Uso de Firma Digital en la Oficina Virtual del Consejo de Seguridad Nuclear

---

Documento de Requisitos

Versión: 1.11

22/11/2016

Control de cambios

Versión	Fecha	Revisado	Resumen de los cambios producidos
1.0	19-10-2009		Versión inicial
1.1	08-02-2010		Actualización referencias a Internet Explorer 8
1.2	11-05-2010		Cambios por establecimiento Sede Electrónica
1.3	19-05-2010		Revisión por última parte de Sede Electrónica: Apartado Acrobat Reader.
1.4	16-12-2010		Revisión para versiones de java superiores a 1.6.0_18
1.5	30-10-2011		Nuevas versiones de Java y otros navegadores
1.6	09/12/2013		Añadidas nuevas versiones de exploradores y de Windows. Nueva versión de Samis para java 1.7
1.7	18/03/2014		Añadir nueva versión de Java 1.7.0_51.
1.8	03/12/2014		Añadir apartado ‘solo para java 32 bits’
1.9	18/03/2015		Revisión general documento. Versiones de Java y de navegador.
1.10	21/05/2015		Configuración de Java y de navegador. Incompatibilidad de Applets con Chrome.
1.11	22/11/2016		Actualización requisitos sobre evolutivos de la sede electrónica.

Tabla de Contenidos

Contenido

1. INTRODUCCION.

El presente documento detalla las condiciones que deben satisfacerse para poder firmar digitalmente información remitida al **Consejo de Seguridad Nuclear** (CSN en adelante) a través de los servicios ofrecidos en su oficina virtual.

2. Establecimiento de Requisitos.

Los usuarios que deseen hacer uso de servicios que requieran firma digital deberán cumplir con los siguientes requisitos:

- Disponer de un **navegador** Internet Explorer 10 o 11 (para proceder al envío de la información).
- Disponer de **Outlook Express** 6.0 o superior (para poder leer y validar el acuse de recibo).
- Disponer de **Adobe Acrobat Reader** 7 o superior (para poder leer la información del acuse).
- Estar en posesión de un certificado de **clase 2 CA** emitido por una de las Autoridades de Certificación aceptadas por la plataforma @firma.
- Tener instalado el certificado raíz de la **Fábrica Nacional de Moneda y Timbre** (FNMT en adelante) como entidad emisora raíz de confianza y el certificado de autoridad subordinada AC APE.
- Tener instalada en el equipo la **máquina virtual de Java** en su versión 1.6.0_31 o superior.

2.1. Outlook Express.

El usuario deberá tener instalado Outlook Express (la instalación del Sistema Operativo Windows incluye la instalación de Outlook Express, por lo que no es necesario realizar ningún tipo de instalación adicional) para la lectura y validación del acuse de recibo que obtiene el usuario después de haber realizado el envío firmado digitalmente.

Si el usuario no tiene Outlook Express Instalado en su PC (y no desea tenerlo instalarlo), y desea leer el acuse de recibo desde Microsoft Outlook (su lector de correo predeterminado) se podría acceder al acuse de recibo de una forma alternativa: el usuario deberá enviarse un e-mail a si mismo adjuntando como fichero el Acuse de Recibo obtenido de la aplicación.

2.2. Adobe Acrobat Reader.

El acuse de recibo generado por la Sede Electrónica consiste en un fichero en formato correo que se leerá tal y como se ha comentado en el apartado 2.1. El contenido de este correo firmado digitalmente, es un fichero en formato PDF que contiene la información del acuse. Esta información consiste básicamente en:

- Identidad del usuario.
- La información facilitada por el usuario en el trámite.
- La denominación de los documentos adjuntados junto a la solicitud y su huella digital. Esta huella digital consiste en un código calculado con una función HASH que representa biunívocamente el documento.
- Fecha y hora de presentación según el reloj del servidor donde se aloja la Sede, que se encuentra sincronizado con el servidor de Hora del Real Instituto y Observatorio de la Armada considerada como la hora oficial de España.

