



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 NO NORMALIZADA TIPO 1

---

**Configuración de entorno para la Firma No Normalizada Tipo 1.**

**Solución mediante *Applets***

Centro de Seguridad de la Información

12/04/2021

Versión: 2.1

Clasificación: Público



Gerencia de Informática  
de la Seguridad Social

| CONTROL DE VERSIONES |            |   |                             |
|----------------------|------------|---|-----------------------------|
| Título               |            | FIRMA NO NORMALIZADA TIPO 1 (Solución mediante <i>Applets</i> ) |                             |
| Autor                |            | CSI   |                             |
| Fecha versión 1.0    |            | 22/08/2017  |                             |
| Versión              | Fecha      | Responsable   | Cambios introducidos        |
| 1.1                  | 30/10/2017 | Dirección de Seguridad, Innovación y Proyectos                  | Primer Documento            |
| 2.0                  | 17/07/2020 | Centro de Seguridad de la Información                           | Actualización de contenidos |
| 2.1                  | 12/04/2021 | Centro de Seguridad de la Información                           | Actualización de contenidos |
|                      |            |   |                             |
|                      |            |   |                             |
|                      |            |   |                             |
|                      |            |   |                             |
|                      |            |   |                             |
|                      |            |   |                             |

## INDICE

|  |           |
|--|-----------|
| <b>1. OBJETIVO .....</b>   | <b>4</b>  |
| 1.1. SERVICIOS DE LA SEDE QUE UTILIZAN <i>APPLETS</i> .....  | 4         |
| <b>2. COMPATIBILIDAD DE SISTEMAS OPERATIVOS Y NAVEGADORES EN EL SISTEMA DE FIRMA<br/>    NO NORMALIZADO TIPO 1 .....</b> | <b>5</b>  |
| <b>3. CONFIGURACION DE JAVA .....</b>  | <b>6</b>  |
| 3.1. PANEL DE CONTROL DE JAVA .....  | 6         |
| 3.1.1. Configuración de opciones avanzadas de Java .....   | 6         |
| 3.1.2. Inclusión de urls de confianza de los servidores de la Seguridad Social.....                                      | 7         |
| 3.1.3. Eliminación de datos temporales y restauración de valores de seguridad de java .....                              | 7         |
| 3.1.4. Importación del certificado Raíz de la FNMT-RCM en el almacén de Java.....  | 8         |
| <b>4. CONFIGURACIÓN DE INTERNET EXPLORER .....</b>   | <b>10</b> |
| 4.1. CERTIFICADOS DE CONFIANZA .....   | 10        |
| 4.1.1. Descarga de los certificados Raíz e intermedios de FNMT-RCM .....   | 10        |
| 4.1.2. Instalación de los certificados Raíz e intermedios de FNMT-RCM en IExplorer .....                                 | 10        |
| 4.1.3. Instalación de los certificados Raíz e intermedios de FNMT-RCM en Safari (Mac OS) .....                           | 12        |
| 4.2. DESBLOQUEAR VENTANAS EMERGENTES PARA OBTENER INFORMES.....  | 14        |
| <b>5. DESCRIPCIÓN DEL PROCESO DE FIRMA NO NORMALIZADO TIPO 1 (<i>APPLETS</i>) .....</b>                                  | <b>15</b> |
| <b>6. COMUNICACIÓN DE INCIDENCIAS .....</b>  | <b>17</b> |

## 1. OBJETIVO

El sistema de Firma No Normalizado Tipo 1 corresponde con el uso de *applets* de Java para realizar el proceso de firma. En este manual se describen las pautas de configuración de Java y de los navegadores que son compatibles con este tipo de firma.

### 1.1. SERVICIOS DE LA SEDE QUE UTILIZAN *APPLETS*









La práctica totalidad de los servicios web de nuestra Sede están adaptados al sistema de firma Normalizado mediando *JNLP*, siendo muy pocos los que realizan el proceso de firma mediante *applets*.

