

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 Cooperera 2020 y que puede llevar a la imposibilidad de realizar la misma.

No pretende ser una guía exhaustiva 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 plataformas @firma o, en el caso de Portugal, de la tarjeta ciudadana.

Esta 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 y la ejecución del applet de firma electrónica sin ningún tipo de problema. Se podría denominar el escenario correcto de ejecución.

ESCENARIO CORRECTO

Los programas que inciden directamente en la firma electrónica, establecidos por la Subdirección General de Explotación (SGE) de los Servicios de Informática Presupuestaria (SIP) 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: Windows 8.1 (tanto de 32 como de 64 bits).

NAVEGADOR: Internet Explorer, versión 11.

MÁQUINA VIRTUAL JAVA: Oracle JRE, versión 1.7_*, solo de 32 bits.

(*) – Significa cualquier versión superior, recomendándose la más alta de la familia 1.7.

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

NOTA: Si se instala el Módulo Criptográfico, no hace falta este cliente por estar incluido 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 8.1

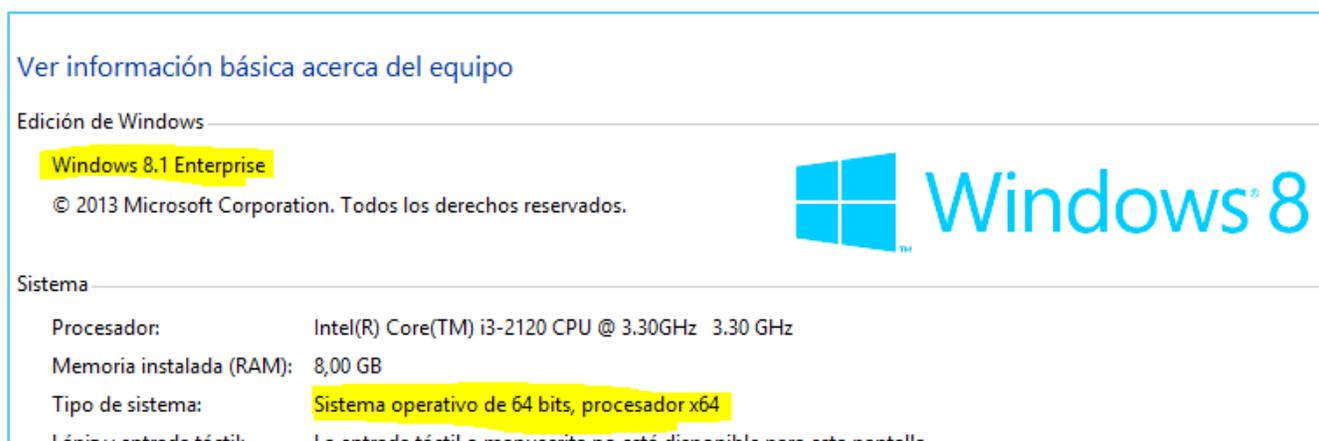
CERTIFICADO DIGITAL COMPATIBLE. Es la pieza más relevante en el proceso de firma electrónica.

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 '*Propiedades*'. En la ventana emergente se pueden comprobar los datos del S.O.



- **NAVEGADOR**

En el S.O. Windows 8.1 el navegador que viene por defecto es Internet Explorer 11 por lo que si la comprobación anterior es correcta la del navegador es implícita.

Independientemente se puede verificar la versión del navegador de la siguiente manera:

- Se pulsa el icono de '*Internet Explorer*' que suele estar en la barra de tareas



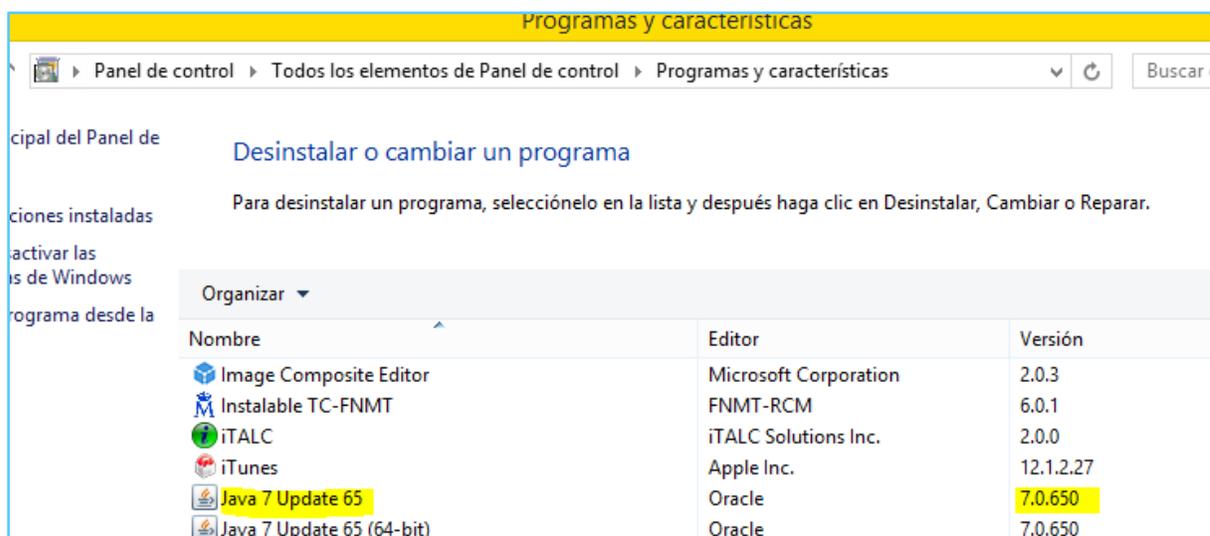
- Una vez abierto el programa, se pulsa en el icono de *rueda dentada* en la parte superior derecha y se elige '*Acerca de Internet Explorer*', mostrándose una ventana con información del navegador, entre ella la versión del mismo.





