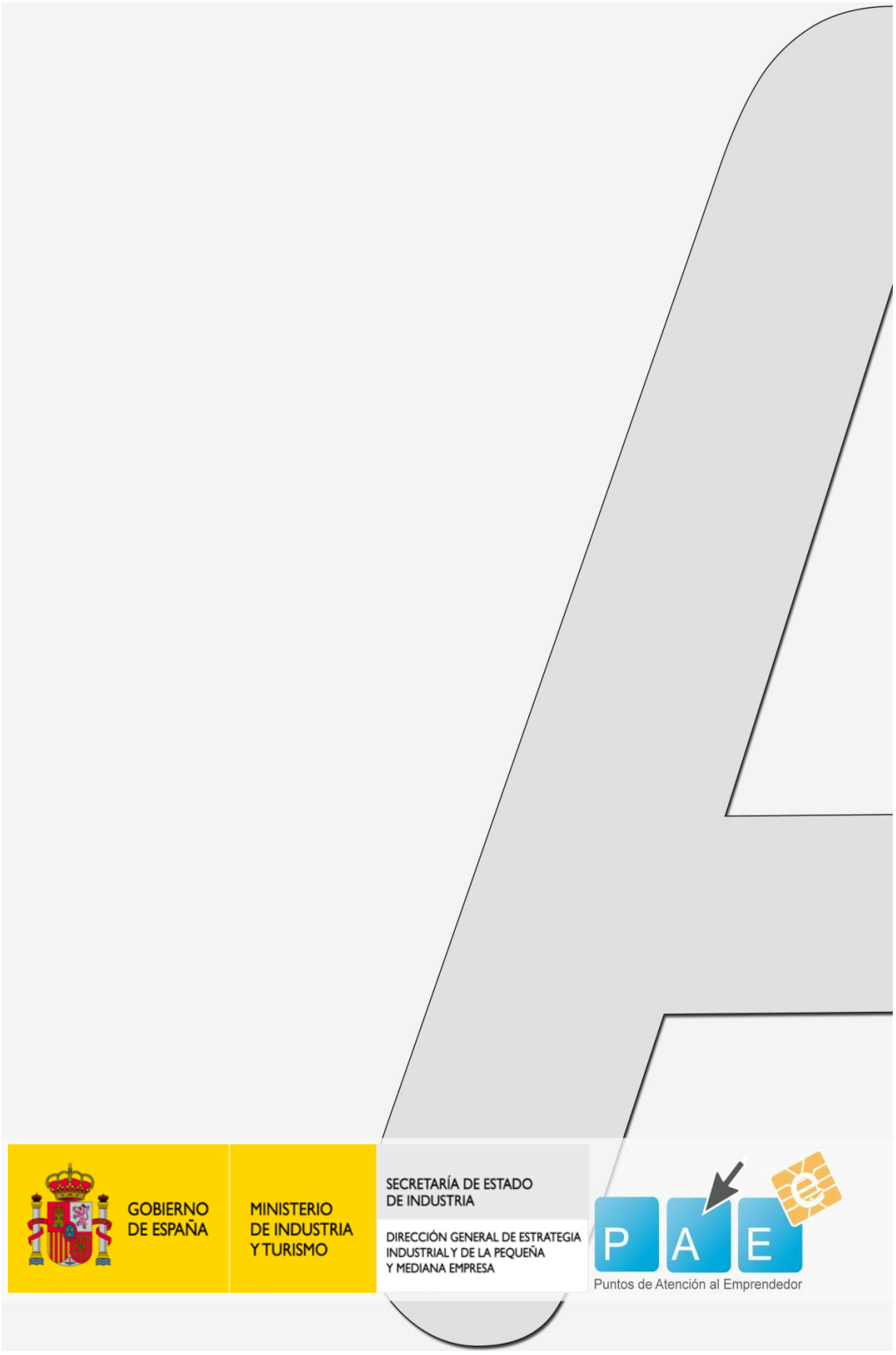


GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA Y TURISMO

SECRETARÍA DE ESTADO DE INDUSTRIA

DIRECCIÓN GENERAL DE ESTRATEGIA INDUSTRIAL Y DE LA PEQUEÑA Y MEDIANA EMPRESA

PAE

Puntos de Atención al Emprendedor

CONTENIDO

1. INTRODUCCIÓN

A lo largo de este manual se tratará de explicar el conjunto de configuraciones que son necesarias a aplicar en un equipo cliente para la correcta configuración de los componentes de firma.

2. GENERALIDADES

En este manual se va a desarrollar un conjunto de configuraciones de software de terceros que han sido probados y verificadas en diferentes entornos y sistemas operativos, aunque en última instancia será siempre recomendable seguir las recomendaciones de los fabricantes y distribuidores de software en lo que se refiere a configuraciones específicas para dichos componentes.

En concreto el proceso de configuración y firma ha sido validado en los siguientes sistemas operativos:

- Windows 7 Enterprise (IExplorer, FireFox, Chrome, Opera).
- Linux Debian 8 (FireFox)
- Windows 8.1 Enterprise (IExplorer, FireFox, Chrome, Opera).

Si dispone de algún tipo de observaciones relacionadas con el proceso de configuración, no dude en ponerse en contacto con el soporte de CIRCE para realizar las observaciones oportunas.

3. CONFIGURACIÓN DEL EQUIPO

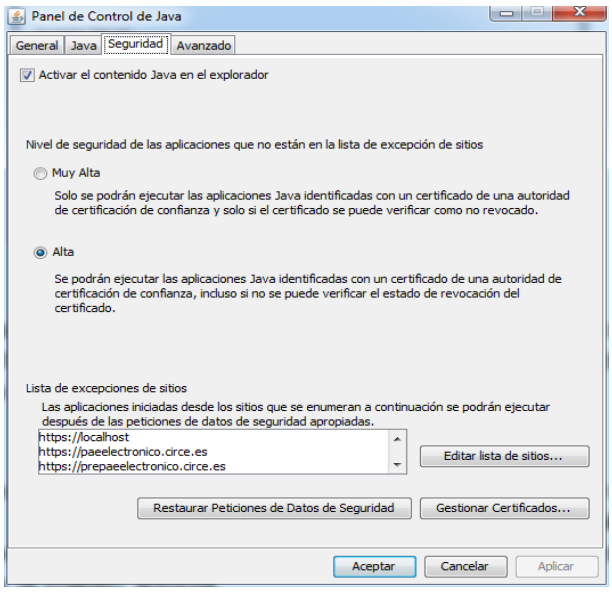
3.1 INSTALACIÓN DE JAVA

La aplicación va a requerir la instalación de la máquina virtual de Java en entornos Windows y Linux para que pueda ser ejecutada la firma en cliente, ya que el componente empleado procedente de @Firma así lo requiere.

