GOBIERNO DE ESPAÑA

MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES

Gerencia de Informática de la Seguridad Social

FIRMA NORMALIZADA

Configuración de entorno para la Firma Normalizada. Solución mediante *Firma Pros@ (jnlp)*

Centro de Seguridad de la Información

22/01/2022

Versión: 2.2

Clasificación: Público

Gerencia de Informática de la Seguridad Social

CONTROL DE VERSIONES			
Título	FIRMA NORMALIZADA (Solución *jnlp*)		
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 *jnlp*
2.0	24/07/2020	Centro de Seguridad de la Información	Actualización de contenidos
2.1	12/04/2021	Centro de Seguridad de la Información	Cambio aceptación certificados de confianza de FNMT-RCM
2.2	22/01/2021	Centro de Seguridad de la Información	Solución direccionamiento erróneo de Red en procesos de firma.

ÍNDICE

1. OBJETIVO

El sistema de **Firma Normalizada** está basado en el sistema de *Protocolo de Ejecución en Red Java* (*jnlp*) y sustituye al de firma mediante *Applets*.

El presente manual describe las pautas de configuración de Java y de navegadores compatibles con este tipo de firma y recoge al final del mismo soluciones a las incidencias más habituales.

1.1. SERVICIOS DE LA SEDE QUE UTILIZAN LA FIRMA NORMALIZADA (*JNLP*)

La práctica totalidad de los servicios web de la Sede de la Seguridad Social utilizan el Sistema de Firma Normalizada. Puede consultar el listado de servicios por tipo de firma en el apartado de Requisitos de Firma Electrónica:

https://sede.seg-social.gob.es/binarios/es/Listados_tipo_firma

En este listado se indica qué servicios admiten Firma Normalizada; si se incluye el icono: permiten además la firma con *certificado centralizado* o ***firma en la nube*** basado en el sistema de identificación de **Cl@ve Permanente**. Puede obtener más información en el portal de Cl@ve:

https://clave.gob.es/clave_Home/clave.html

ÍNDICE

2. COMPATIBILIDAD DE SISTEMAS OPERATIVOS Y NAVEGADORES EN EL SISTEMA DE FIRMA NORMALIZADA

Cuadro de compatibilidad de Sistemas Operativos y navegadores para la firma mediante certificado digital:

FIRMA NORMALIZADA (JNLP) Certificado Digital	Internet Explorer	Microsotf Edge	Google Chrome	Mozilla Firefox	Safari
Windows	✓	✓	✓	ⓘ	
Mac OS			✓	ⓘ	✓
Linux					

Actualmente los siguientes sistemas operativos y navegadores son los únicos compatibles con este tipo de firma:

Sistemas Windows: Internet Explorer, Microsoft Edge, Google Chrome**.**

Sistemas Mac/OS: Safari y Google Chrome.

ⓘ En el caso de Firefox, hay que indicar que sólo funciona en su versión de 64 Bits. Además, requiere que el certificado del usuario esté instalado en el almacén de certificados del Sistema Operativo correspondiente, es decir, para sistemas Windows el certificado debe instalarse en el almacén del sistema visible desde los navegadores Internet Explorer, Chrome o Edge, y en sistemas Mac/OS en el *llavero* de claves. Recomendamos pues el uso de los navegadores indicados en la imagen como compatibles.

ÍNDICE

3. CONFIGURACION DE JAVA

Puede descargar o actualizar la Máquina Virtual de Java desde su página oficial: www.java.com

3.1. CONFIGURACIÓN DE LA MÁQUINA VIRTUAL DE JAVA

- Para acceder al panel de control de Java **en sistemas Windows**:

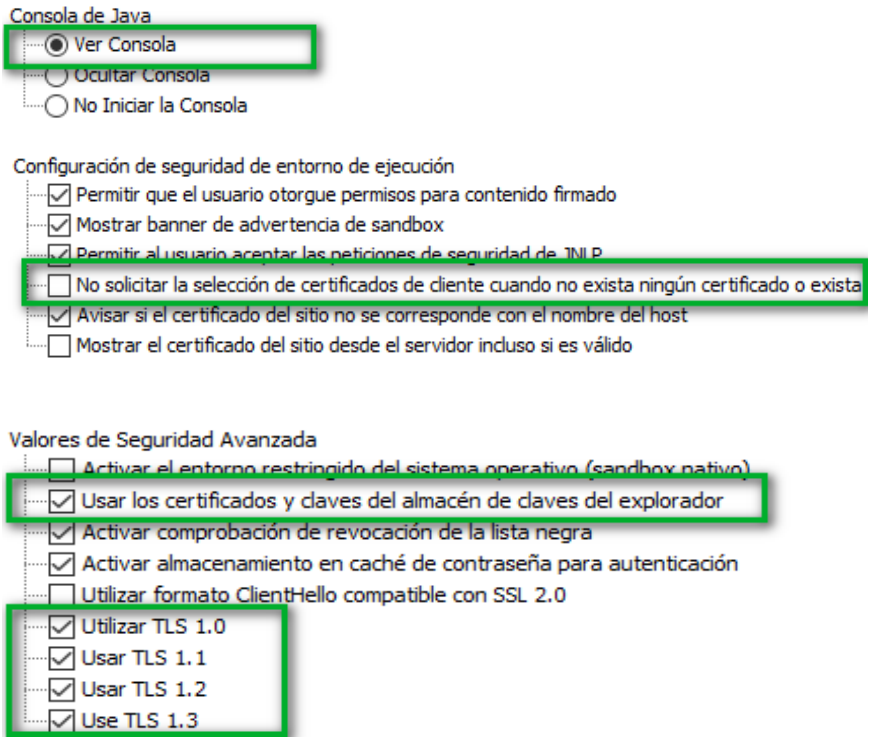
1. Pulse con el ratón en el menú *Inicio* de Windows.
2. Busque Java en los programas que aparecen
3. Haga clic con el botón derecho del ratón sobre *Configurar Java* -> pulse en *Más* -> finalmente ***Ejecutar como administrador***.

- Para acceder al panel de control de Java en **Mac OS X (10.7.3 y versiones posteriores):**

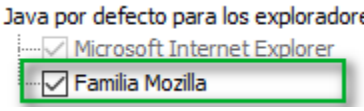
1. Haga clic en el icono de *Apple* en la esquina superior izquierda de la pantalla.
2. Vaya a *Preferencias del sistema*
3. Haga clic en el icono de Java para acceder al panel de control de Java.

3.1.1. Configuración de opciones avanzadas de Java

Una vez dentro del Panel de Control, acceda a la pestaña *"Avanzado"*. Verifique que las siguientes opciones están **marcadas o desmarcadas** tal y como se indica a continuación:



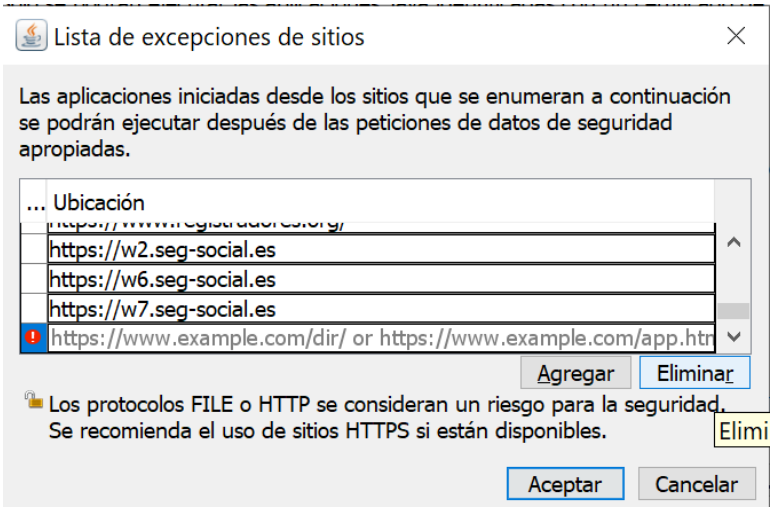
En el caso de que desee utilizar *Firefox* deberá marcar, además:



3.1.2. Inclusión de excepciones en la lista de confianza: Servidores de la Seguridad Social

Para evitar bloqueos de seguridad a la hora de descargar el fichero ***ProsaFirma.jnlp*** se recomienda incluir en la lista de sitios de confianza de *Java* las siguientes direcciones de servidor:

Habiendo accedido al *panel de control de java* en ***modo administrador***, tal y como se indica en el apartado anterior, Acceda a la pestaña *Seguridad* y pulse en el botón ***Editar lista de Sitios***:



Añada las siguientes direcciones:

- https://w2.seg-social.es
- https://w6.seg-social.es
- https://w7.seg-social.es

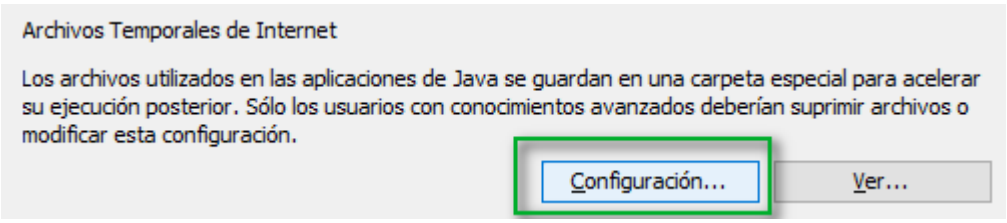
Acepte y continúe con el siguiente apartado de configuración.

3.1.3. Eliminación de datos temporales y restauración de valores de seguridad de java

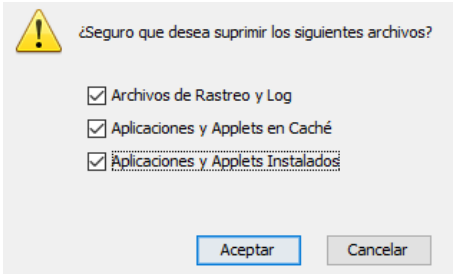
Es recomendable realizar estas operaciones si tiene sospechas que los procesos relacionados *Java* muestran un comportamiento inadecuado o dejan de funcionar.

Abrir el *Panel de Control de Java* en ***modo administrador***, tal y como se explica en el apartado anterior.