- **MÁQUINA VIRTUAL JAVA**

En *Panel de Control – Programas y características* se busca la línea '*Java 7 Update XX*', siendo '*XX*' cualquier número. Si no se encuentra esta línea puede que no se tenga Java instalado o que esté una versión incorrecta. En este caso habría que instalarla desde la página www.java.com/es y buscar la versión correcta.



El '*Nombre*' no debe incluir el término (*64-bit*) para asegurarse que es la versión de 32 bits.

En el supuesto de que figure una versión posterior, se recomienda desinstalar esta (desde esta misma pantalla, se selecciona y se pulsa el botón '*Desinstalar*'), e instalar la versión recomendada en esta guía. Esta versión se encuentra disponible en el Portal de la Administración Presupuestaria siendo el proceso reversible.

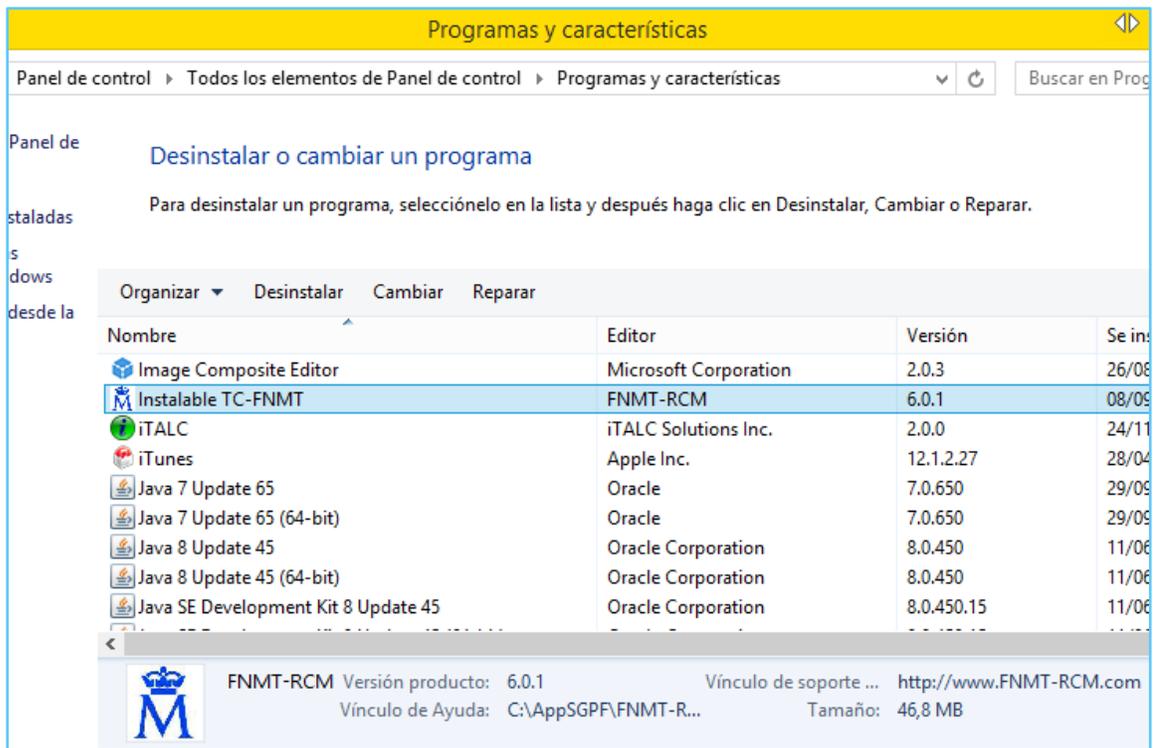
CLIENTE FNMT (opcional)

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.

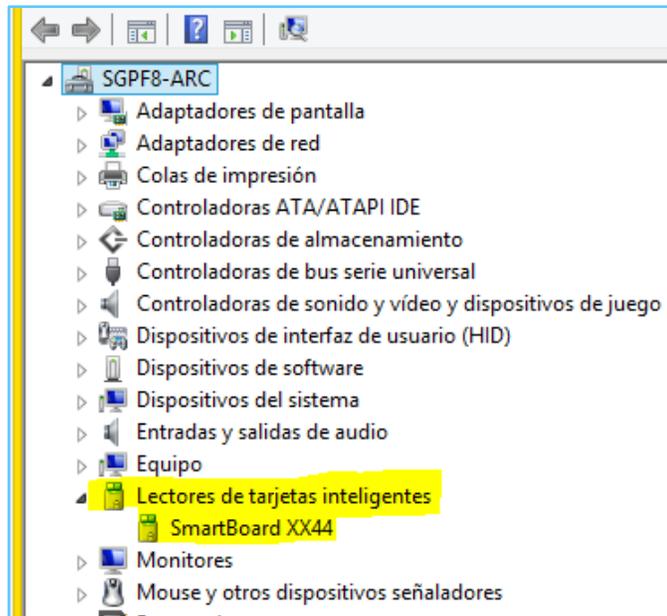


- **MÓDULO CRIPTOGRÁFICO**

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:



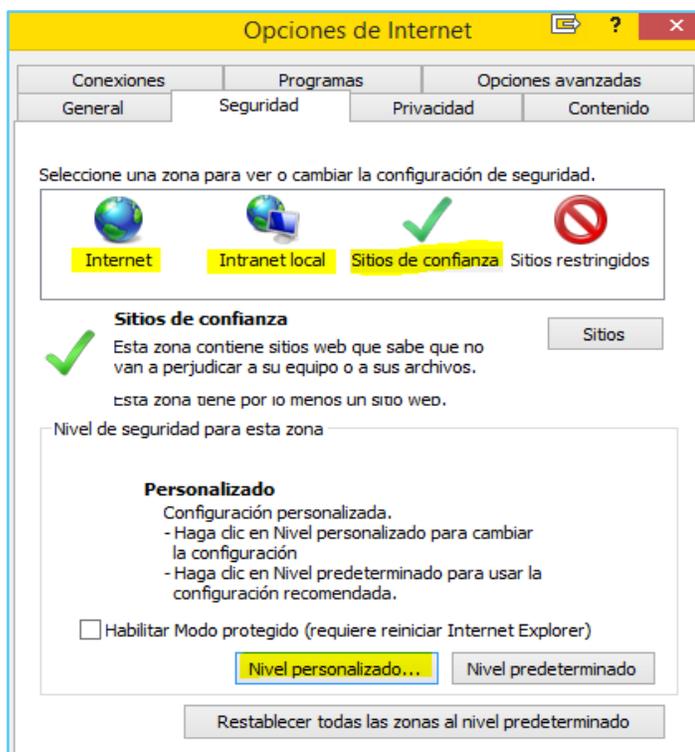
Además de tener instalados los programas anteriores con sus respectivas versiones es importante la configuración correcta de los mismos, ya que una configuración errónea puede causar que no se ejecute el software (applet) correspondiente en el proceso de firma electrónica.

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

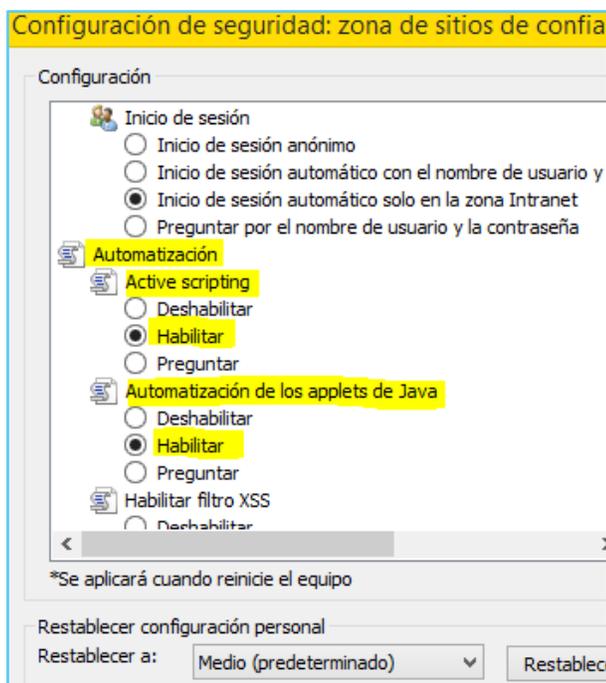
Para verificar estos puntos se necesita abrir el navegador Internet Explorer. Para comprobar que los Plug-in de Java están habilitados se pulsa en la *rueda dentada*, que ya se ha utilizado para verificar la versión del mismo, y se selecciona '*Administrar complementos*', buscando el grupo '*Oracle America,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

Nombre	Editor	Estado	Arquite
Adobe Systems, Incorporated			
Adobe Acrobat Create PDF Toolbar	Adobe Systems, Incorpo...	Deshabilita...	32 bits y
Adobe Acrobat Create PDF Helper	Adobe Systems, Incorpo...	Habilitado	32 bits y
Adobe Acrobat Create PDF from Selection	Adobe Systems, Incorpo...	Habilitado	32 bits y
Microsoft Corporation			
Groove GFS Browser Helper	Microsoft Corporation	Deshabilita...	32 bits
Office Document Cache Handler	Microsoft Corporation	Deshabilita...	32 bits y
Microsoft Windows Third Party Application Component			
Shockwave Flash Object	Microsoft Windows Thir...	Habilitado	32 bits y
No disponible			
⊗ Edit with Altova XMLSpy	No disponible	Habilitado	32 bits
Enviar a OneNote	No disponible	Habilitado	32 bits y
Notas vinculadas de OneNote	No disponible	Habilitado	32 bits y
Oracle America, Inc.			
Java(tm) Plug-In SSV Helper	Oracle America, Inc.	Habilitado	32 bits y
Java(tm) Plug-In 2 SSV Helper	Oracle America, Inc.	Habilitado	32 bits y

Para comprobar que se pueden ejecutar los applet de Java y 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.

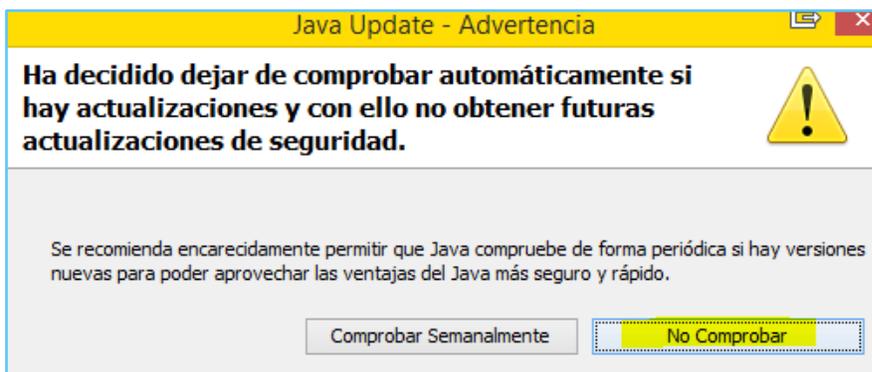
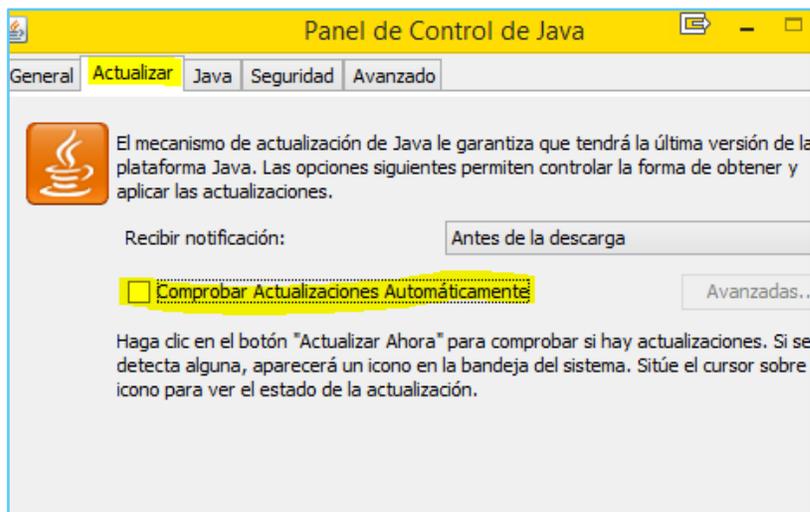


