GUÍA RÁPIDA DE INCIDENCIAS EN LA FIRMA ELECTRÓNICA

INTRODUCCIÓN

Este documento pretende dar solución, de una manera concisa, a las incidencias que se presentan a la hora de realizar una firma electrónica en la aplicación Coopera 2020 y que puede llevar a la imposibilidad de realizar la misma.

No pretende ser una guía exahustiva de todas las incidencias que pueden surgir, sino más bien una fuente de consulta para las más comunes, que por otro lado son el porcentaje más significativo, así como facilitar la comprobación y configuración correcta de los programas afectados para la realización de aquella.

Se parte de la base de que se conocen los conceptos básicos relativos a la identificación, autenticación y firma electrónica (al respecto, se puede consultar información en el Portal de la Administración Electrónica http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html), así como estar en posesión en España de un certificado digital compatible con la plataforma @firma, o en el caso de Portugal, de la tarjeta ciudadana (cartao portuguesa). A partir del 8 de abril de 2021, para usuarios portugueses también es posible utilizar la Chave Móvel Digita (CMD) como sistema de identificación electronica para acceder a Coopera 2020. No obstante, este sistema no podrá utilizarse para firmar electrónicamente, debiendose utilizar en este caso la cartao.

sta guía se centra en la casuística derivada de los certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT) por ser los de uso más común, por lo que los usuarios que utilicen otros certificados digitales tendrán que realizar la interpretación analógica oportuna para determinar qué es aplicable en su caso (módulo criptográfico, instalación del certificado raíz de la entidad emisora…). A tales efectos, se recomienda acudir al sitio web del Prestador de Servicios de Certificación (PSC) que haya emitido su certificado.

El ordenador donde se ejecute la aplicación deberá reunir una serie de especificaciones (programas instalados, configuración de los mismos, lector de tarjetas inteligentes en su caso, etc.), bajo las cuales está garantizado el funcionamiento de la aplicación sin ningún tipo de problema. Se podría denominar el escenario óptimo de ejecución.

En Coopera 2020 se utiliza AutoFirma (autofirm@) en todos sus escenarios.

INSTALACIÓN DE AUTOFIRM@

Instalación de “AutoFirma”

Se puede realizar la descarga del ejecutable AutoFirma desde el Portal de Administración Electrónica, eligiendo la opción: http://firmaelectronica.gob.es/Home/Descargas.html Al descomprimir el archivo,

encontrará al menos un fichero ejecutable, que es el que debe instalar, y un documento denominado "AF_manual_instalacion_usuarios_ES.PDF", que contiene toda la información relativa a la instalación de este software. Se debe instalar en el equipo, confirmando todo lo que el asistente proporcione por defecto. Si se instala el navegador posteriormente a la instalación de Autofirma o bien se realizan actualizaciones de dicho navegador y se aprecia que el proceso de AutoFirma está dando problemas, se recomienda proceder de nuevo a la instalación de AutoFirma a través del ejecutable descargado del Portal de Administración Electrónica y el problema quedará solucionado. Se recomienda realizar la instalación de la aplicación AutoFirma con los navegadores cerrados.

ÚLTIMOS CAMBIOS

A continuación, se detalla cómo comprobar o modificar configuraciones relativas a la aplicación Coopera 2020, aunque no tengan relación directa con el proceso de firma electrónica pero sí con el correcto funcionamiento de la citada aplicación.

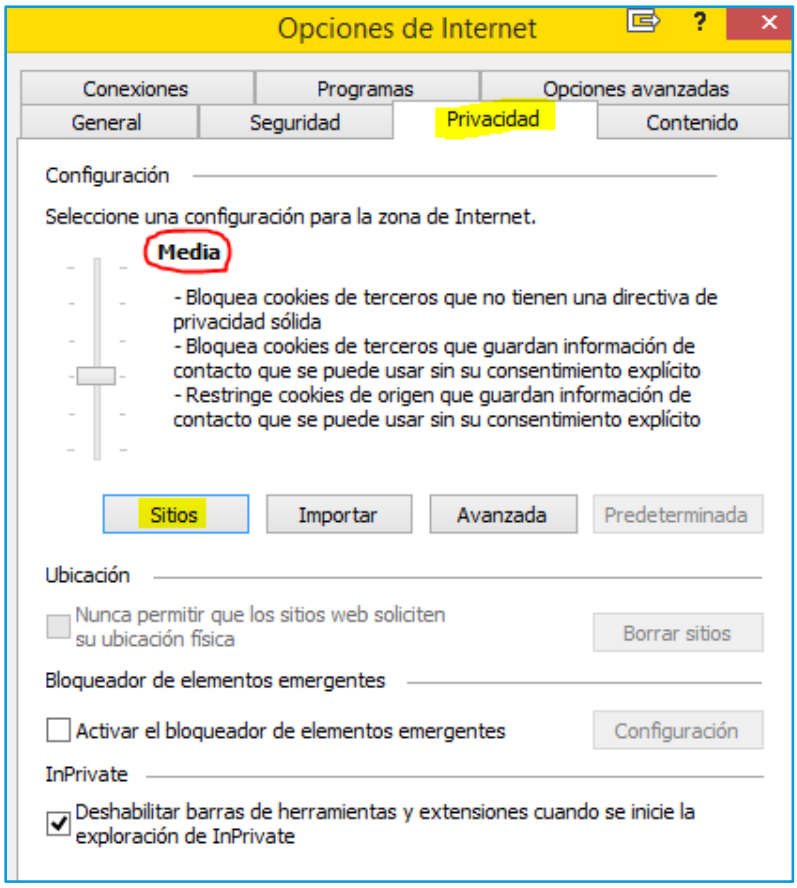
NAVEGADOR: INTERNET EXPLORER

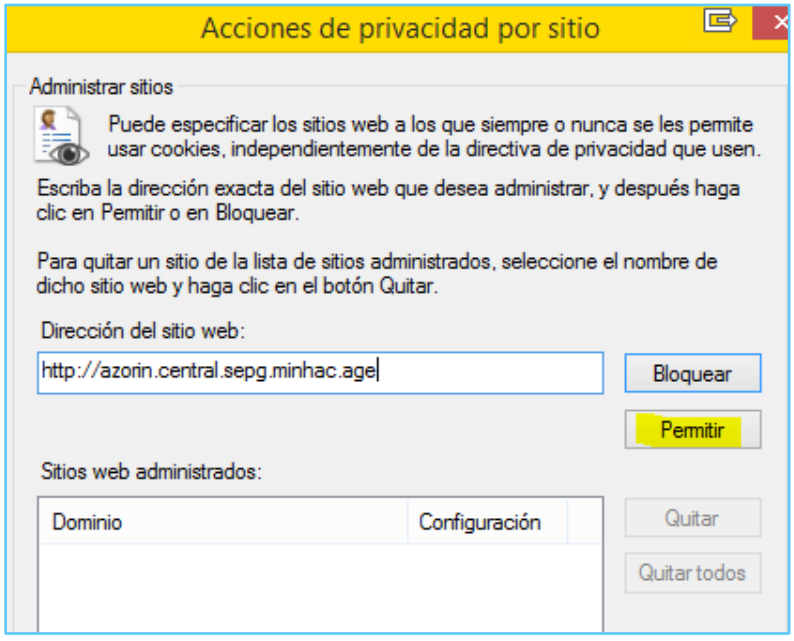
Javascript activado

La activación de javascript se ha detallado en el apartado *'Escenario óptimo'* al especificar la configuración del navegador para las distintas zonas de Seguridad del mismo. Es el parámetro *'Active scripting'*, dentro de la lista de configuración del *'Nivel personalizado…'*.