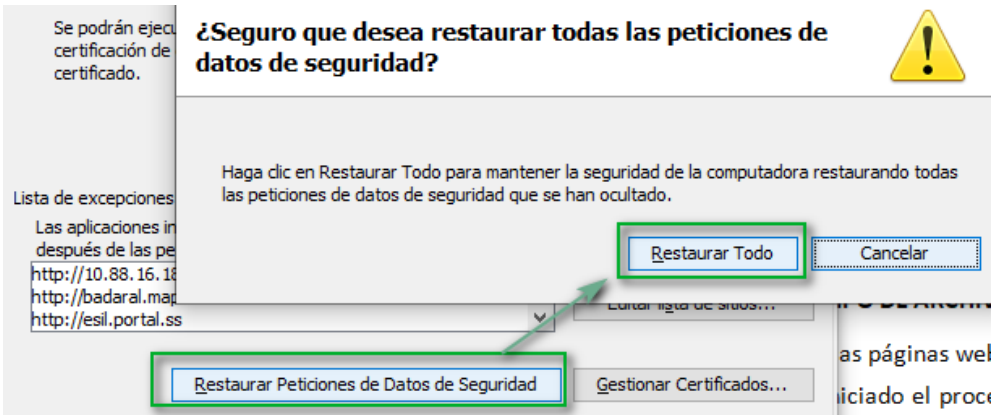
- En la pestaña *General*, apartado *Archivos temporales de internet,* pulse *Configuración:*



A continuación, pulse *Suprimir Archivos,* marque las tres opciones y Acepte.



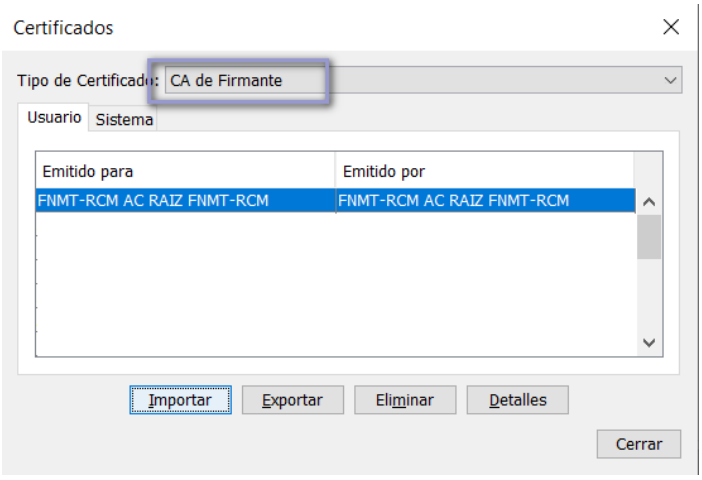
- Posteriormente, en la pestaña *Seguridad*, pulsar en *Restaurar Peticiones de Datos de Seguridad,* finalmente *Restaurar todo:*



3.1.4. Importación del certificado Raíz de la FNMT-RCM en el almacén de Java.

Descargue el certificado Raíz de la FNMT en una unidad local del equipo, siguiendo las indicaciones del *apartado: 4.1.1*

En el panel de control de Java, acceda a la pestaña *Seguridad* -> Botón: *Gestionar Certificados.* una vez allí seleccione la carpeta ***CA Firmante*** y pulse el botón ***Importar.*** Localice el certificado raíz de la FNMT descargado en su equipo; puede que tenga que seleccionar en *Archivos de tipo:* "*todos los archivos"* para localizar el certificado. Una vez localizado selecciónelo y pulse *Abrir.* Debería incorporarse al almacén de certificados como se muestra a continuación:



ÍNDICE

4. CONFIGURACIÓN DE NAVEGADORES

4.1. CERTIFICADOS DE CONFIANZA

Por lo general, la Autoridad de Certificación de la FNMT-RCM (Fábrica Nacional de la Moneda – Real Casa de la Moneda) está incluida en los navegadores. Esta Autoridad de Certificación valida y da confianza a los certificados electrónicos de los servidores de la Seguridad Social y al certificado con el que se ha firmado (*ProsaFirma.jnlp*), No obstante, se aconseja verificarlo y en caso de producirse algún error el proceso de firma por falta de confianza en la entidad firmante deberá instalar los siguientes certificados raíz e intermedio de la FNMT-RCM.

4.1.1. Descarga de los certificados Raíz e intermedios de FNMT-RCM

La página de descarga de certificados de la Autoridad de Certificación de la FNMT-RCM es:

Certificados raíz de la FNMT - Sede

Descargar los siguientes certificados a una unidad local del equipo.

Certificado Raíz:

Descarga certificado AC Raíz FNMT-RCM

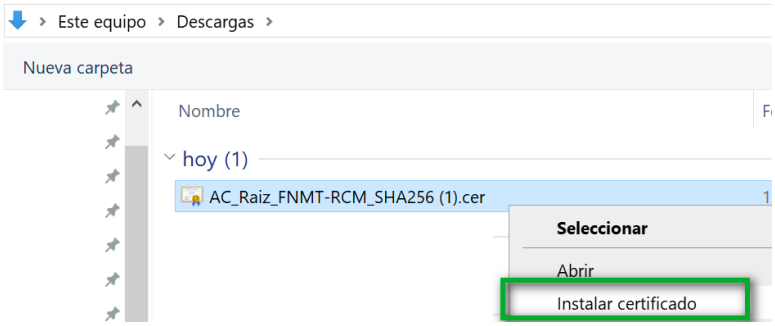
Certificados Intermedios:

Descarga certificado AC FNMT Usuarios

Descarga certificado AC Componentes Informáticos

4.1.2. Instalación de los certificados Raíz e intermedios de FNMT-RCM en IExplorer, Chrome y Edge

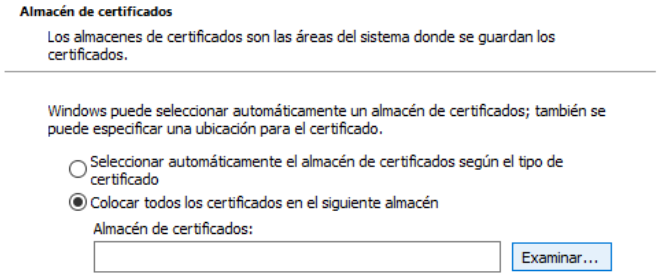
Localice la carpeta donde se ha descargado los certificados y en cada uno pulsar con el botón derecho del ratón y seleccionar: "*Instalar certificado*".



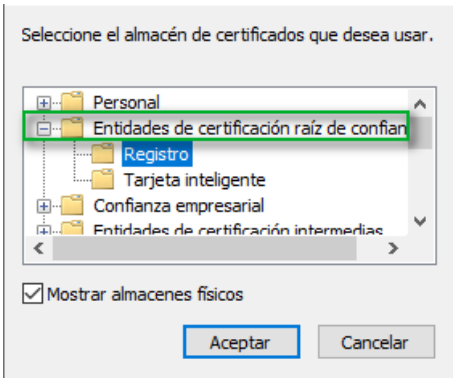
Se iniciará el proceso de importación.

Seleccione *"Usuario actual" y* Pulse "*Siguiente*".

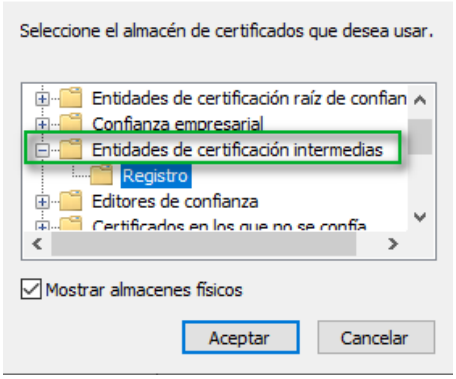
Marque "*Colocar todos los certificados en el siguiente almacén*" y pulse "*Examinar*"



Para el certificado Raíz: Marque la opción "*Mostrar almacenes físicos*" y seleccione la carpeta "***Entidades de certificación Raíz de Confianza***" -> Carpeta "*Registro*". Pulse "*Aceptar*".

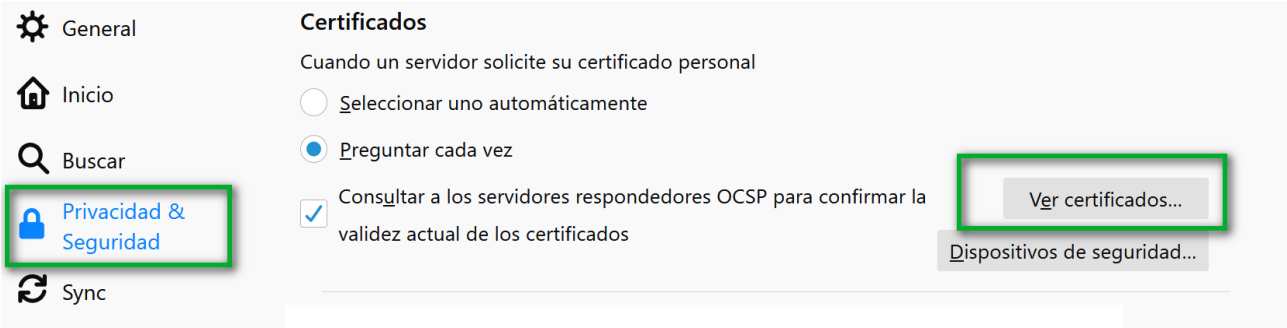


Para los certificados intermedios: Marque la opción "*Mostrar almacenes físicos*" y seleccione la carpeta "***Entidades de certificación intermedias***" -> Carpeta "*Registro*". Pulse "*Aceptar*" y "*finalizar*".

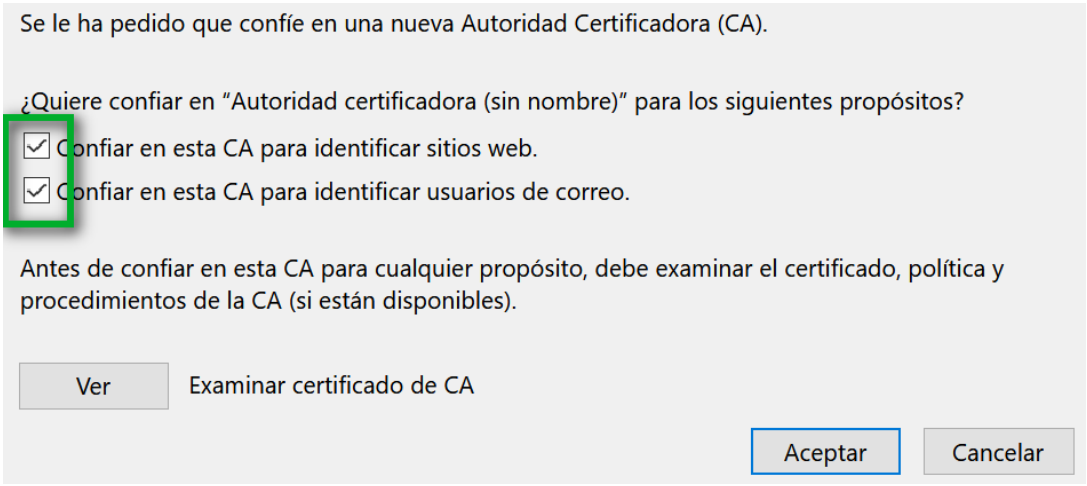


4.1.3. *Instalación de los certificados Raíz e intermedios de FNMT-RCM en Firefox*

Abra *Firefox* y seleccionar *Herramientas -> Opciones -> Privacidad y Seguridad -> Ver Certificados*



Seleccione la pestaña "***Autoridades***" y pulse "***Importar***". Localizar y seleccionar el certificado raíz de la FNMT descargado. Habilitar "***Confiar en esta CA***" en ambos casos y acepte.

