Adobe PDF (*.pdf)
Ocultar carpetas
Guardar
Cancelar

De esta forma el documento queda firmado digitalmente.



CIFRADO DE ARCHIVOS CON LA HERRAMIENTA PGP DE LA CNSF

INTRODUCCIÓN

Este apartado tiene como finalidad dar a conocer la forma, paso a paso, para la generación del cifrado de la información que se envía a esta Comisión.

La implementación del uso de los medios de identificación electrónica en la CNSF tiene los siguientes objetivos:

- Permitir su utilización para la gestión de asuntos administrativos que determine la propia Comisión;
- Utilizar un mecanismo que otorgue seguridad técnica y certeza jurídica en la suscripción de documentos vía electrónica;
- Establecer los procedimientos que permitan resguardar documentos electrónicos suscritos con un medio de identificación electrónica.
- Se debe contar con permisos de administrador sobre el equipo a instalar el PGP.

REQUISITOS DEL SISTEMA

Requisitos mínimos recomendados para utilizar el PGP de la CNSF son:

Para equipos con Windows 7, 8 o 10:

- Contar con una versión mínima de java 1.8 update 45 (Se recomienda instalar una sola versión de Java, para un correcto funcionamiento)
- Tener instalada la versión de Internet Explorer 9, 10 u 11
- Sistema Operativo Windows 7, 8 o 10 a 32 o 64 bits
- Acceso Internet.
- **Para equipos a 64 bits, la versión de java debe ser a 32 bits. Y se recomienda ampliamente que sea la versión mas reciente de Java.**

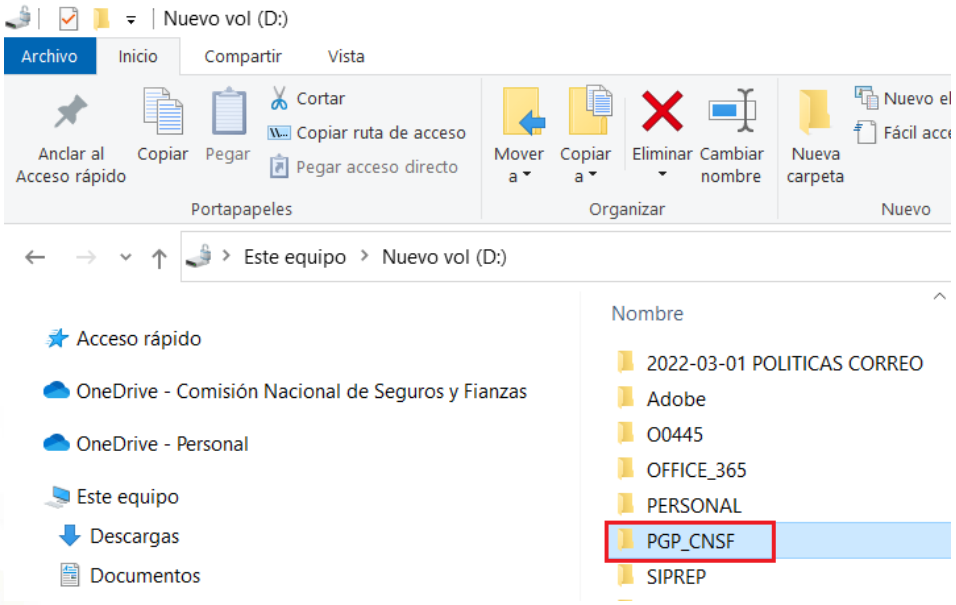
Para equipos con Windows XP:

- Contar con una versión mínima de java 1.7 update 55 (Se recomienda instalar una sola versión de Java, para un correcto funcionamiento) o Java 1.8 update 45 como máximo.
- Tener instalada la versión de Internet Explorer 9, 10 u 11
- Acceso Internet.

Nota: Sí el sistema operativo es a 64 bits, las versiones de Java, deben ser a 32 bits, para un óptimo funcionamiento del programa.

DESCARGA EJECUTABLE PGP

Dentro del explorador de Windows crear una carpeta, donde, el nombre de la misma indentifique, que en ella se encuentra el programa PGP de la CNSF y con la finalidad de que en ella se descargue de la pagina de la CNSF, el progma del PGP y desde esta se ejecute.



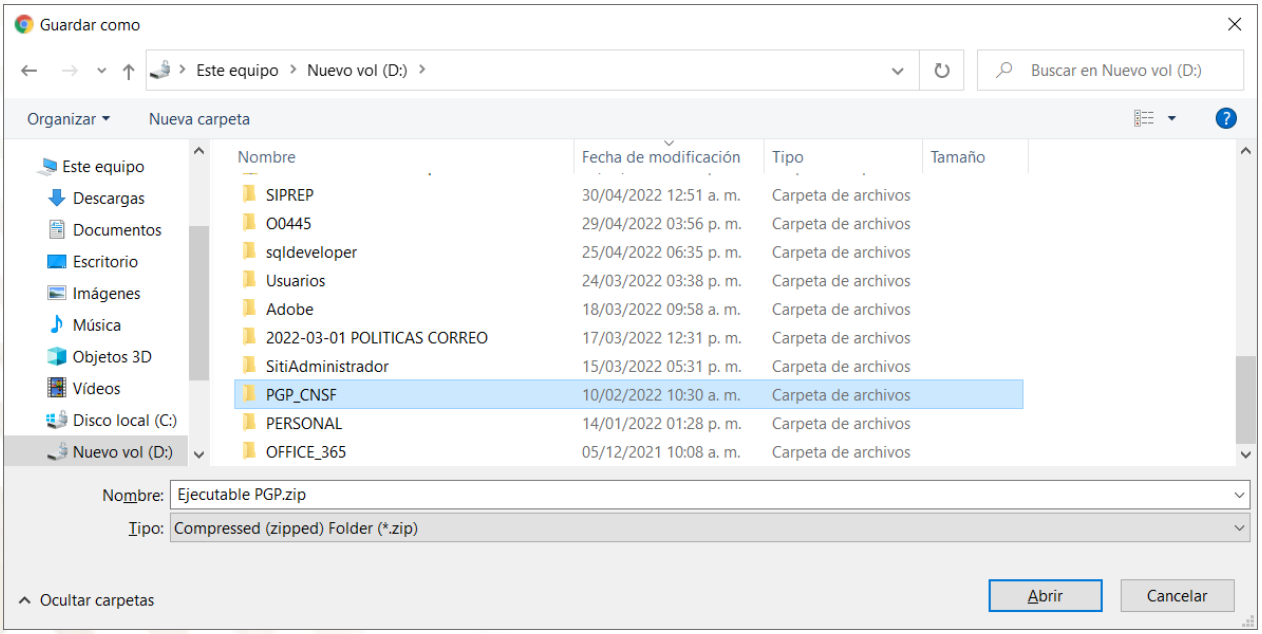
Descargar de la página de la CNSF el archivo Ejecutable PGP, ubicado en la siguiente dirección electrónica:
https://www.cnsf.gob.mx/Sistemas/Paginas/SEIVE.aspx

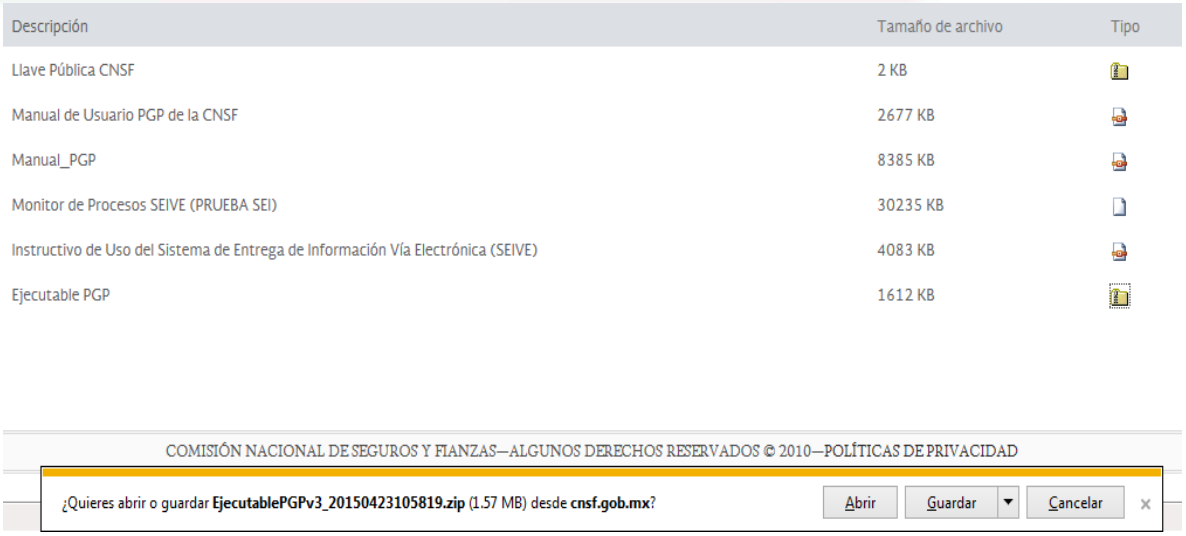
SEIVE

El Sistema de Entrega de Información Vía Electrónica (SEIVE) es una aplicación a través de la cual se recibe en la CNSF diferente información por parte de las instituciones del sector asegurador y afianzador a través de la página de Internet de este organismo.

Dar clic sobre la carpeta comprimida del "**Ejecutable PGP**"

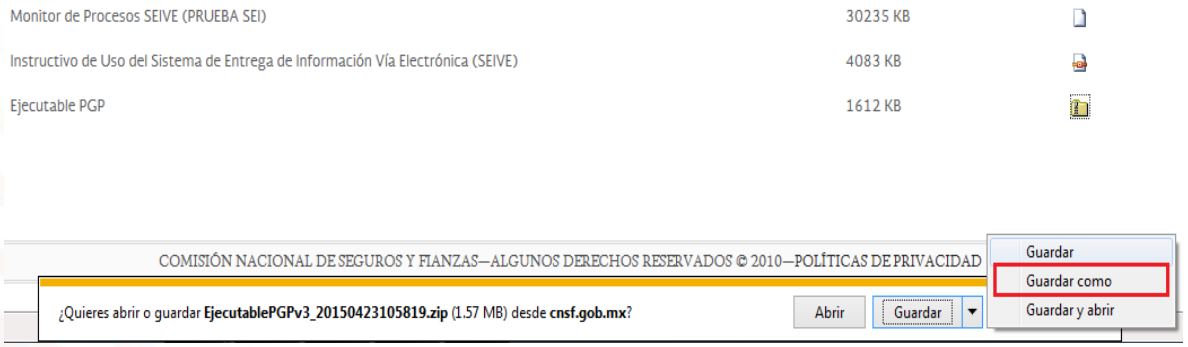
Dependiendo de la configuración de su navegador de internet, puede que este le solicite la carpeta donde desea descargarlo, o bien lo guarde automaticamente en la capeta "Descargas" de su equipo.