Para ello, será necesario conectarse a la siguiente página instalando el componente, siempre la última versión disponible en la web de Oracle:

https://www.java.com/es/download/

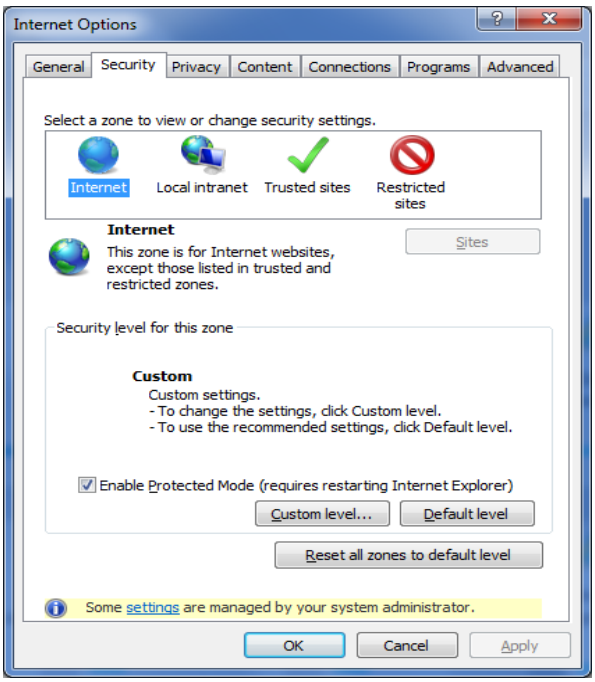
Una vez descargado se seguirán los pasos indicados por Oracle para la instalación del mismo, por consiguiente será necesario resolver cualquier duda que pueda surgir con el servicio técnico de Oracle.



Debe estar habilitada la parte de Java para los browser y el nivel de seguridad puede ser Alto o Muy Alto, en función de los requerimientos de seguridad definidos para la máquina cliente.

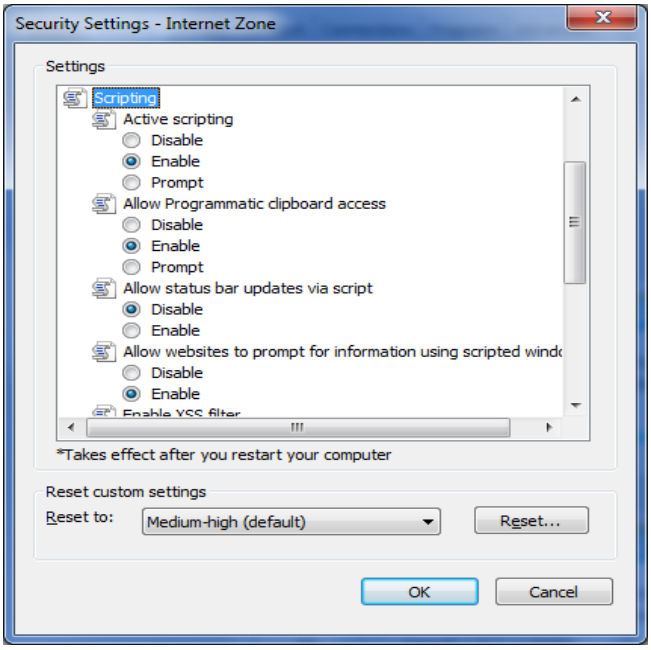
En la lista de excepciones, podemos apreciar que se encuentran introducidas las siguientes direcciones (**Exception**) las direcciones **localhost** y **prepaeelectronico.circe.es, paeelectronico.circe.es** (para el protocolo https), como muestra la imagen adjunta.

Una vez desarrollada la configuración del componente de Java, deberemos desarrollar la configuración del explorador, para ello debemos acceder a las opciones de internet, que podremos encontrar al acceder a **Herramientas**, **Opciones de Internet**.



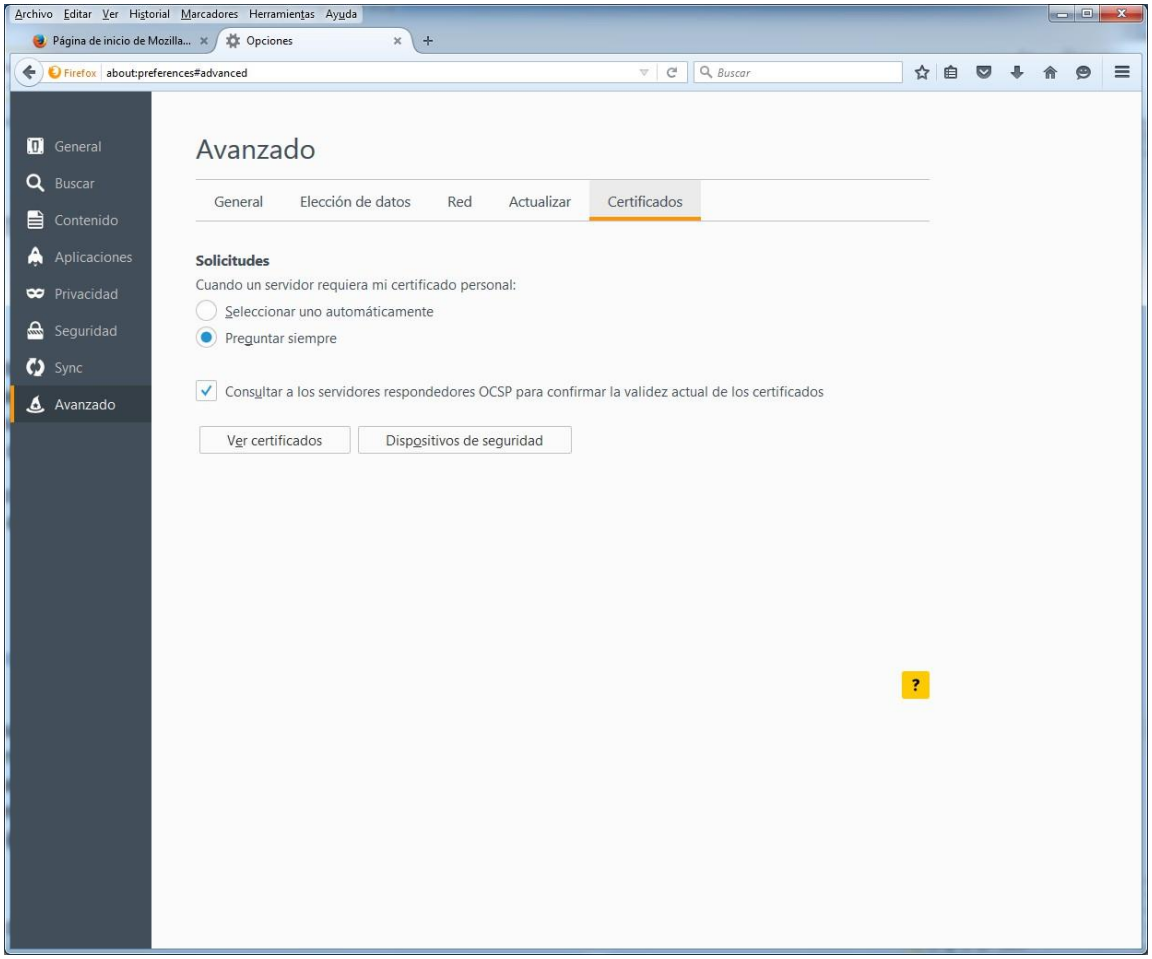
Se activará la configuración **Habilitar Modo Protegido** (Enable Protected Mode).