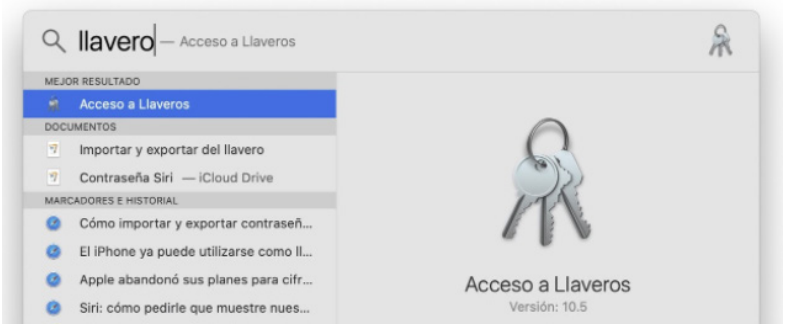


Repetir este mismo procedimiento con el resto de los certificados intermedios descargados.

4.1.4. *Instalación de los certificados Raíz e intermedios de FNMT-RCM en Safari (MacOS)*

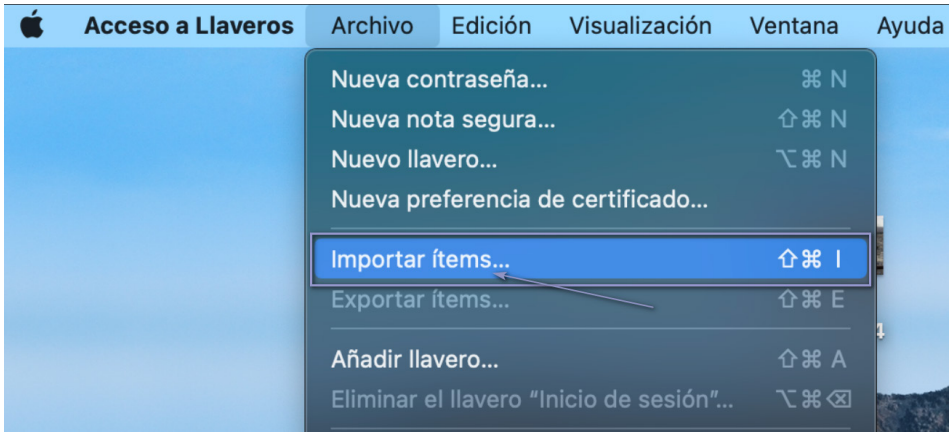
(*) Es posible que las imágenes siguientes difieran según la versión de Mac/OS que disponga

Con la utilidad ***Spotlight*** buscar y ejecutar la aplicación ***Acceso a Llaveros.app***

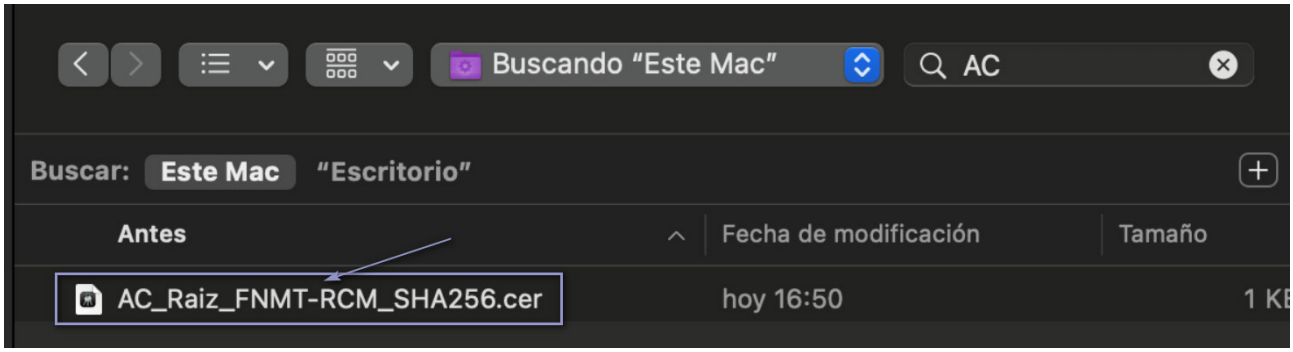


Pulsar en la **Categoría "*Certificados*"** donde importaremos los certificados raíz e intermedios descargados.

En el menú de la barra superior despliegue la opción "***Archivo"*** y pulse en "***Importar elementos"*** **o** **"*Importar Items"***



Localice el certificado a importar, una vez seleccionado pulsar "***Abrir***".



El certificado quedará instalado en el llavero:

Repita este mismo procedimiento con el resto de los certificados.

ÍNDICE

5. ARCHIVO *PROSAFIRMA.JNLP*

Por razones de seguridad los navegadores por defecto no descargan o ejecutan ciertos tipos de archivos sin el consentimiento del usuario. El usuario deberá siempre aceptar la descarga y la ejecución del archivo ***ProsaFirma.jnlp*** para que el proceso de firma se lleve a cabo.

Si tras descargar el archivo y ejecutarlo, la firma no progresa o bien se muestra un error, es muy probable que el tipo de archivo *jnlp* no esté correctamente asociado a la aplicación ***Java™ Web Start Launcher***, módulo que se incluye en la *Máquina Virtual de Java* (*JRE*), por lo tanto, si no dispone de Java o si tiene que actualizarlo, antes de continuar, siga las instrucciones descritas en el *apartado 3* de este manual.

A continuación, se explica el modo de asociar adecuadamente el tipo de archivo *jnlp* a *Java™ Web Start Launcher*.

5.1. DESCARGA DEL ARCHIVO *PROSAFIRMA.JNLP* AL DISCO

Iniciado el proceso de firma y según el navegador utilizado, los mensajes de seguridad mostrados a la hora de descargar el módulo *Prosafirma.jnlp* pueden variar:

- **En Internet Explorer**

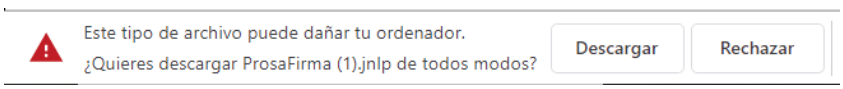
  Si por algún motivo el tipo de archivo *jnlp* estuviera asociado a otra aplicación o simplemente no estuviera asociado a *Java™ Web Start Launcher*, se mostrará al pie de página el siguiente mensaje:

  Pulse *Guardar* o *Guardar Como,* ubicando 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 siguiente:

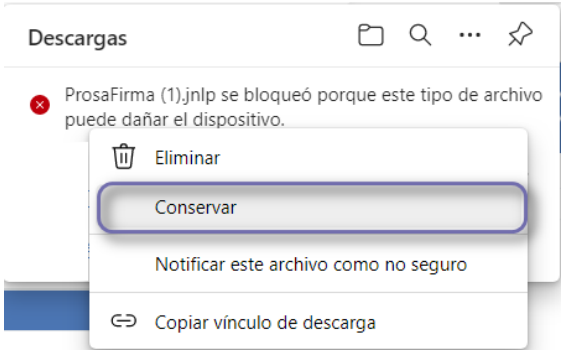
  Pulsar ***Descargar***.

Una vez finalizada la descarga, pulsar en el desplegable y elegir *Mostrar en carpeta.*

Se abrirá el administrador de archivos del sistema.

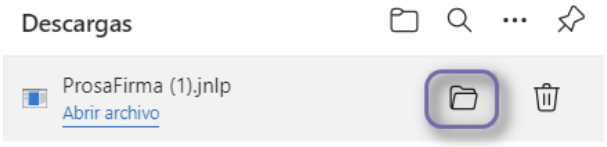
- **En Edge**

Tras pulsar *Firmar y Enviar* se puede mostrar en la parte superior derecha de la pantalla la advertencia: "*ProsaFirma.jnlp se bloqueó porque este tipo de archivo puede dañar el dispositivo.*"



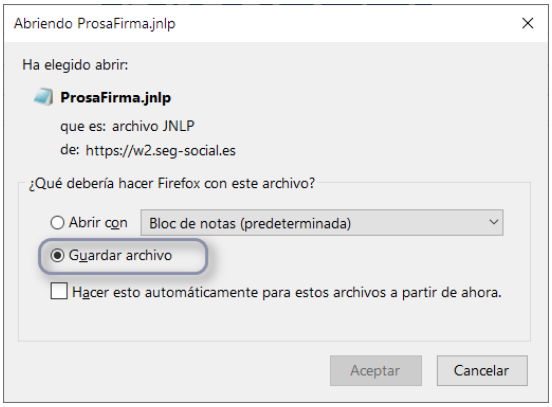
Pulse en los tres puntos de la derecha (*más acciones*) y seleccione *"Conservar"*

Finalizada la descarga pulsar en el icono de la carpeta a la derecha del nombre del archivo:

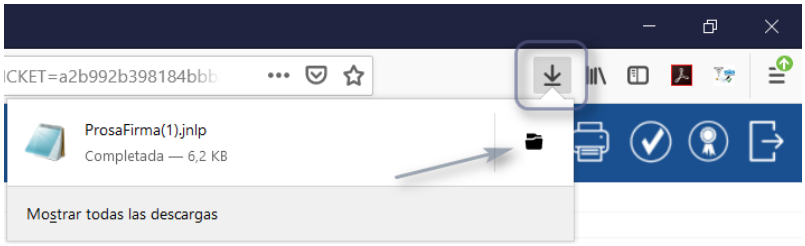


- **En Mozilla Firefox**

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



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

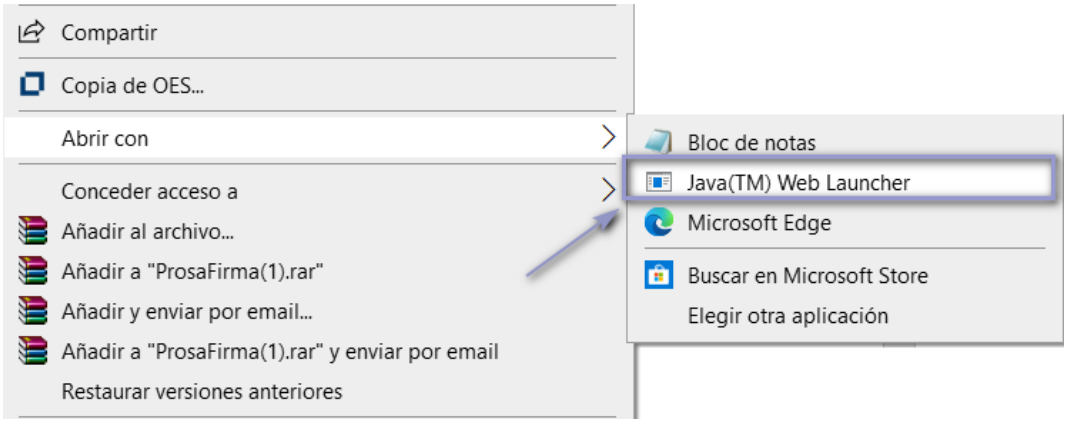


Pulsar en la carpeta asociada al archivo y situarse en la carpeta donde está ubicado.