Consulte el listado de servicios y tipo de firma asociado en el apartado de Requisitos de Firma Electrónica:

[https://sede.seg-social.gob.es/binarios/es/Listados\\_tipo\\_firma](https://sede.seg-social.gob.es/binarios/es/Listados_tipo_firma)

## 2. COMPATIBILIDAD DE SISTEMAS OPERATIVOS Y NAVEGADORES EN EL SISTEMA DE FIRMA NO NORMALIZADO TIPO 1

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

| FIRMA NO NORMALIZADA TIPO 1 (Applets) Certificado Digital                                    | <br>Internet Explorer | <br>Microsoft Edge | <br>Google Chrome | <br>Mozilla Firefox | <br>Safari |
|--|--|---|--|--|---|
| <br>Windows | ✓  |   |  |  |   |
| <br>Mac OS  |  |   |  |  | ✓   |
| <br>Linux  |  |   |  |  |   |

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

- En **Sistemas Windows**: navegador **Internet Explorer**.
- En **Sistemas Mac/OS** navegador **Safari**.

### 3. CONFIGURACION DE JAVA

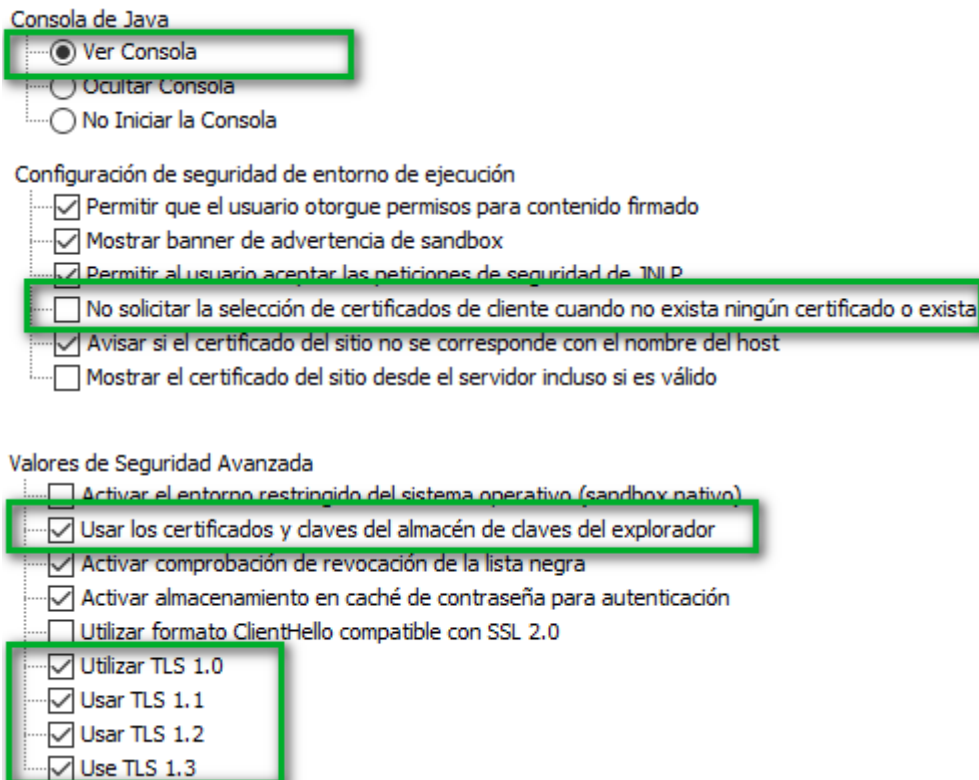
Puede descargar e instalar la Máquina Virtual de Java desde su página oficial: [www.java.com](http://www.java.com)

#### 3.1. PANEL DE CONTROL 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.

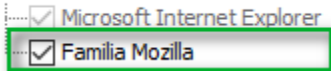
#### 3.1.1. CONFIGURACIÓN DE OPCIONES AVANZADAS DE JAVA

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:

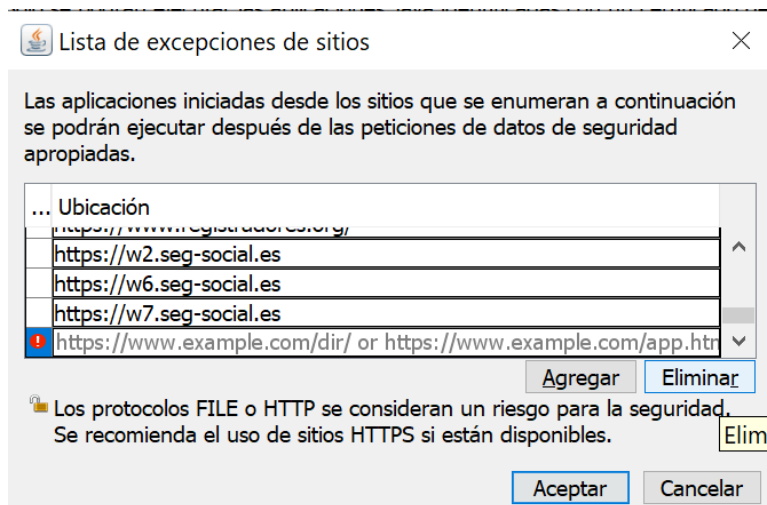
Java por defecto para los exploradores



### 3.1.2. INCLUSIÓN DE URLS DE CONFIANZA DE LOS 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**, en la pestaña Seguridad pulse en el botón **Editar lista de Sitios**:



Añada una a una las siguientes direcciones:

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

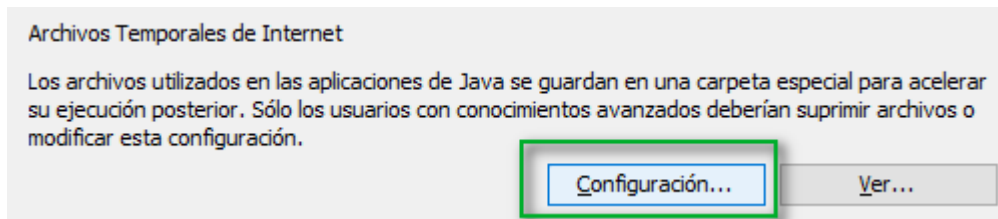
Acepte y continúe con el siguiente apartado de configuración.

### 3.1.3. ELIMINACIÓN DE DATOS TEMPORALES Y RESTAURACIÓN DE VALORES DE SEGURIDAD DE JAVA

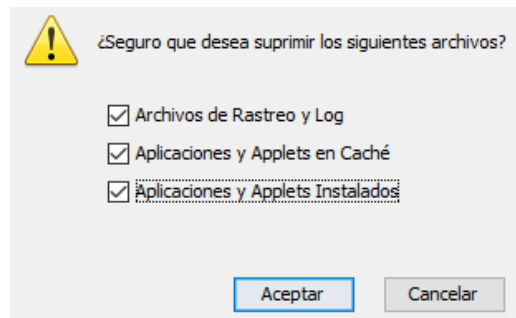
Es recomendable realizar estas operaciones si tiene sospechas que los procesos relacionados *Java* muestran un comportamiento inadecuado o dejan de funcionar.

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

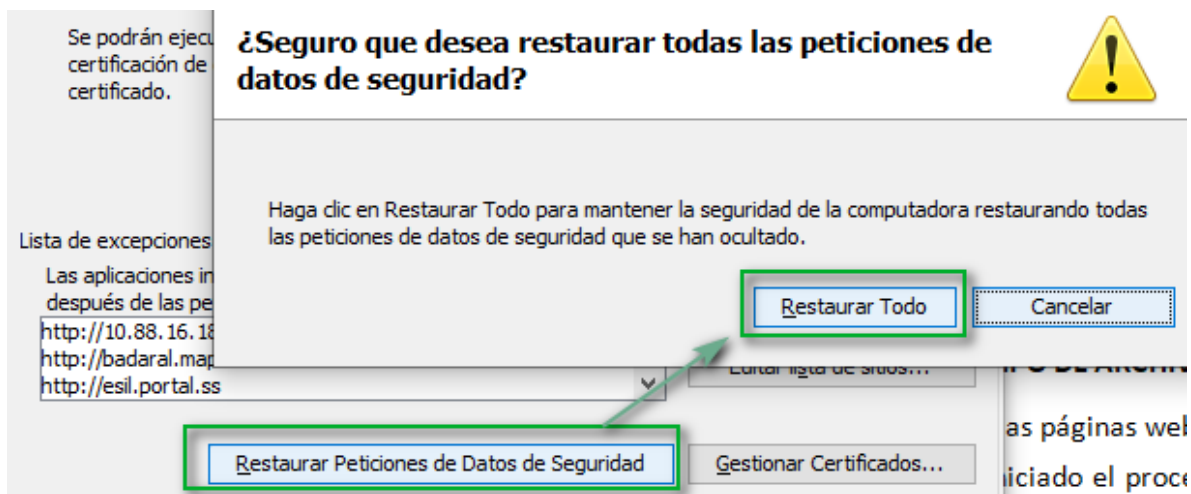
- En la pestaña *General*, en el apartado *Archivos temporales de internet*, pulse *Configuración*:



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



- En la pestaña *Seguridad*, pulsar en *Restaurar Peticiones de Datos de Seguridad*, posteriormente *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 y pulse *Abrir*. Puede que tenga que “*todos los archivos*” para localizar el certificado.



