



GOBIERNO
DE ESPAÑA

MINISTERIO
DE TRABAJO, MIGRACIONES
Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

Manual de usuario - Proceso de firma *JNLP* y resolución de incidencias

Aplicaciones normalizadas con el sistema Pros@ (solución *JNLP*)

Dirección de Seguridad de la Información

2/09/2019

Versión: 1.3.2

Clasificación: Público



**CONTROL DE VERSIONES**

Título	Documento tratamiento de firma Electrónica		
Autor	AISS		
Fecha versión 1.0	22/08/2017		
Versión	Fecha	Responsable	Cambios introducidos
1.1	30/10/2017	Dirección de Seguridad, Innovación y Proyectos	Actualización en la resolución de incidencias
1.2	25/09/2018	Dirección de Seguridad, Innovación y Proyectos	Actualización del proceso de firma
1.3	26/09/2018	Dirección de Seguridad, Innovación y Proyectos	Actualización requisitos de java
1.3.1	19/07/2019	Dirección de Seguridad de la Información	Incremento del tiempo disponible para firmar
1.3.2	02/09/2019	Dirección de Seguridad de la Información	Ayuda al proceso de descarga y ejecución del módulo <i>JNLP</i>

INDICE

1. INTRODUCCIÓN.....	4
2. OBJETIVO	5
3. CUADRO DE COMPATIBILIDAD DE JNLP (FIRMA NORMALIZADA)	6
4. CONFIGURACION DE JAVA.....	7
4.1. Configuración en la Máquina Virtual de Java (Windows)	7
4.2. Configuración de safari para Mac/OS.....	8
5. PROCESO DE FIRMA	10
6. RESOLUCIÓN DE INCIDENCIAS	13
6.1. Exención número máximo de reintentos	13
6.1.1. Mensaje que se muestra.....	13
6.1.2. Explicación del error	13
6.1.3. Solución.....	13
6.2. El servidor ha devuelto un valor inesperado.....	14
6.2.1. Mensaje que se muestra.....	14
6.2.2. Explicación del error	14
6.2.3. Solución.....	14
6.3. Error al acceder al certificado.....	15
6.3.1. Mensaje que se muestra.....	15
6.3.2. Explicación del error	15
6.3.3. Solución.....	15
7. ANEXO I. ASOCIACIÓN DEL TIPO DE ARCHIVO JNLP EN WINDOWS.	16
7.1. Descargar el archivo JNLP al disco.....	16
7.2. Asociación del archivo JNLP a la aplicación Java™ Web Start Launcher	17
8. COMUNICACIÓN DE INCIDENCIAS Y SUGERENCIAS	19

1. INTRODUCCIÓN

A medida que los sistemas operativos y navegadores de internet mejoran sus medidas de seguridad, los desarrollos han de adaptarse a las nuevas restricciones que los estándares van dictando. Una de estas restricciones afecta a los desarrollos web basados en Java, al que se le van descubriendo con cierta frecuencia vulnerabilidades que afectan al tratamiento de los datos y a la protección de los mismos.

Los procedimientos de firma electrónica, cada vez más frecuentes en el tratamiento e intercambio electrónico de información, requieren igualmente una vigilancia especial para no incurrir en vulnerabilidades o defectos de forma.

Hasta la fecha, el sistema de firma electrónica más difundido en los servicios electrónicos de la Seguridad Social basados en desarrollos Java se ha venido realizando mediante Applets. Pequeños desarrollos realizados en Java, descargados y ejecutados en cliente que la mayoría de los navegadores han ido restringiendo por seguridad, hasta el punto de no incorporar los *plugins* necesarios para su ejecución.

Para solventar este problema, la Seguridad Social ha adoptado diversas alternativas con el fin principal de permitir aprovechar los desarrollos ya realizados, y dependiendo de la arquitectura del desarrollo utilizado, incorporar un sistema de firma u otro.

Paralelamente, la Seguridad Social está involucrada en un proceso de normalización de desarrollo de aplicaciones que hacen que actualmente se contemplen dos sistemas de firma, uno para aplicaciones normalizadas (basadas en el sistema Pros@) y otro para aplicaciones que no están normalizadas.