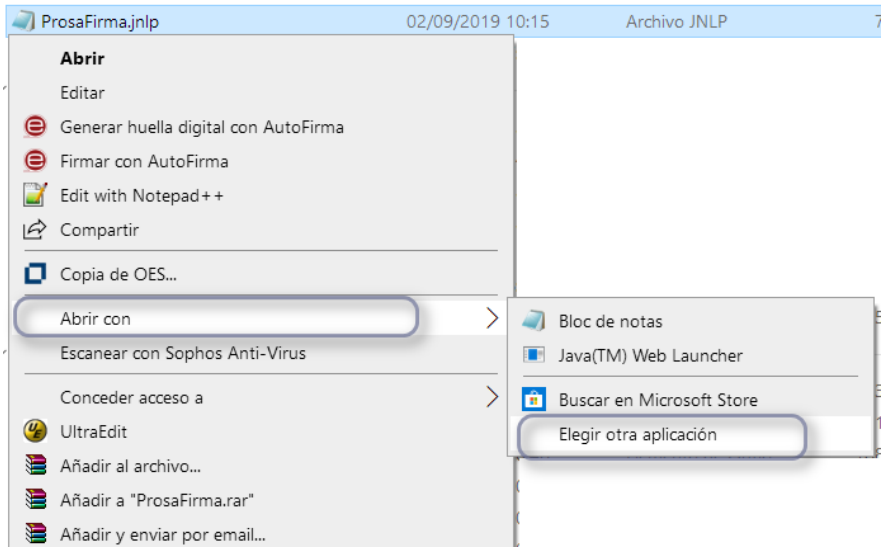
5.2. ASOCIAR EL TIPO DE ARCHIVO *JNLP* A LA APLICACIÓN *JAVA™ WEB START LAUNCHER*

5.2.1. En Windows

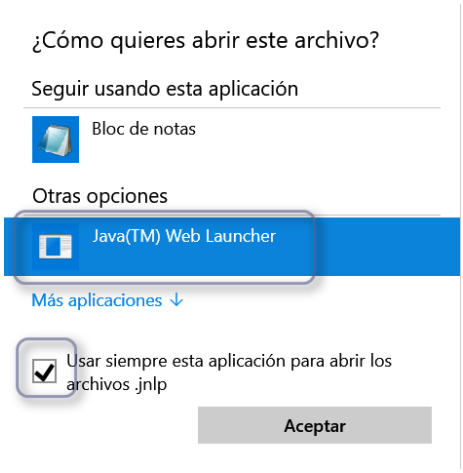
Una vez salvado el archivo y localizado en el disco, pulsar con el botón derecho del ratón sobre él y seleccionar "*Abrir con"* y seleccionar posteriormente "*Java ™ Web Launcher"*



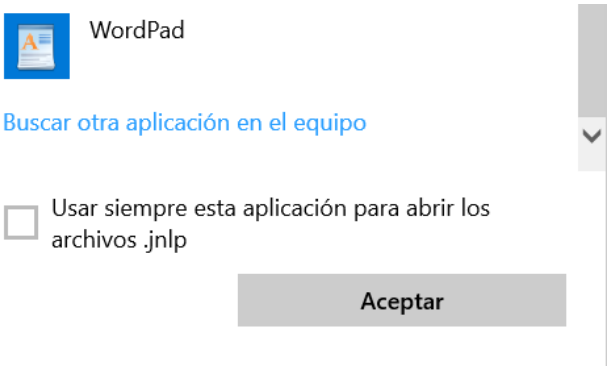
Si no aparece en el listado, seleccionar *Elegir otra aplicación*



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



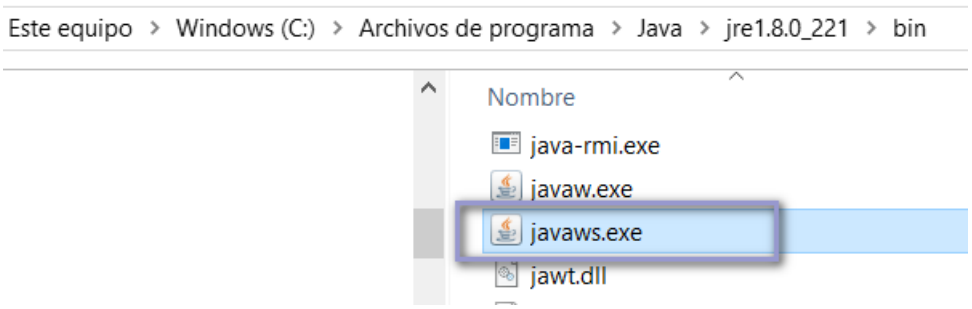
Si tampoco apareciera en el listado de aplicaciones por defecto, pulse en *Más Aplicaciones* y al final del listado seleccionar *Buscar otra aplicación en el equipo:*



Abierto el administrador de archivos, situarse en *C:\Archivos de programa\Java\Jre<versión>\Bin*

(*) puede que su versión de java sea de 32 bits, en cuyo caso se encontrará en C:\archivos de programa x86\java\jre<versión>\bin

Seleccione la aplicación ***javaws.exe***



5.2.2. En Mac/OS

a) Habilitar la descarga y ejecución de aplicaciones desde internet:

Por defecto *Mac* no permite ejecutar aplicaciones descargadas de internet, y éste puede ser el caso al descargar el fichero *ProsaFirma.jnlp*, por lo tanto, habrá que desbloquear esta opción de seguridad.

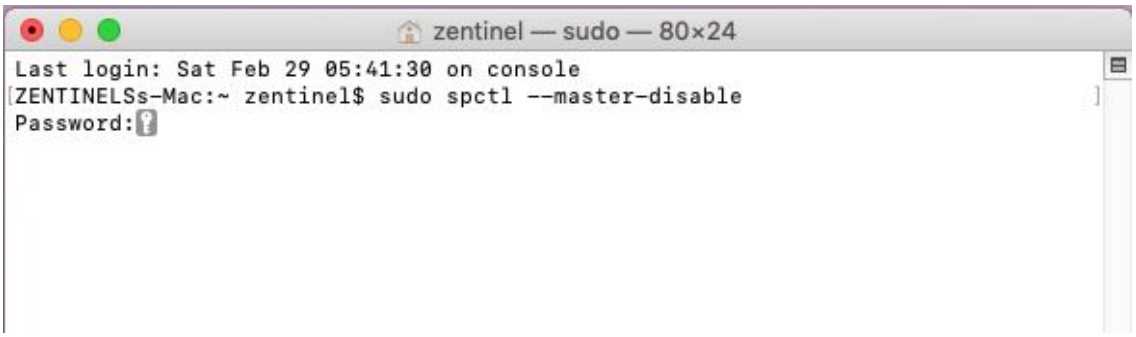
(*) Hay que tener en cuenta que las imágenes pueden variar según la versión de Mac/OS que se tenga.

- **En versiones Yosemite, Capitán**:

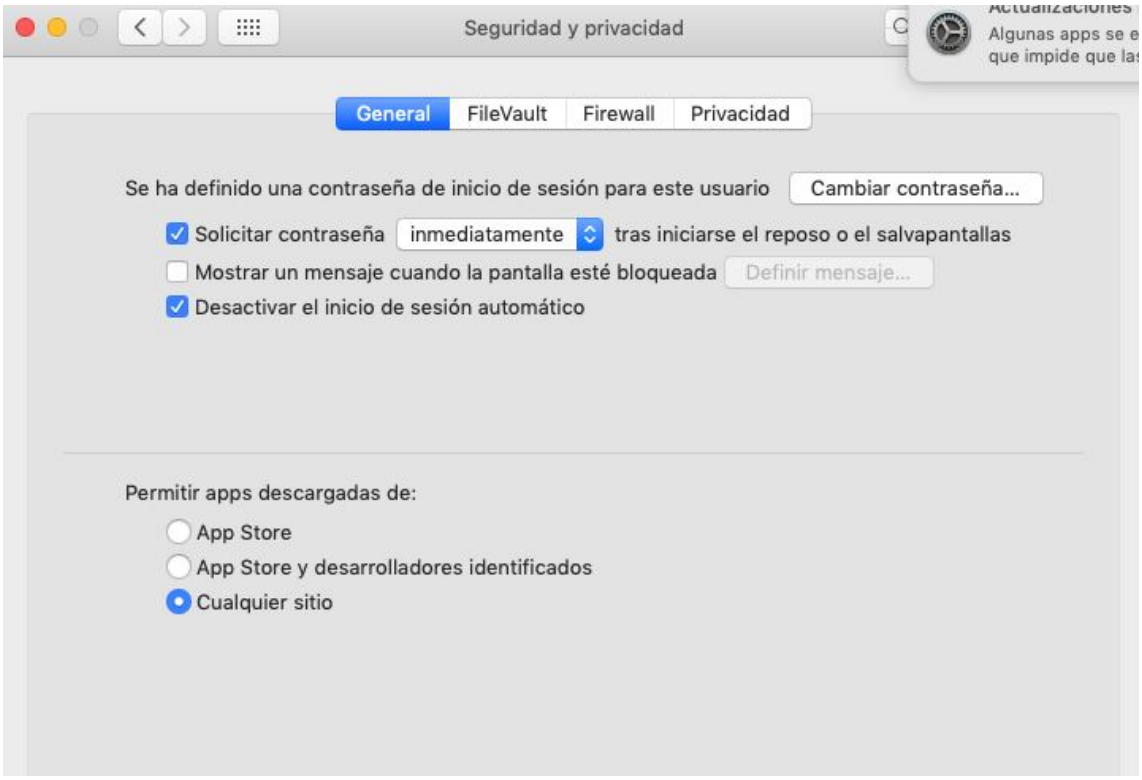
1. *Preferencias del Sistema > Seguridad y Privacidad*. Debemos estar dentro de la pestaña General y verificar que se muestra la opción: *"Permitir aplicaciones descargadas de Cualquier sitio"*
2. Si la opción está bloqueada, pulse el candado para su desbloqueo.