Certificados ✕

Tipo de Certificado: CA de Firmante ▾

Usuario Sistema

| Emitido para              | Emitido por               |
|---------------------------|---------------------------|
| FNMT-RCM AC RAIZ FNMT-RCM | FNMT-RCM AC RAIZ FNMT-RCM |

Importar Exportar Eliminar Detalles Cerrar

## 4. CONFIGURACIÓN DE INTERNET EXPLORER

### 4.1. CERTIFICADOS DE CONFIANZA

Los certificados de confianza firmantes actuales, tanto el de los servidores de la Seguridad Social como el que certifica el software involucrado en los procesos de firma, por lo general ya vienen incluidos en los navegadores de internet más habituales. No obstante, se aconseja verificarlo y en caso de que dé 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 (Fábrica Nacional de la Moneda – Real Casa de la Moneda).

#### 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](#)

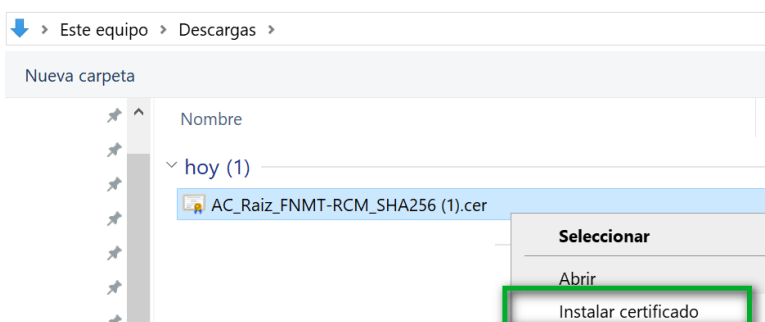
**Certificados Intermedios:**

[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

Localizar la carpeta donde se han descargado los certificados y con cada uno pulsar con el botón derecho del ratón y seleccionar: “Instalar certificado”.



Se iniciará el proceso de importación. Pulse *Siguiente*.

## Este es el Asistente para importar certificados

Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados.

Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Ubicación del almacén

Usuario actual

Equipo local

Marque “Colocar todos los certificados en el siguiente almacén” y pulse “Examinar”

### Almacén de certificados

Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.

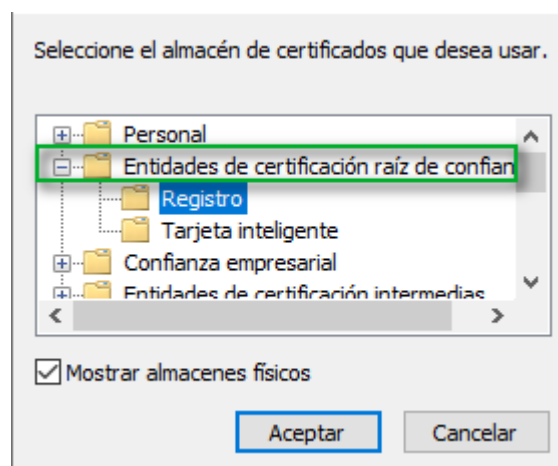
Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.

- Seleccionar automáticamente el almacén de certificados según el tipo de certificado
- Colocar todos los certificados en el siguiente almacén

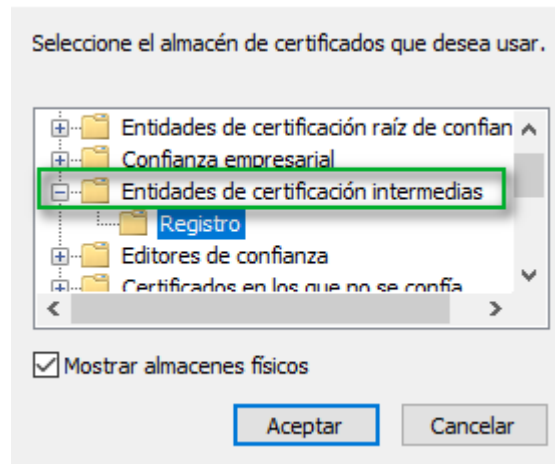
Almacén de certificados:

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”.