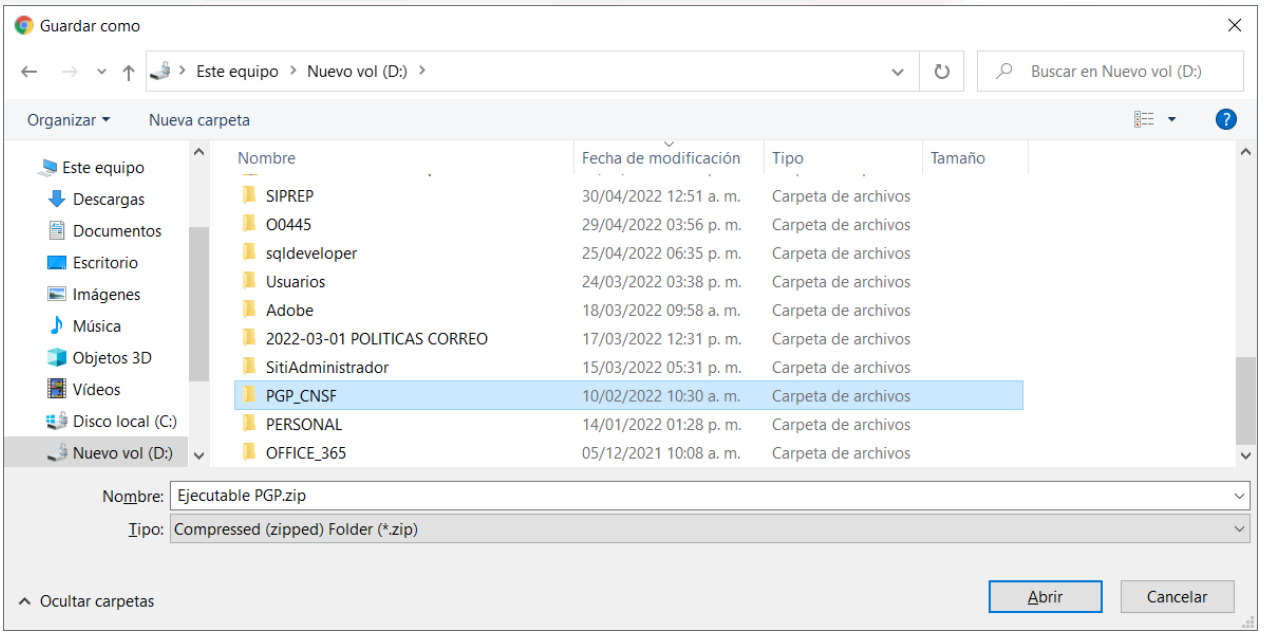


De la opción de ***"Guardar"***, dar clic en la parte derecha del botón 

, para seleccionar la opción de ***"Guardar como"***, para poder elegir la carpeta de destino donde se guardará el archivo.

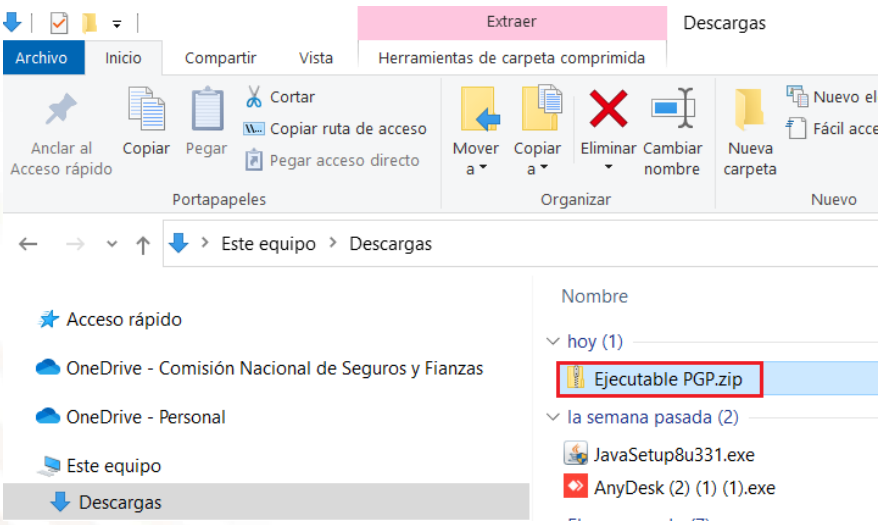


Al seleccionar la opción de "Guardar como", se mostrará la siguiente pantalla donde se debe de seleccionar la carpeta que previamente se ha creado, para el programa PGP.



Dar clic en ***"Guardar"***, para descargar el archivo del programa PGP.

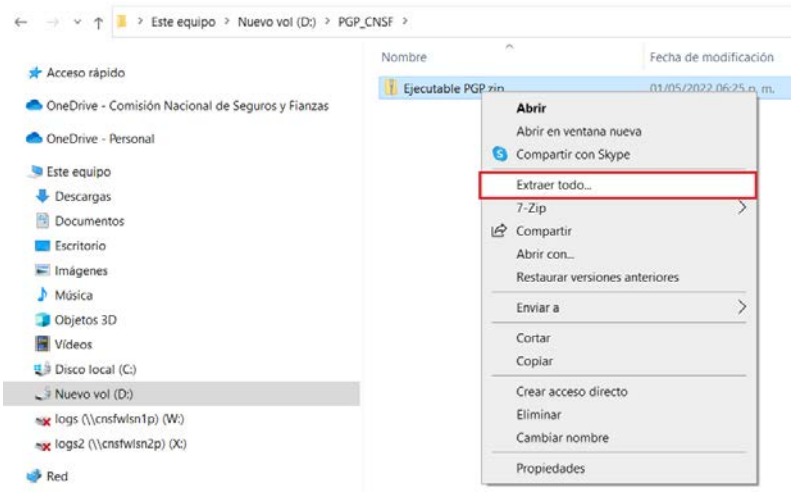
NOTA: SI NO APARECE LA PANTALLA PARA SELECCIONAR LA CARPETA DE DESTINO PARA GUARDAR EL ARCHIVO, ESTE ULTIMO ESTÁ EN LA CARPETA DE DESCARGAS DEL EQUIPO.



INSTALACIÓN DEL EJECUTABLE PGP

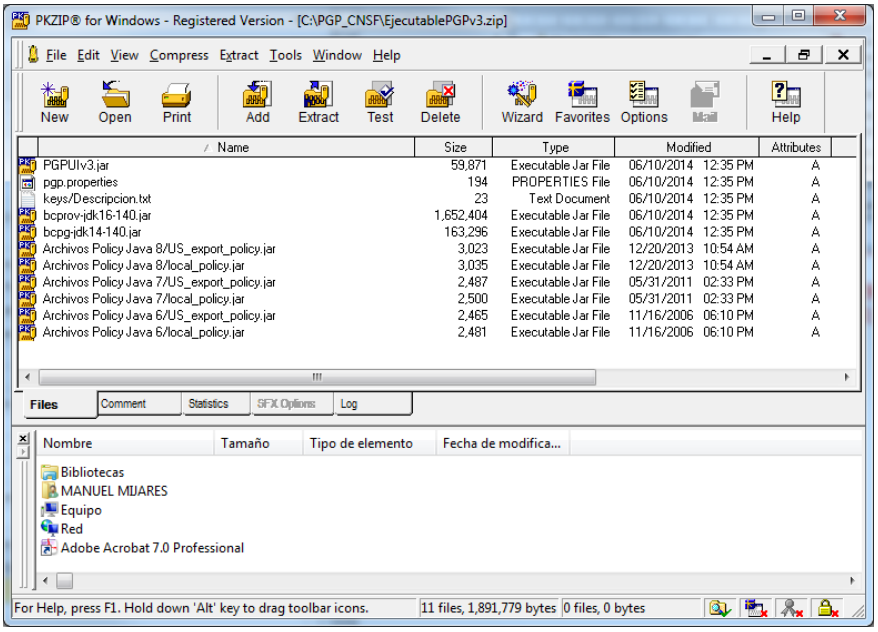
Una vez descargado el ejecutable y que este se encuentre dentro de la carpeta que se creó para su almacenamiento, se deben extraer los archivos contenidos en el archivo "EjecutablePGPv3.zip". Dando clic derecho sobre el archivo antes mencionado y de acuerdo al programa para abrir archivos *.ZIP, que se tenga instalado, seleccionar alguna de las siguientes opciones:

- Extraer aquí
- Abrir
- Extraer todo

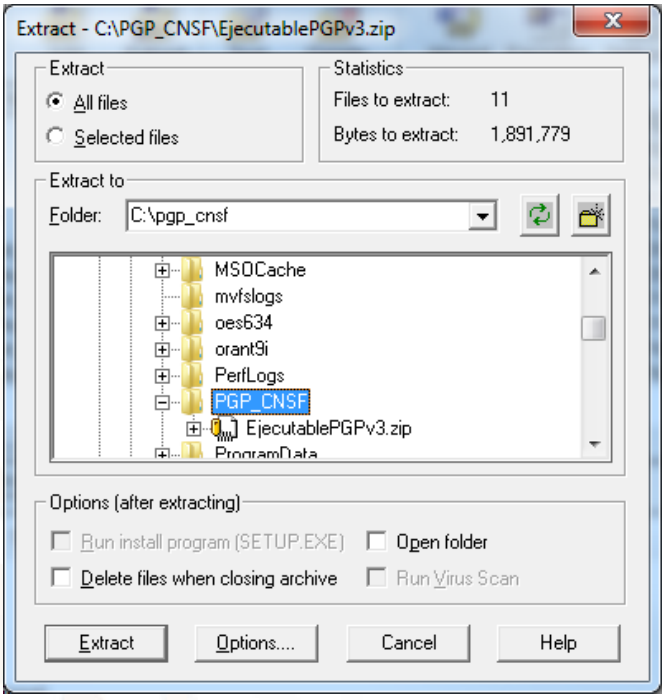


Para poder extraer el contenido del archivo en la carpeta que se creó previamente para el PGP de la CNSF.

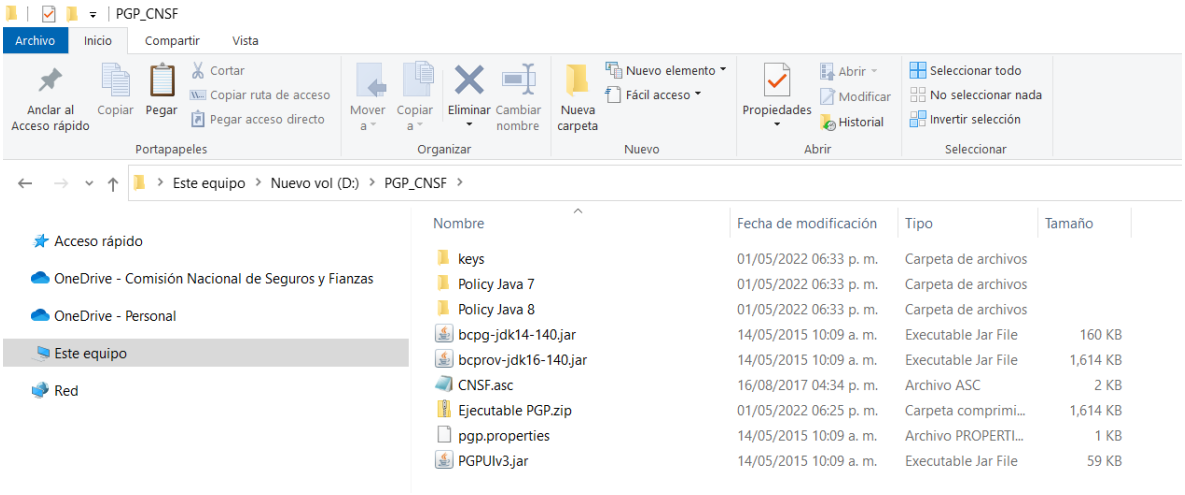
Ejemplo: Si se cuenta con algún programa para abrir o crear archivos *.ZIP, al seleccionar la opción “Abrir” se muestra el contenido del archivo en la aplicación



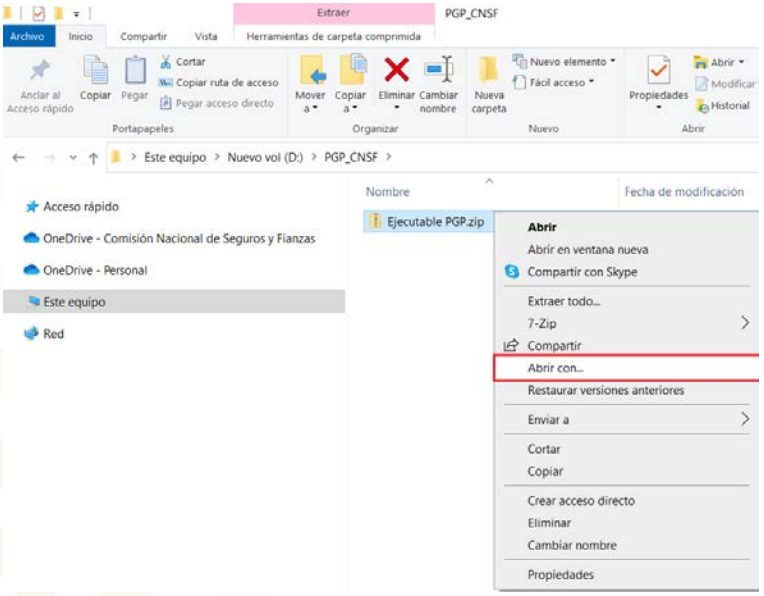
A través de la opción de “Extraer” del programa, se debe seleccionar la carpeta donde se extraerán los archivos contenidos en el ZIP, esta carpeta es la que se creó para el programa PGP.