En general, para las aplicaciones normalizadas, se ha desarrollado un nuevo proceso de firma basado en el sistema de Ejecución de Protocolo de Red Java (en inglés: *JNLP*) que funciona en todos los navegadores probados (IE, Firefox, Chrome, Edge y Safari) y cuyo proceso se describe en este manual.

Para simplificar la nomenclatura acerca del tipo de firma, el tipo de firma *JNLP* se identifica con el ***Tipo de Firma Normalizado***.









En la Sede se publica un documento con el listado completo de los servicios y su tipo de firma.




2. OBJETIVO

El presente documento describe el nuevo proceso de firma basado en el sistema de *Ejecución de Protocolo de Red Java (JNLP)*, sistema que sustituye al de firma mediante *applets*, en todos aquellos trámites ya **normalizados** de la Sede de la Seguridad Social.

Se recoge un resumen de los sistemas operativos y navegadores que soportan *JNLP*, así como los valores de configuración básicos, incorporándose todas las incidencias que van surgiendo desde su implantación junto a las soluciones.

3. CUADRO DE COMPATIBILIDAD DE JNLP (FIRMA NORMALIZADA)

	 Internet Explorer	 Mozilla Firefox	 Google Chrome	 Safari	 Microsoft Edge
 Windows	✔	✔	✔	⊖	✔
 Mac	⊖	✔	✔	✔	⊖
 Linux	⊖	✘	✘	⊖	⊖

 Funciona
  No funciona
  No Aplica

Cuestiones importantes a tener en cuenta

(1) En Firefox y Chrome, el usuario ha de aceptar la descarga del *JNLP* y posteriormente ejecutar el fichero descargado, haciendo clic en el elemento que se muestra en la barra de descargas (parte inferior de la ventana).

(2) En Safari para Mac, cuando se descarga el *JNLP* no le muestra al usuario ningún aviso para que éste lo pueda ejecutar. El usuario debe abrir la ventana de descargas y ejecutar el último *JNLP* que se haya descargado.

(3) En el caso de Linux, no ha funcionado con ninguna de las versiones habituales, ni para 64 bits ni para 32 bits.

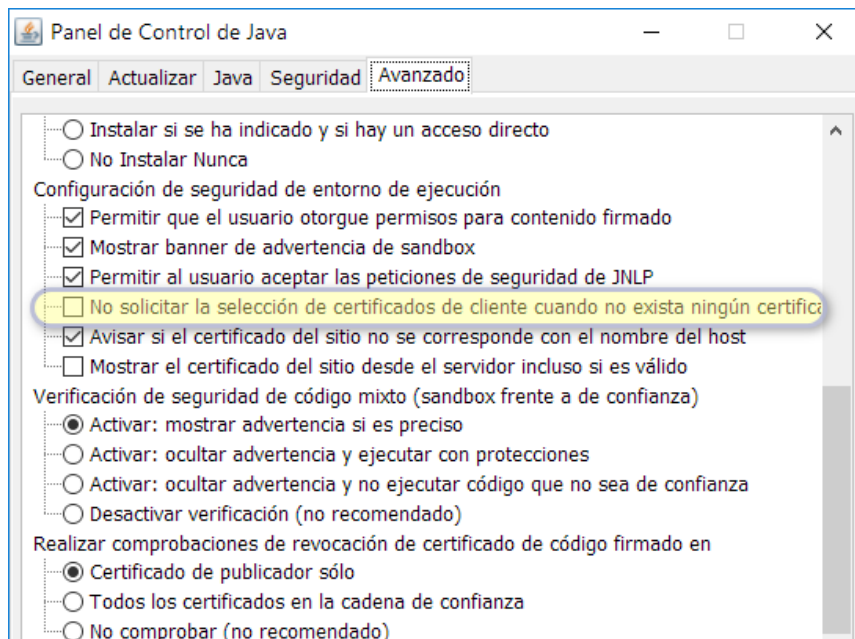
Para una información más detallada de la configuración de los navegadores puede consultar los manuales de configuración de navegadores publicados en la sede de la Seguridad Social en el siguiente enlace de requisitos técnicos:

<http://run.gob.es/bciqer>

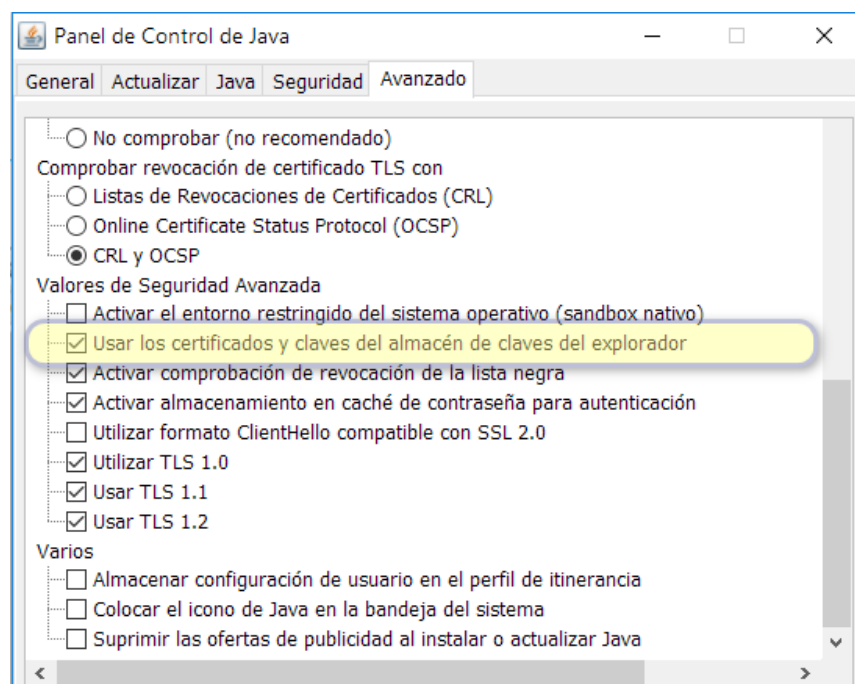
4. CONFIGURACION DE JAVA

4.1. Configuración en la Máquina Virtual de Java (Windows)

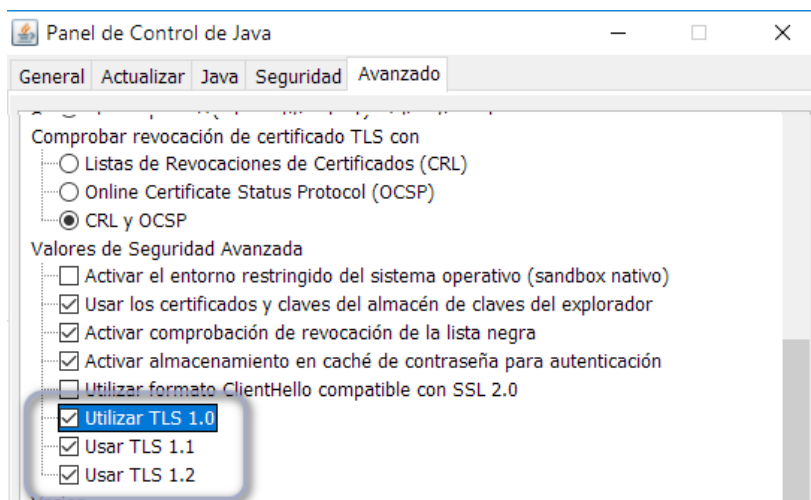
- a. **No activar la opción “No solicitar la selección de certificados de cliente cuando no exista ningún certificado o exista sólo uno”**



- b. **Activar la opción “Usar los certificados y claves del almacén de claves del explorador”**



- c. Activar los protocolos de seguridad en las comunicaciones *TLS* para una correcta conexión con los servidores de la Seguridad Social.



4.2. Configuración de safari para Mac/OS

Por defecto Mac no permite ejecutar aplicaciones descargadas de internet, como en este caso, la descarga del *JNLP* en el proceso de firma. Para que se pueda ejecutar:

- En versiones de Mac Yosemite, Capitán
 1. Preferencias del Sistema > Seguridad y Privacidad. Debemos estar dentro de la pestaña General y ver que abajo del todo aparezca *“Permitir aplicaciones descargadas de Cualquier sitio”*
 2. Si las opciones están bloqueadas hay que pulsar el candado para su desbloqueo.
- En versión de Mac Sierra:
 1. Lo primero será abrir la Aplicación de Terminal: En *“Aplicaciones”* escribir *“terminal”* para buscar esta aplicación.
 2. Una vez abierto escribir el siguiente comando:
`sudo spctl --master-disable`
 3. Se solicitará la contraseña de Administrador para confirmar los cambios.
 4. En Preferencias del Sistema > Seguridad y Privacidad. Debemos estar dentro de la pestaña *“General”*; en la parte inferior aparece: *“Permitir aplicaciones descargadas de Cualquier sitio”*