Dentro del **Nivel personalizado** (Custom Level), será necesario activar en la parte de **Automatización** (Scripting), la opción **Active scripting** como muestra la imagen adjunta.

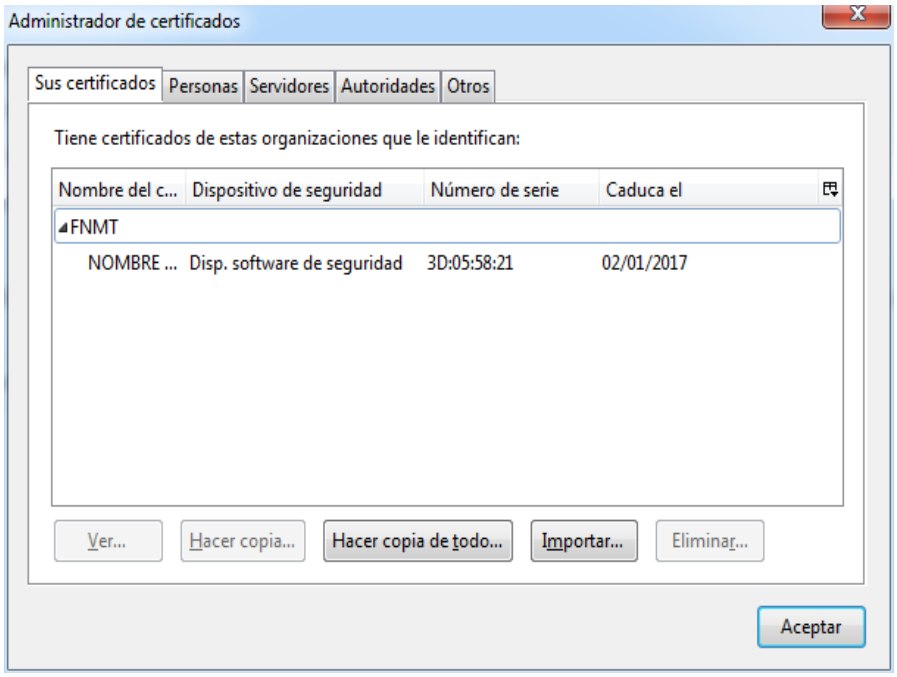


Para el resto de navegadores, **Chrome** y **FireFox** (en sus últimas versiones), no se deberán aplicar configuraciones específicas, únicamente debemos asegurarnos de que los certificados están correctamente instalados en los almacenes de certificados de la máquina.

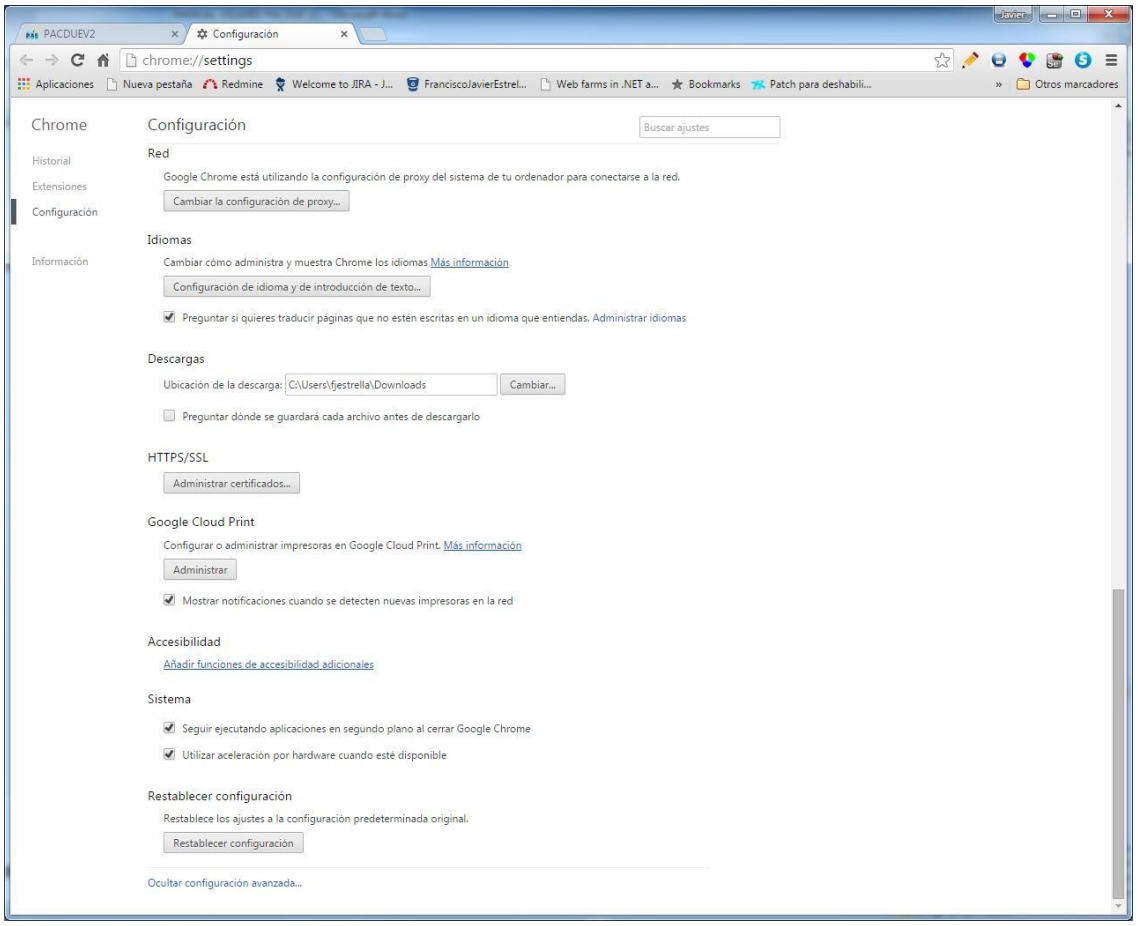
En el caso de **FireFox**, deberemos acceder en la parte de **Herramientas**, **Opciones**, a la siguiente ventana tal como muestra la imagen adjunta.