Además de esta información el archivo PDF va firmado con el certificado de la Sede Electrónica. Para que el Acrobat Reader confíe en la firmas emitidas por la Sede Electrónica hay que realizar unas modificaciones. Al abrir por primera vez un PDF firmado por el BOE, se puede añadir el certificado raíz del certificado de firma a las identidades de confianza, de la siguiente manera:

a) Abrir el documento.

b) Seleccionar la ficha de firmas, bien eligiendo del menú principal “Ver” > “Paneles de navegación” > “Firmas”, o bien seleccionando la ficha “Firmas” que se muestra en la parte izquierda del documento.

c) Seleccionar la firma (se mostrará el icono o uno similar, junto a la firma para indicar que la identidad del firmante es desconocida porque no se ha incluido en la lista de identidades de confianza y ninguno de sus certificados principales es una identidad de confianza).

d) Una vez seleccionada la firma, pulsar el botón derecho del ratón y elegir la opción “Mostrar propiedades de la firma...” del menú que se despliega. Se abrirá la ventana “Propiedades de la firma”, en la que se muestran varias pestañas. Elegir la primera (“Resumen”) y pulsar el botón “Mostrar certificado...”

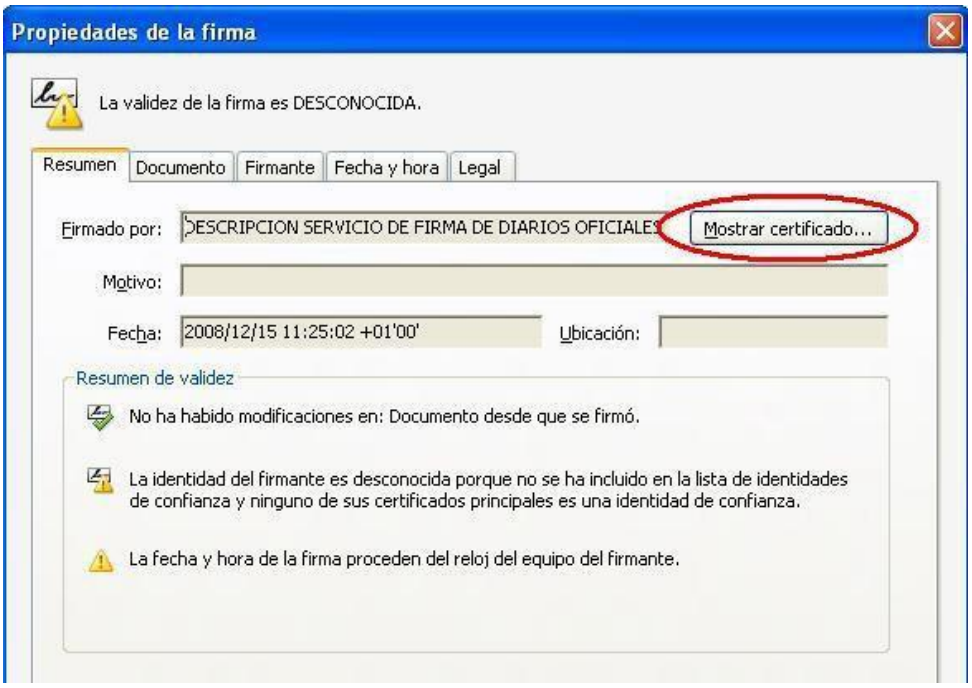


Figura 1.- Propiedades de firma del documento dentro de Acrobat Reader

e) Se abrirá una nueva ventana, “Visor de certificados”, en la que se muestra en el panel de la izquierda la lista de certificados que componen la ruta de certificación completa. Seleccionar el certificado raíz (el primero en la jerarquía).