- **versiones posteriores**

1. Lo primero será abrir la ***Aplicación de Terminal***: En "*Aplicaciones*" escriba "*terminal*" para buscar esta aplicación.
2. Una vez abierto escriba 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*, dentro de la pestaña "*General*"; en la parte inferior verifique que está marcada la opción correspondiente para ***Permitir aplicaciones descargadas de cualquier sitio.***

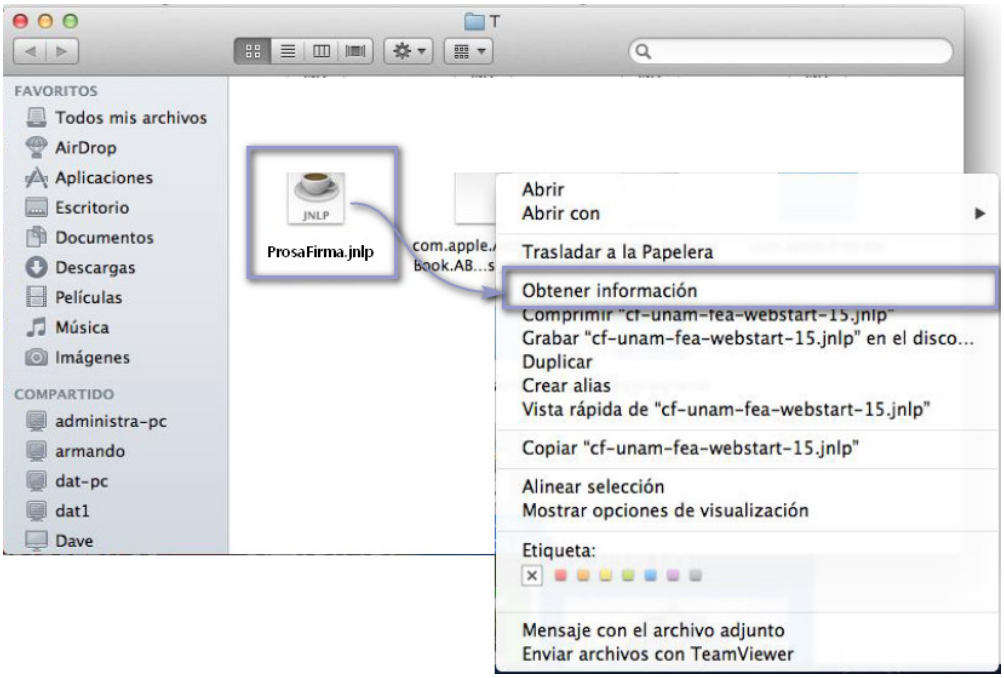


(*) Si deseara volver a la configuración original abra la ***Aplicación de Terminal*** y escriba el siguiente comando:

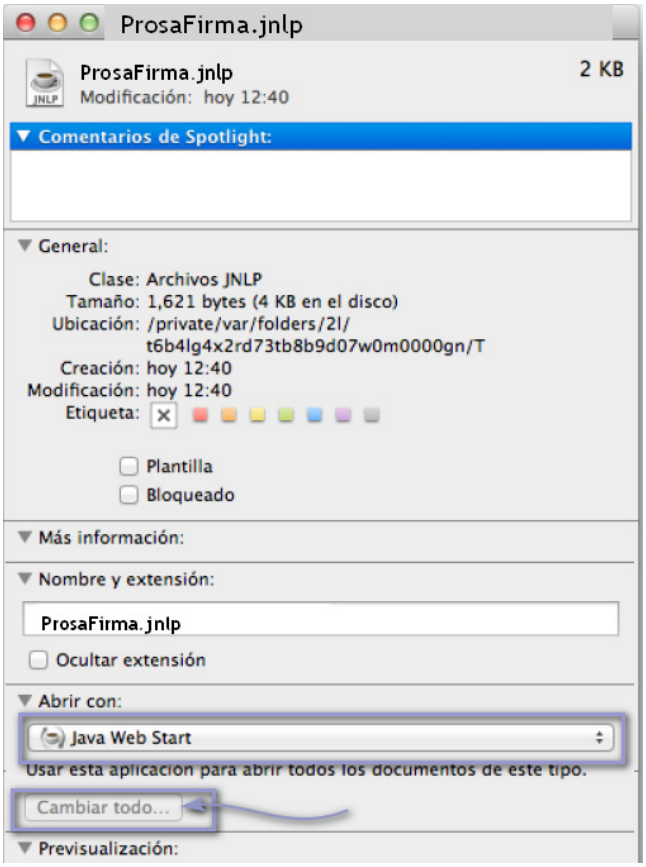
sudo spctl --master-enable

b) Asociar el tipo de archivo jnlp a la aplicación Java™ Web Start Launcher:

Localice mediante *Finder* el archivo descargado *ProsaFirma.jnlp.* Pulse con el botón derecho del ratón sobre él para que aparezca el menú emergente:



Seleccione *Obtener información*. En la parte inferior de la siguiente ventana seleccione la aplicación *Java Web Start,* y presione el botón *Cambiar todo* para que el cambio sea permanente.

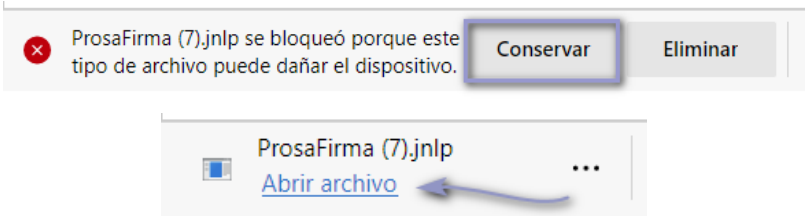


ÍNDICE

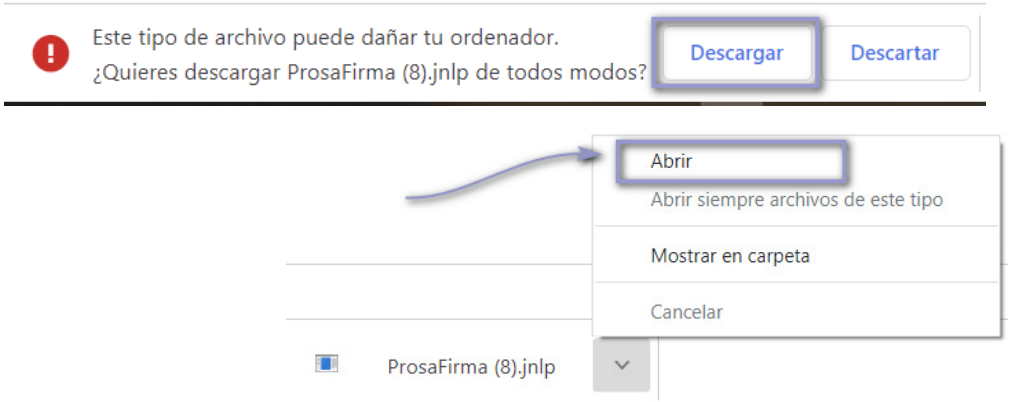
6. DESCRIPCION DEL PROCESO DE FIRMA NORMALIZADA (*JNLP*)

Una vez configurado Java, el navegador a utilizar y habiendo asociado correctamente el tipo de archivo *jnlp* a *Java Web Start (Java web Launcher),* una vez se pulse el botón *Firmar* se iniciará la descarga de *ProsaFirma.jnlp.* Según el navegador utilizado, los mensajes de aviso de seguridad pueden variar, en todos los casos deberá aceptar la descarga del archivo *jnlp* y posteriormente abrirlo para su ejecución:

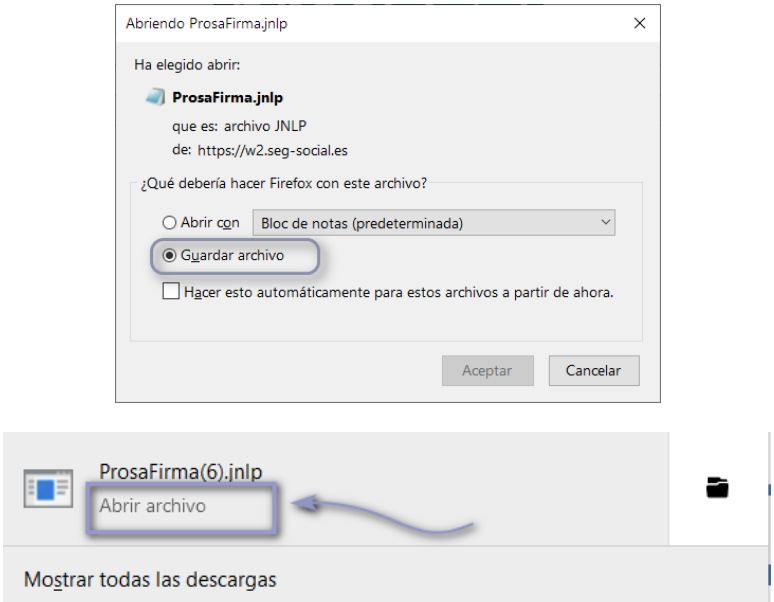
- **En *Edge*:**



- **En *Chrome*:**



- **En *Firefox*:**

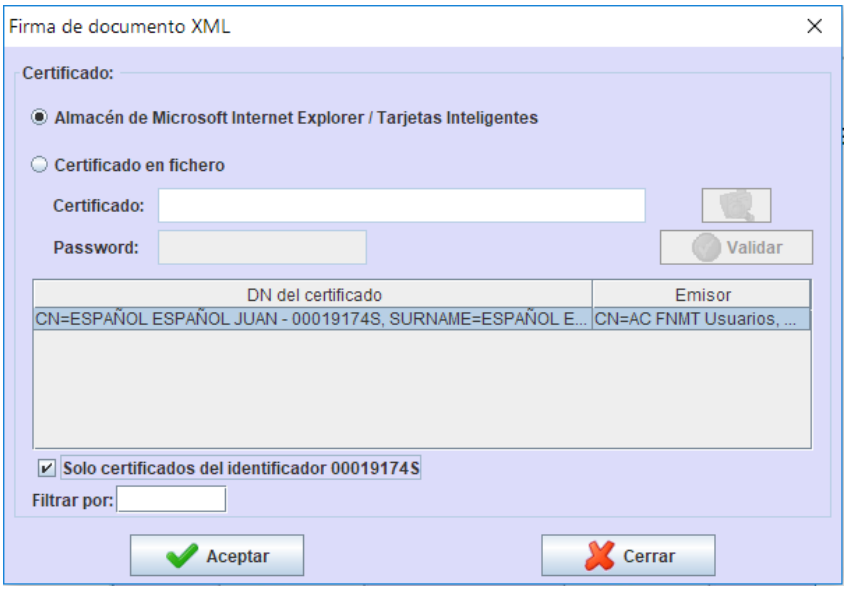


- En ***IExplorer*** **y** ***Safari:*** si están correctamente configurados y asociado el tipo *jnlp* a *Java Web Start*, la aplicación se iniciará inmediatamente.