Cookies activadas

Las cookies, en Internet Explorer 11, las administra automáticamente el navegador**.** Para asegurarse de no tener problemas con ellas, hay que acceder a las *Opciones de Internet* desde el navegador y seleccionar la pestaña *'Privacidad'*, pulsar el botón *'Sitios'* y, en la ventana emergente, añadir la dirección URL del sitio de la aplicación. En su primer tramo como se ha explicado en el inicio del apartado Incidencias de esta guía, en la caja de texto *'Dirección del sitio web:'*, se pulsa el botón *'Permitir'*. De esta manera se estará permitiendo explícitamente las cookies del sitio web de la aplicación.



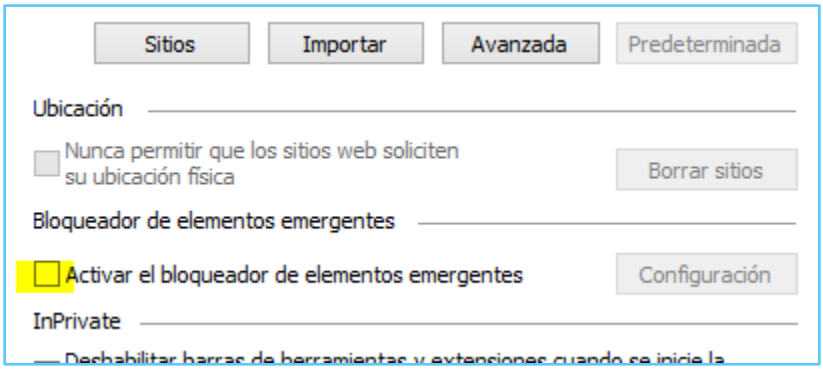


En la lista *'Sitios web administrados'* aparecerá el dominio del sitio web con la configuración de *'Permitir siempre'*.

El nivel de configuración para la zona de Internet en la pestaña de *'Privacidad'* se recomienda que esté en ***'Media'***.

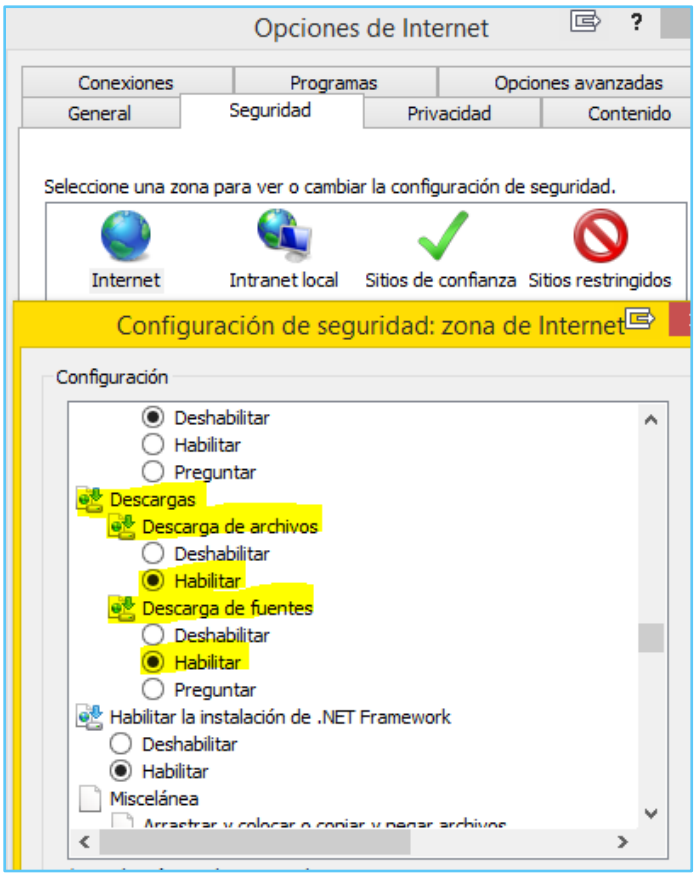
Pop-ups (ventanas emergentes) activadas

En la ventana anterior de *'Privacidad'*, se encuentra la activación o desactivación de las ventanas emergentes, dentro del apartado *'Bloqueador de elementos emergentes'*. Tiene que estar como se muestra en la imagen siguiente (permite las ventanas emergentes).



Habilitar descarga de archivos y fuentes

Se encuentra en la configuración de las zonas de seguridad del navegador ('*Internet*', '*Intranet local*', '*Sitios de confianza*') que ya se ha comentado en reiteradas ocasiones a lo largo de esta guía. Se pulsa en el botón *'Nivel personalizado…'* y buscando en el grupo *'Descargas'*, los apartados *'Descarga de ficheros'* y *'Descarga de fuentes'* deben estar con el valor *'Habilitar'*.