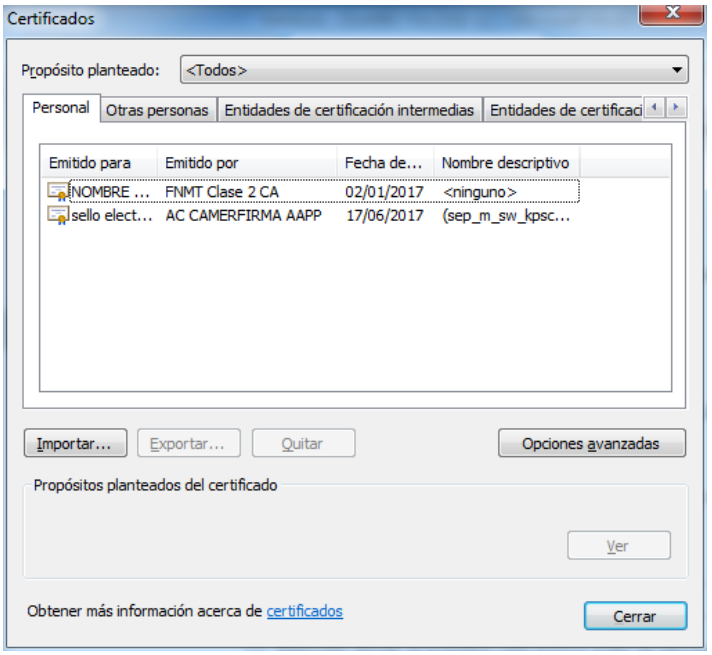
En la opción Ver Certificados, podremos visualizar los certificados instalados a nivel de **FireFox**, como muestra la imagen adjunta:



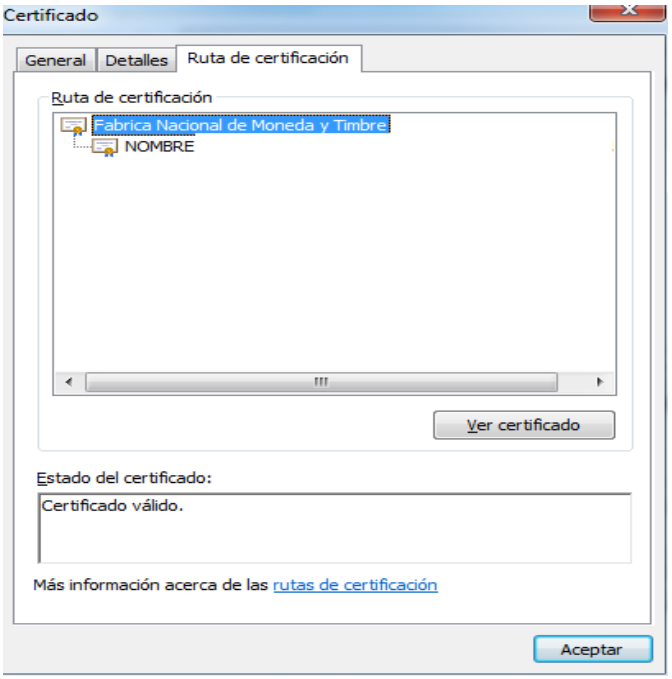
En el caso de **Chrome**, podremos acceder a través de la opción de configuración, donde se mostrará una imagen como la adjunta (en función de las versiones).



En la opción **HTTP/SSL** podremos administrar los certificados que se encuentran disponibles en el almacén de certificados.



Es recomendable comprobar la validez de los certificados y que se encuentran perfectamente instalados los certificados raíz en la máquina, para ello, al acceder al almacén de certificados, podemos verificar la validez de los certificados raíz.



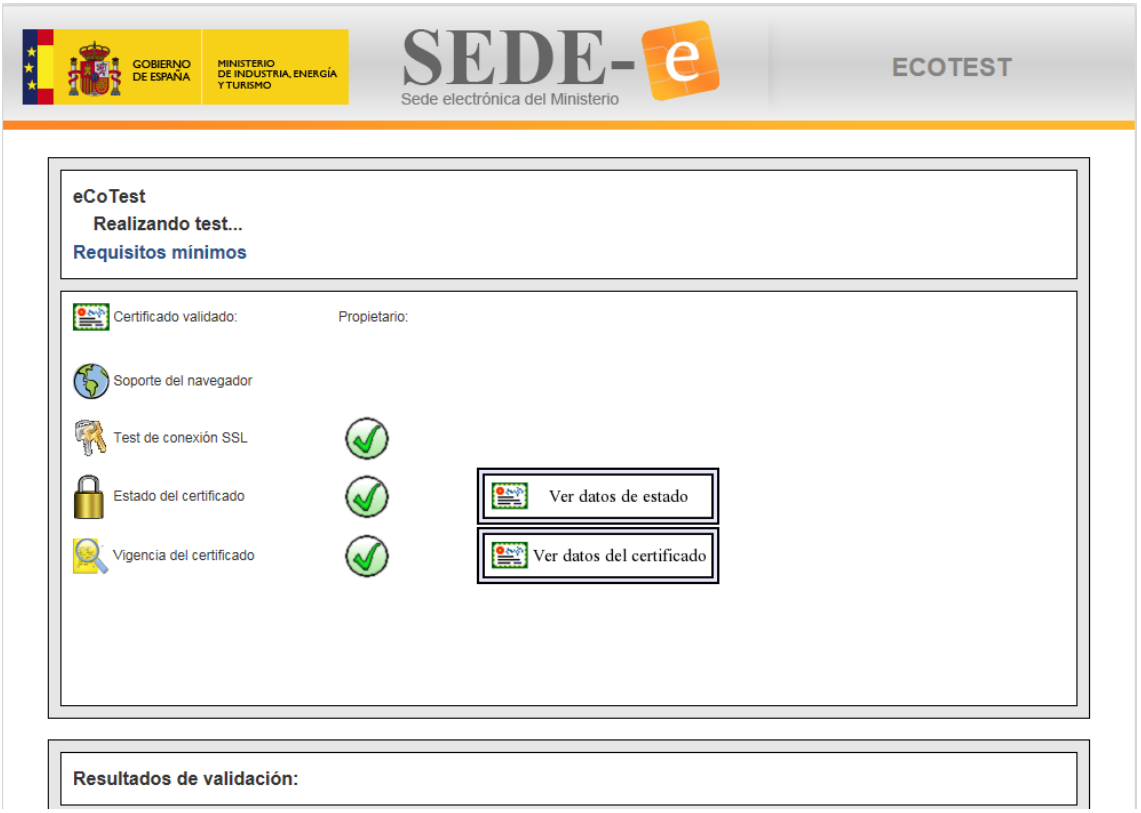
En la anterior imagen podemos ver que el certificado **FNMT** del usuario dispone de su raíz perfectamente configurada en la máquina.

Existe una herramienta, suministrada por el **Ministerio de Industria, Energía y Turismo,** que nos puede permitir desarrollar un test completo para comprobar que el sistema se encuentra correctamente configurado, podemos pasar el test desde cualquier navegador sobre la siguiente url.