Puede ser '*Internet*', '*Intranet local*' o '*Sitios de confianza*', se pulsa en el botón '*Nivel personalizado...*' y se busca el grupo de valores '*Automatización*'. Una vez localizado en la lista emergente, se comprueba que los items '*Active scripting*' y '*Automatización de los applets de Java*'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



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'.

Es importante deshabilitar las actualizaciones automáticas de la máquina virtual Java, para ello en 'Panel de Control – Java – Actualizar' se desmarca la casilla 'Comprobar Actualizaciones Automáticamente', y en la ventana emergente se confirma la acción con el botón 'No comprobar'.

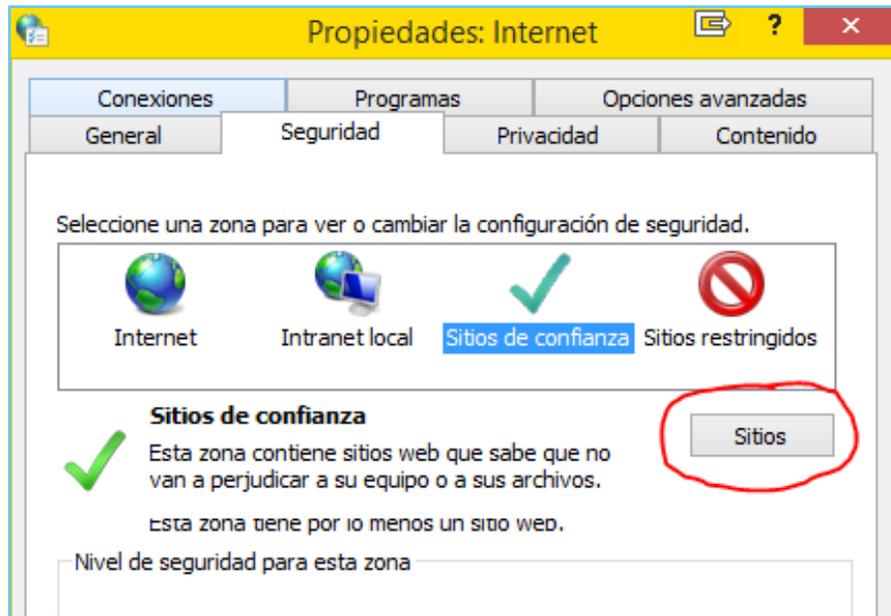


Si no aparece la pestaña 'Actualizar' es que ya están deshabilitadas.

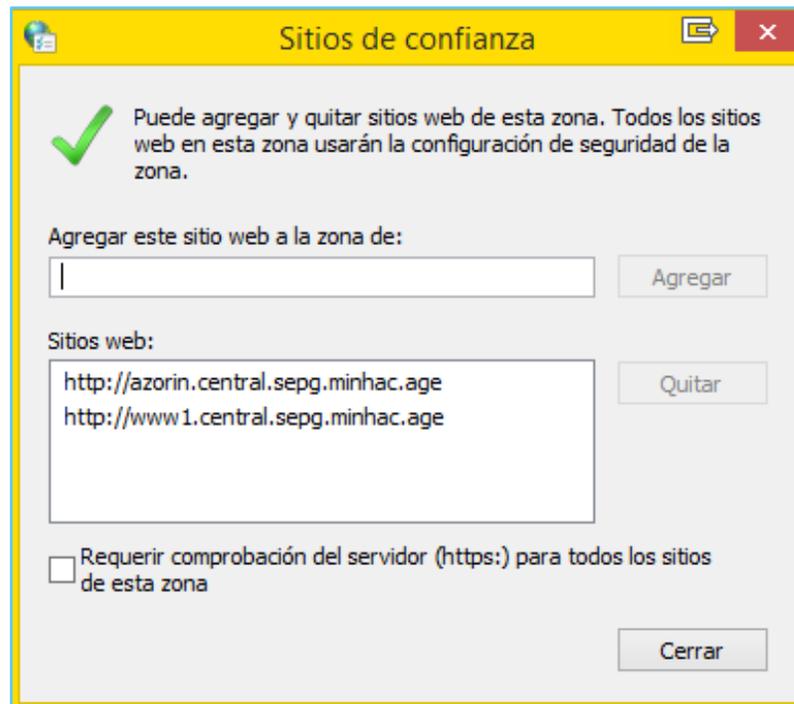
INCIDENCIAS

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. Una vez que se carga el applet de firma está activo mientras el navegador se mantiene abierto.