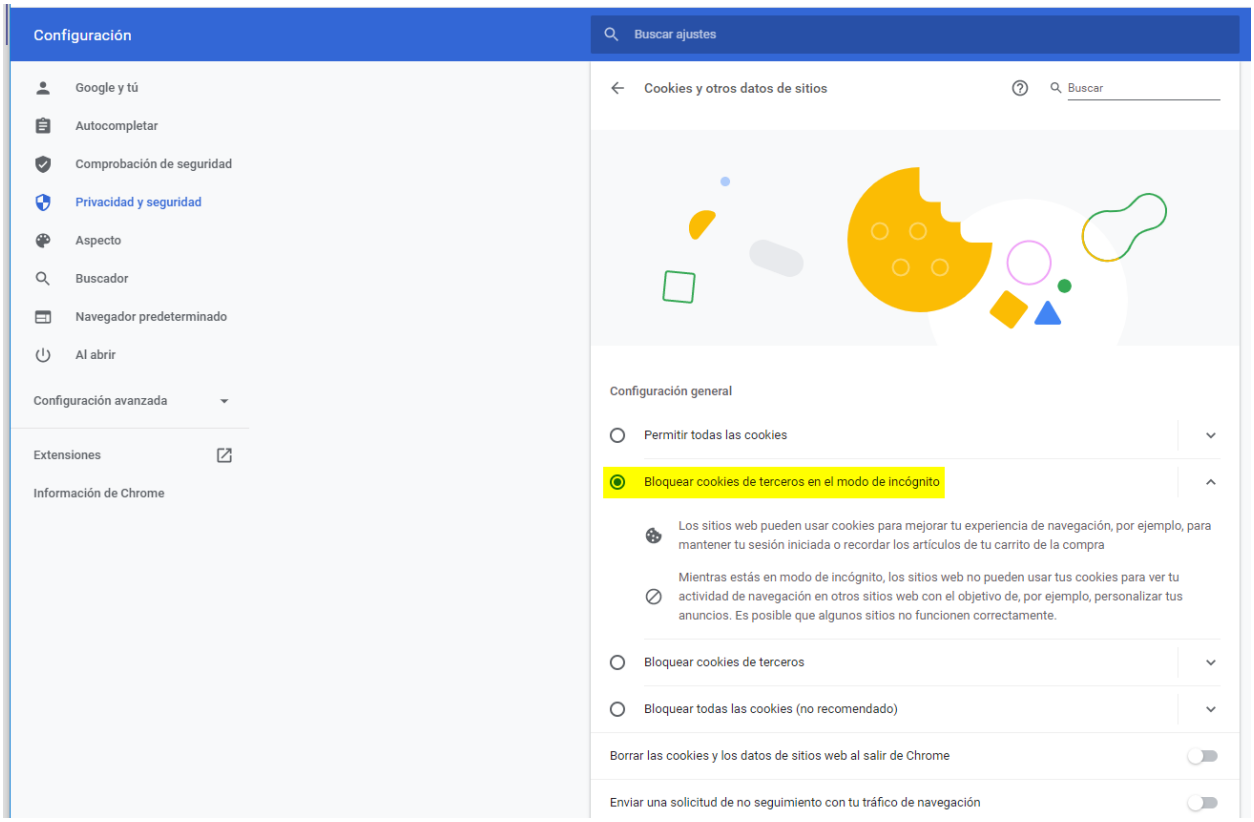
NAVEGADOR: CHROME

Javascript activado

La activación de javascript se realiza en “personaliza y controla Google Chrome“ (Tres puntos verticales). En “configuración”, se selecciona “Privacidad y seguridad”, en esta opción, se selecciona “Configuración de sitios web” y dentro de esta opción debe de estar “**JAVASCRIPT” permitido**.

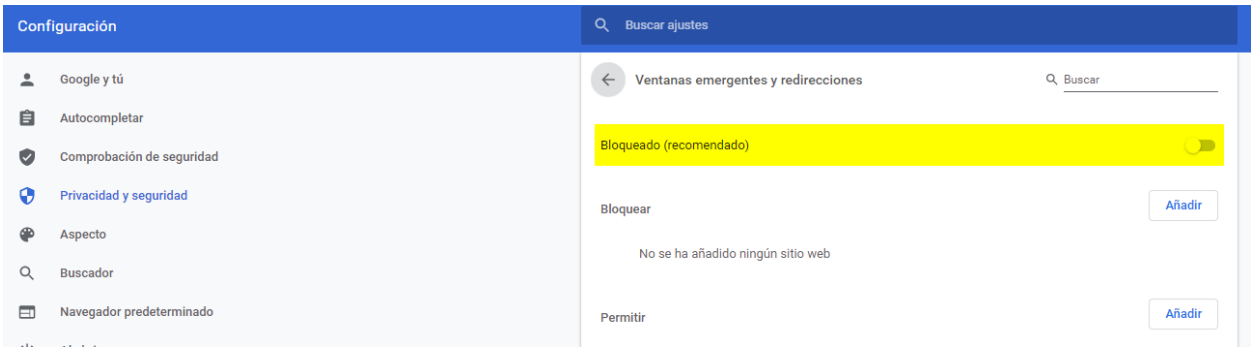
Cookies activadas

Esta opción se encuentra en “personaliza y controla Google CHROME “(Tres puntos verticales). En “configuración”, se selecciona “Privacidad y seguridad”, en esta opción, se selecciona “Configuración de sitios web” y dentro de esta opción debe de estar en “**Cookies y otros datos de sitios**” **como se muestra en pantalla.**



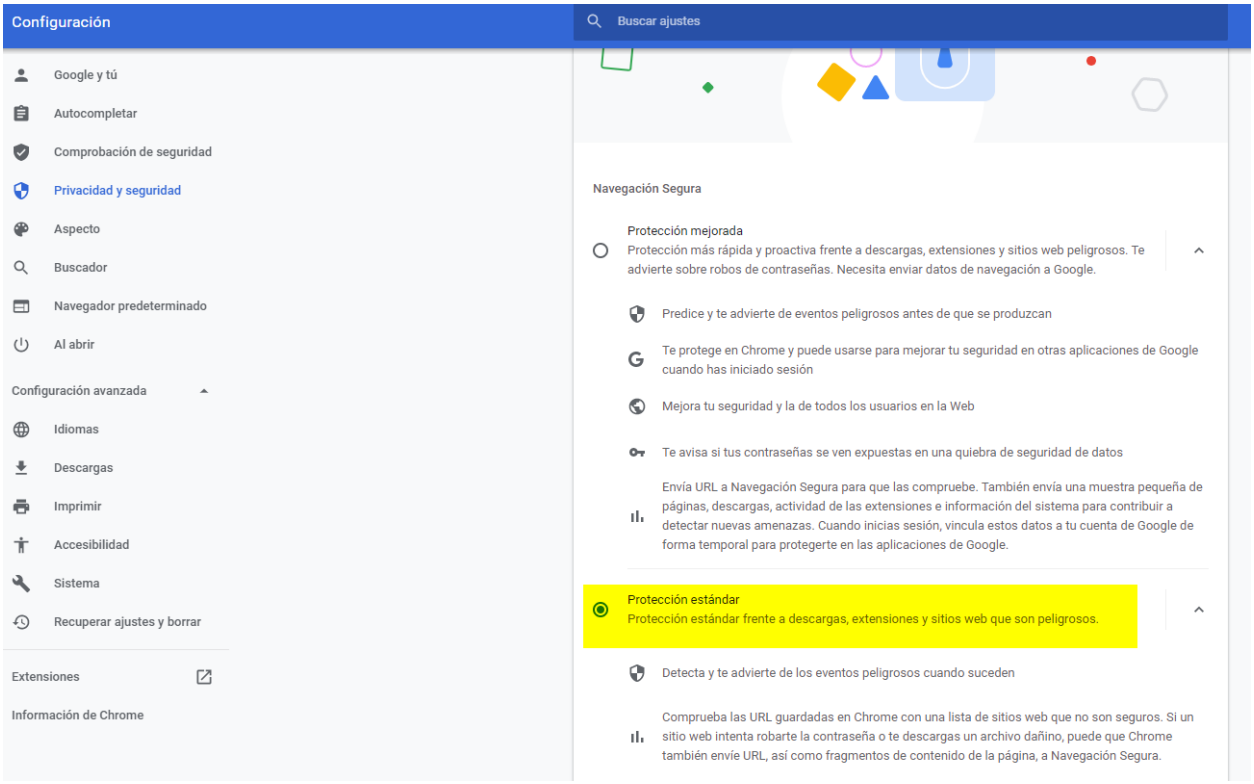
Pop-ups (ventanas emergentes) activadas

Esta opción se encuentra en “Personaliza y controla Google Chrome“ (Tres puntos verticales). En “configuración”, se selecciona “Privacidad y seguridad”, en esta opción, se selecciona “Configuración de sitios web” y dentro de esta opción debe de estar en “**Ventanas emergentes y redireccionados**” c**omo se muestra en pantalla (Desactivado).**



Habilitar descarga de archivos y fuentes

Esta opción se encuentra en “Personaliza y controla Google Chrome“ (Tres puntos verticales). En “configuración”, se selecciona “Privacidad y seguridad”, en esta opción, se selecciona “Seguridad” y dentro de esta opción debe de estar marcada “**Protección estándar**” **marcada**, **como se muestra en pantalla.**



ESCENARIO ÓPTIMO

Los programas que inciden directamente en la firma electrónica, establecidos por la División de Explotación (DIVE) de la Oficina de Informática Presupuestaria (OIP) de la Intervención General de la Administración del Estado (IGAE) para los entornos integrados de la Administración Presupuestaria (AP), son los que se indican:

SISTEMA OPERATIVO: A partir de Windows 8.1

NAVEGADOR: CHROME, Internet Explorer.