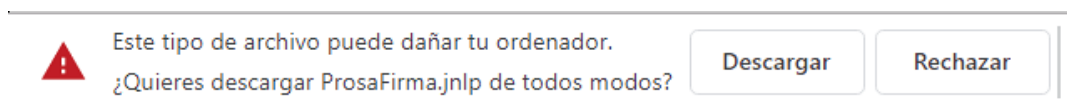
5. Para volver a la configuración original abrir “Terminal” desde Aplicaciones y escribir el siguiente comando:

```
sudo spctl --master-enable
```

5. PROCESO DE FIRMA

- Iniciado el proceso de firma y según el navegador utilizado, puede mostrarse un mensaje de seguridad a la hora de descargar el módulo *JNLP*. Por razones de seguridad las páginas web no ejecutan archivos *JNLP* en la computadora sin el consentimiento del usuario.

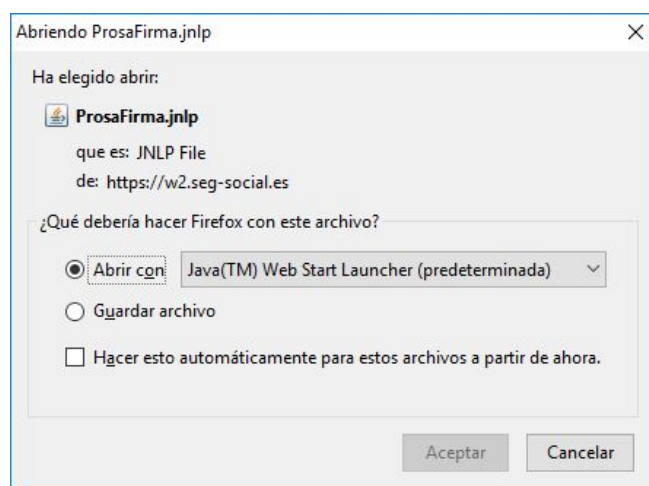
Por ejemplo, en Chrome se mostrará una advertencia en la parte inferior izquierda de la pantalla en la que solicita al usuario aceptar la descarga del módulo *JNLP*:



- Para continuar el proceso de firma es necesario que se pulse *Descargar*; una vez descargado, se mostrará en la parte inferior izquierda el nombre del módulo *JNLP*, y se pulsará, bien en el nombre del módulo o en el desplegable de opciones seleccionando *Abrir* para ejecutarlo.

Si el tipo de archivo *JNLP* no estuviera asociado a ninguna aplicación, el sistema no podrá ejecutarlo directamente, siendo necesario elegir una aplicación para ello.

Por ejemplo, en Internet Explorer se mostrará una ventana como ésta:



Se marcará *Abrir con* y en el desplegable se seleccionará *Java™ Web Start Launcher*. Se aconseja marcar la opción *Hacer esto automáticamente para estos archivos a partir de ahora*.

Si no se mostrara en el desplegable la aplicación *Java™ Web Start Launcher*, y se tiene la certeza de tener instalado *Java* (ya que es obligatorio), esta asociación deberá realizarse a través de las opciones de configuración del sistema (ver apartado *Anexo I*)