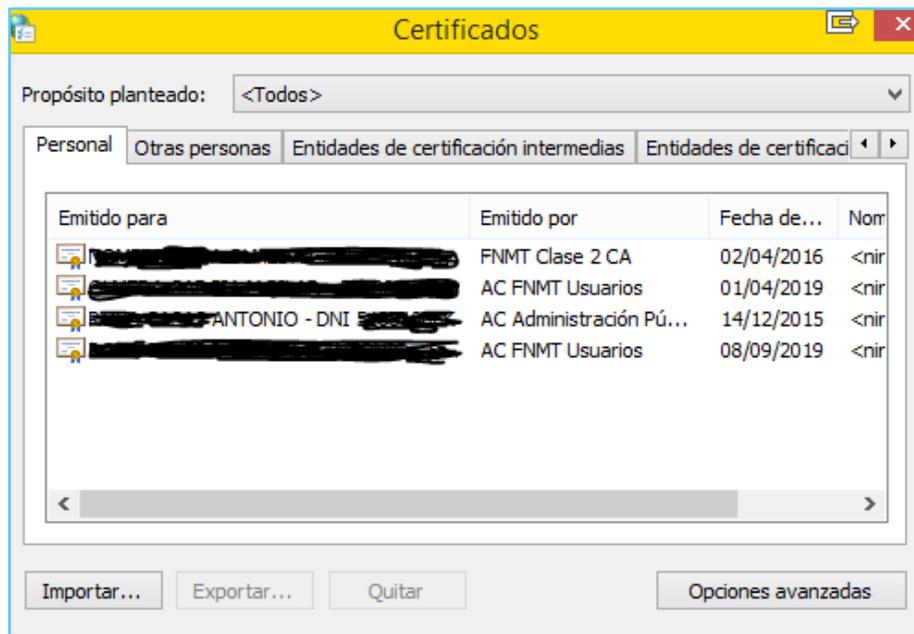
Es altamente recomendable añadir el sitio desde donde se ejecuta la aplicación (URL), poniendo solamente el primer tramo de la misma (por ejemplo: <http://azorin.central.sepg.minhac.ape>) en los 'Sitios de confianza' del navegador para evitar los bloqueos del applet por la máquina virtual. Esto se consigue 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, desmarcando la casilla 'Requerir comprobación.....' y pulsando el botón 'Agregar'. Debería aparecer la URL introducida en la lista de 'Sitios web:'

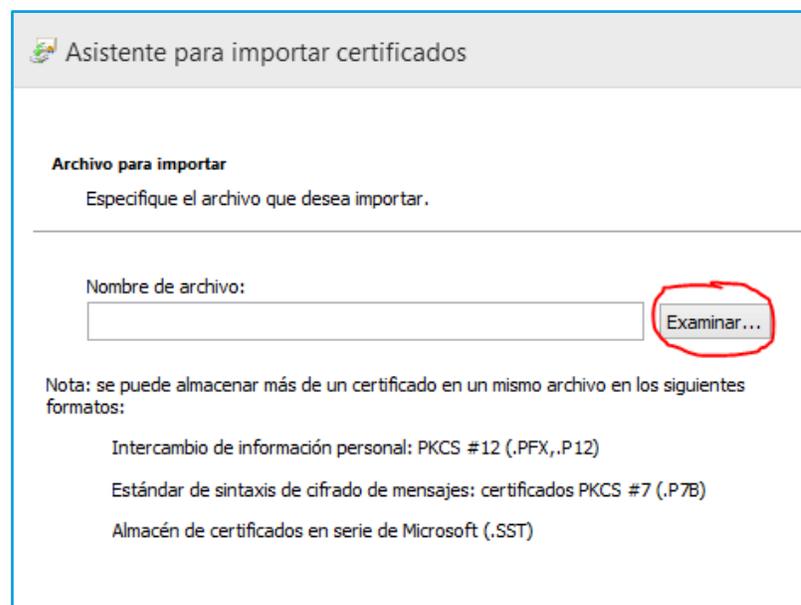


Antes de iniciar el proceso, recomendable al entrar en la aplicación, se debería comprobar la accesibilidad al certificado digital. Se accede al menú *Herramientas – Opciones de Internet*, solapa de 'Contenido' y botón 'Certificados', y en la pestaña 'Personal' debería figurar el certificado que se va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

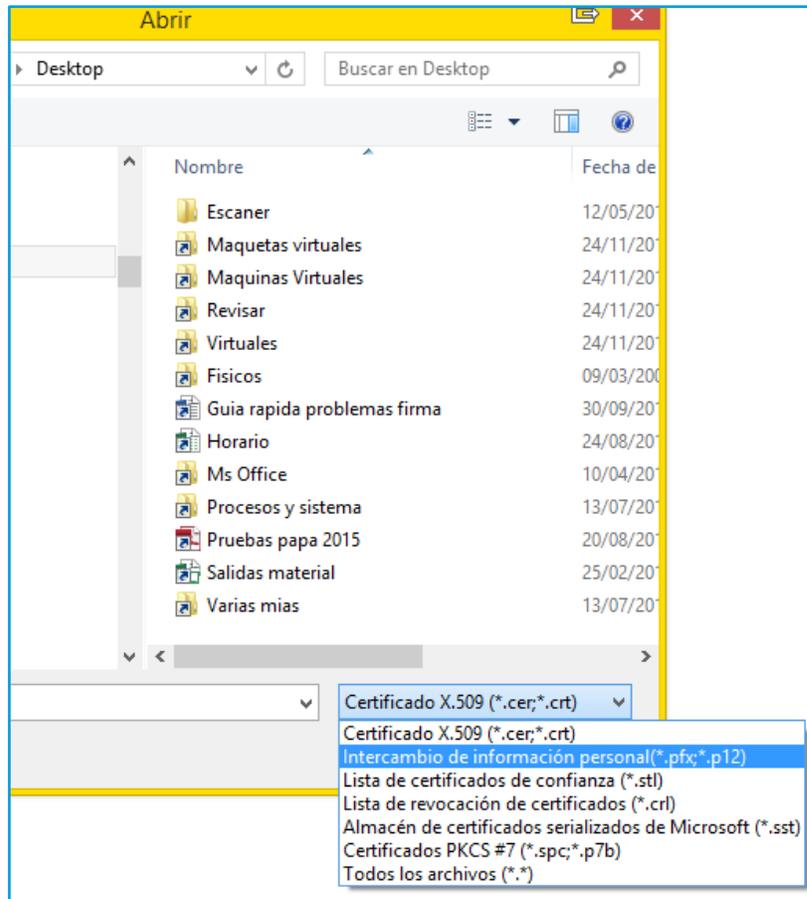


Si no se tiene ningún certificado instalado en el navegador pero se dispone de él en un fichero, habrá que instalarlo manualmente. Para ello, en la pantalla anterior (*Herramientas-Opciones de Internet-Contenido-Certificados, pestaña 'Personal'*), se pulsa en el botón 'Importar' y se siguen las instrucciones 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'.