CLIENTE FNMT: Configurador FNMT. Versión 3.5 ó superior (opcional).

NOTA: Si se instala el Módulo Criptográfico, no hace falta este cliente por estar incuido en aquel.

MÓDULO CRIPTOGRÁFICO (*): TC-FNMT, versión 5.3.0 ó superior

(*) – Este software solo hace falta si el certificado digital se encuentra en una tarjeta criptográfica.

NOTA: No hace falta instalar ningún cliente para usar el DNIe ya que Microsoft lo incorpora por defecto en Windows 10

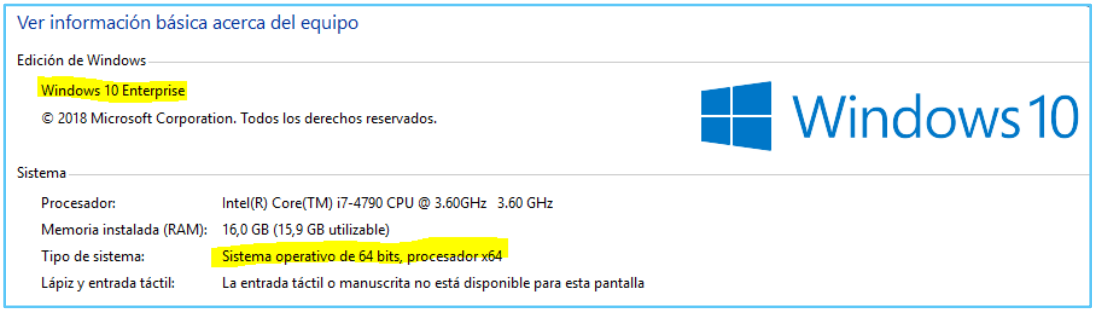
CERTIFICADO DIGITAL COMPATIBLE. Es la pieza más relevante en el proceso de firma electrónica.

Como antes se ha indicado, para certificados emitidos por otros PSC el software a instalar será el que en cada caso corresponda.

Para comprobar que los programas instalados son de las versiones correctas se puede proceder como sigue:

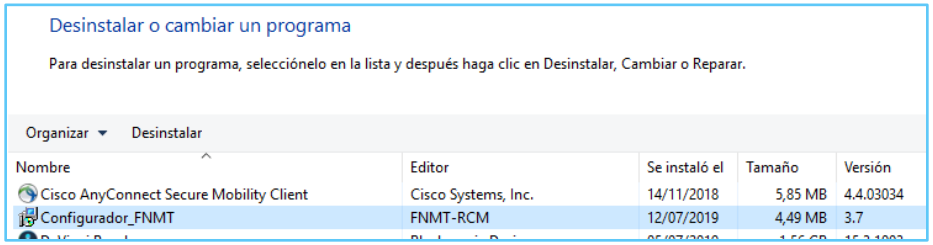
- **SISTEMA OPERATIVO (S.O.)**

  Se pulsa con el botón derecho del ratón en el icono del escritorio *'Este equipo'* y se selecciona 'P*ropiedades'.* En la ventana emergente se pueden comprobar los datos del S.O.

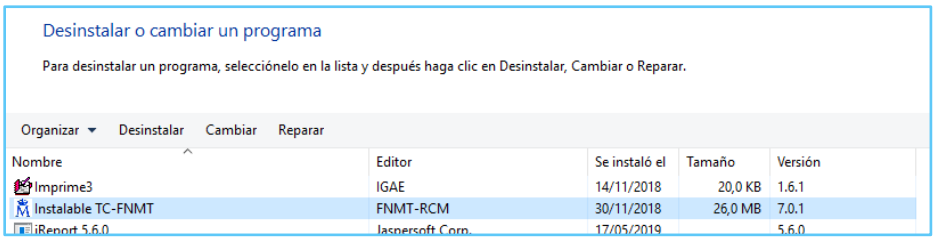


CLIENTE FNMT (opcional)

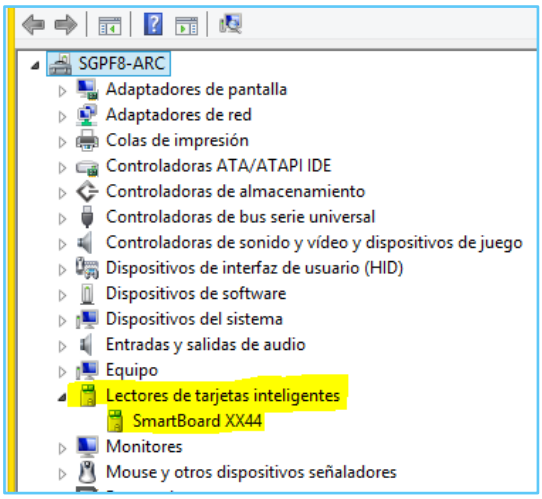
En la localización anterior *(Programas y características)*, se busca la línea *'Configurador_FNMT'*. En la columna *'Versión'* se localiza la versión del programa que está instalado. Recordar que no es necesario este software si se tiene instalado el Módulo Criptográfico al estar incluido en este. En caso de necesitar instalarlo hay que visitar la web www.fnmt.es de la FNMT.



- **MÓDULO CRIPTOGRÁFICO**
  En el mismo lugar se busca la línea *'Instalable TC-FNMT'*.



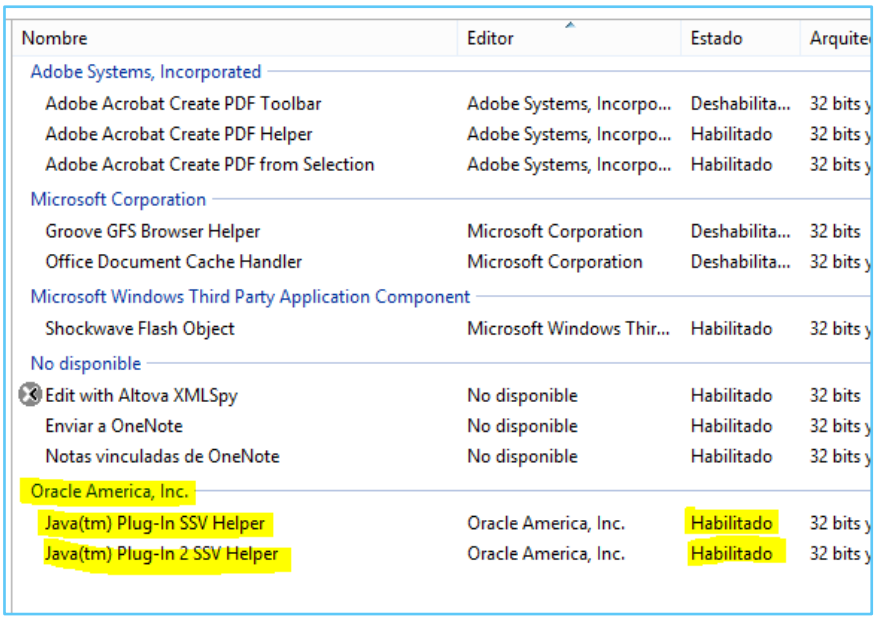
Si se utiliza una tarjeta inteligente que contenga el certificado digital o el DNIe, hace falta que el ordenador disponga de un lector de tarjetas criptográficas (inteligentes) y que esté correctamente instalado. La manera rápida de verificar si está instalado el mencionado lector es accediendo al *Panel de Control - Administrador de Dispositivos* y comprobando que existe un apartado de *'Lectores de tarjetas inteligentes'* parecido al siguiente:



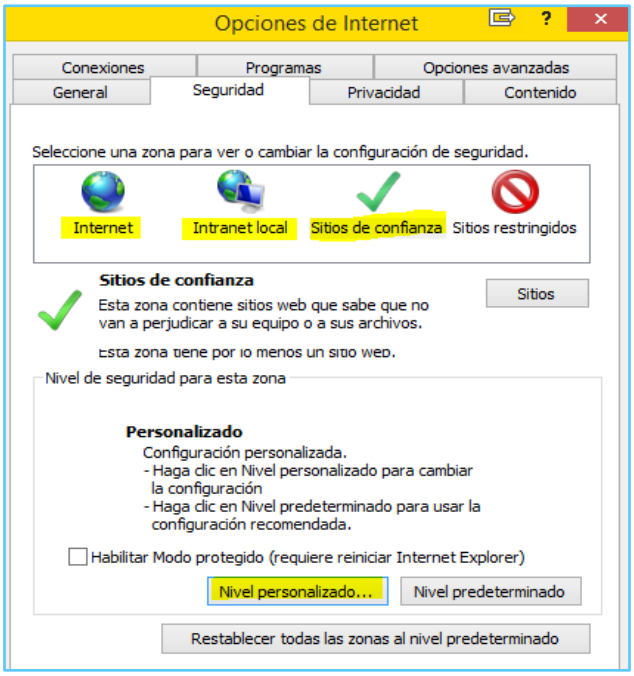
Además de tener instalados los programas anteriores con sus respectivas versiones es importante la configuración correcta de los mismos, ya que una configuración errónea puede causar que no se ejecute el software (AUTOFIRMA) correspondiente en el proceso de firma electrónica.

Una configuración relevante es la del navegador de Internet (Internet Explorer), que tiene que tener habilitados los complementos de Java (Plug-In) y javascript en la zona correspondiente de seguridad.

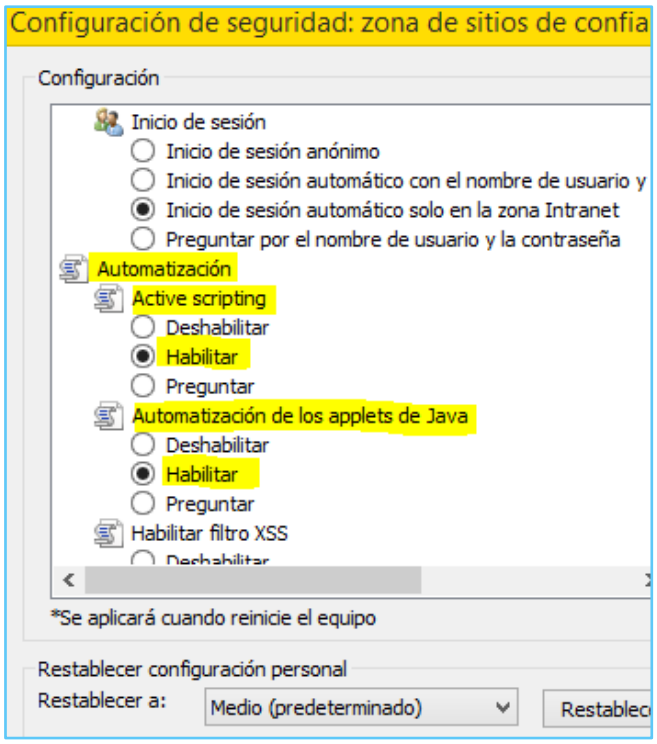
Para verificar estos puntos se necesita abrir el navegador Internet Explorer. Para comprobar que los Plug-in de Java están habilitados se pulsa en la *rueda dentada*, que ya se ha utilizado para verificar la versión del mismo, y se selcciona *'Administrar complementos'*, buscando el grupo *'Oracle America, Inc.'*. Las dos lineas que comprende este grupo tienen que tener *'Habilitado'* la columna *'Estado'*.



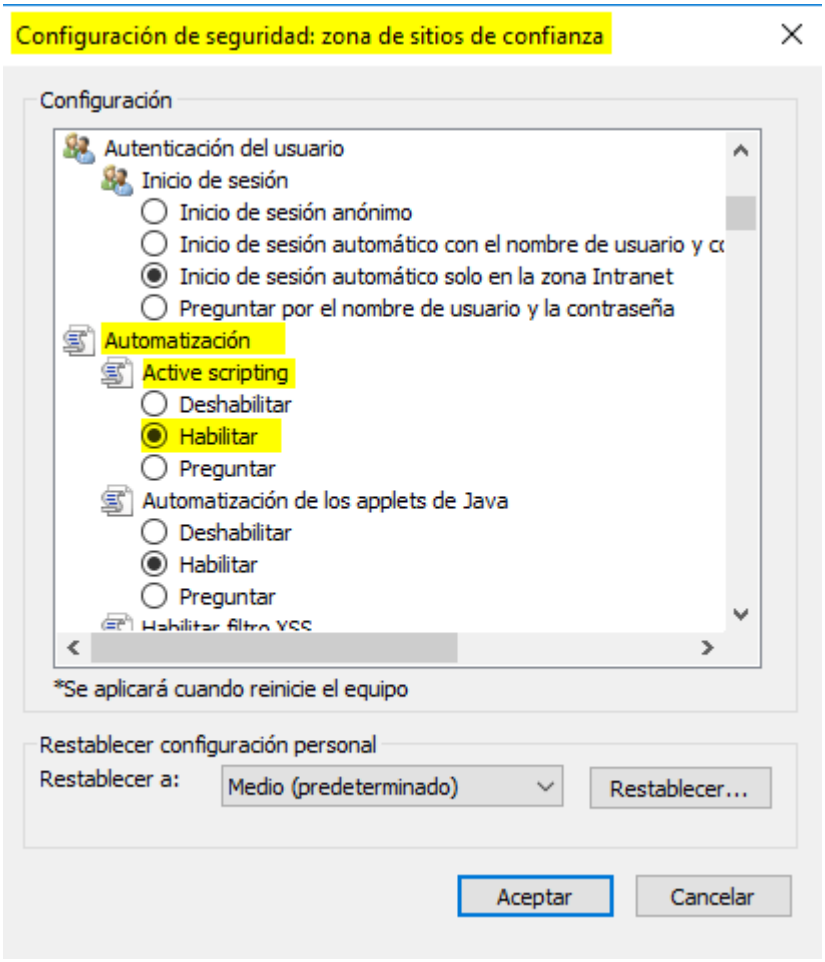
Para comprobar que se pueden ejecutar el código javascript, se pulsa la *rueda dentada* y se selecciona *'Opciones de Internet'*, y en la pestaña *'Seguridad'* se selecciona la zona en la que se quieren comprobar estos valores.