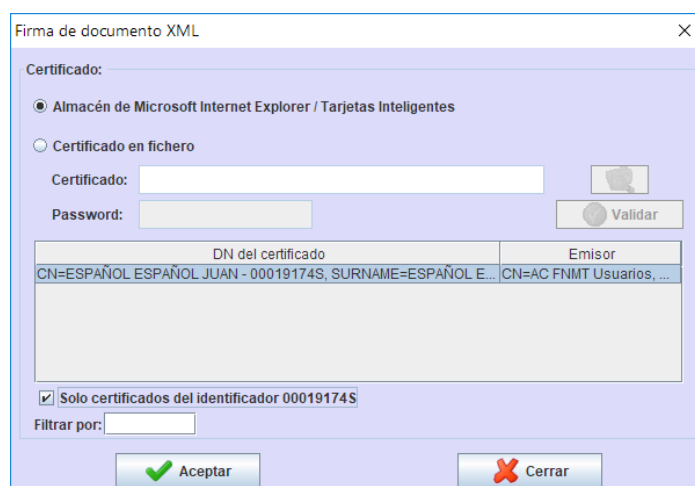
- Iniciado el proceso de firma, el sistema analiza la seguridad el módulo *JNLP* descargado, mostrándose una ventana con información sobre la seguridad del certificado con el que se firmó el propio módulo *JNLP*. Esta firma certifica la integridad y autenticidad del módulo *JNLP*



Si lo desea, puede marcar la opción “No volver a mostrar esto otra vez...” Para que no aparezca esta ventana en futuras ocasiones.

En el enlace inferior *Más información*, podrá obtener información precisa del tipo de certificado que se utilizó para firmar el módulo y la Autoridad de Certificación emisora.

- Tras pulsar en Ejecutar aparecerá la ventana de selección de certificados para realizar la firma:

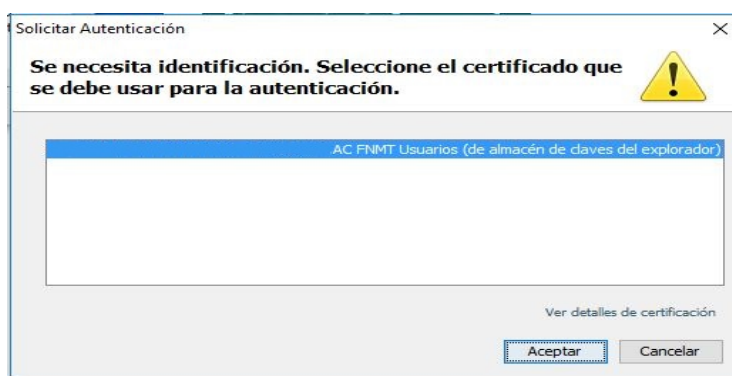


Si se marca la primera opción se podrán seleccionar certificados válidos del almacén del sistema o de una tarjeta criptográfica; en este caso se puede aplicar un filtro en la parte inferior del diálogo para mostrar los certificados de un determinado DNI; esto es útil si se dispone de varios certificados en el almacén.

Si se marca la segunda opción se podrá seleccionar el certificado en formato fichero almacenado en el equipo. Pulsar el icono a la derecha de esta opción para *Examinar* y localizar el certificado deseado, éste debe estar en formato *pkcs#12* (con extensión *pxf* o *p12*). Una vez seleccionado, introduzca la contraseña que protege el archivo.

- A continuación se inicia el proceso de envío del documento firmado a los servidores de la Seguridad Social. Se mostrará una ventana con un listado de los certificados disponibles en el sistema.

Importante: Asegúrese de elegir el mismo que seleccionó al entrar en el servicio web.



Si no ha habido incidencias en el proceso, el documento se enviará correctamente.

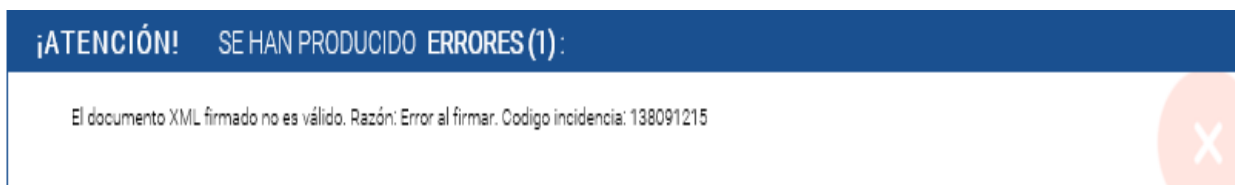
6. RESOLUCIÓN DE INCIDENCIAS

La apariencia de los mensajes de error que pueden mostrarse en el proceso de firma, depende del modo en el que la propia aplicación captura y gestiona las incidencias, por lo tanto, los mensajes que se muestran aquí, **a modo de ejemplo**, pueden diferir algo en su apariencia. No obstante, para este tipo de firma (Tipo 1), por el momento, sólo se han detectado 2 tipos de incidencia:

6.1. Exención número máximo de reintentos

6.1.1. Mensaje que se muestra

Error: El documento XML firmado no es válido. Error al firmar. Código de incidencia:xxxxxxxx



6.1.2. Explicación del error

Este error se produce porque se ha agotado el tiempo de espera en el **momento de elegir el certificado** o bien **no aparece un certificado para seleccionar en pantalla**. Esta situación se puede dar en 2 instantes, ya que puede haber 2 momentos en los que se solicita el certificado. Ver apartado 6 del proceso de firma.

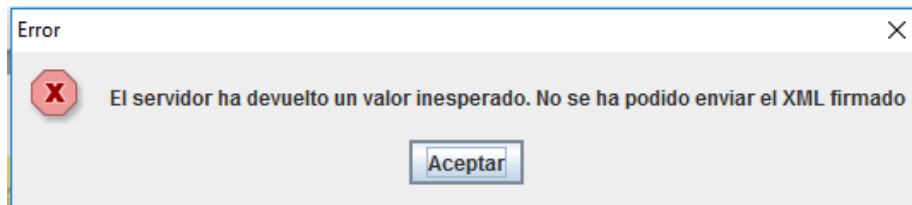
6.1.3. Solución

Configurar Java para que muestre los certificados del almacén. Ver apartado 5.1.

6.2. El servidor ha devuelto un valor inesperado

6.2.1. Mensaje que se muestra

Error: El servidor ha devuelto un valor inesperado, no se ha podido enviar el XML firmado



6.2.2. Explicación del error

Este error es porque no se ha realizado el proceso de firma en el tiempo esperado que dura la ejecución de la firma *JNLP*.

El tiempo que se dispone para realizar el proceso de firma y envío es de 5 minutos.

6.2.3. Solución

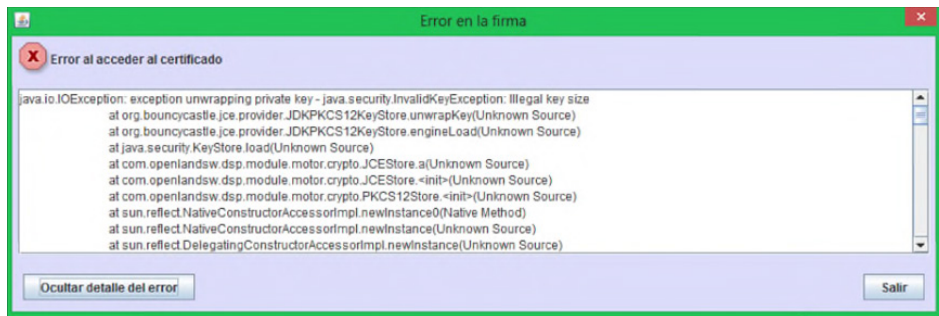
Verificar que el proceso completo se ha realizado dentro del tiempo esperado.

Comprobar que se han atendido adecuadamente los mensajes de alerta y se han respondido adecuadamente los requerimientos de seguridad.

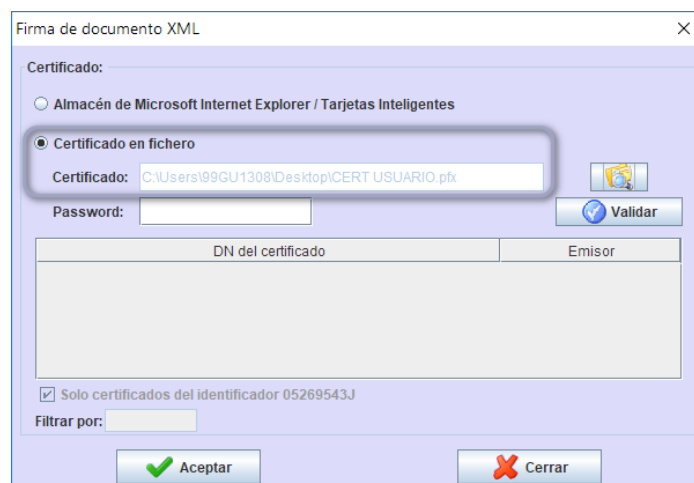
6.3. Error al acceder al certificado

6.3.1. Mensaje que se muestra

Error: Error al acceder al certificado



6.3.2. Explicación del error



Este error puede aparecer sólo en el caso de elegir firmar desde “*Certificado en fichero*”.