Protección de clave privada
Para mantener la seguridad, la clave privada se protege con una contraseña.

Escriba la contraseña para la clave privada.

Contraseña:

••••••••

Mostrar contraseña

Opciones de importación:

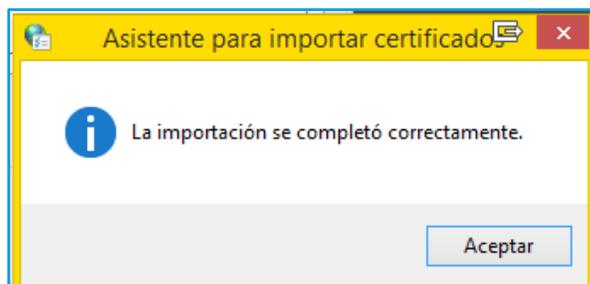
Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.

Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.

Incluir todas las propiedades extendidas.

- Las dos pantallas siguientes se pasan con el botón 'Siguiente' y 'Finalizar'.

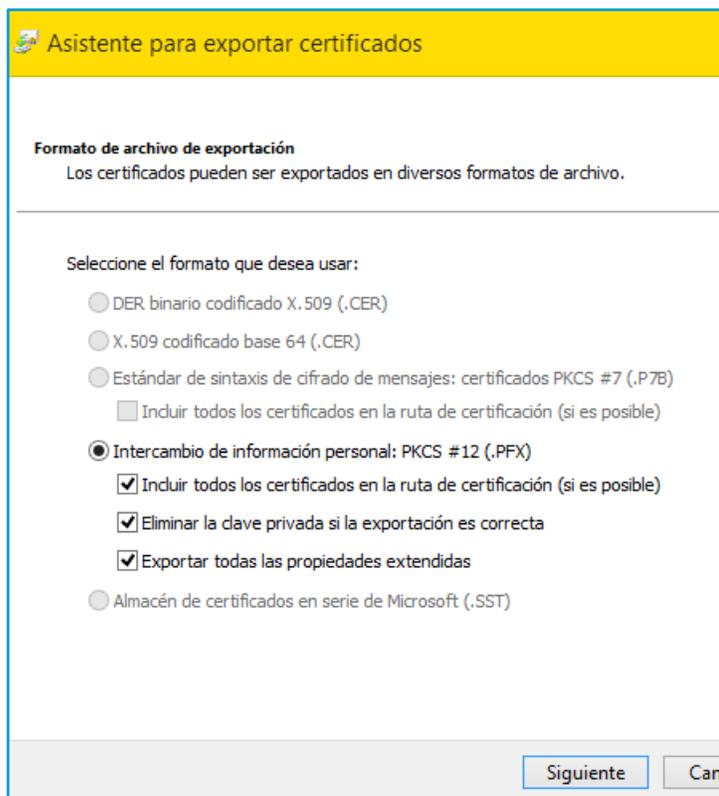
- El proceso mostrará una pantalla para confirmar la importación de la clave privada, se acepta y, si todo ha ido bien, se mostrará un mensaje confirmando que la importación se ha realizado correctamente.



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'.

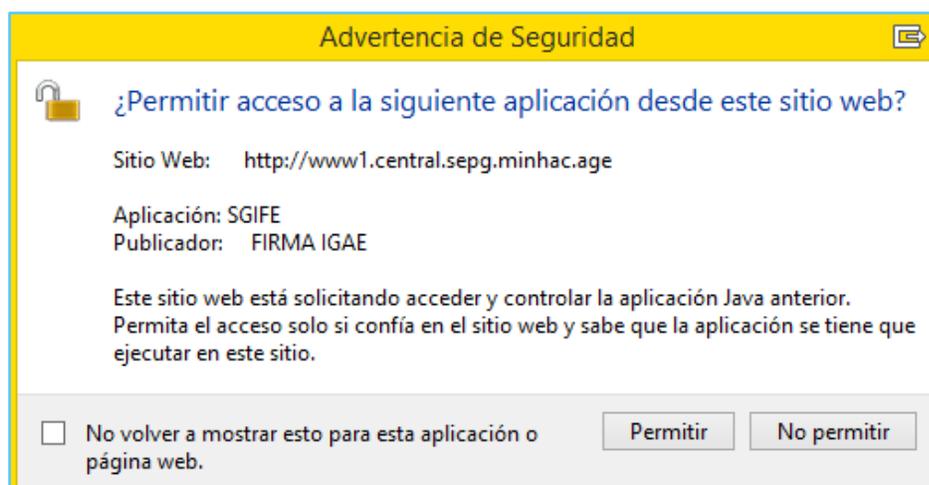
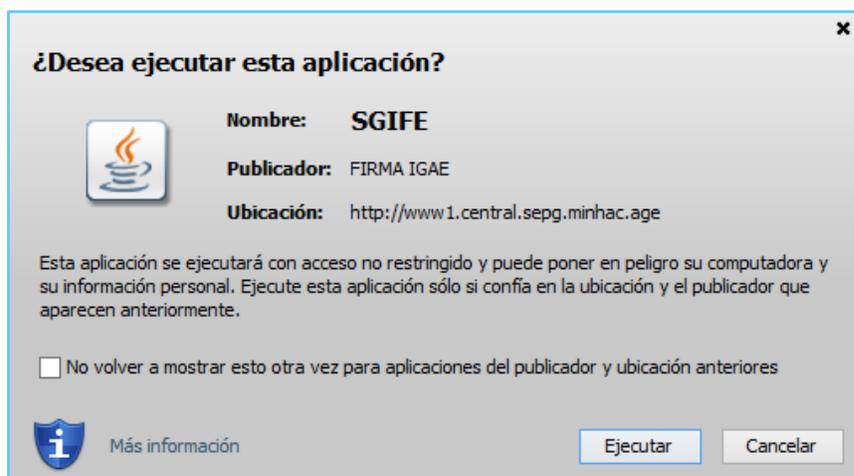


- Se selecciona 'Contraseña' se introduce una contraseña y se confirma. Esta contraseña sirve para proteger la clave privada que se va a exportar y que pedirá el proceso de importación antes citado.