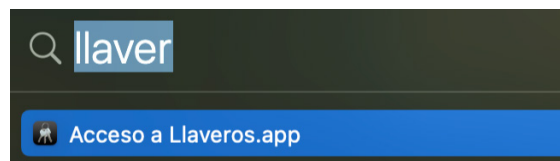


**Para los certificados intermedios:** Marque la opción “Mostrar almacenes físicos” y seleccione la carpeta “Entidades de certificación Raíz de Confianza” -> Carpeta “Registro”. Pulse “Aceptar” y “finalizar”.



#### 4.1.3. INSTALACIÓN DE LOS CERTIFICADOS RAÍZ E INTERMEDIOS DE FNMT-RCM EN SAFARI (Mac OS)

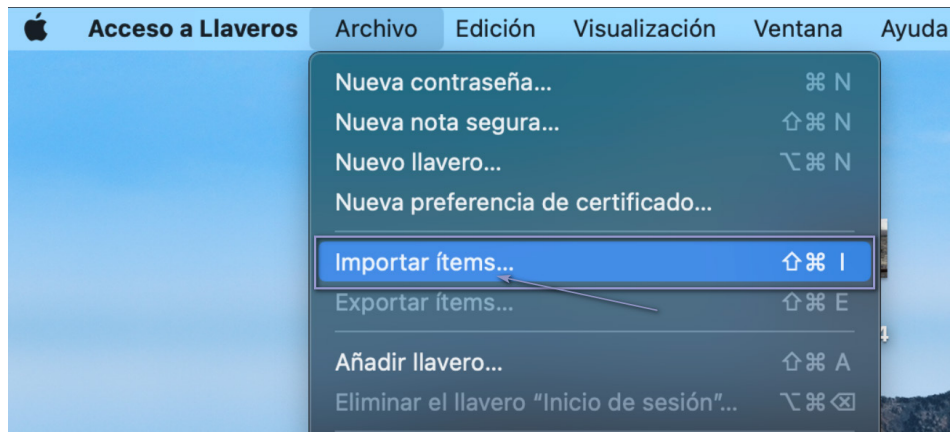
(\*) Es posible que las imágenes siguientes difieran según la versión de Mac/OS que disponga  
Con la utilidad **Spotlight** buscar y ejecutar la aplicación **Acceso a Llaveros.app**



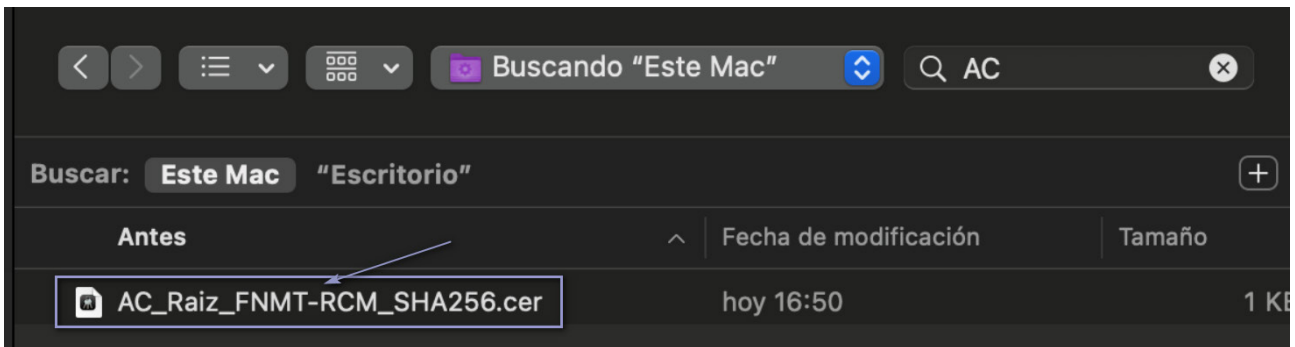
Pulsar en la **Categoría Certificados** donde importaremos los certificados raíz e intermedios descargados.