Puede ser *'Internet'*, *'Intranet local'* o *'Sitios de confianza'*, se pulsa en el botón *'Nivel personalizado…'* y se busca el grupo de valores *'Automatización'*. Una vez localizado en la lista emergente, se comprueba que los items *'Active scripting'* esté con el valor *'Habilitar'* .



La ventana anterior es sustituida por la siguiente



Esta operación se puede realizar en las 3 zonas o como se verá en el apartado de Incidencias, solo en la zona de *'Sitios de confianza'*.

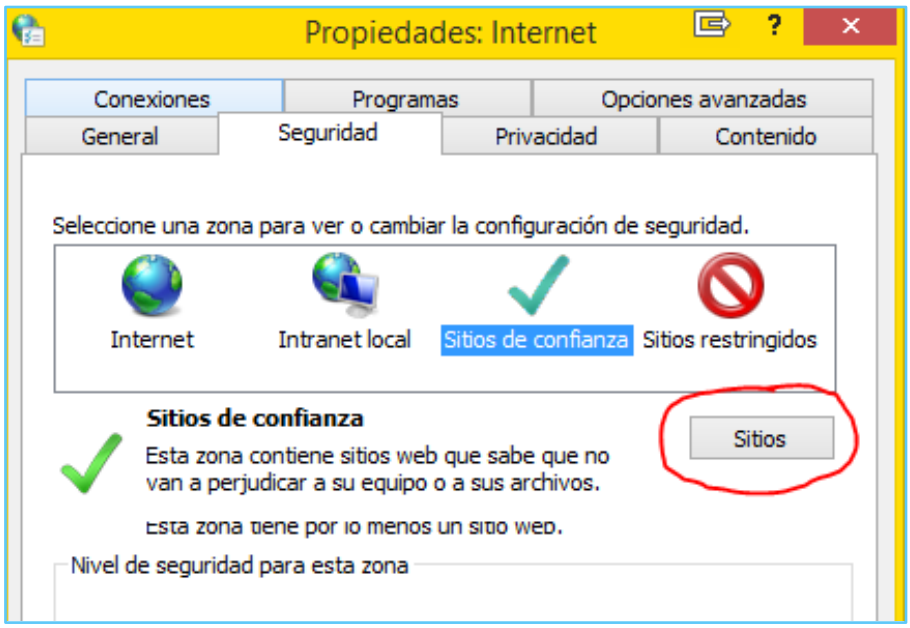
INICIDENCIAS

Con carácter general, si en el transcurso del proceso de firma se produce algún error o incidencia que hiciera que no se terminase el proceso, hay que **cerrar completamente el navegador** y reiniciar la operación.

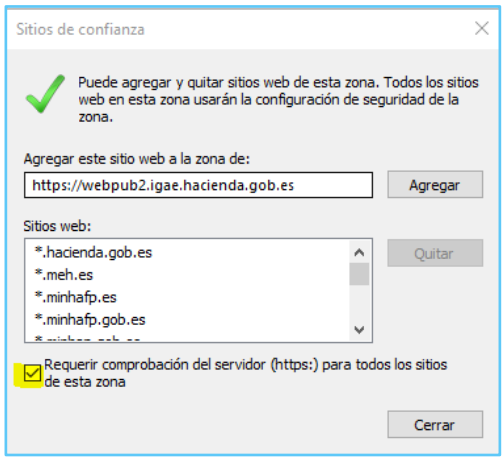
Es altamente recomendable añadir el sitio desde donde se ejecuta la aplicación (URL), poniendo solamente el primer tramo de la misma (por ejemplo: *https://webpub2.igae.hacienda.gob.es*) en los *Sitios de confianza* del navegador para evitar los bloqueos.

En INTERNET EXPLORER:

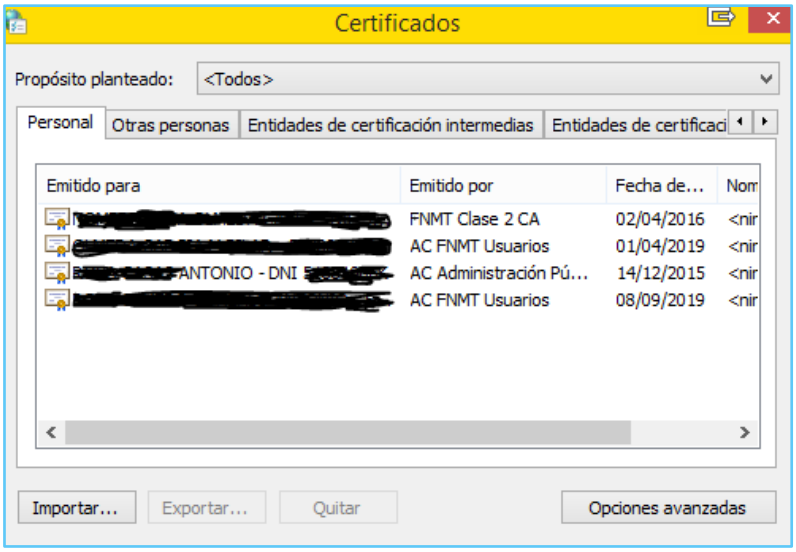
Esto se consigue en '*Panel de control - Opciones de Internet*', en la pestaña de *'Seguridad'*, eligiendo la zona 'Sitios de confianza':



Se pulsa el botón *'Sitios'* y en *'Agregar este sitio web en la zona de:'* se escribe o copia la URL anteriormente citada, marcando la casilla *'Requerir comprobación…..'* y pulsando el botón *'Agregar'*. Debería aparecer la URL introducida en la lista de *'Sitios web:'*

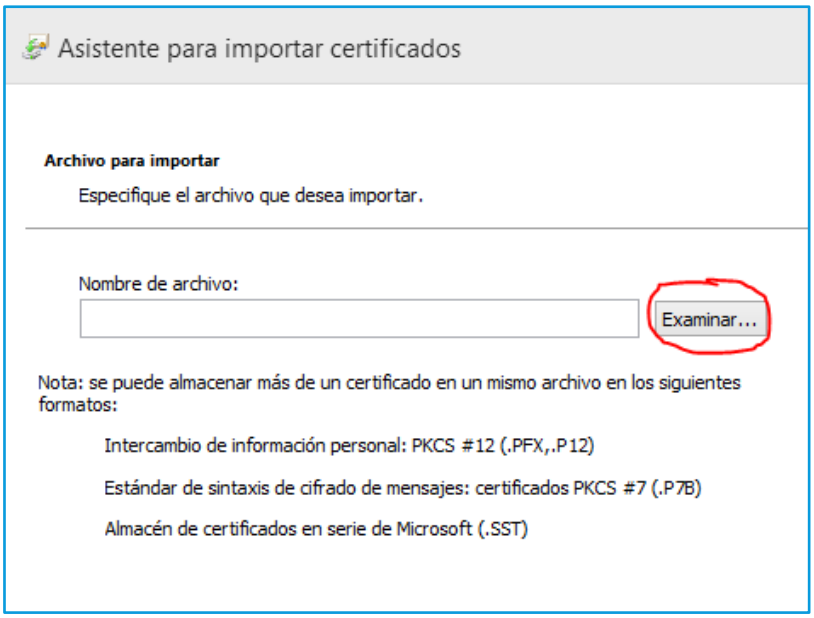


Antes de iniciar el proceso, recomendable al entrar en la aplicación, se debería comprobar la accesibilidad al certificado digital. Se accede al menú *Herramientas – Opciones de Internet*, solapa de '*Contenido*' y botón '*Certificados*', y en la pestaña '*Personal*' debería figurar el certificado que se va a usar, indistintamente de si está instalado en el navegador o en tarjeta inteligente.