- 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.

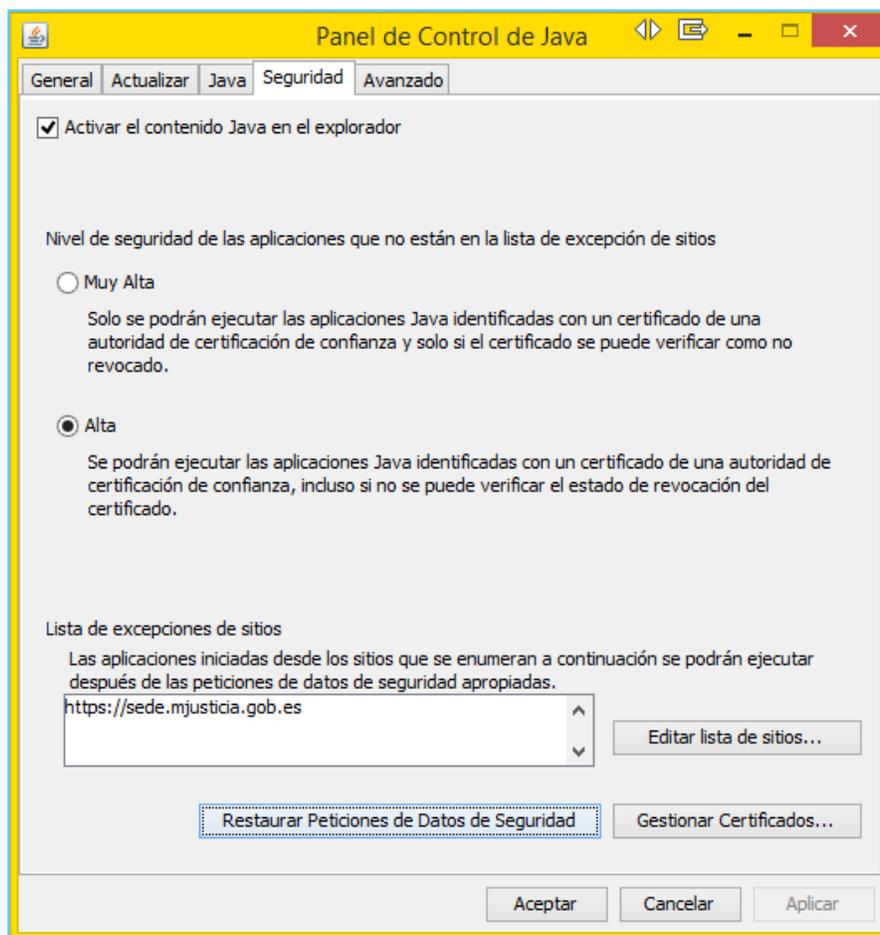
No se sabe si se ejecuta el applet de firma

La primera vez que se ejecuta el applet de firma, se pide autorización al usuario para ejecutar dicho applet con una pantalla parecida a la siguiente:



Hay que dársela a través del botón *‘Ejecutar’* o *‘Permitir’* y, si no se quiere que la vuelva a pedir, marcar la casilla *‘No volver a mostrar esto otra vez’*, pero si marcamos esta casilla y le damos al botón *‘Cancelar’* o *‘No Permitir’*, se está desautorizando la ejecución del applet para siempre. Para volver a mostrar el aviso hay que ir a *‘Panel de Control – Java – Seguridad’* y pinchar en el botón *‘Restaurar Peticiones de Datos de Seguridad’*:

Pedirá confirmación y se da esta con el botón *‘Restaurar todos’*.



Esto se realizará con el navegador cerrado, al volver a entrar en la aplicación volverá a pedir autorización para ejecutar el applet.

La aplicación está bloqueada por la seguridad de Java

Si aparece una ventana advirtiendo del bloqueo de la aplicación por configuración de seguridad hay que desbloquearla, para ello en la ventana de la imagen anterior, se pulsa el botón *'Editar lista de sitios...'*. En la pantalla que aparece pulsar el botón *'Agregar'* y añadir la URL de la aplicación en su primer tramo.

Pide insertar una tarjeta criptográfica

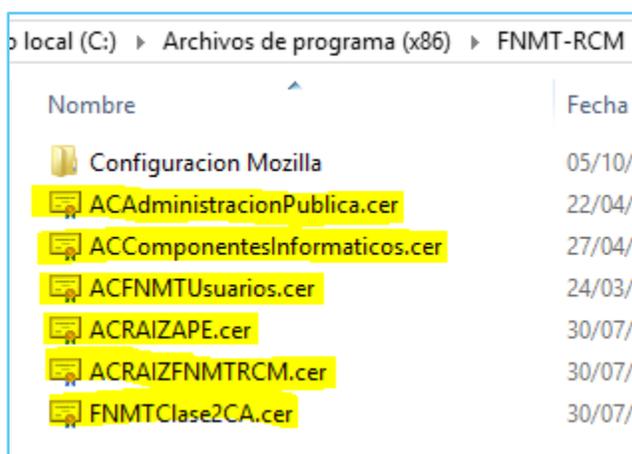
Aun teniendo el certificado instalado en el navegador, se solicita, en una ventana emergente, introducir una tarjeta criptográfica. Esto puede ocurrir si se tiene el lector de tarjetas inteligentes instalado y no se tiene ninguna tarjeta o DNIe introducido en el mismo. Hay que pulsar el botón *'Cancelar'* 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 correcto. Esta carpeta se suele localizar en 'C:\Archivos de programa\FNMT-RCM', en sistemas operativos de 32 bits, o en 'C:\Archivos de programa (x86)\FNMT-RCM', en sistemas de 64 bits. 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.