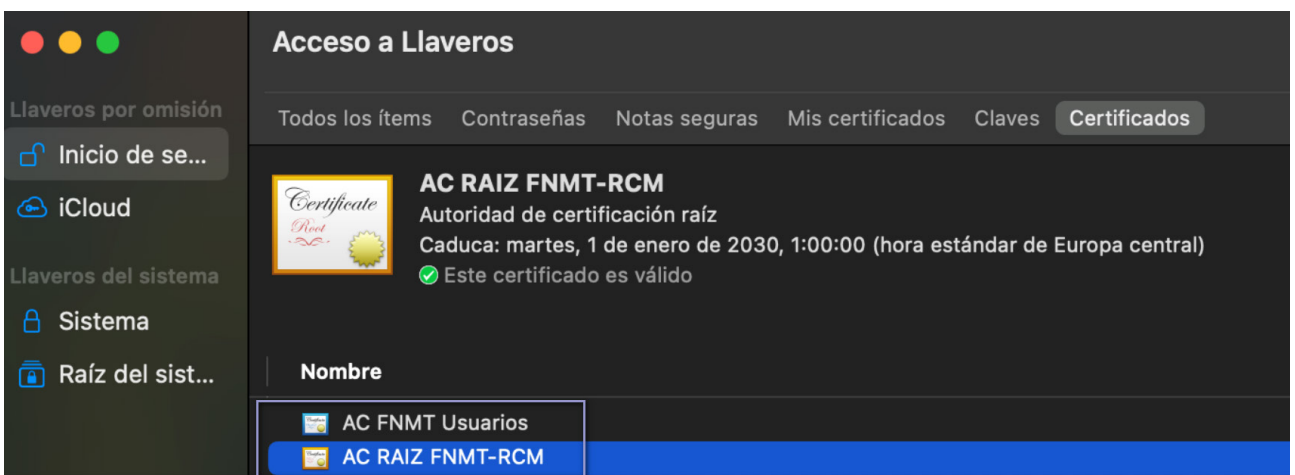
En el menú de la barra superior desplegar la opción **Archivo** y pulsar en **Importar elementos o Importar Ítems**



Localizar el certificado a importar, seleccionarlo y pulsar **Abrir**.



El certificado quedará instalado en el llavero:

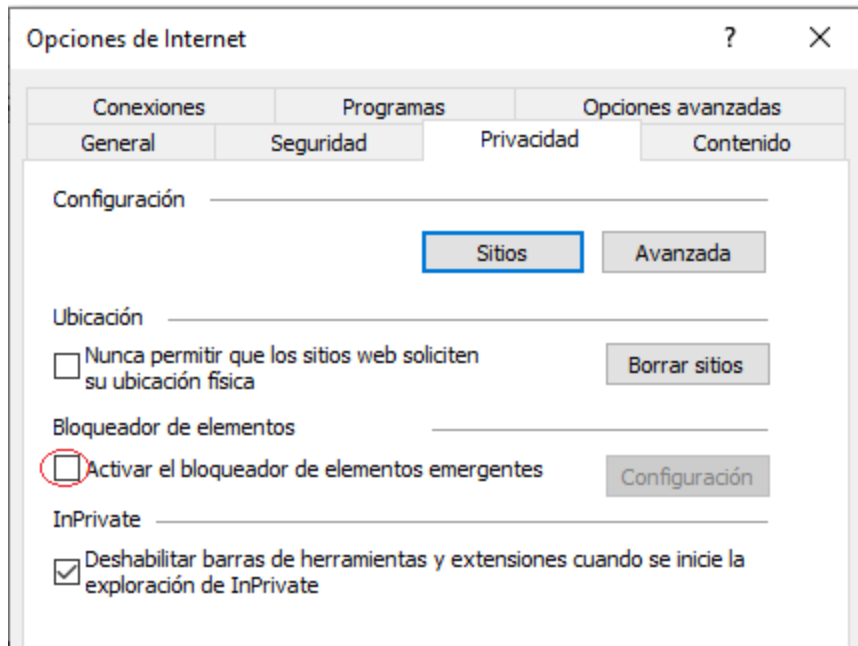


Repetir esta misma operación con el resto de los certificados.