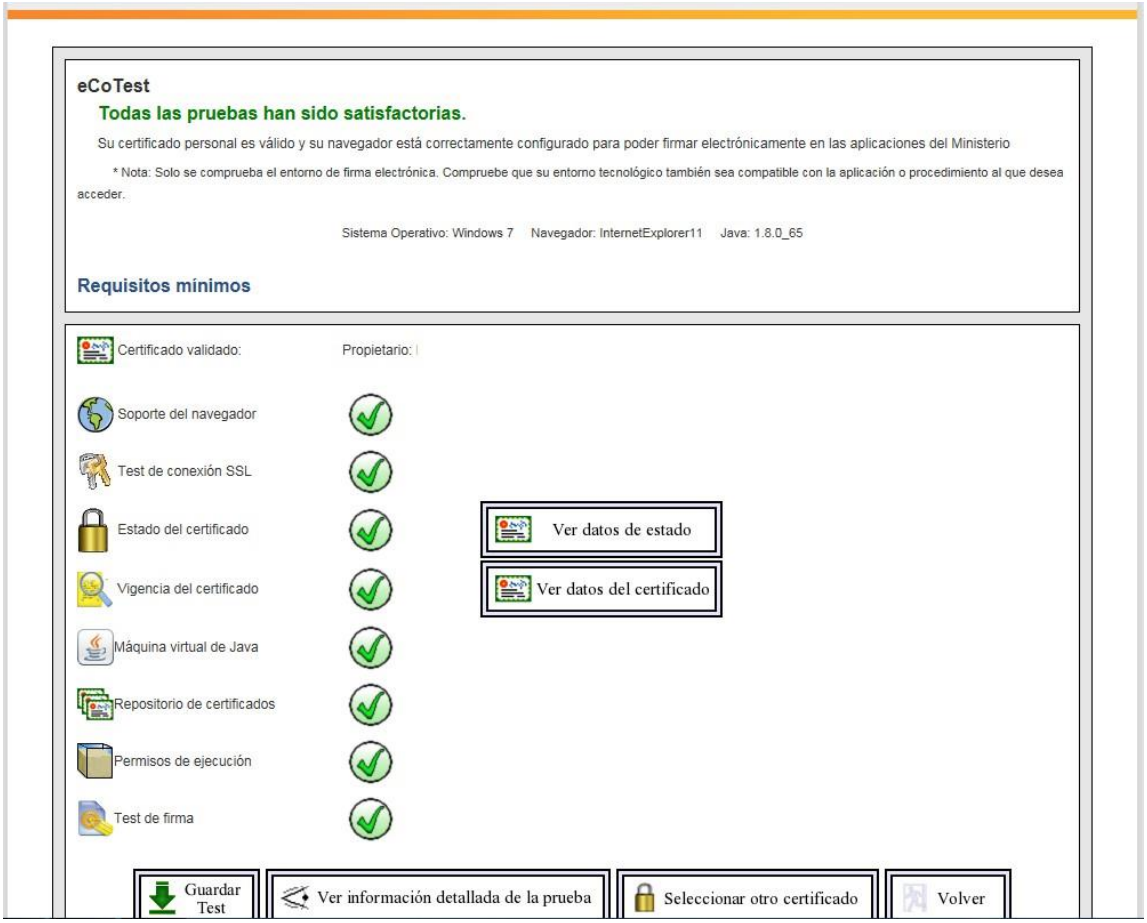
https://sede.minetur.gob.es/es-ES/firmaelectronica/Paginas/eCoTest.aspx

La herramienta nos va a solicitar el certificado sobre el cual se va a desarrollar la prueba, deberemos siempre seleccionar el certificado con el cual nos logaremos en el sistema o realizaremos el proceso de firma.

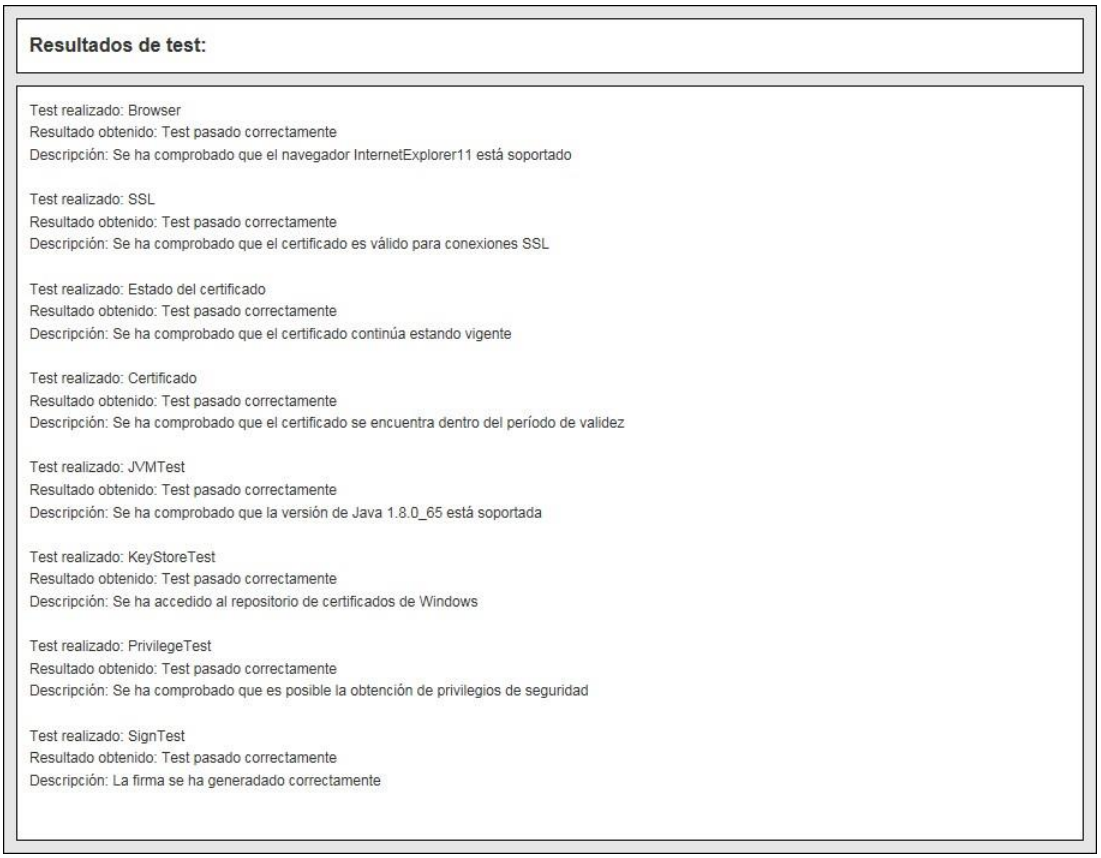
Se nos mostrará una ventana como la siguiente, donde se nos informa de algunas de las características del equipo y del certificado, informando que nos encontramos en el proceso de test.



Una vez finalizado el test, podremos ver la información del test, que debe ser ok en todos sus puntos como muestra la siguiente imagen.