OTRAS CONFIGURACIONES

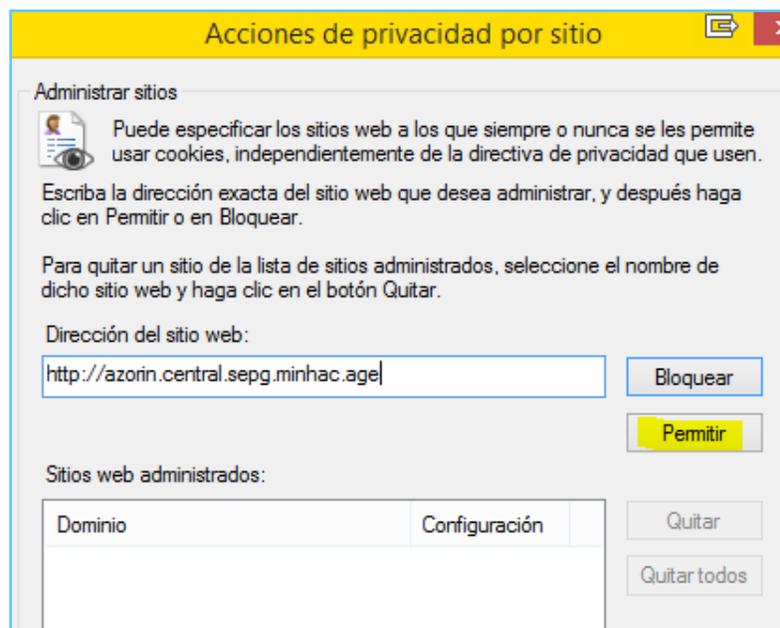
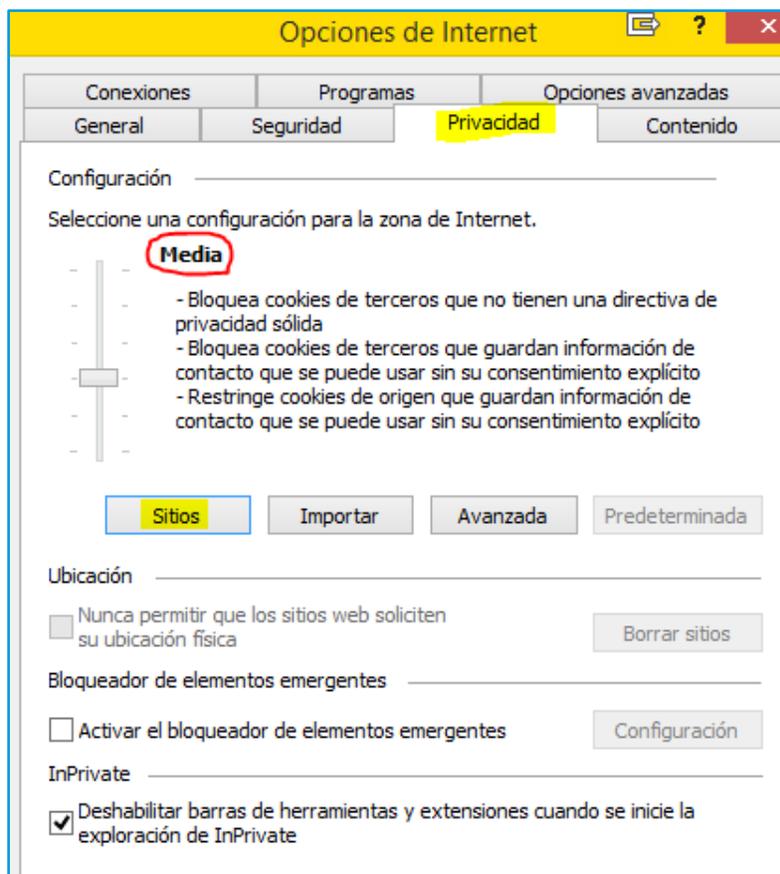
A continuación se detalla cómo comprobar o modificar otras configuraciones relativas a la aplicación Coopera 2020, aunque no tengan relación directa con el proceso de firma electrónica pero sí con el correcto funcionamiento de la citada aplicación.

Javascript activado

La activación de javascript se ha detallado en el apartado 'Escenario correcto' 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.

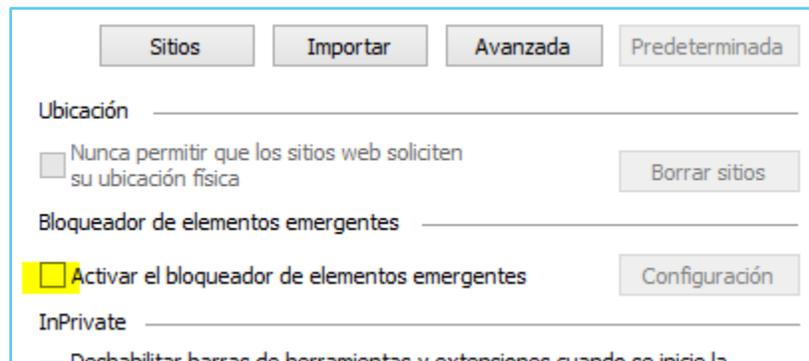


En la lista *'Sitios web administrados'* aparecerá el dominio del sitio web con la configuración de *'Permitir siempre'*.

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'*.