El motivo es porque la longitud de clave del certificado no es compatible no permitiendo realizar la firma.

6.3.3. Solución

Actualice a la última versión de Java: <https://java.com/es/>

En las últimas versiones de Java, en la carpeta de instalación se ubican las dos versiones de las políticas de restricción de clave. Localice la siguiente carpeta en su equipo:

`C:\Program Files (x86)\Java\jre1.8.0_152\lib\security\policy\unlimited\`

Copie su contenido a la siguiente carpeta, aceptando la sustitución de los ficheros coincidentes. Es posible que deba otorgar permisos como administrador del equipo para realizar la copia: `C:\Program Files (x86)\Java\jre1.8.0_152\lib\security\policy\`

7. ANEXO I. ASOCIACIÓN DEL TIPO DE ARCHIVO *JNLP* EN WINDOWS.

7.1. Descargar el archivo *JNLP* al disco

- En Internet Explorer

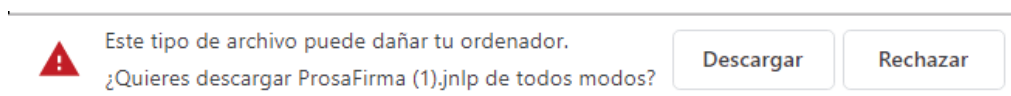
Si por algún motivo el tipo de archivo *JNLP* estuviera asociado a otra aplicación o simplemente no estuviera asociado a *Java™ Web Start Launcher*, se mostrará al pie de página el siguiente mensaje al pie de página:



Pulse en *Guardar* → *Guardar Como...* Ubique el archivo en un directorio donde poder localizarlo posteriormente.

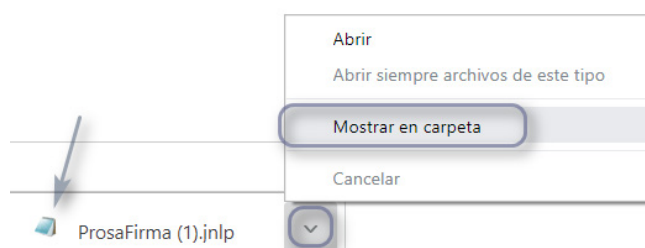
- En Chrome

Tras pulsar *Firmar* y *Enviar* se mostrará en la parte inferior de la pantalla la advertencia de seguridad ya mencionada en el apartado 5:



Pulsar *Descargar*

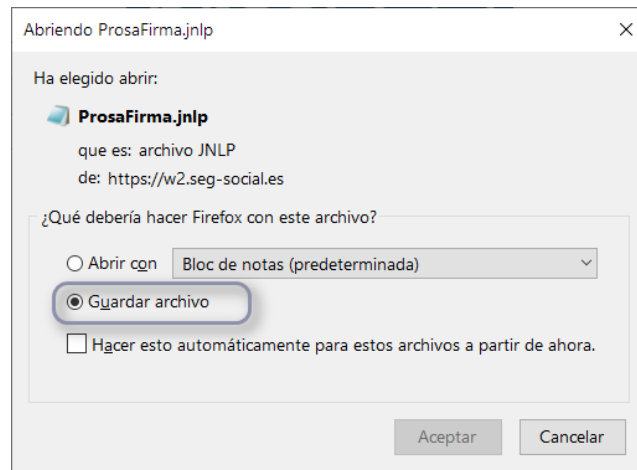
Una vez descargado se puede comprobar que está erróneamente asociado a una aplicación distinta:



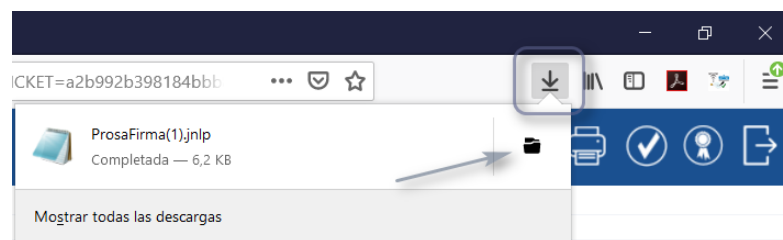
Pulsar en el desplegable y elegir *Mostrar en carpeta*. Se abrirá el administrador de archivos del sistema.