Una vez Iniciado el proceso de firma, el sistema analiza la seguridad del 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.

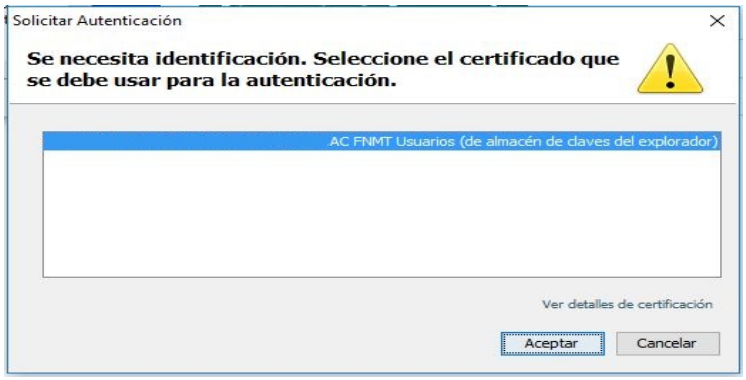
Tras pulsar en *Ejecutar* aparecerá la ventana de selección de certificados para realizar la firma:



Si se marca la primera opción se podrá seleccionar uno de los 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.

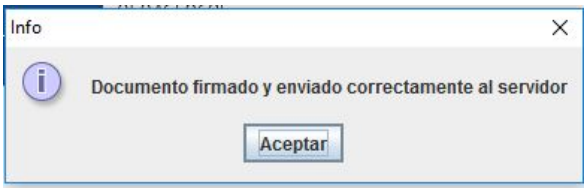
Si se marca la segunda opción se podrá seleccionar el certificado en fichero almacenado en el equipo. Pulsar el icono a la derecha de esta opción para *Examinar* y localizar el certificado deseado, éste debe estar en formato *pkcs#12* (con extensión *pfx* o *p12*). Una vez seleccionado, introduzca la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

A continuación, se inicia el proceso de envío del documento firmado a los servidores de la Seguridad Social. Dependiendo del navegador utilizado puede aparecer una ventana con un listado de los certificados disponibles en el sistema.



Importante: Si se le solicita en este punto seleccionar un certificado, asegúrese de **elegir el mismo certificado** que seleccionó para identificarse al iniciar la aplicación o servicio.

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



ÍNDICE

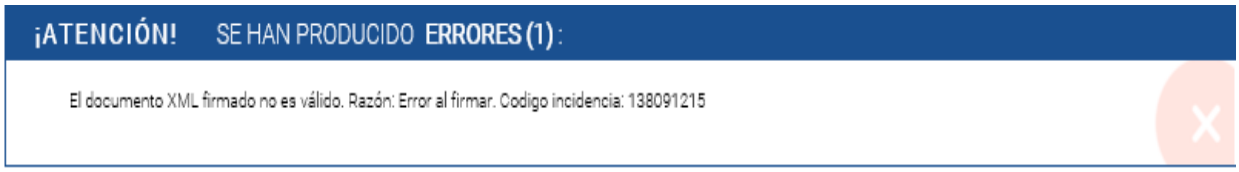
7. RESOLUCIÓN DE INCIDENCIAS

Los mensajes de error que se muestran aquí pueden diferir algo en su apariencia a los que usted visualizar en su equipo.

7.1. SUPERADO NÚMERO MÁXIMO DE REINTENTOS

7.1.1. Mensaje que se muestra

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



7.1.2. Explicación del error

Este error se puede producir por diversos motivos y deberá ser analizada por nuestro equipo de soporte.

7.1.3. Solución

Para su análisis y resolución, apunte el código de incidencia y abra una consulta a través del *Buzón de Consultas* de la página de la Seguridad Social:

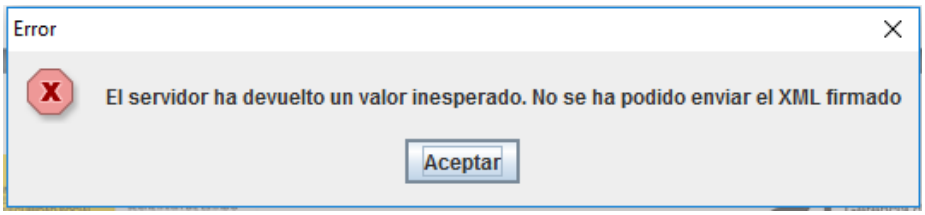
https://www.seg-social.es/wps/portal/wss/internet/FAQ

Una vez en la página, haga *clic* en "*Formule aquí su propia consulta".* Una vez en el formulario seleccione en el apartado *"Tema:" -> "Soporte Informático".* Explique brevemente el servicio que intentaba ejecutar, el tipo de certificado utilizado en la firma, su DNI y el código de error recibido en el mensaje. El equipo de Soporte Técnico se podrá en contacto con usted, bien a través del teléfono de contacto o correo electrónico que facilite.

7.2. EL SERVIDOR HA DEVUELTO UN VALOR INESPERADO

7.2.1. Mensaje que se muestra

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



7.2.2. Explicación del error

Se ha sobrepasado el tiempo límite de 5 minutos para completar el proceso de firma y envío.

7.2.3. Solución

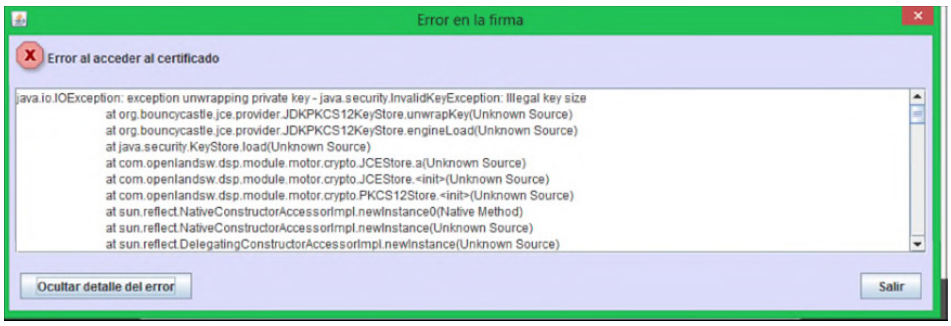
Verificar que el proceso completo se ha realizado dentro del tiempo límite de 5 minutos.

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

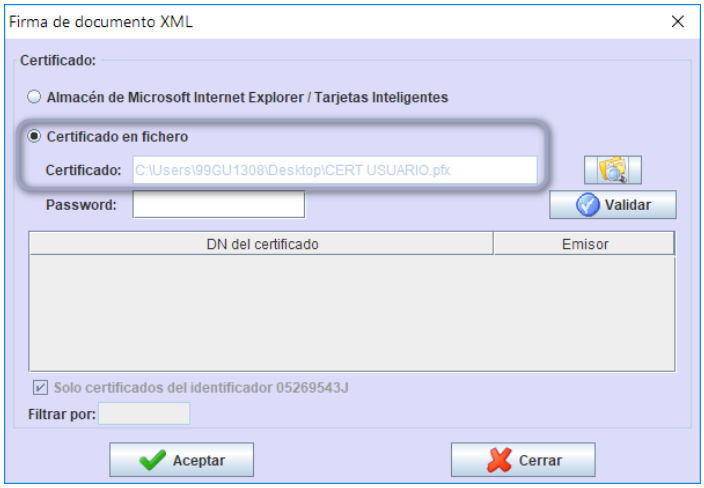
7.3. ERROR AL ACCEDER AL CERTIFICADO

7.3.1. Mensaje que se muestra

Error: Error al acceder al certificado



7.3.2. 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.

7.3.3. Solución

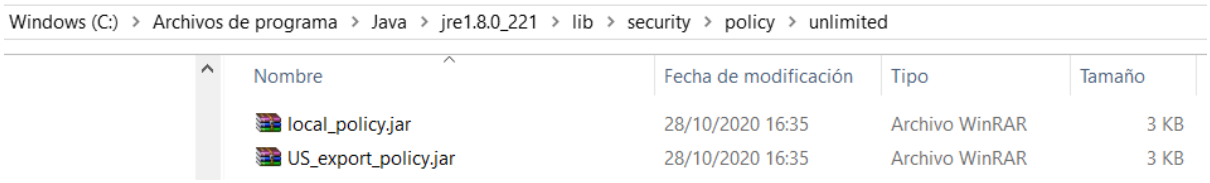
Actualice a la última versión de Java: https://java.com/es/

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:\Archivos de Programa\Java\jre1.8.0_xxx\lib\security\policy\unlimited

Si la versión de java que tiene es de 32 bits se ubicará:

C:\Archivos de Programa (x86)\Java\jre1.8.0_xxx\lib\security\policy\unlimited

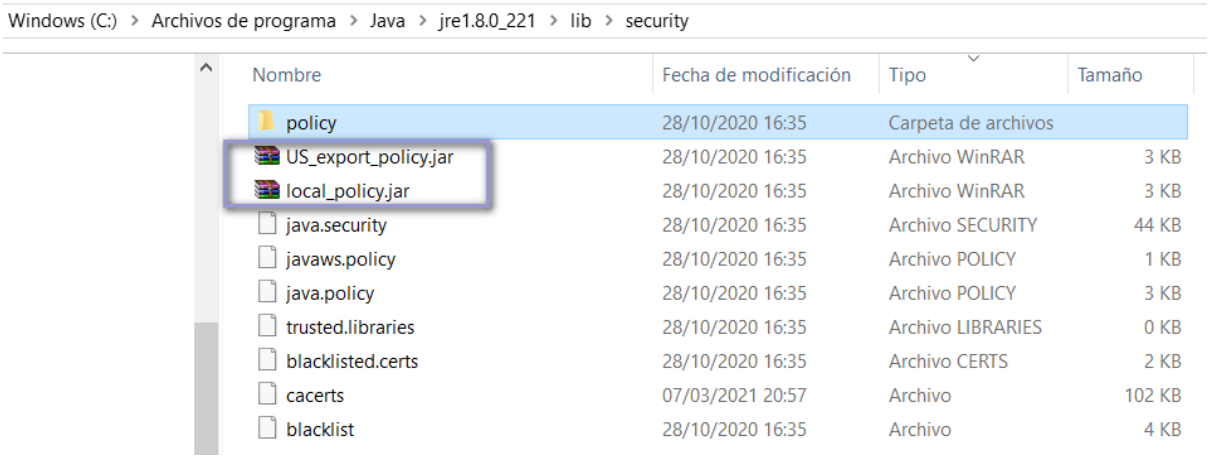


Copie su contenido a la siguiente carpeta, aceptando la sustitución de los ficheros coincidentes. Es posible que deba otorgar permisos como administrador del equipo para realizar la copia:

C:\Archivos de Programa\Java\jre1.8.0_xxx\lib\security

Si la versión de java que tiene es de 32 bits deberá copiar los ficheros en:

C:\Archivos de Programa (x86)\Java\jre1.8.0_xxx\lib\security



7.4. AL FIRMAR, JAVA SOLICITA UNA CONTRASEÑA

7.4.1. Mensaje que se muestra

Tras seleccionar el certificado y pulsar firmar, *Java* solicita una contraseña.