Al final de la página podemos ver con más detalle el resultado del test para las características más importantes, como se muestra en la siguiente imagen.

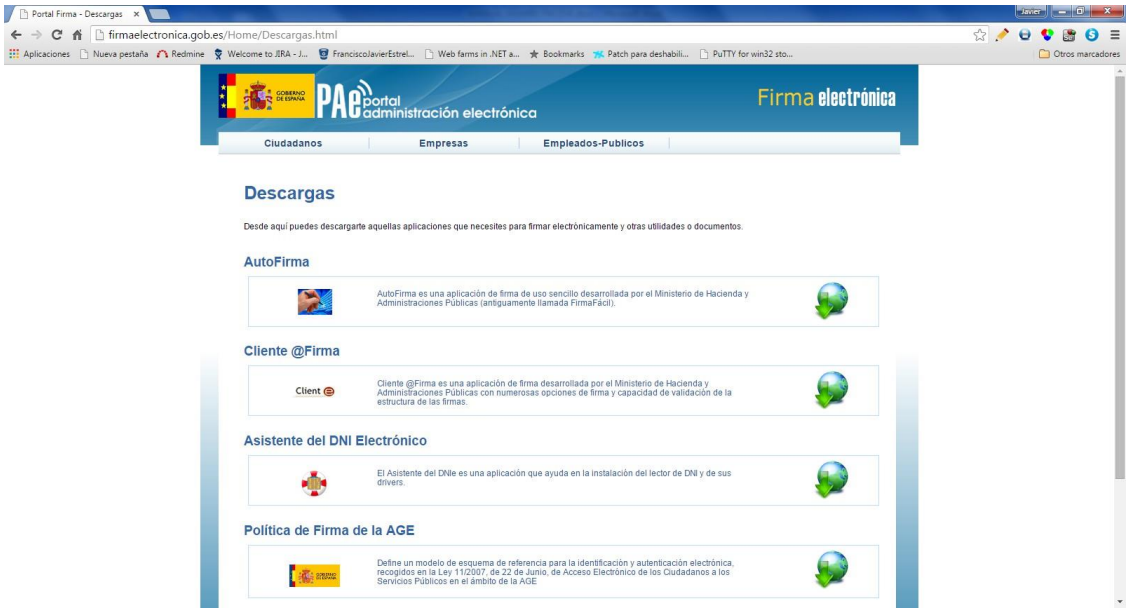


3.2 INSTALACIÓN DE LA APLICACIÓN AUTOFIRMA

Será necesario que el usuario instale la aplicación de **AutoFirma** para el correcto funcionamiento de la firma, tanto en navegadores de tipo Chrome, como en navegadores o configuración en las cuales no quede soportado Java o se presenten errores a la hora de cargar el **MiniApplet** de Java de la plataforma **@Firma**.

Por favor, descargue e instale el programa de **AutoFirma** desde la siguiente url:

http://firmaelectronica.gob.es/Home/Descargas.html



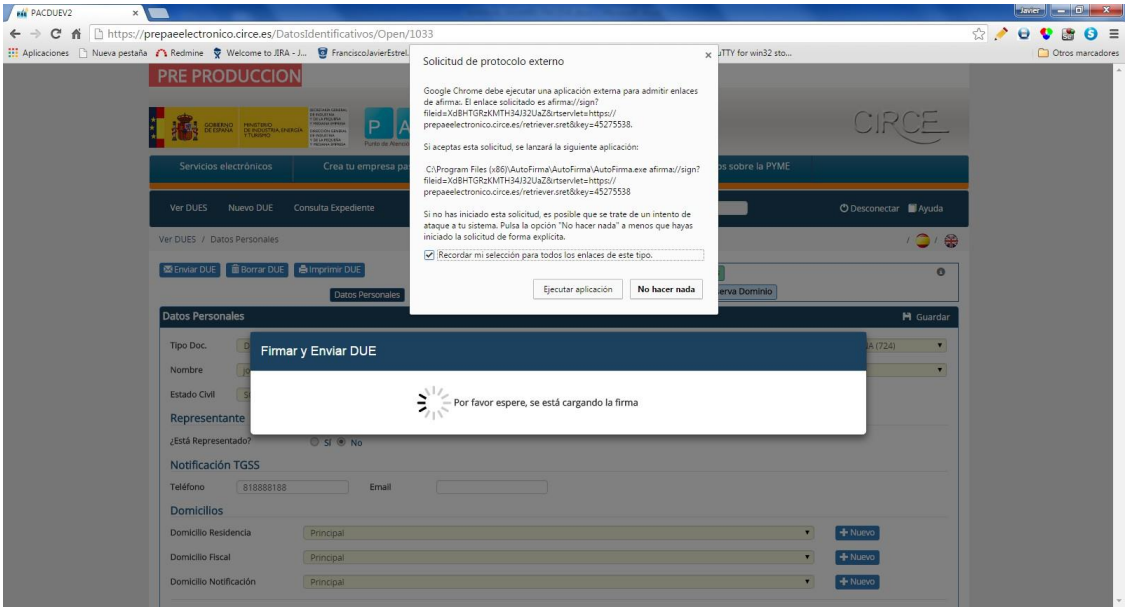
Por favor instale el programa en su equipo, siguiendo las instrucciones del mismo.

Este programa debe estar instalado en el equipo cliente con permisos de administrador para que el usuario pueda ejecutarlo correctamente.

En caso de problemas de conexión entre el navegador y AutoFirma, motivados por una configuración de firewall, deberá de ser comprobada por los administradores de las máquinas asociadas.

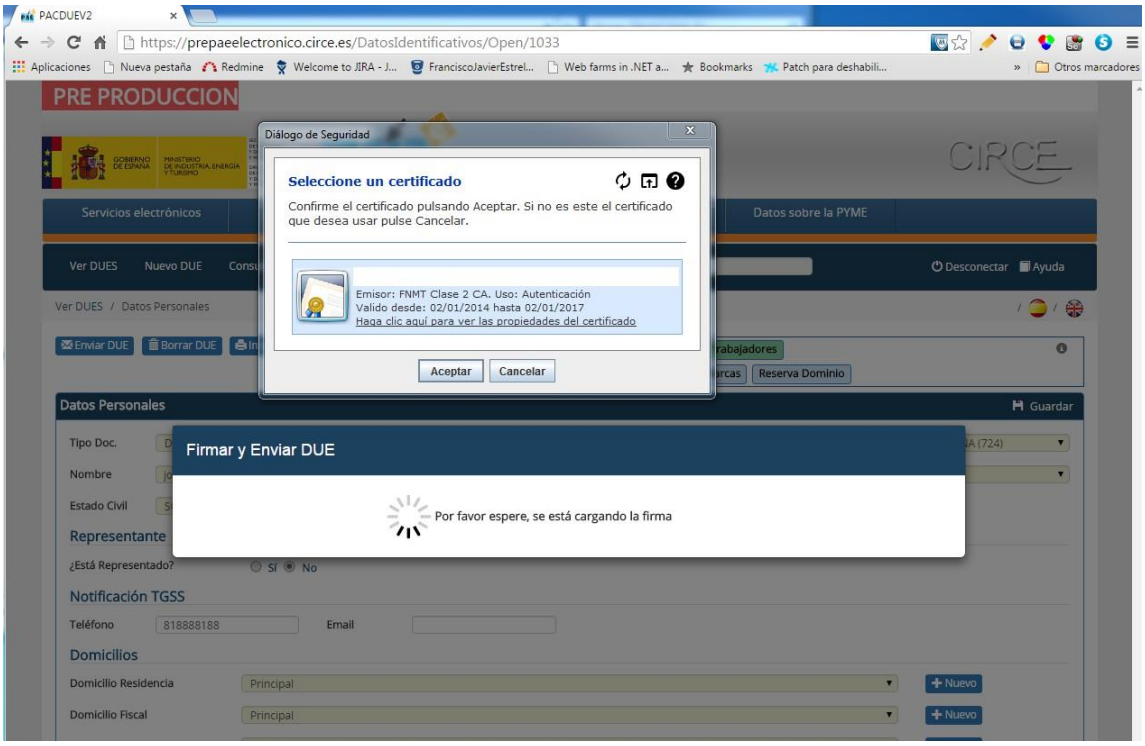
3.3 DESARROLLO DE UN PROCESO DE FIRMA EN CHROME