- **En Mozilla Firefox**

Tras pulsar *Firmar* y *Enviar*, se mostrará una ventana como ésta:



Marcar *Guardar archivo* y pulsar *Aceptar*. Pulsar *Ctrl + J* o bien acceder al apartado de descargas, icono que se encuentra en la parte superior derecha del navegador:

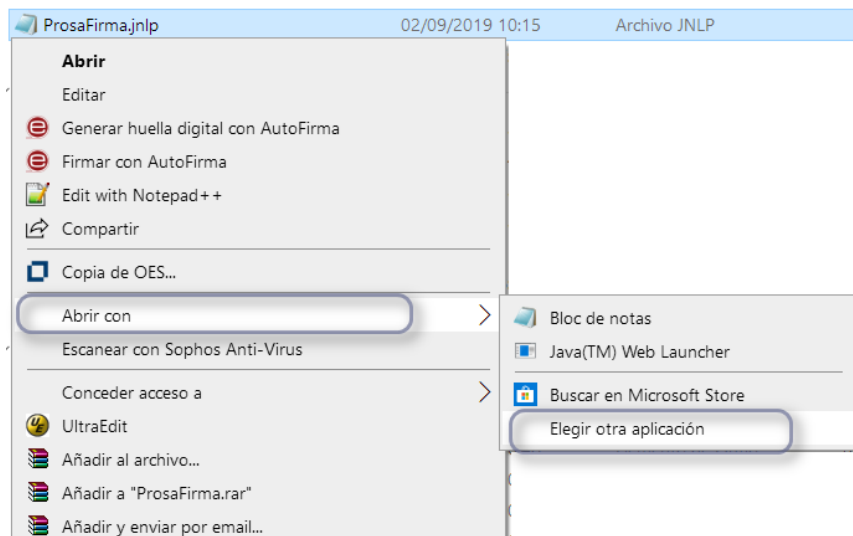


Pulsar en la carpeta asociada al archivo.

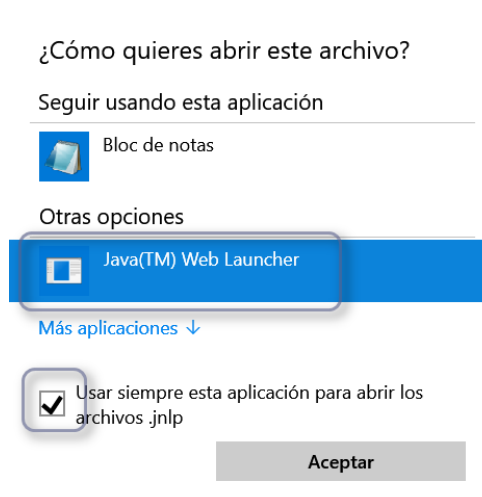
Localizado el archivo descargado en el disco el proceso es común para todos los navegadores:

7.2. Asociación del archivo *JNLP* a la aplicación *Java™ Web Start Launcher*

Una vez salvado el archivo y localizado en el disco, pulsar con el botón derecho del ratón sobre él y seleccionar *Abrir con...* → *Elegir otra aplicación*.



Se mostrará un listado de aplicaciones instaladas en el sistema, seleccionar *Java™ Web Start Launcher*, marcar en la parte inferior *Usar siempre esta aplicación...*



Una vez asociado correctamente, repetir el proceso de firma. Podría ser necesario reiniciar el navegador.

Importante: Si la aplicación *Java™ Web Start Launcher* no apareciera en el listado de aplicaciones del sistema, revise la instalación de Java; si fuera necesario instale la última versión disponible desde: <https://java.com/es/>

8. COMUNICACIÓN DE INCIDENCIAS Y SUGERENCIAS

Si tiene problemas relacionados con el acceso a las aplicaciones, errores en el procesamiento de los datos, incidencias en el proceso de firma, tiene a su disposición el formulario del **Buzón de Consultas** en la página de la Seguridad Social:

<http://run.gob.es/chmavw>