7.4.2. Explicación del error

En las aplicaciones del portal *Tu Seguridad Social* (TUSS) puede producirse en el proceso de firma un cambio de direccionamiento de red (*cambio en el sistema de dominio – DNS*) diferente al que se estableció cuando el usuario entró en la aplicación. Cuando *Java* detecta este cambio de direccionamiento de red solicita identificarse nuevamente, hecho que provoca un error y consecuentemente detiene la aplicación.

Para solucionar este problema de direccionamiento erróneo se requiere eliminar de la *caché* o memoria temporal del sistema y/o navegadores el historial de los direccionamientos de red guardados.

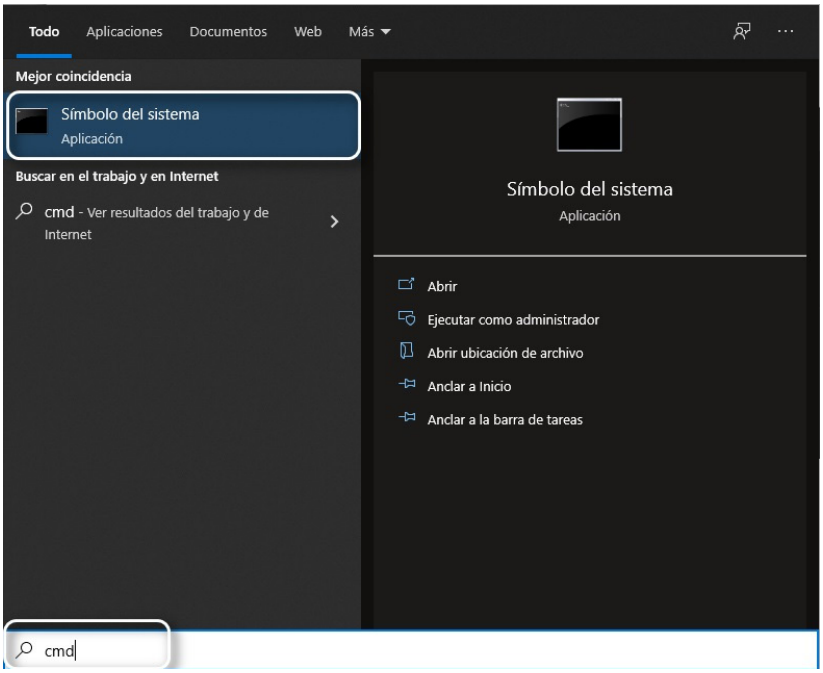
7.4.3. Solución

La eliminación del contenido de la caché de DNS se puede realizar sobre el sistema operativo, aunque el uso más frecuente de protocolos de seguridad avanzados en la navegación para hacerla más privada hace que el almacenamiento de las resoluciones DNS se realice en los navegadores, por lo tanto si el borrado de la *caché DNS* del sistema no funciona pruebe a eliminar la de los navegadores tal y como se explica a continuación

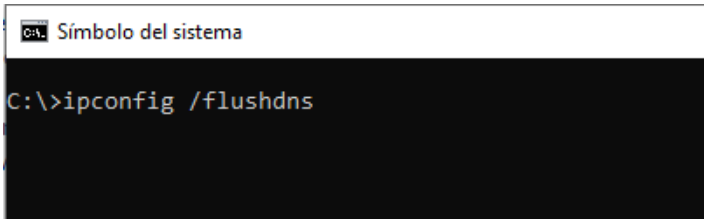
- *Borrar la caché DNS en Windows.*
- *Borrar la caché DNS en Mac/OS.*
- *Borrar la caché DNS del navegador Mozilla Firefox*
- *Borrar la caché DNS del navegador Google Chrome*
- *Borrar la caché DNS del navegador EDGE*

7.4.3.1. Borrar la caché DNS en Windows

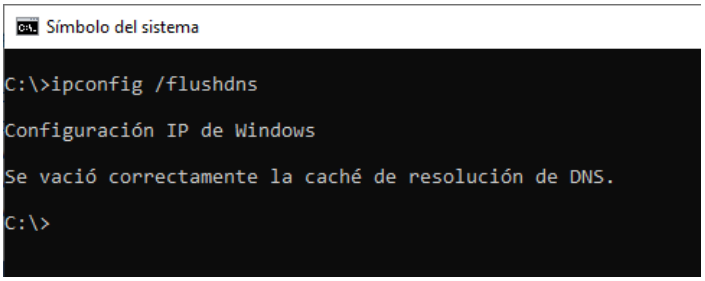
Para ello es necesario abrir una ventana de comandos del sistema operativo (pantalla de símbolo de sistema): Pulse el botón de **Inicio** (o tecla de Windows) y escriba "*cmd*", seleccione la aplicación llamada "***Símbolo del sistema***":



Una vez dentro tiene que escribir el siguiente comando: **ipconfig /flushdns** pulse *Intro*.



Como resultado debería mostrarse:

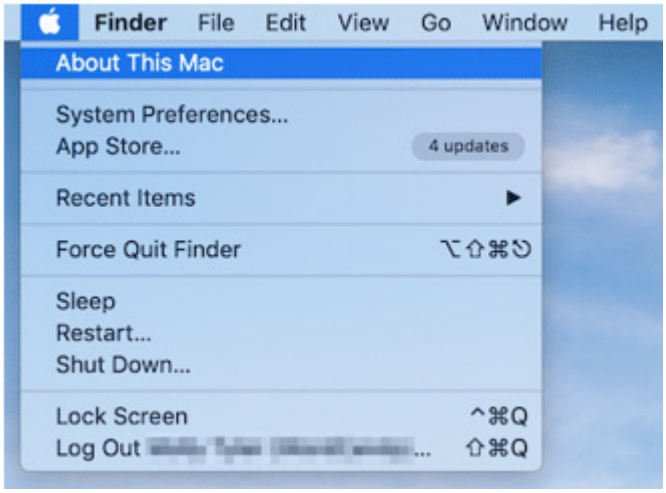


Finalizado el proceso puede cerrar la ventana. Antes de probar nuevamente la aplicación del TUSS cierre todos los navegadores abiertos.

7.4.3.2. Borrar la caché de DNS en MacOS

Para borrar la caché de DNS en *Mac/OS*, deberá abrir la interfaz de línea de comandos nativa conocida como ***Terminal*** y ejecutar el comando apropiado. Este proceso varía según la versión de *Mac/OS*.

Si no está seguro de con qué versión está trabajando, haga clic en el icono *"Apple"* en la esquina superior izquierda de su escritorio y seleccione "*Acerca de este Mac*"



Su versión actual será la primera información enumerada:

Una vez que conozca esta información, puede seguir los pasos relevantes a continuación.

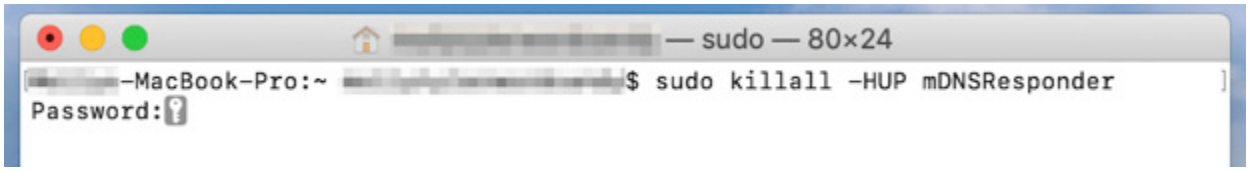
macOS El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15)

Si estás trabajando en macOS versión 10.11 o superior, abre la interfaz de línea de comandos haciendo clic en **Ir > Utilidades:**

A continuación, seleccione ***Terminal***. Una vez que se abra, ejecute el siguiente comando:

```
sudo killall -HUP mDNSResponder
```

Se le pedirá que introduzcas la contraseña de su ordenador:



Finalizado el proceso, la Caché se habrá borrado

macOS Yosemite (10.10)

Puede acceder a ***Terminal*** por el mismo método descrito anteriormente para cualquier versión de macOS. En Yosemite (10.10), una vez que se abra la ventana, deberá ejecutar el siguiente comando:

```
sudo discoveryutil udnsflushcaches
```

Ingrese la contraseña de su ordenado. Finalizado el proceso la caché quedará borrada.

macOS Lion (10.7), Mountain Lion (10.8), and Mavericks (10.9)

Para las versiones 10.7 a 10.9 de macOS, abra *Terminal* y ejecute el siguiente comando para borrar la caché de DNS:

```
sudo killall -HUP mDNSResponder
```

Puede notar que este es el mismo comando utilizado por las versiones 10.11 y superiores. Ingrese su contraseña para ejecutarla. Finalizado el proceso la caché quedará borrada.

Leopardo de nieve de macOS (10.6)

Acceda a la opción del sistema ***Terminal*** como se explicó en párrafos precedentes e introduce este comando:

```
sudo dscacheutil -flushcache
```

Luego, ingrese su contraseña para proceder con la eliminación de la caché de DNS.