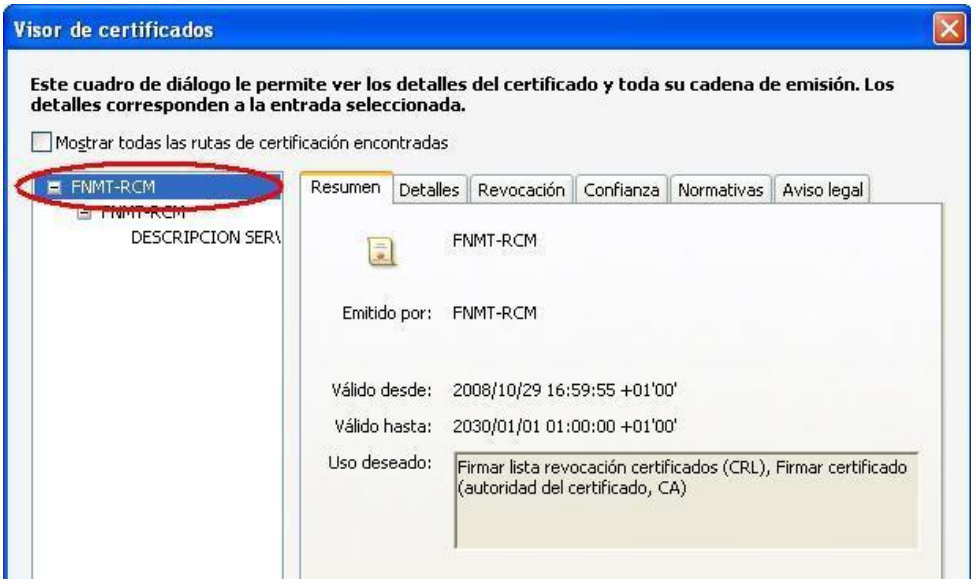


Figura 2.- Visor de certificados dentro de Acrobat Reader

f) Seleccionar la pestaña “Confianza” y pulsar el botón “Agregar identidades de confianza”.

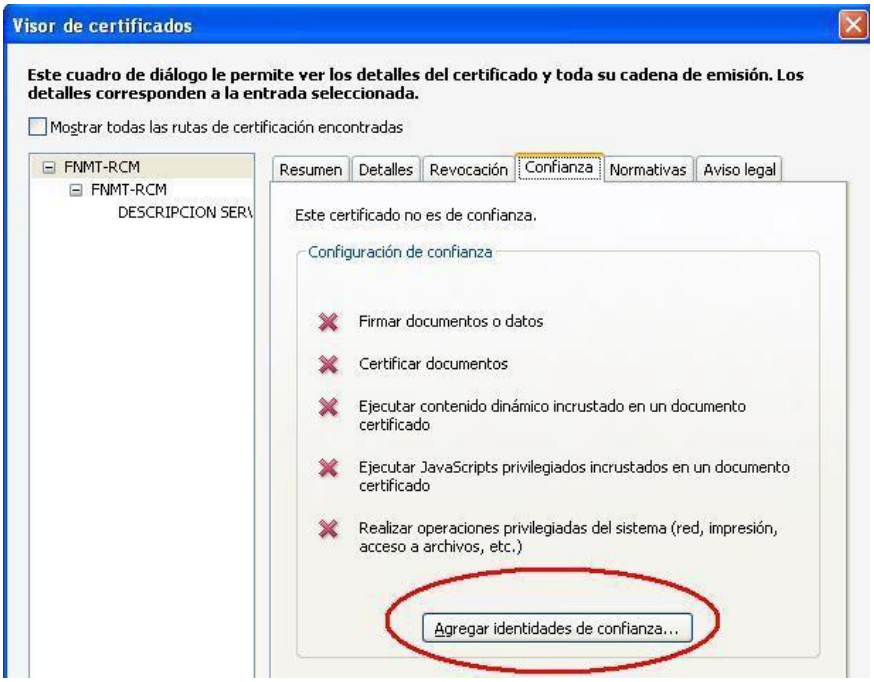


Figura 3.- Agregación de identidades de confianza

g) Se abre una nueva ventana, “Importar configuración de contactos”, en ella, marcar en la sección “Confianza” la casilla “Utilizar este certificado como raíz de confianza”.