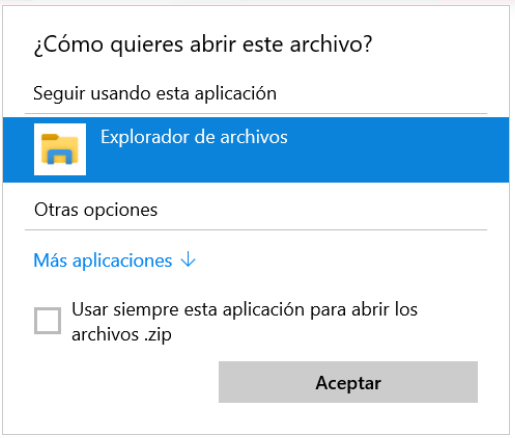


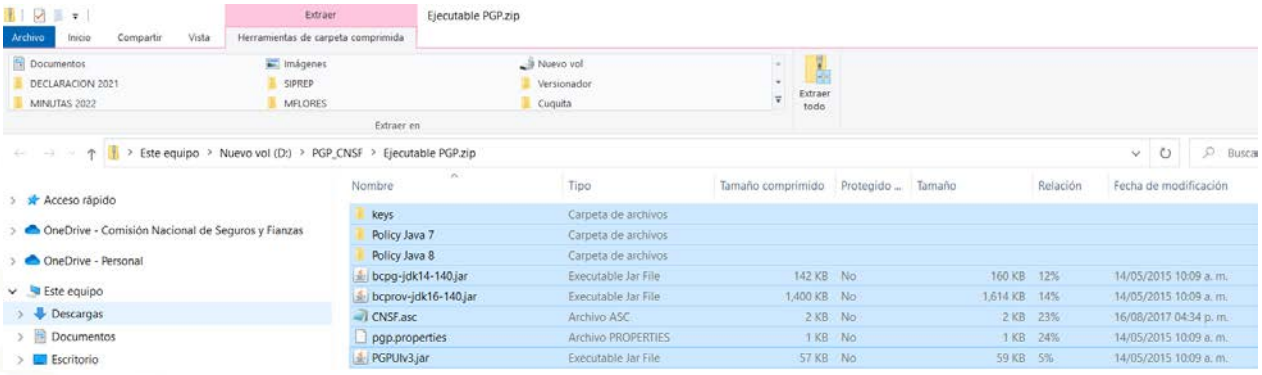
Dar clic en el botón de extraer, de esta forma, quedarán los archivos contenidos en el archivo ZIP, dentro de la carpeta mencionada.



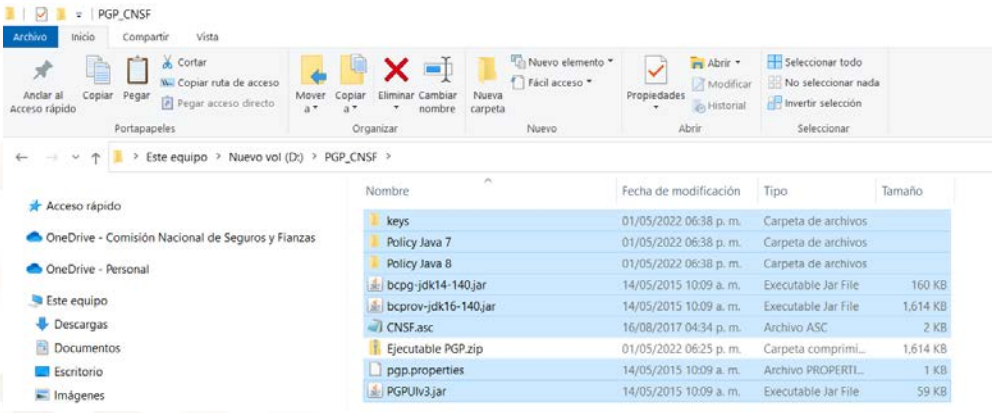
En caso de no contar con un programa para abrir o crear archivos .Zip, bastará seleccionar el archivo, y seleccionar la opción **“Explorador de Windows”** del menú **“Abrir con”,** para que se muestre dentro del explorador de Windows y seleccionar todos los archivos, copiarlos y pegarlos en la carpeta que se ha creado para el programa PGP de la CNSF.







Archivos seleccionados dentro del archivo .Zip



Archivos copiados en la carpeta para el PGP

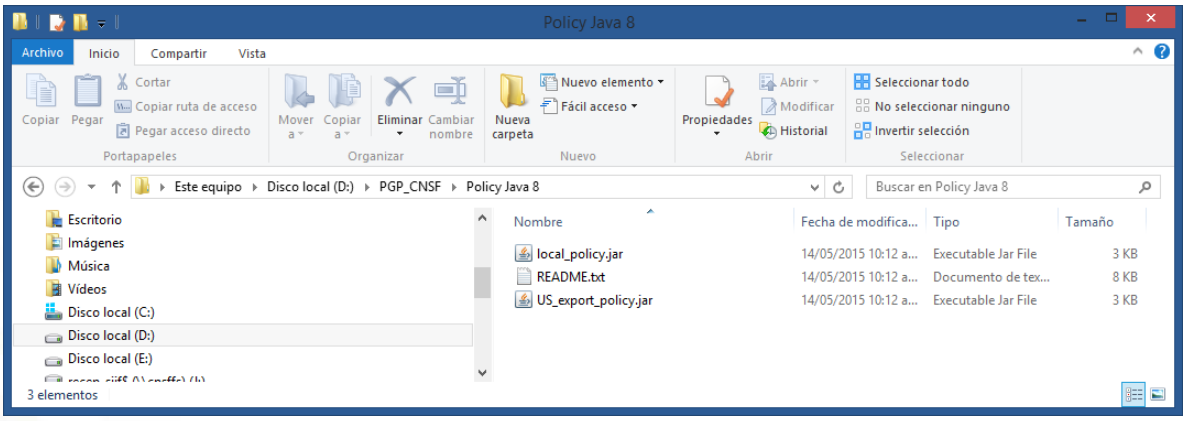
EL SIGUIENTE PROCEDIMIENTO SOLO APLICA PARA EQUIPOS CON UNA VERSION DE JAVA INFERIOR A JAVA 1.8 UPDATE 161.

Dentro de la carpeta que se creó para el ejecutable, se tiene las siguientes carpetas

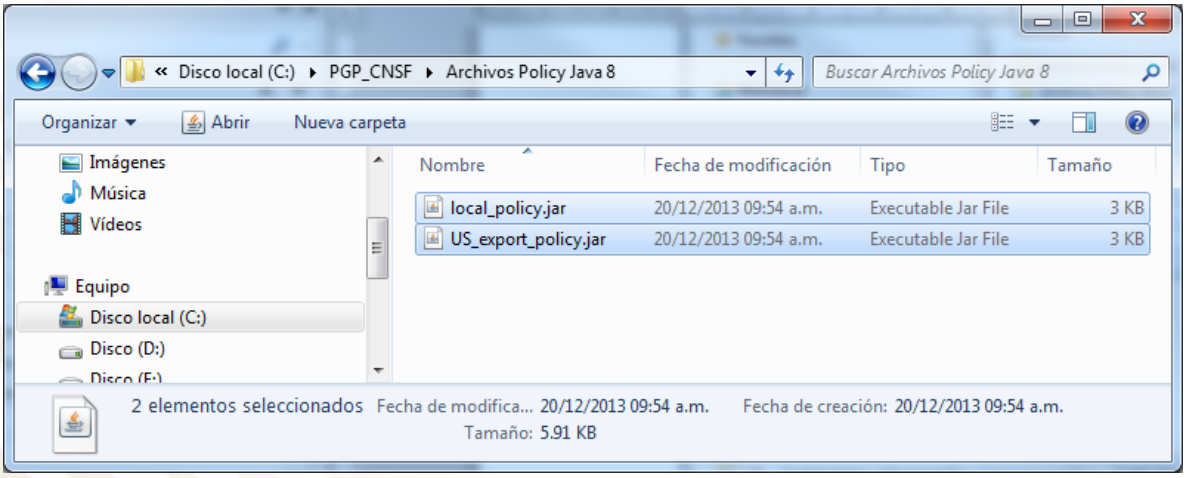
- Archivos Policy Java 7
- Archivos Policy Java 8

Que corresponden a los archivos policy de Java, para cada una de las versiones soportadas por el PGP. **Si se cuenta con la versión de Java 1.8 update 161, no será necesario realizar el procedimiento que se menciona a continuación.**

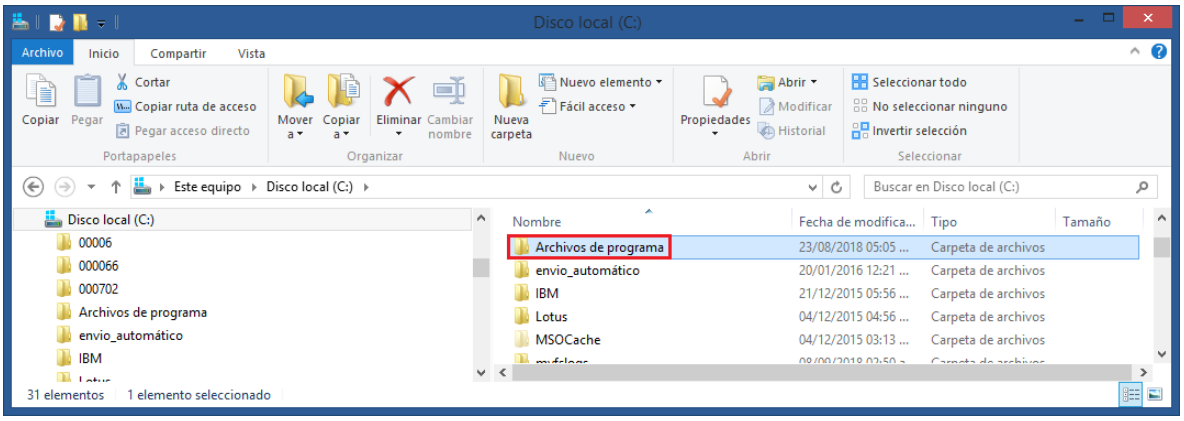
De acuerdo a la versión de Java que se tenga instalada en el equipo deberá:



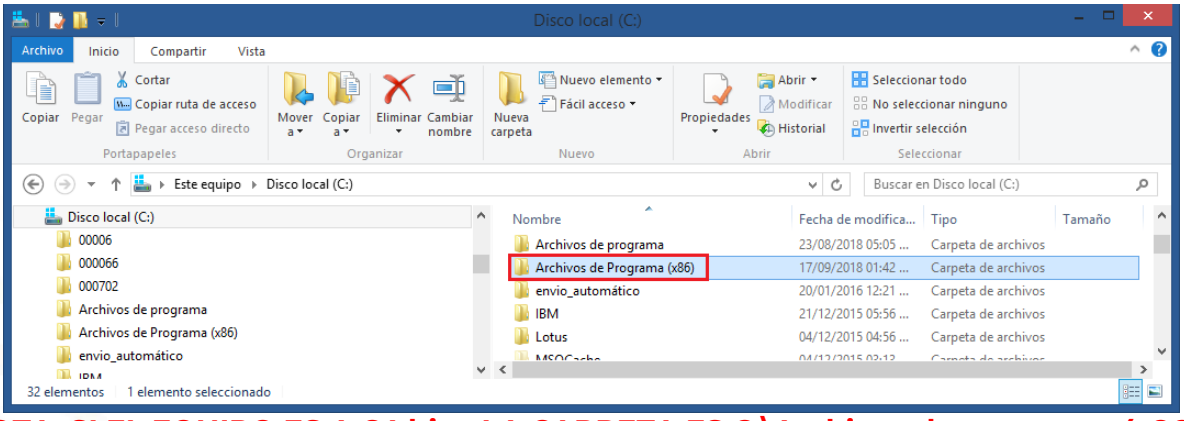
Ingresar a la carpeta correspondiente a la versión de Java Instalada.