MacOS Leopard (10.5)

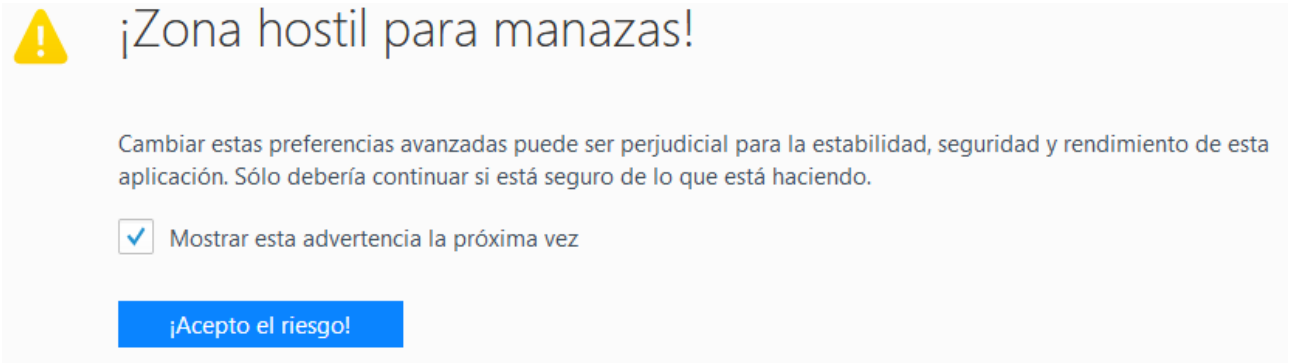
En una ventana de ***Terminal*** ejecute el siguiente comando:

```
sudo lookupd -flushcache
```

Una vez que ingrese su contraseña, la caché de DNS será vaciada.

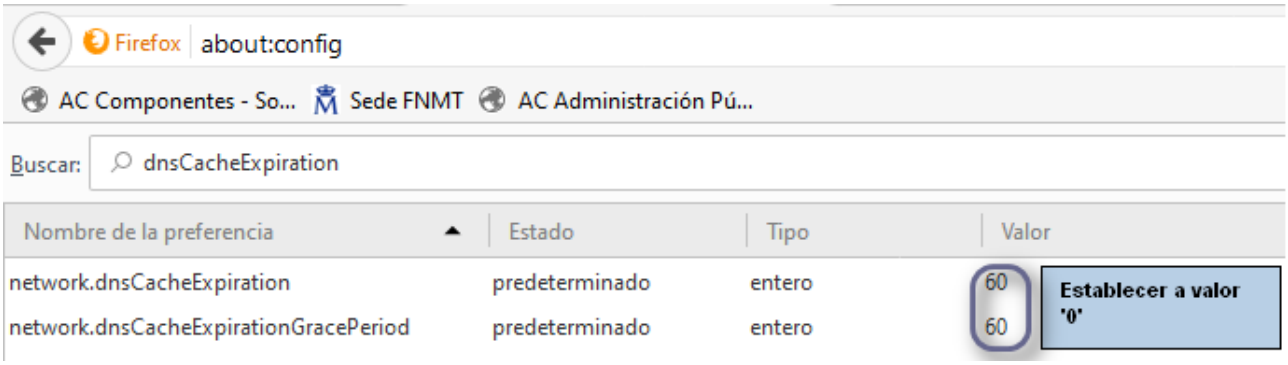
7.4.3.3. Borrar la caché DNS en el navegador web Mozilla Firefox

En el navegador Firefox escriba en la línea de direcciones: ***about:config*** y pulse *intro*. Acepte el mensaje de alerta siguiente.



Una vez se muestren la lista de preferencias y opciones avanzadas del navegador, localice las entradas:

«network.dnsCacheExpiration»
«network.dnsCacheExpirationGracePeriod»

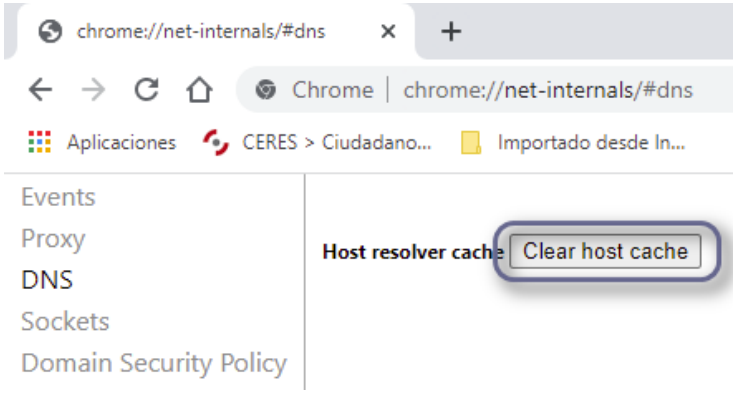


Haciendo un doble *clic* en **cada entrada**, podrá editar el valor que viene por defecto en ‘60’ y establecerlo a **‘0’**. De este modo se eliminará la caché DNS. Si se deja este valor, nunca se guardará en la caché las resoluciones de dominio o DNS; puede no obstante, restablecer su valor original a ‘60’ una vez finalice la aplicación que esté ejecutando en el *TUSS*.

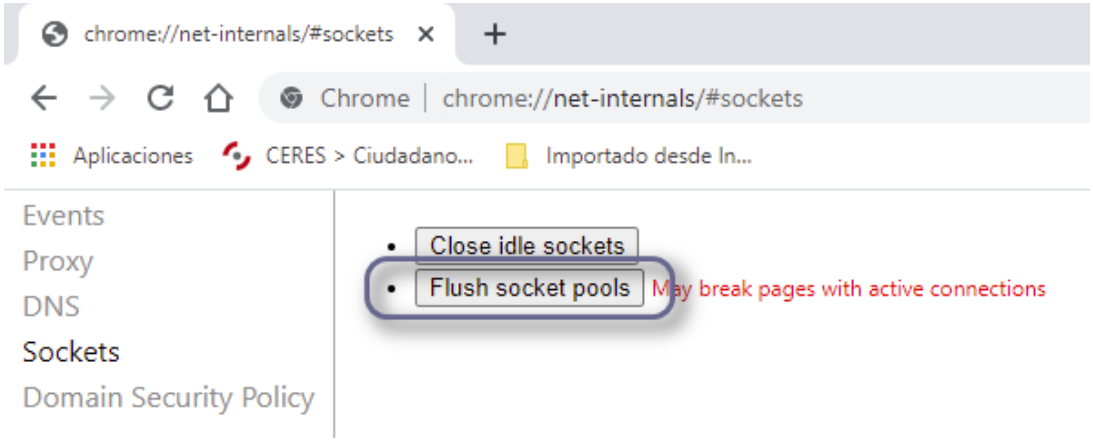
7.4.3.4. Borrar la caché DNS en el navegador web Google Chrome

En un navegador Chrome y escribir en la línea de direcciones ***chrome*://net-internals/#dns** y pulse *Intro.*

Una vez dentro, haga *clic* en el botón ***Clear host caché***:



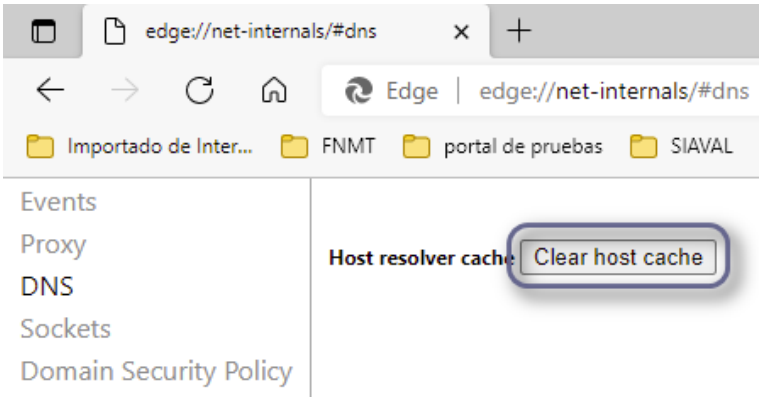
Para eliminar todas las conexiones guardadas y activas actualmente en Chrome, seleccione del menú de la izquierda la sección ***Sockets*** y haga *clic en* ***Flush socket pools***.



7.4.3.5. Borrar la caché DNS en el navegador Microsoft Edge

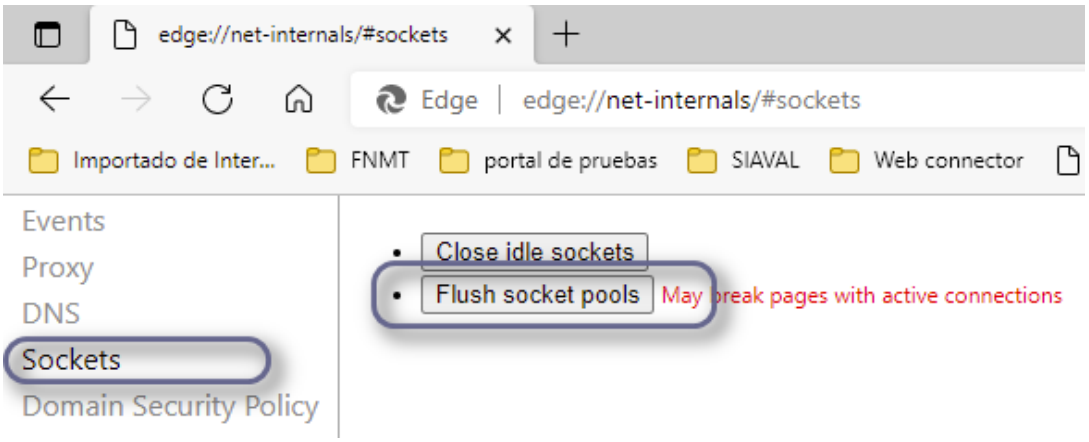
En un navegador EDGE, escriba en la línea de direcciones**: edge://net-internals/#dns** y pulse Intro.

Se mostrará una página con todas las resoluciones DNS guardadas hasta el momento.



Haga *clic en* ***Clear host caché*** para eliminar la caché DNS almacenada en Edge.

Para eliminar todas las conexiones guardadas y activas actualmente en Edge, seleccione del menú de la izquierda la sección ***Sockets*** y haga *clic en* ***Flush socket pools***.



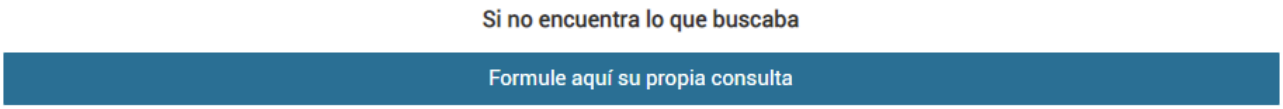
ÍNDICE

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:

https://www.seg-social.es/wps/portal/wss/internet/FAQ

Si su incidencia es técnica, dentro de esta página diríjase al apartado *"Formule aquí su propia pregunta":*



y en el apartado "*Tema*" seleccione "*Soporte informático*". Explique brevemente el servicio que intentaba ejecutar y en qué momento se produce el error. Toda información que pueda incluir será de gran ayuda, por ejemplo, la relativa al sistema operativo utilizado (Windows, Mac/OS o Linux), navegador utilizado, medio para autenticarse y firmar, (certificado, tarjeta criptográfica, Cl@ve), su DNI y el código de error si se muestra en pantalla. El equipo de Soporte Técnico se podrá en contacto con usted, bien a través del teléfono de contacto o correo electrónico que facilite.

ÍNDICE