La primera vez que se desarrolle el proceso de firma desde Chrome (u otro tipo de navegador o entorno que no soporte Java o el **MiniApplet**), se va a solicitar al usuario que se realice una asociación a nivel de su equipo sobre el protocolo "**afirma://",** con respecto el programa **AutoFirma** que se acaba de instalar. Deberemos señalar la opción mostrada en el check de la imagen adjunta, presionando el botón Ejecutar aplicación del diálogo que se muestra.

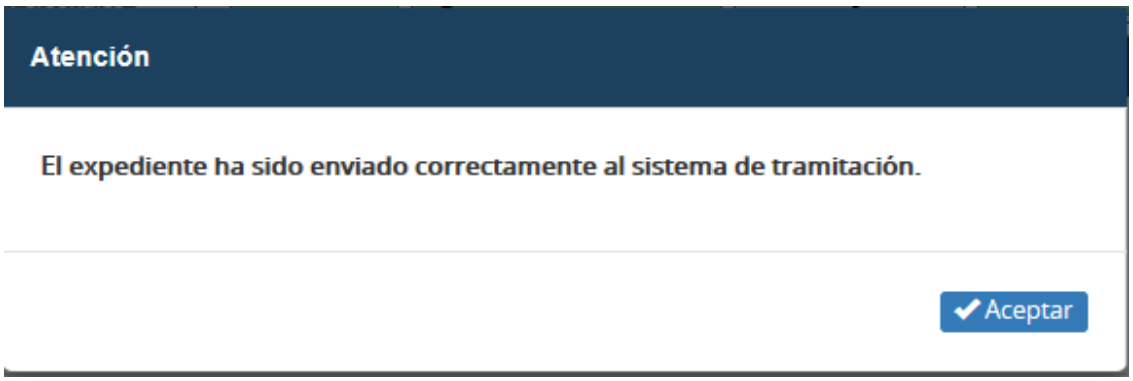


Una vez desarrollado el proceso, veremos que se muestra el diálogo de la aplicación **AutoFirma** cada vez que se desarrolle un proceso de Firma en el cliente, como muestra la imagen adjunta.

Se va a requerir al usuario, que seleccione el certificado de entre los que tenga disponibles en la máquina y asociados con él. Para ello se mostrará el siguiente diálogo solicitando el mismo, pulsando el botón Aceptar **continuará** el proceso de firma y el comienzo del proceso de tramitación.

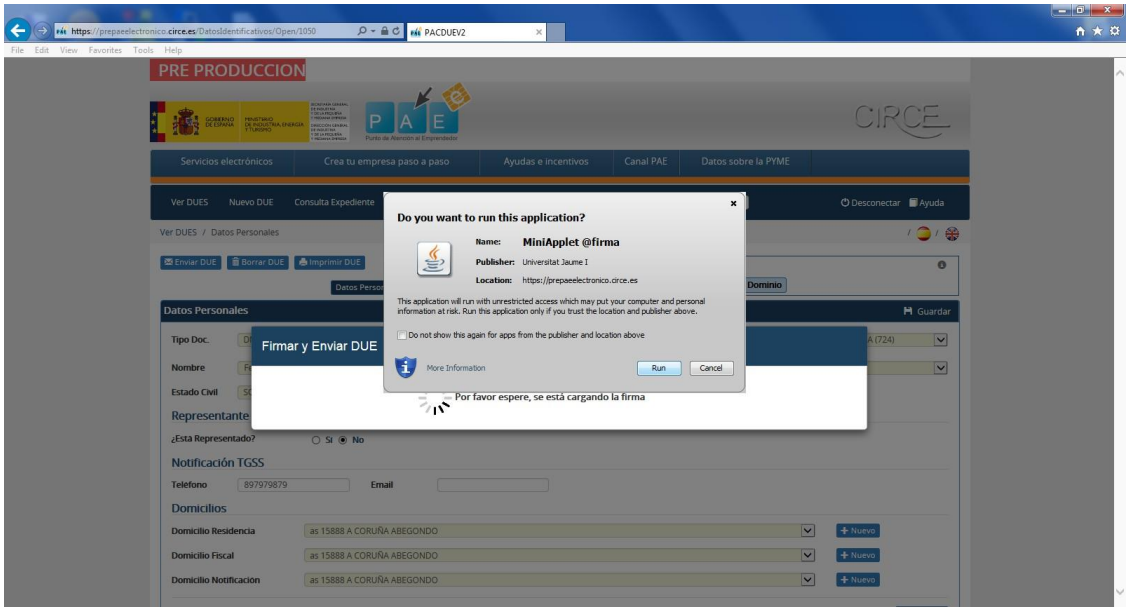


Por último se informará al usuario del envío del DUE al Sistema de Tramitación Telemática, tal como refleja la siguiente imagen, en este caso se dará por concluido el envío del DUE junto con su firma por parte del técnico.