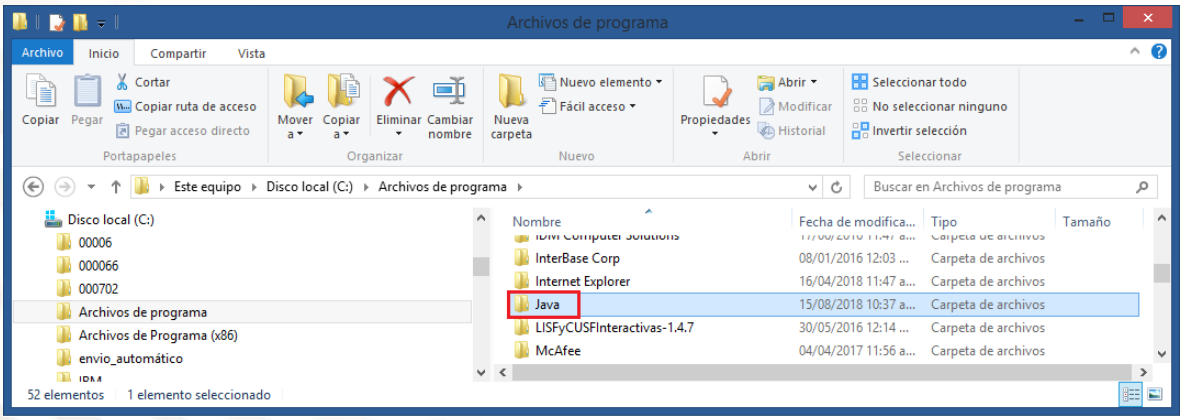
Seleccionar los archivos: ***local_policy.jar*** y ***US_export_policy.jar*** y copiarlos



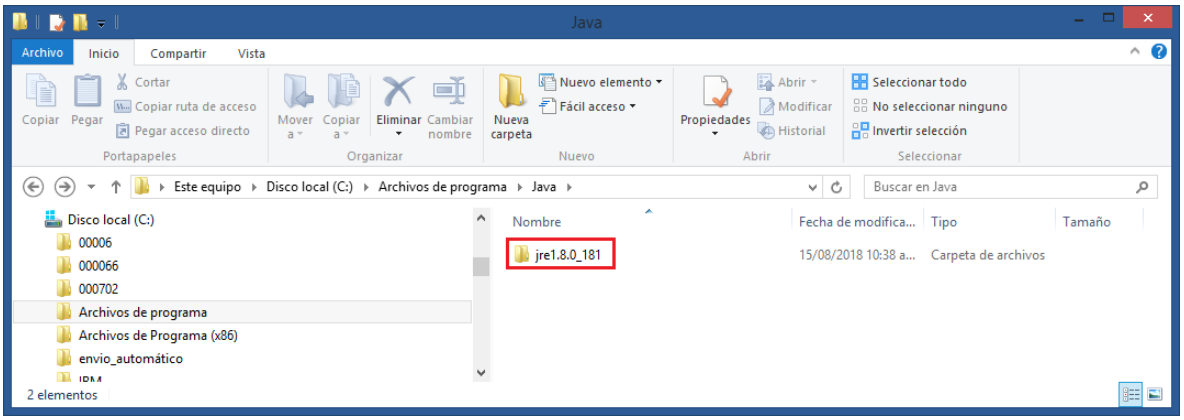
Ingresar a la carpeta de archivos de Programa, que se encuentra en el disco local C:\



NOTA: SI EL EQUIPO ES A 64 bits, LA CARPETA ES C:\Archivos de programa (x86)



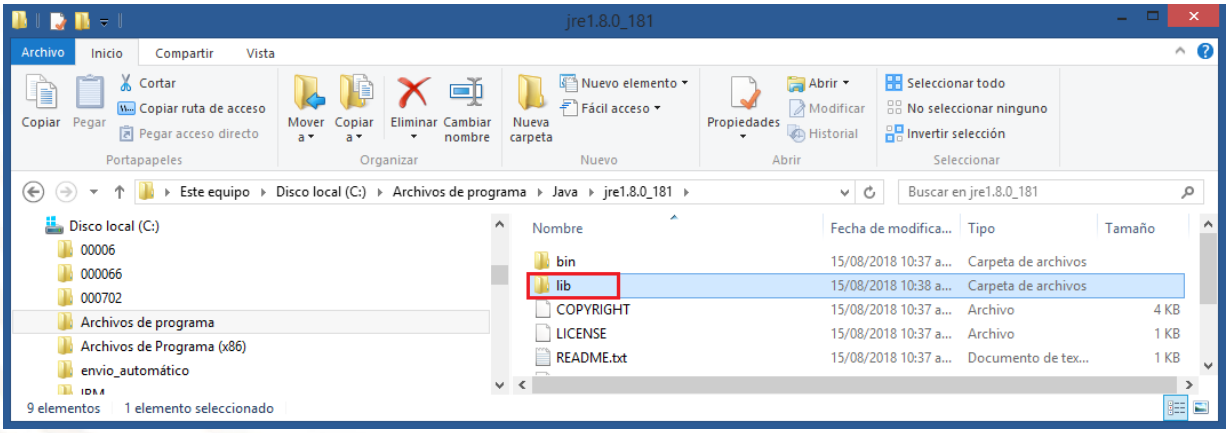
Ingresar a la carpeta Java, que se encuentra de C:\Archivos de Programa



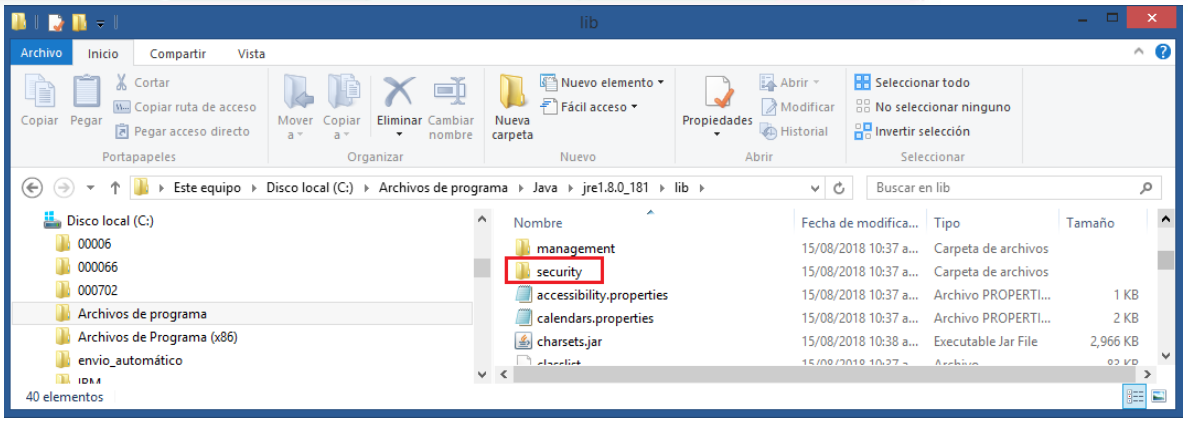
Ingresar a la carpeta que corresponda a la versión de Java, que se encuentra en C:\Archivos de programa\Java.

Nota: El nombre de la carpeta es de acuerdo a la versión de Java, este puede ser:

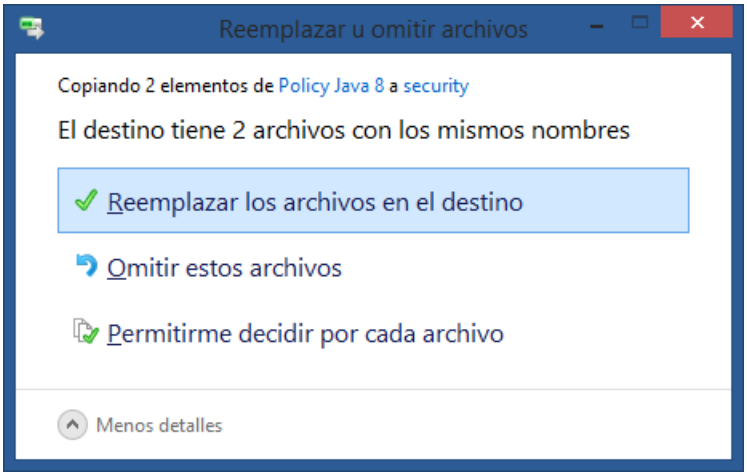
- jre7
- jre1.8.0_20 (El valor después del guion bajo (_) indica el update.
- jre1.8.0_25 (El valor después del guion bajo (_) indica el update.



Ingresar a la carpeta ***lib***

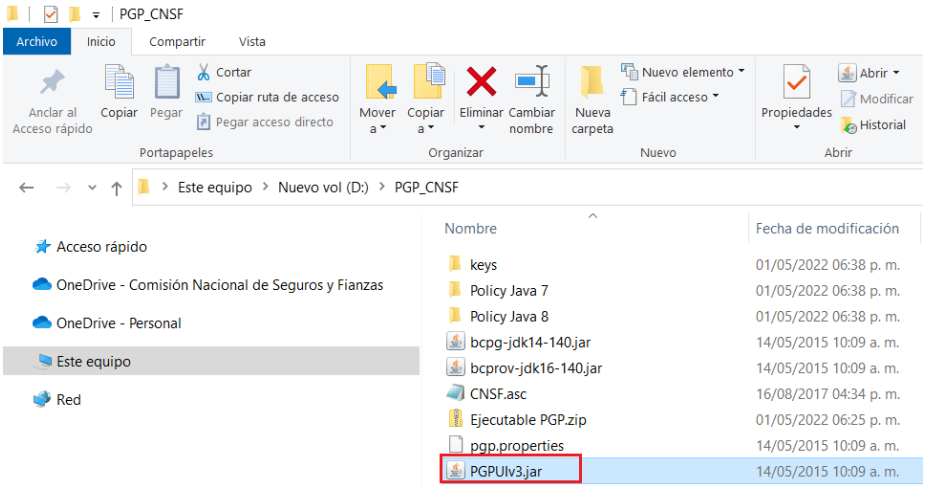


Ingresar a la carpeta ***security***

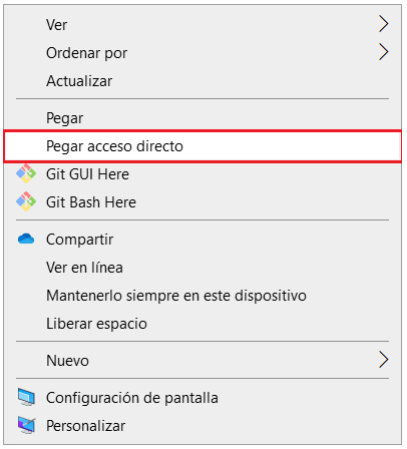


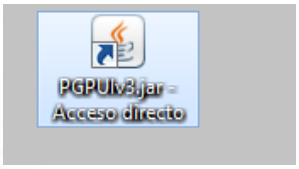
Pegar y remplazar los archivos previamente copiados. (Para esto se requieren privilegios de administrador sobre el equipo).

Para tener un acceso fácil al programa PGP de la CNSF, se debe de crear un acceso directo. Esto se hace seleccionando el archivo ***"PGPUIv3.jar"***, que se encuentra dentro de la carpeta donde se encuentra el programa y copiándolo.