## 4.2. DESBLOQUEAR VENTANAS EMERGENTES PARA OBTENER INFORMES

Es necesario permitir mostrar ventanas emergentes, ya que los informes se muestran de este modo en el navegador, por lo tanto, es imprescindible establecer este permiso en el navegador. Para ello, abierto Internet Explorer, seleccione del menú “Herramientas” -> Opciones de Internet -> pestaña “privacidad”

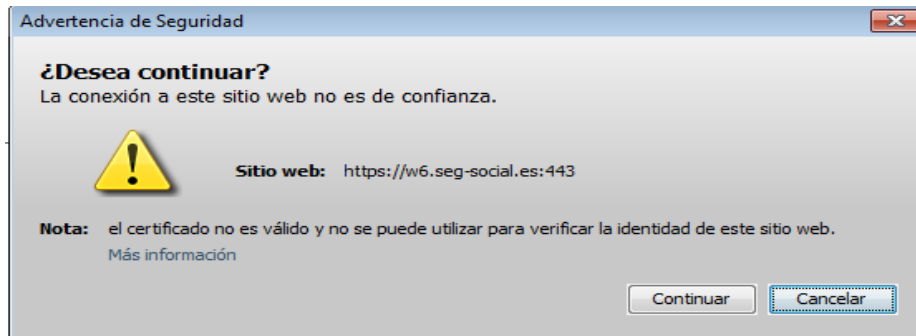
Desmarcar la opción “Activar el bloqueador de elementos emergentes”



## 5. DESCRIPCIÓN DEL PROCESO DE FIRMA NO NORMALIZADO TIPO 1 (APPLETS)

El siguiente ejemplo simula un proceso de firma en un sistema Windows con Internet Explorer.

Tras acceder al servicio web se solicitará verificar la autenticidad de la conexión, es decir, si confiamos en el servidor al que nos vamos a conectar. Para confirmar la confianza en el sitio pulsaremos sobre el botón continuar.

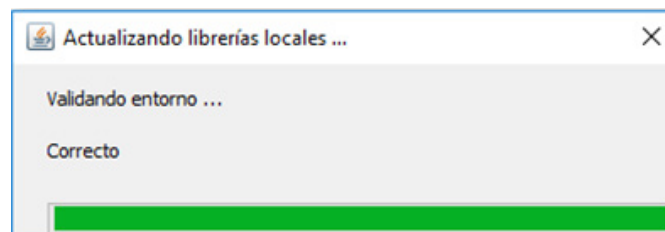


Se solicitará a continuación confianza en el certificado firmante del *applet*. Puede consultar los datos del certificado firmante pulsando en “Más información”.

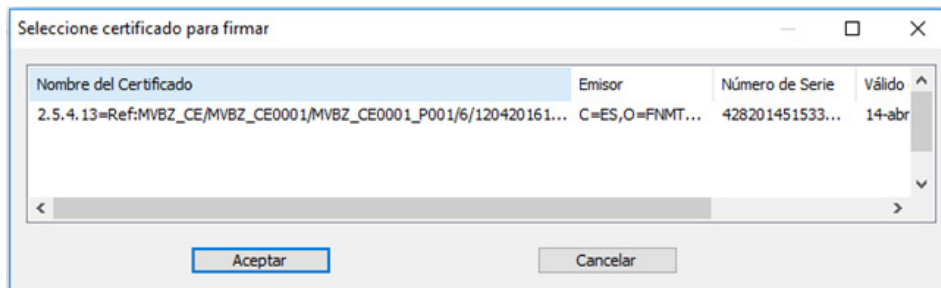


Si lo desea, puede marcar la opción “No volver a mostrar esto otra vez...” Para que no aparezca esta ventana en futuras ocasiones.

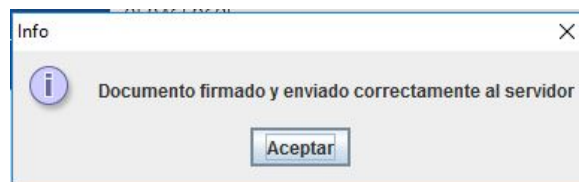
Pulse en “Ejecutar”, se iniciará el proceso de firma.



**Importante:** Si se le solicita en este punto seleccionar un certificado, asegúrese de **elegir el mismo certificado** que seleccionó para autenticarse en el servicio web.



Una vez seleccione el certificado y acepte se iniciará el proceso de firma. Si éste finaliza correctamente aparecerá una ventana de confirmación.





## 6. COMUNICACIÓN DE INCIDENCIAS

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

Si su incidencia es técnica, en el apartado *“Formule aquí su propia pregunta”*, incluya en el texto de la consulta la siguiente información de su entorno de trabajo: Sistema Operativo, navegador utilizado, tipo de certificado utilizado, Autoridad de Certificación emisora, nombre del servicio o trámite que intenta realizar y código de la incidencia si se muestra en el mensaje de error.