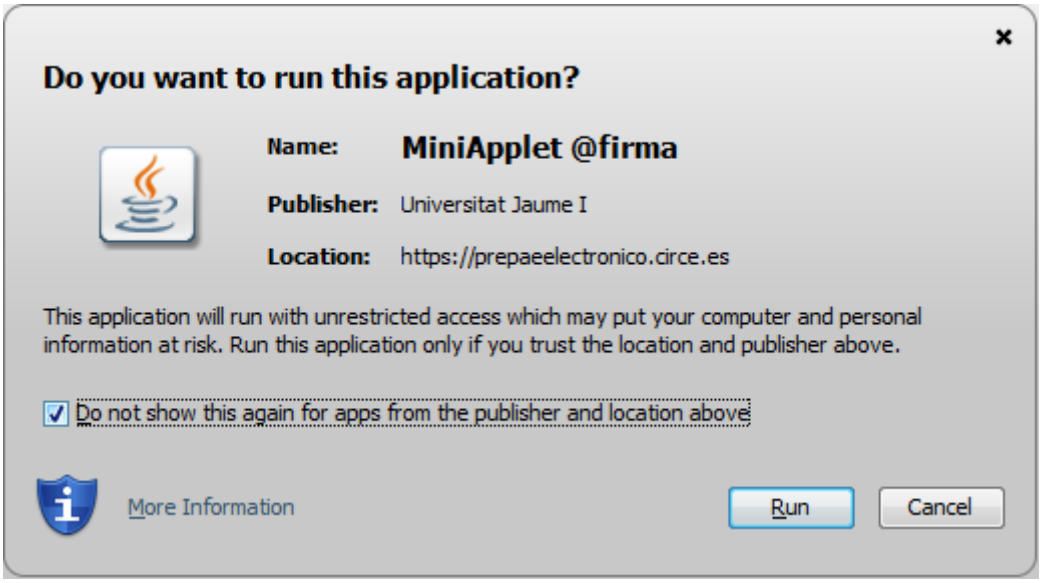


3.4 DESARROLLO DE UN PROCESO DE FIRMA EN EXPLORER

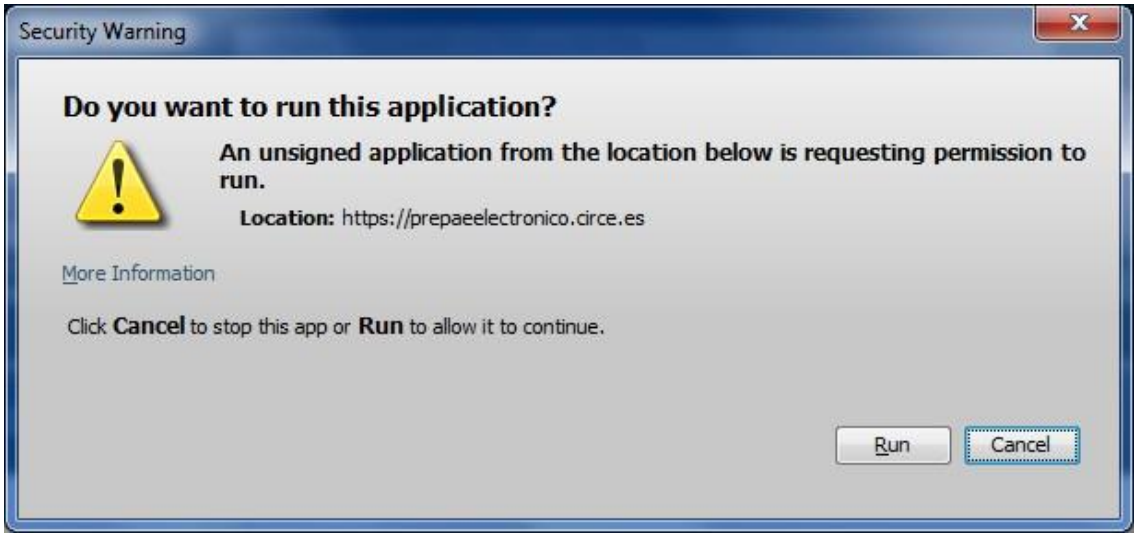
Inicialmente al presionar el botón Enviar DUE que va a desarrollar el proceso de firma en cliente y el envío del DUE al Sistema Telemático de Tramitación, va a solicitar confirmación para la ejecución del MiniApplet, podemos marcar el check visible en el diálogo donde se solicita que no se vuelva a mostrar el diálogo, de esta forma en la siguiente iteración, no se mostrará de nuevo el diálogo.



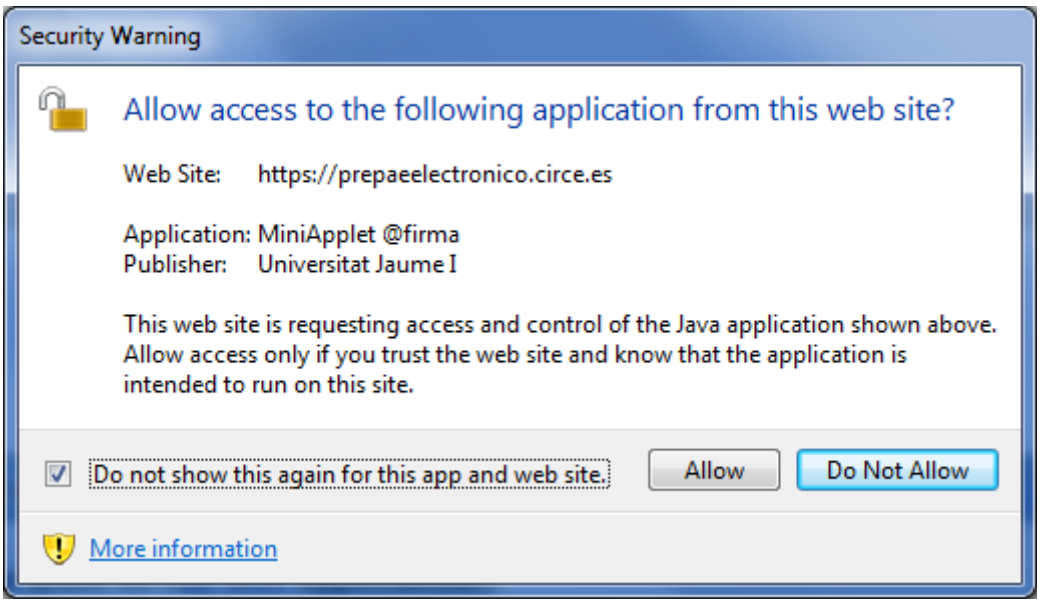
A continuación, en función de la configuración del equipo, se puede solicitar al usuario permiso para la ejecución del **MiniApplet**, mostrando el siguiente diálogo. Se puede seleccionar la opción de no volver a mostrar el diálogo.



A continuación, se va a solicitar al usuario la ejecución de la aplicación, en este caso será necesario presionar el botón Run.



Por último, la seguridad va a solicitar el acceso a la url del entorno, como en casos anteriores podemos configurar el sistema para que no se vuelva a mostrar este diálogo, seleccionando la opción **Allow** (Permitir).



Por último, se va a solicitar un certificado con el cual desarrollar el proceso de firma del DUE, como muestra el diálogo siguiente.

En función de la configuración y librerías de la máquina es posible que se acceda a la clave privada por parte de la aplicación **CryptoAPI**, debiendo aceptar la misma.

Por último, se informará al usuario del envío del DUE al Sistema de Tramitación Telemática, tal como refleja la siguiente imagen, en este caso se dará por concluido el envío del DUE junto con su firma por parte del técnico.