Estando en el escritorio dar clic con el botón derecho del mouse y seleccionar la opción ***"Pegar acceso directo"***

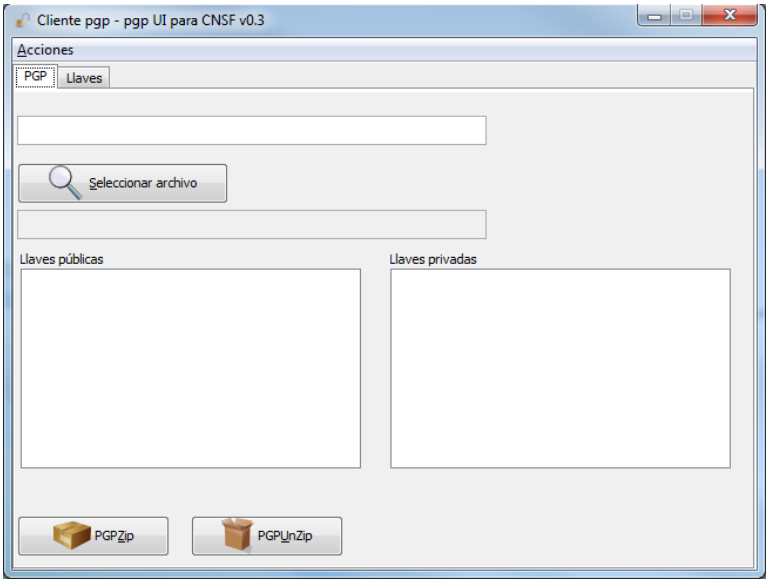


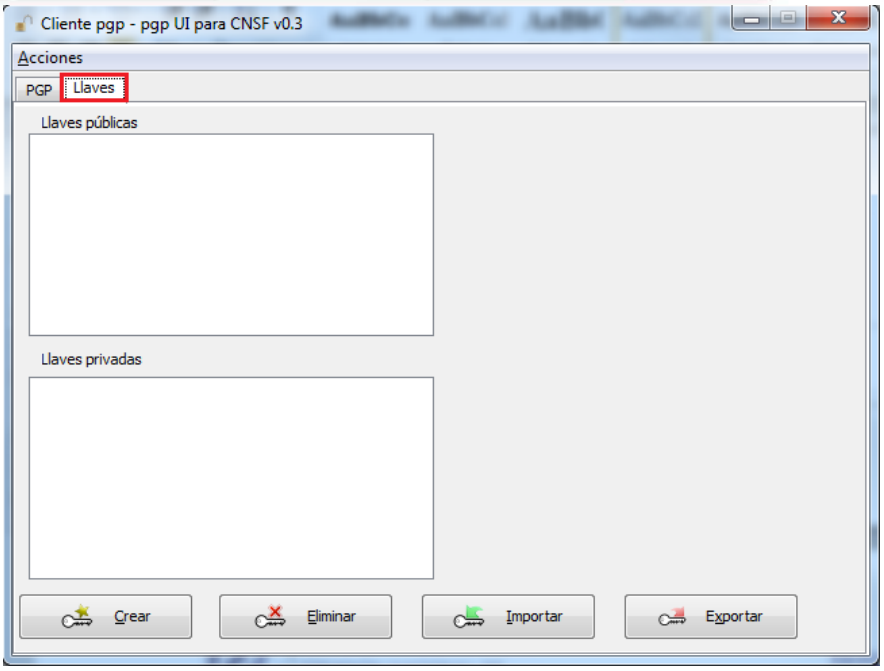


De esta forma queda instalado el programa y se tiene un fácil acceso.

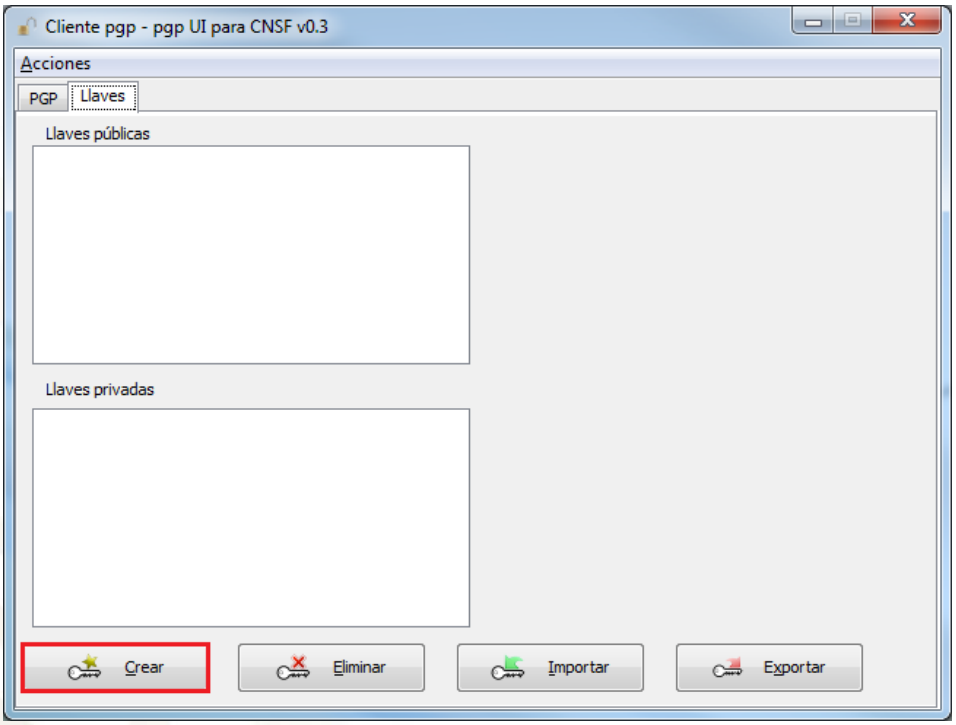
GENERACIÓN DE LLAVES PARA INSTITUCIONES DE SEGUROS, FIANZAS, SOCIEDADES MUTUALISTAS E INTERMEDIARIOS DE REASEGURO, FONDOS DE ASEGURAMIENTO AGROPECUARIO Y ORGANISMOS INTEGRADORES

Cuando se trata de una compañía nueva, que se encuentre en certificación, se deben de crear las llaves pública y privada de la Institución, para ello se debe de ingresar al programa PGP.



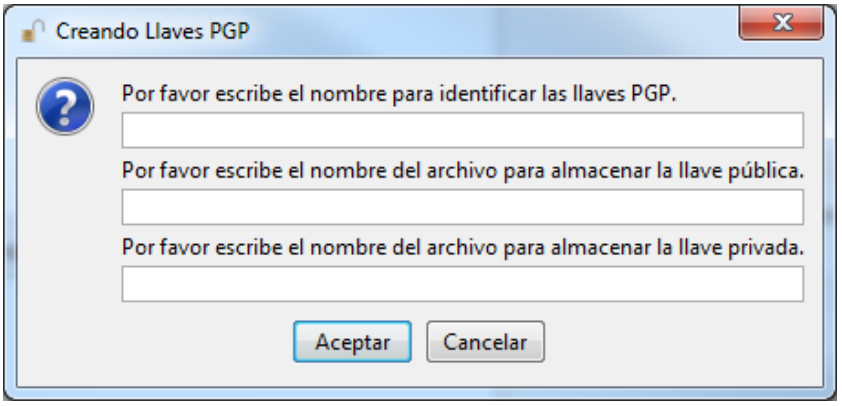


Dando clic en la pestaña de **Llaves.**



Y dando clic en el botón ***"Crear"***

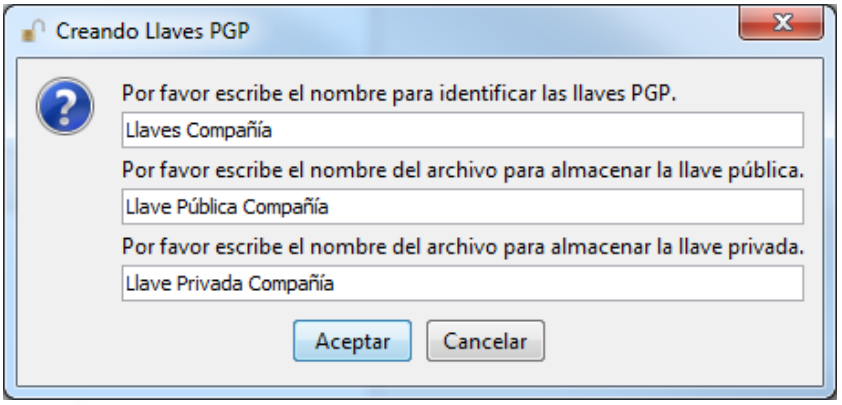
Haciendo lo anterior mostrará la siguiente pantalla:



Donde se debe indicar:

- El nombre para identificar las llaves dentro del programa PGP.
- El nombre de la llave publica, como se guardará en la PC.
- El nombre de la llave privada, como se guardará en la PC.

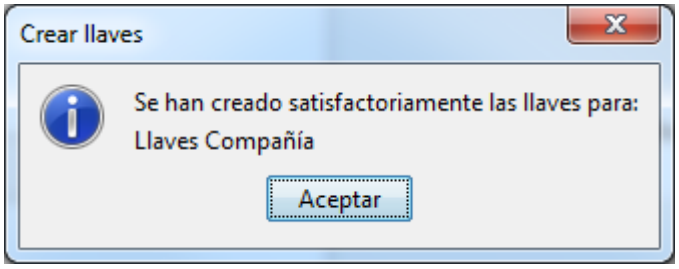
Estos son libres



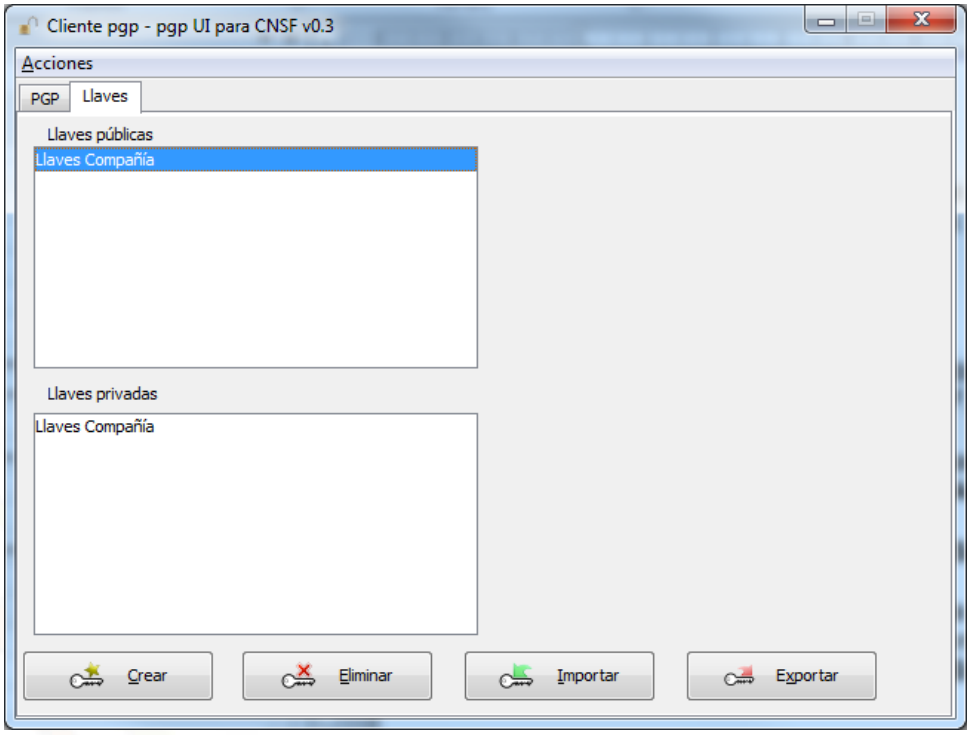
Pantalla en la cual se deberán escribir los nombres para identificar las llaves PGP y los nombres para almacenar las llaves pública y privada dentro de la carpeta correspondiente (el programa lo guarda en la carpeta keys), al terminar de llenar los campos requeridos, dar clic en el botón de aceptar (el proceso puede tardar unos segundos).

NOTA: LOS NOMBRES DE LAS LLAVES QUEDAN A DECISION DEL USUARIO.

Al terminar de crearse las llaves, el programa mostrará el siguiente mensaje, dar clic en aceptar para continuar:



De esta forma quedan creadas las llaves pública y privada de la compañía, como se muestra en la siguiente pantalla:



NOTA: El archivo de la llave pública de la institución, deberá exportarse a una carpeta o directorio (Esta se encuentra en la carpeta ***"keys"*** dentro de la carpeta del programa PGP) generada por la institución deberá ser entregada a través del Sistema de Citas, conforme a la disposición 39.1.5 de la Circular Única de Seguros y Fianzas. La llave privada, solo debe enviarse a esta CNSF y no es utilizada para el cifrado de archivos. En caso de requerir sustituir su llave, también podrá entregarla a la siguiente dirección de correo entregaelectronica@cnsf.gob.mx indicando la razón social de la institución y la clave de esta. Será el administrador del SEIVE quien se encargue de entregarla.