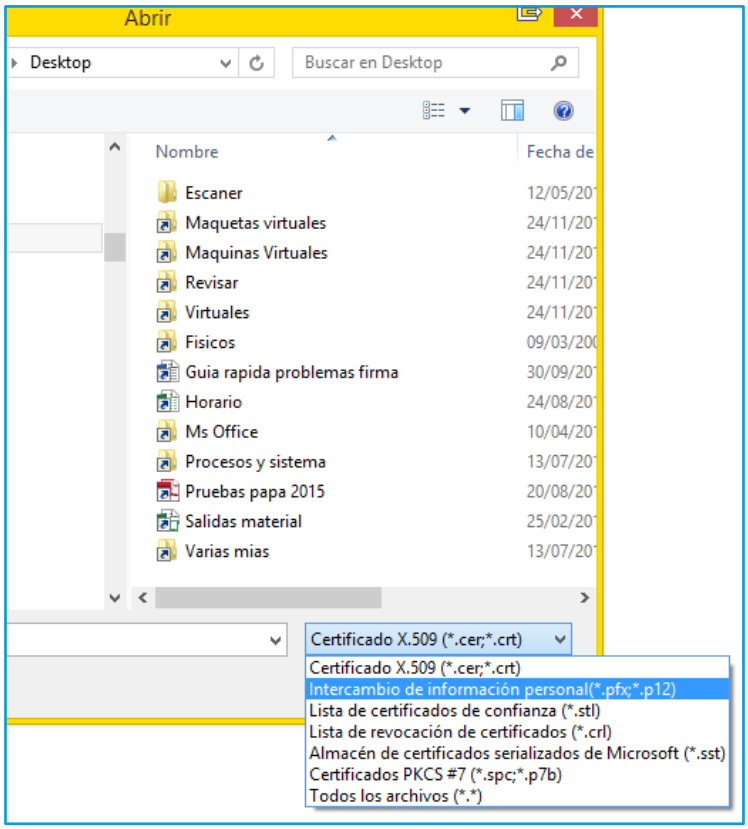


Si no se tiene ningún certificado instalado en el navegador, pero se dispone de él en un fichero, habrá que instalarlo manualmente. Para ello, en la pantalla anterior *(Herramientas-Opciones de Internet-Contenido-Certificados, pestaña 'Personal')*, se pulsa en el botón *'Importar'* y se siguen las instrucciones del asistente. En lo que sigue, se comenta la importación de un certificado personal ubicado en un fichero con extensión *.pfx*, por ser el más común de ellos.

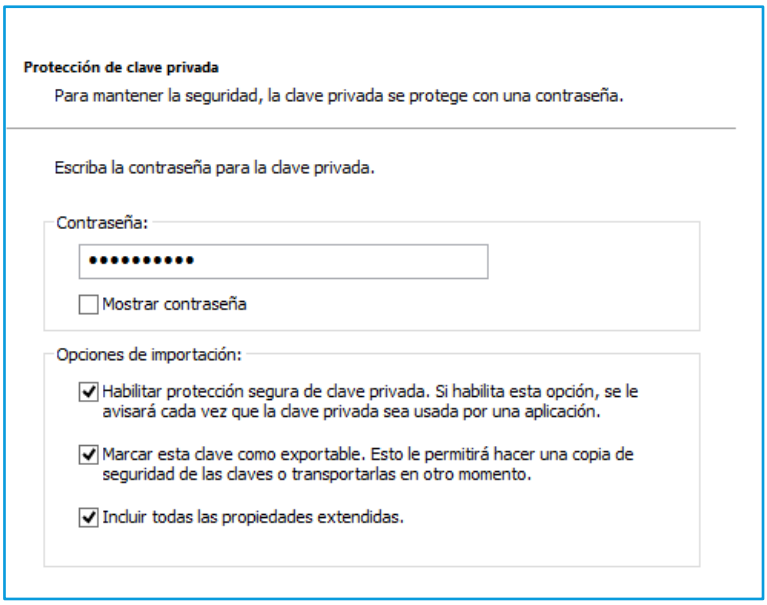
- Se pasa la primera pantalla de *Bienvenida* pulsando el botón *'Siguiente'*.
- En la siguiente pantalla hay que seleccionar el fichero del certificado, pulsando en el botón *'Examinar'.*



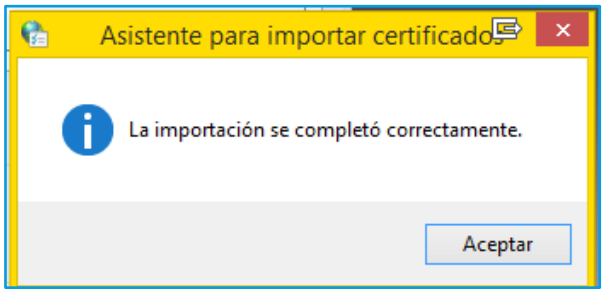
- En el cuadro *'Abrir'* hay que ir hasta donde esté ubicado el fichero y seleccionar el tipo de fichero adecuado en el desplegable correspondiente.



- Pulsar el botón *'Abrir'* y *'Siguiente'*. En esta pantalla hay que introducir la *'Contraseña'*, que sirve para proteger la clave privada del certificado, que tiene que ser conocida (creada en el proceso de exportación detallado más adelante) y habilitar todas las *'Opciones de importación'.*



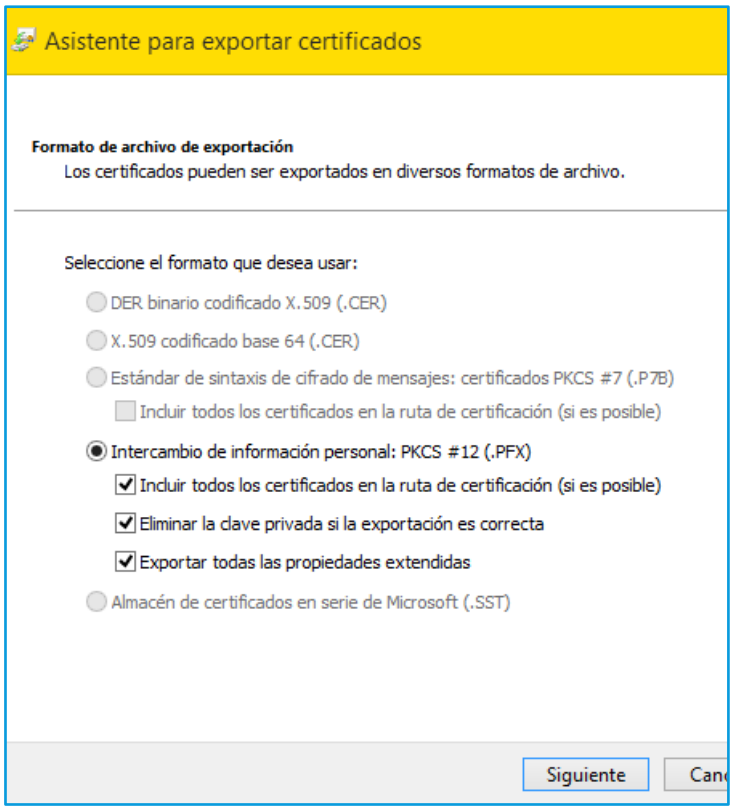
- Las dos pantallas siguientes se pasan con el botón *'Siguiente'* y *'Finalizar'*.
- El proceso mostrará una pantalla para confirmar la importación de la clave privada, se acepta y, si todo ha ido bien, se mostrará un mensaje confirmando que la importación se ha realizado correctamente.