LLAVE PRIVADA PARA ENTIDADES Y PERSONAS SUPERVISADAS

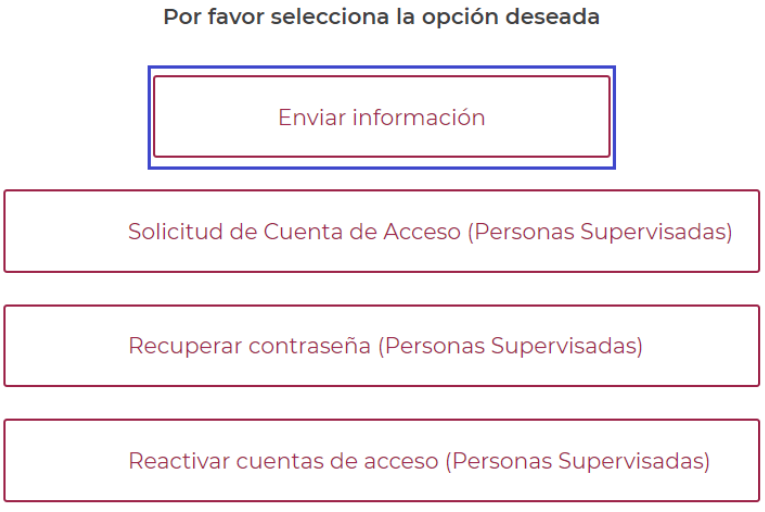
Como **"Entidad Supervisada"** se debe de entender a toda aquella persona o entidad que este obligada a enviar información a la CNSF.

Las personas supervisadas son:

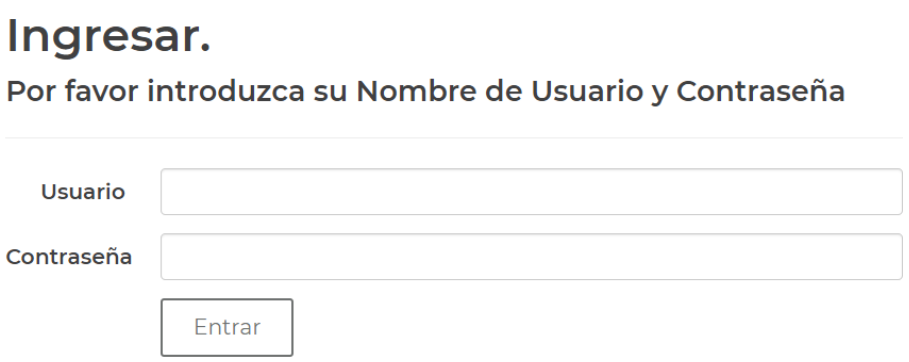
- Actuario
- Agente Persona Moral
- Auditor Externo Independiente
- Centro de Valuación de Exámenes
- Contralor Médico
- Dictaminador Jurídico
- Liquidador Administrativo / Convencional

Una vez que se ha completado la solicitud de cuenta de acceso como persona supervisada, de acuerdo al **"39.1.9 Instructivo de Uso del Sistema de Entrega de Información Vía Electronica SEIVE"**.

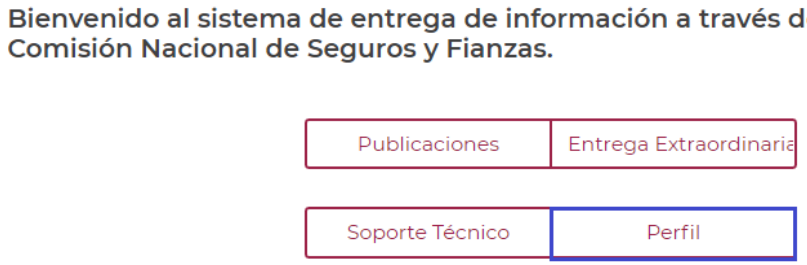
Para descargar la llave privada que la persona supervisada utilizará para realizar el cifrado de los archivos con la información correspondiente y enviarla a la CNSF, deberá ingresar al sistema a través de la opción **"Enviar información"** en la página principal.



Después de la acción anterior aparecera una pantalla en donde vamos a ingresar el **“Nombre de usuario”** y el “**Password”**, como se muestra a continuación:

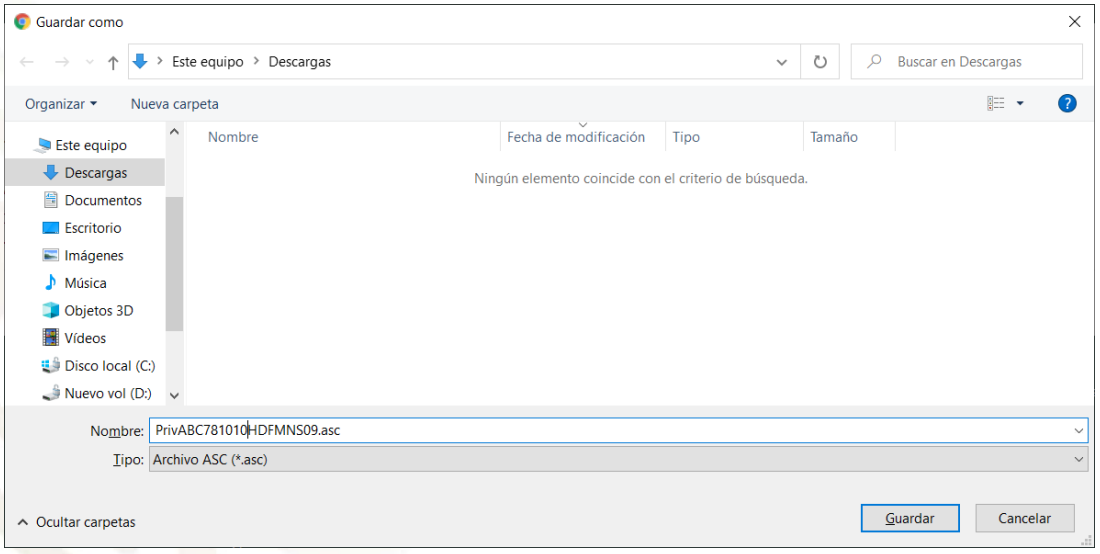


Posteriormente seleccionar la opción **“Perfil”,** que aparece entre las opciones siguientes:



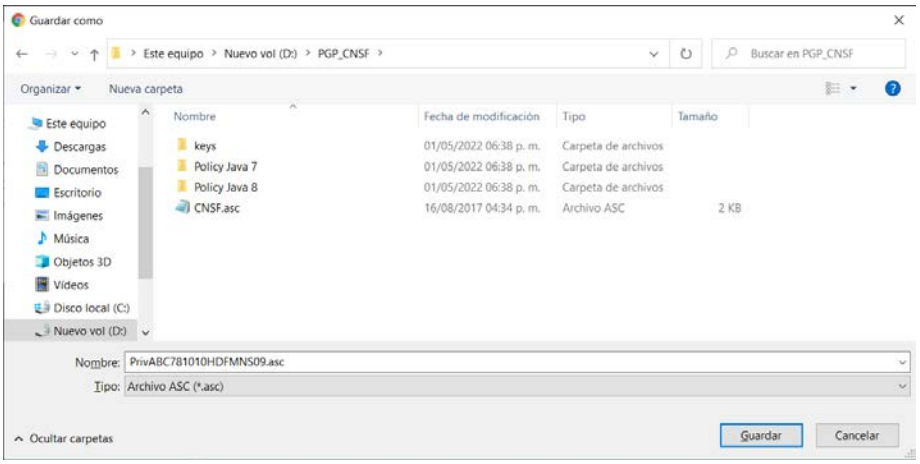
La opción anterior mostrará los datos del usuario, así como los productos o reportes que puede entregar ante la CNSF.

Para descargar la llave privada de la persona supervisada, el usuario deberá seleccionar la opción **"Llave"** como se muestra en la pantalla anterior y posteriormente el usuario deberá almacenar en un lugar seguro el archivo .asc que corresponde a la llave privada.



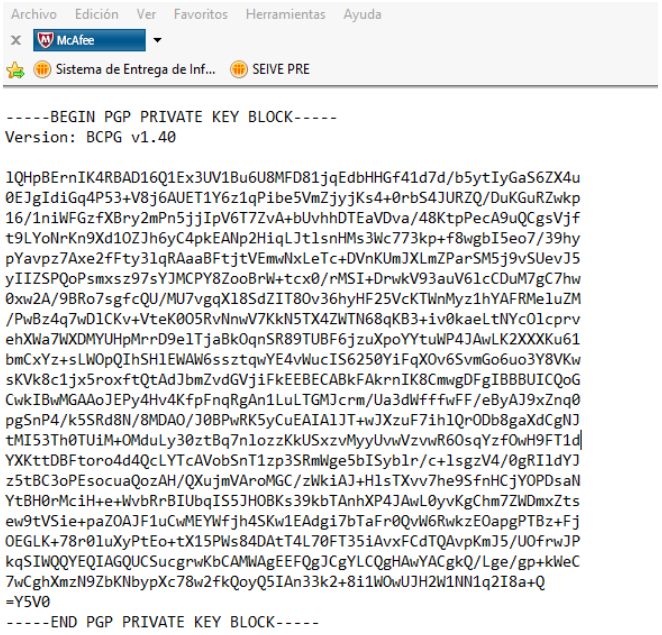
O bien:

El sistema solicitará la carpeta en donde se desea guardar la llave privada, como se muestra a continuación **(Se recomienda guardarla en la carpeta corresponiente al programa PGP)**:

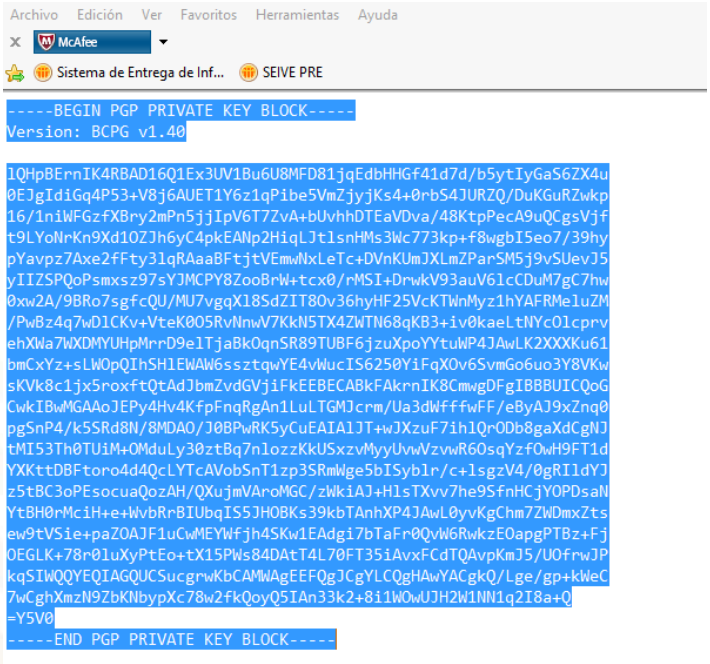


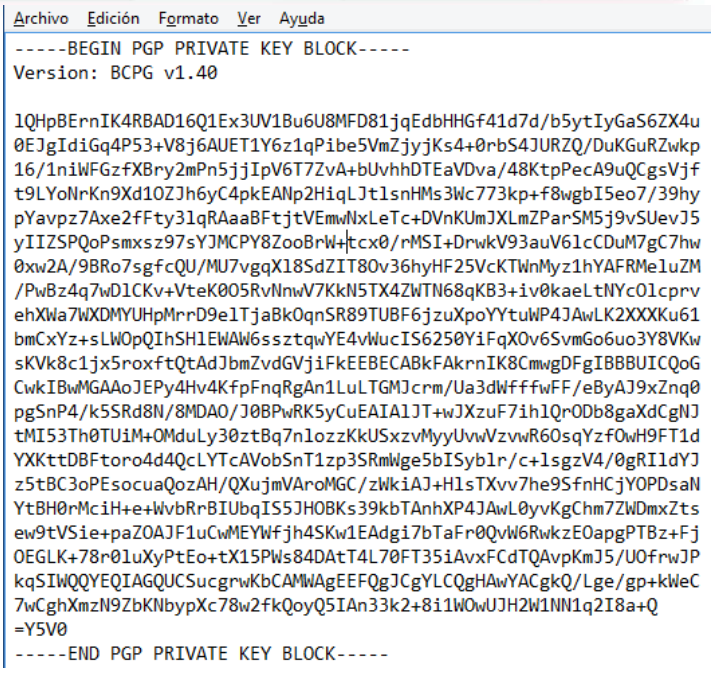
Nota: El usuario podrá cambiar el nombre del archivo al descargarlo, para que sea más sencillo su reconocimiento. Es recomendable guardar el archvio en la carpeta que se creó pata el programa PGP.

En caso de que la llave se muestre en el explorador de internet de la siguiente forma:

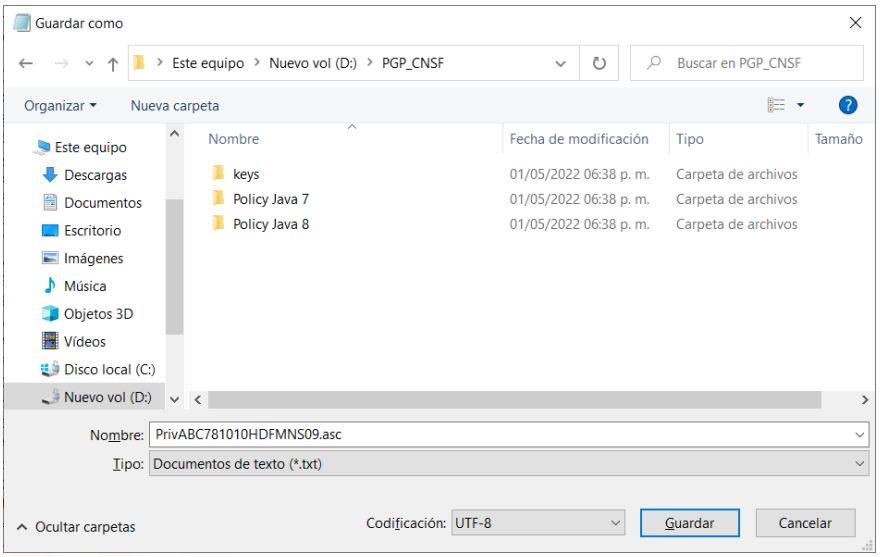


Se debe seleccionar todo el texto, copiarlo y pegarlo en un bloc de notas (Notepad).

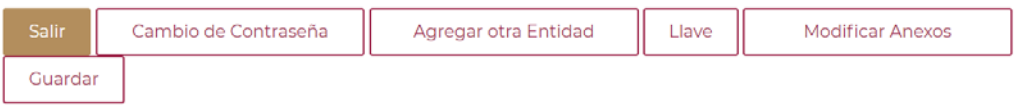




Y en el bloc de notas guardar la llave privada dentro de la carpeta del PGP, con el nombre que se desee y con extensión **.asc**

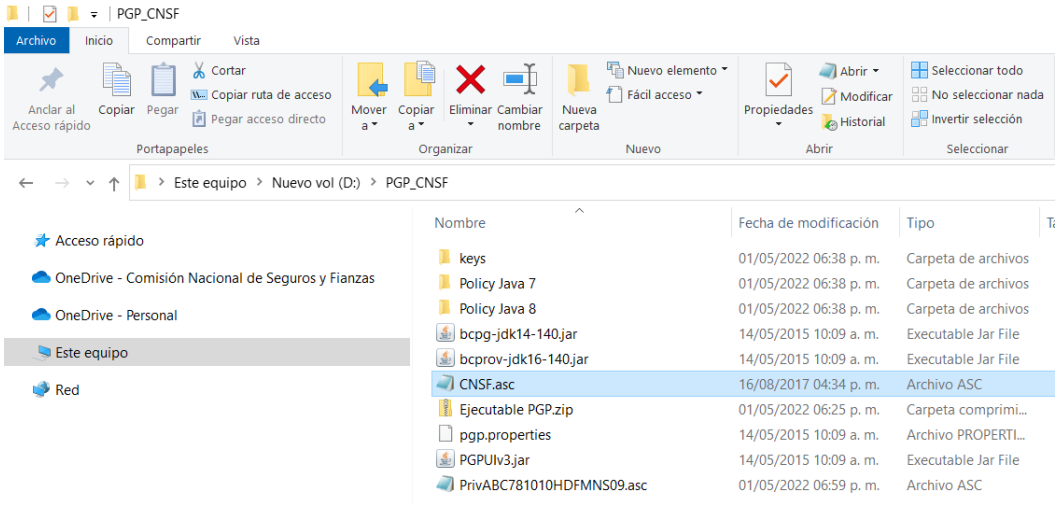


Una vez descargada la llave, dentro del SEIVE, dar clic en la opción **"Salir"**, para volver a la pantalla principal del sistema y salir de la aplicación.



LLAVE PÚBLICA DE LA CNSF

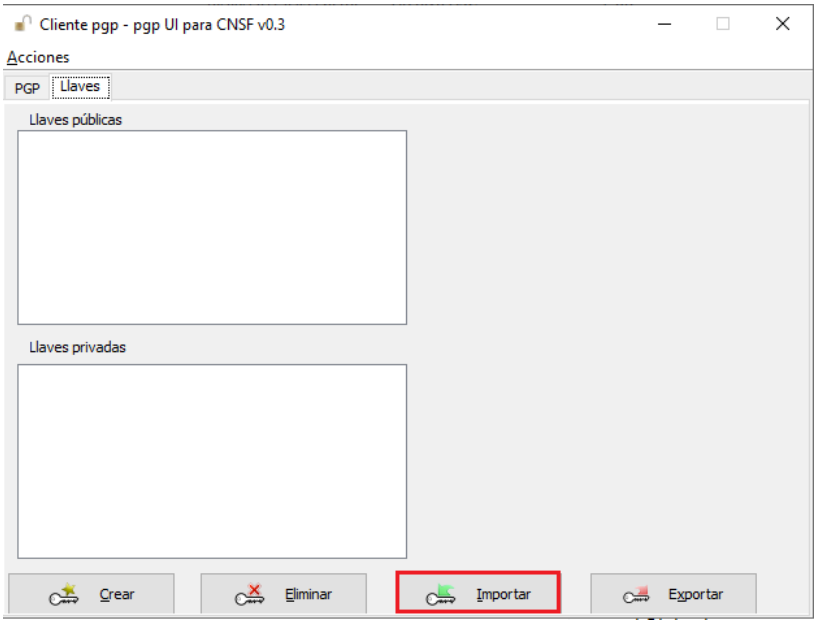
La llave pública de la CNSF, se encuentra dentro del archivo “Ejecutable PGP.ZIP” que previamente se descargó y del cual se extrajeron los archivos contenidos, en la carpeta que se creo previamente para el programa. Se encuentra con el nombre **“CNSF.asc”**



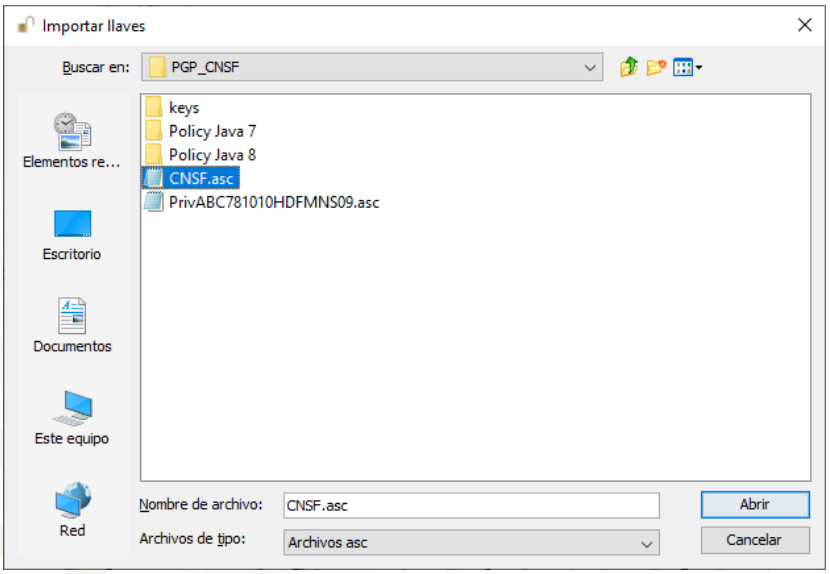
NOTA: La llave pública de la CNSF en conjunto con la llave privada de las instituciones o de las personas supervisadas, siempre se utilizarán para realizar entregas de información o envios a esta Comisión. En ningún momento deberán ocuparse otras llaves para tales efectos.

IMPORTAR LLAVES PUBLICA CNSF Y PRIVADA

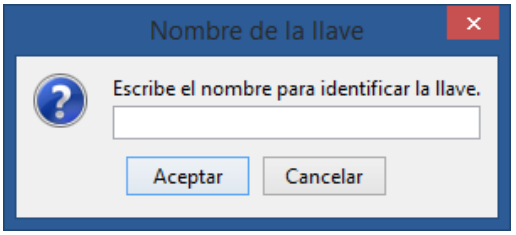
Para importar la llave pública de la CNSF o la llave privada como Institución o Entidad Supervisada, al programa PGP. Dentro de la pestaña de Llaves, seleccionamos la opción de ***"Importar"***. En el presente instructivo se hará el caso práctico importando la llave pública de la CNSF, ya que el procedimiento es el mismo para ambas llaves.



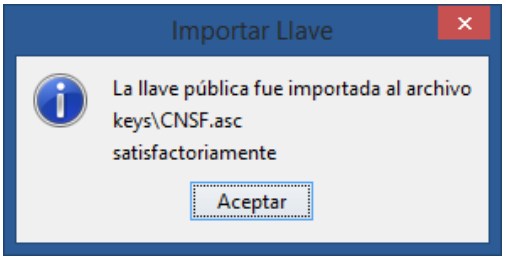
En la siguiente pantalla se debe abrir o seleccionar la carpeta que se generó para el programa.



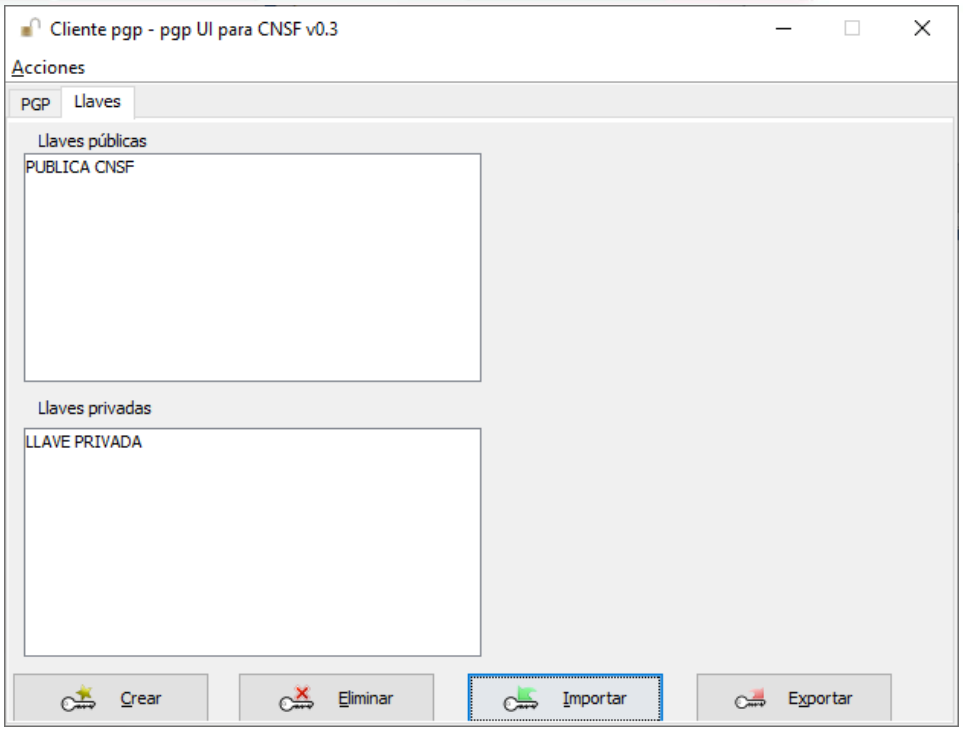
Donde se encuentra el archivo **“CNSF.asc”** que es la llave pública de la CNSF. Se debe seleccionar este archivo y dar clic en **“Abrir”** lo que mostrará la siguiente pantalla, en la cual se solicita ingresar un nombre para identificar la llave.



El nombre de la llave es libre, pero debe de identificar que es la llave de la CNSF. Dar clic en **“Aceptar”** para continuar.