Ahora se podrá confirmar la accesibilidad al certificado digital detallado al inicio del apartado.

Si lo que se necesita es, teniendo el certificado instalado en un ordenador, llevarlo a otro para instalarlo en este, hay que realizar el proceso de exportación del mismo a través del botón *'Exportar'* desde la pantalla de *'Certificados':*

- Como en el proceso de importación, se pasa la pantalla de Bienvenida y en la siguiente se selecciona *'Exportar la clave privada',* pasando a la siguiente pantalla.
- En esta se seleccionan todas las opciones disponibles y se pulsa el botón *'Siguiente'*.



- Se selecciona *'Contraseña'* se introduce una contraseña y se confirma. Esta contraseña sirve para proteger la clave privada que se va a exportar y que pedirá el proceso de importación antes citado.
- A continuación, a través del botón *'Examinar'* se selecciona el destino del fichero resultante de la exportación, naturalmente hay que asegurarse de que el destino del fichero va a ser accesible después de terminar este proceso y se le da un nombre. La extensión del fichero la pone automáticamente el sistema (*pfx*).
- Las siguientes pantallas son iguales al proceso de importación hasta terminar con el mensaje confirmando que la exportación se ha realizado con éxito.

Pide insertar una tarjeta criptográfica

Aun teniendo el certificado instalado en el navegador, se solicita, en una ventana emergente, introducir una tarjeta criptográfica. Esto puede ocurrir si se tiene el lector de tarjetas inteligentes instalado y no se tiene ninguna tarjeta o DNIe introducido en el mismo. Hay que pulsar el botón *'Cancelar'* para que siga el proceso y poder utilizar el certificado instalado en el navegador. En ningún caso hay que cerrar la ventana desde la X blanca situada en la esquina superior derecha.

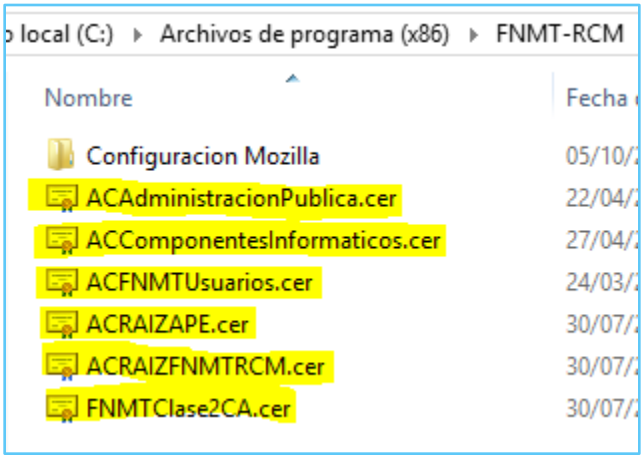
El certificado digital no se puede validar contra el certificado raíz del PSC (FNMT)

A la hora de usar el certificado digital, este no se puede validar porque falta el certificado de la entidad de certificación raíz de confianza (FNMT).

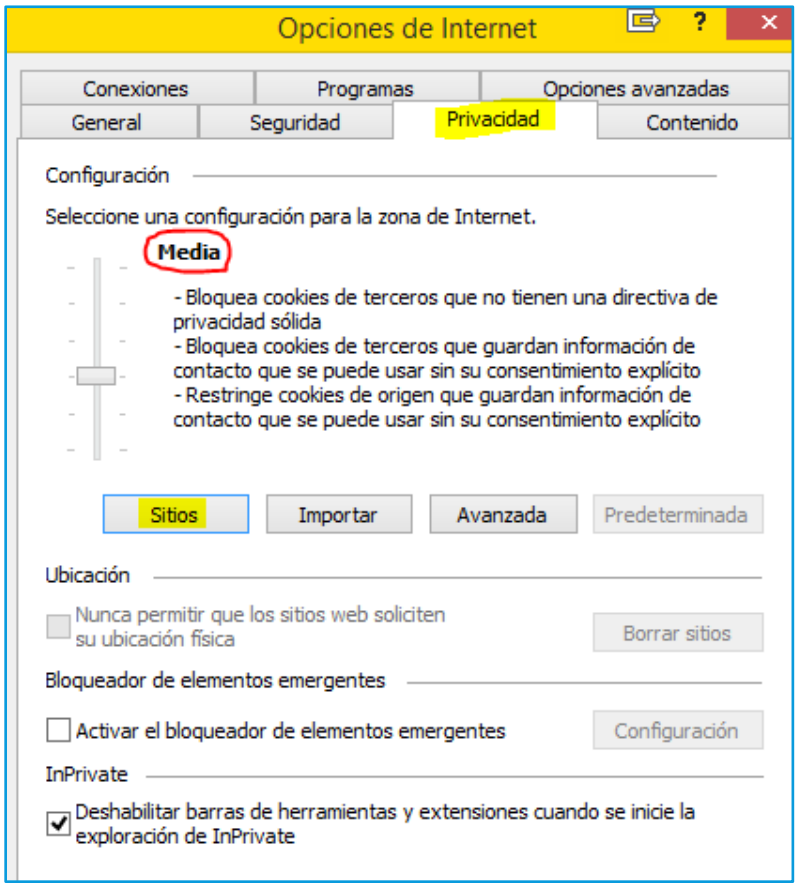
Para resolver esta incidencia hay que instalar manualmente dicho certificado raíz desde la carpeta de instalación del '*Cliente FNMT*' o '*Módulo Criptográfico*' que debe tenerse instalado según se ha visto en el apartado Escenario óptimo. Esta carpeta se suele localizar en '*C:\Archivos de programa\FNMT-RCM*'. En

ella se encontrarán todos los certificados que proporciona la FNMT, como entidad de certificación raíz, durante la instalación de los clientes anteriores.

La lista de estos certificados es la de la siguiente imagen y la instalación de los mismos se realiza como se ha explicado en la '*Importación*' del certificado de usuario al navegador, o bien, haciendo doble-clic en cada uno de los ficheros de dicha lista y siguiendo el asistente.



Se recomienda instalar todos los certificados para tener una mayor seguridad.


Opciones de Internet
Conexiones
Programas
Opciones avanzadas
General
Seguridad
Privacidad
Contenido
Configuración
Seleccione una configuración para la zona de Internet.
Media
- Bloquea cookies de terceros que no tienen una directiva de privacidad sólida
- Bloquea cookies de terceros que guardan información de contacto que se puede usar sin su consentimiento explícito
- Restringe cookies de origen que guardan información de contacto que se puede usar sin su consentimiento explícito
Sitios
Importar
Avanzada
Predeterminada
Ubicación
Nunca permitir que los sitios web soliciten su ubicación física
Borrar sitios
Bloqueador de elementos emergentes
Activar el bloqueador de elementos emergentes
Configuración
InPrivate
Deshabilitar barras de herramientas y extensiones cuando se inicie la exploración de InPrivate