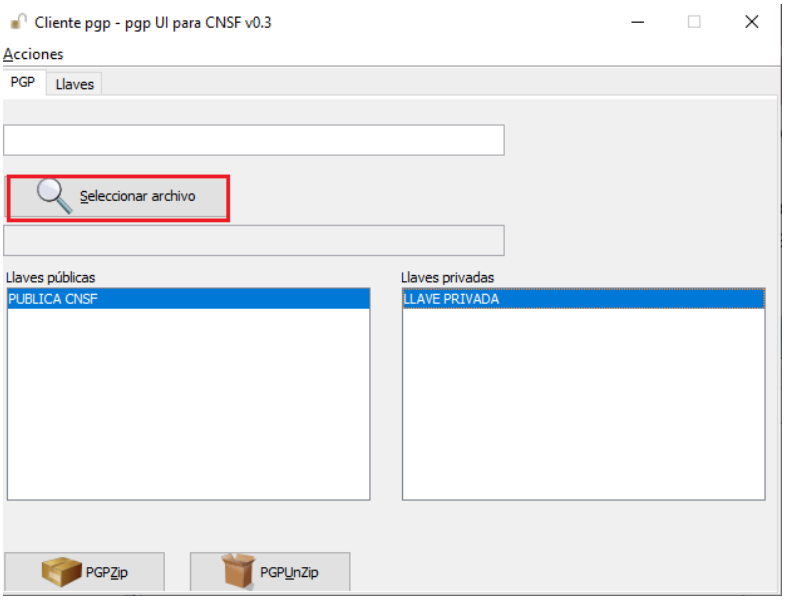
De esta forma queda agregada la llave pública de la CNSF al programa del PGP



Quedando de esta manera, la llave privada de la Institución o Persona Supervisada y la llave pública de la CNSF, las cuales serán utilizadas SIEMPRE en los procesos de cifrado de información, para su envío a esta CNSF.

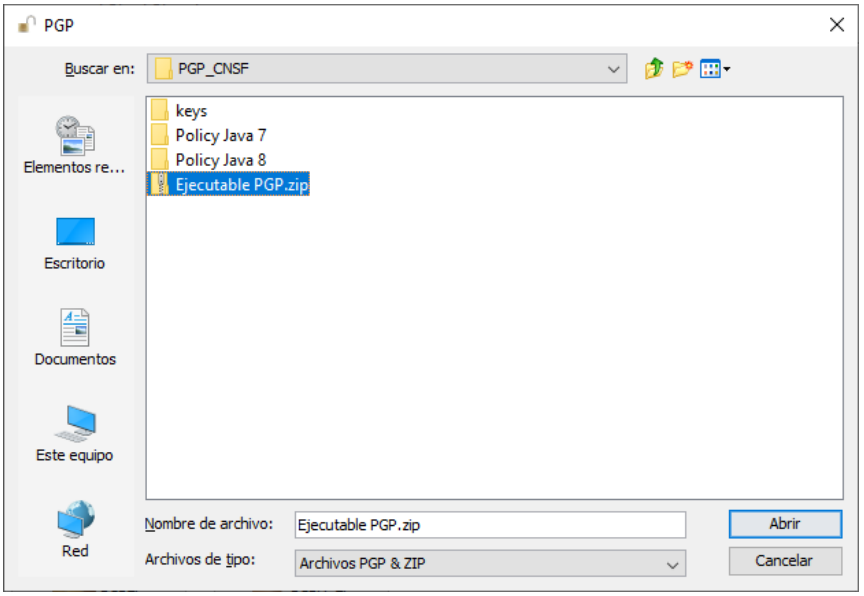
CIFRADO DE ARCHIVOS

Para realizar el proceso de cifrado de archivos, es necesario contar con las llaves, pública de la CNSF y privada de la Institución o Entidad Supervisada que han sido previamente instaladas.

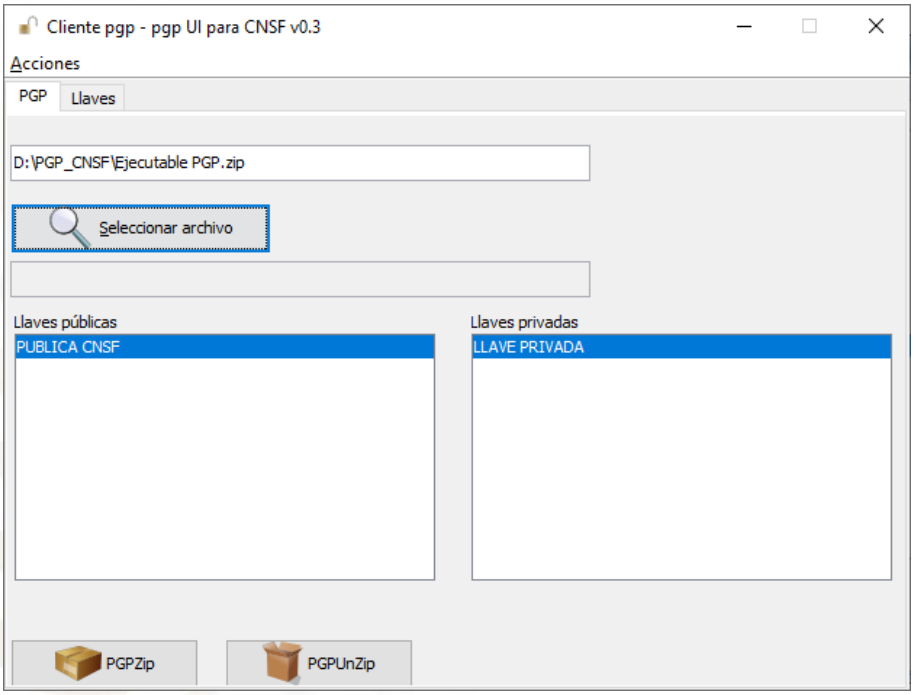


Seleccionando la llave privada de la Institución o Persona Supervisada y la llave pública de la CNSF, dar clic en la opción de ***"Seleccionar Archivo".***

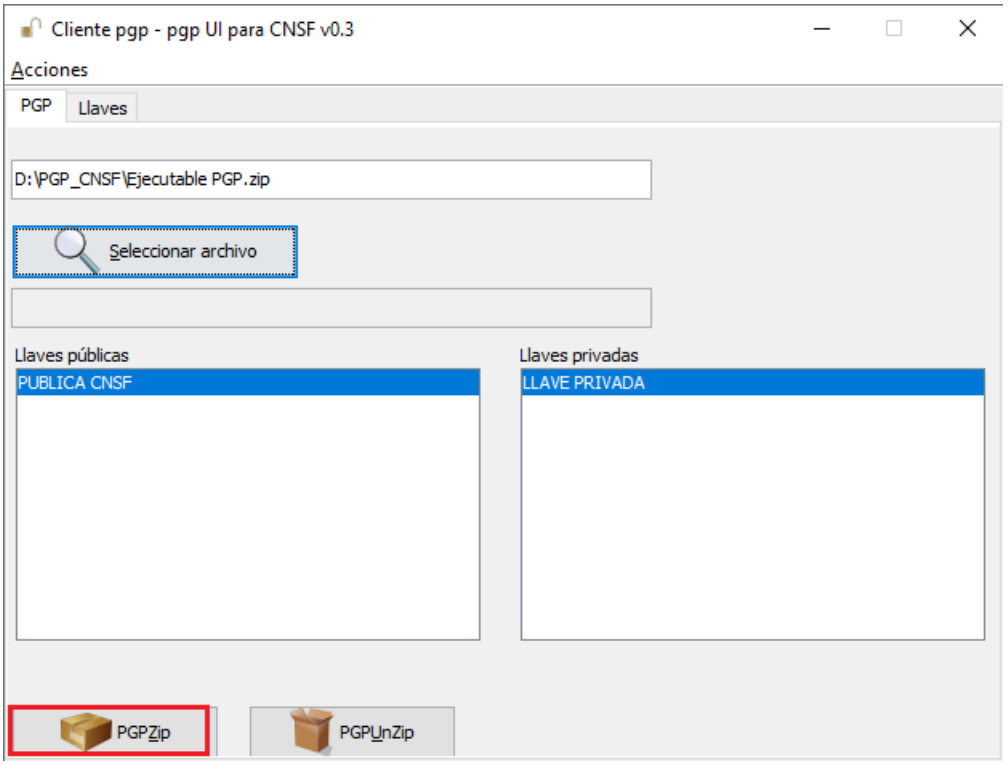
Lo anterior mostrará la pantalla en donde se deberá seleccionar el archivo a cifrar. Una vez seleccionado el archivo, dar clic en ***"Abrir"*** para regresar a la pantalla principal del programa.



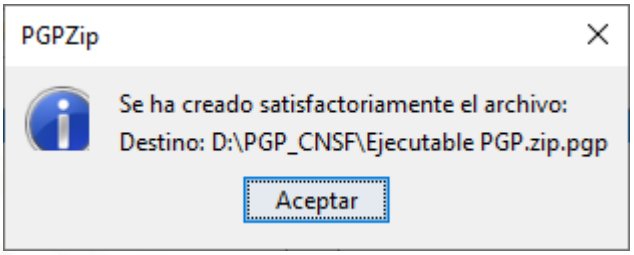
Seleccionar la llave pública de la CNSF y privada de la Institución o Persona Supervisada.



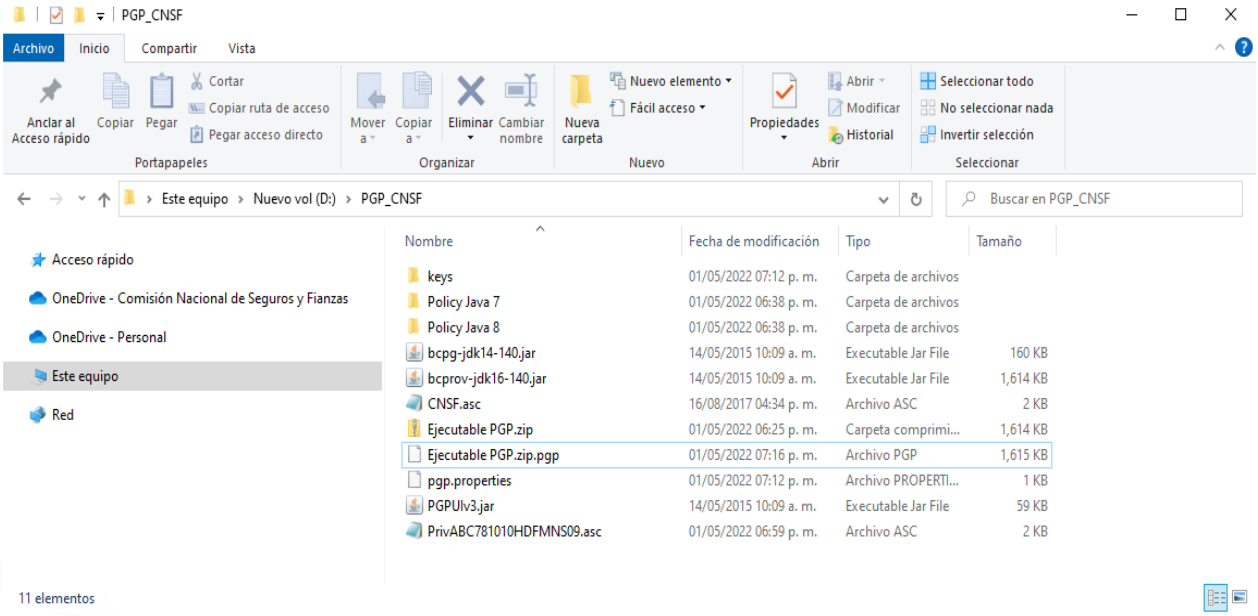
Y Dar clic en el botón de ***PGPZip***



De acuerdo al tamaño del archivo a cifrar, el programa tardará en presentar el siguiente mensaje, el cual indica que se ha creado el archivo satisfactoriamente.



El archivo cifrado se encuentra en la carpeta de donde se seleccionó el archivo para cifrar, con extensión **.zip**. Quedando tanto el archivo .zip como el archivo .zip.pgp en la misma carpeta.



NOTA: Es importante mencionar que se deben seleccionar correctamente la llave pública (CNSF) y privada (Compañía o Persona Supervisada).
La llave pública de la Institución, su único propósito es enviarla a la CNSF. Para el caso de las Personas o Entidades Supervisadas no existe la llave publica, ya que el SEIVE, genera y almacena de manera automática esta llave.