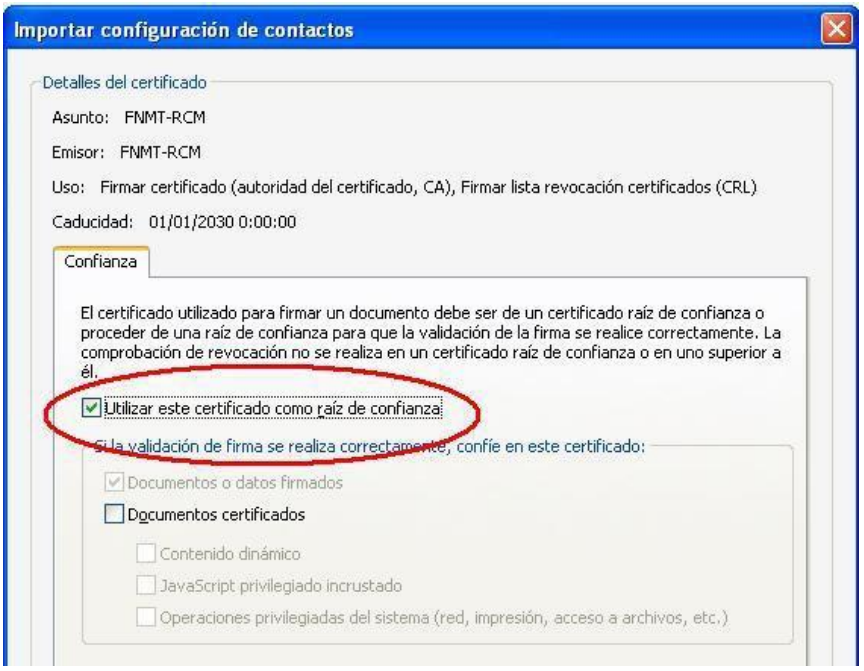


Figura 4.- (Continuación) Agregación de identidades de confianza

h) Pulsar “Aceptar” para cerrar la ventana “Importar configuración de contactos” y de nuevo “Aceptar” en la ventana “Visor de certificados”.

2.3. Máquina virtual de Java.

Para que el applet de firma funcione correctamente, es necesario tener instalada en el PC la máquina virtual de Java JVM en su versión 1.6.0_31 o superior.

Web oficial de Oracle:
www.oracle.com/technetwork/java/javase/downloads/index.html
Web alternativa:
www.java32bit.com/

3. Resolución de Problemas de ejecución del applet de Firma.

Al ejecutar el applet de firma, el usuario puede encontrarse con los siguientes problemas:

3.1. La configuración del certificado raíz de la FNMT no es correcta.

Si el certificado raíz de la FNMT no está instalado, o está mal configurado, no es posible ejecutar el applet de firma. El mensaje que se presenta al usuario es similar al siguiente:

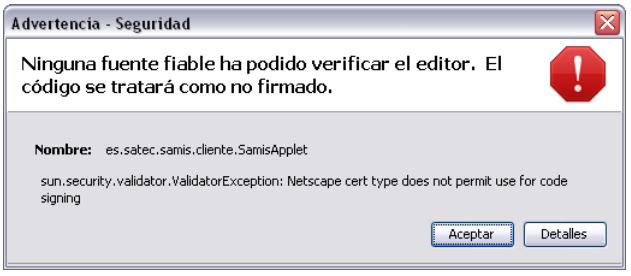


Figura 5.- Mensaje de error relativo a la configuración del certificado raíz de la FNMT

El proceso de firma se realiza en el equipo del usuario a partir de un applet de firma que está firmado digitalmente con un certificado emitido por la FNMT. Para poder ejecutar dicho applet es necesario tener configurado correctamente dicho certificado raíz.

Para configurarlo correctamente se deben realizar los siguientes pasos:

1. Abrir el navegador Internet Explorer y acceder a:

Herramientas | Opciones de Internet | Contenido | Certificados | Entidades Emisoras Raíz de Confianza

2. Seleccionar el certificado FNMT Clase 2 CA y pulsar en:

Ver | Detalles | Modificar Propiedades

NOTA: Con Windows 7, esta opción aparece deshabilitada. Se debe entrar al sistema con el usuario “Administrador”, pero éste por defecto está deshabilitado. Se debe hablar con el administrador del sistema para que habilite la cuenta “Administrador” y entrar con este usuario.

3. Marcar la opción “Habilitar sólo los siguiente propósitos” y marcar sólo las opciones:

“Autenticación del servidor” y “Correo seguro” y pulsar sobre “Aceptar”

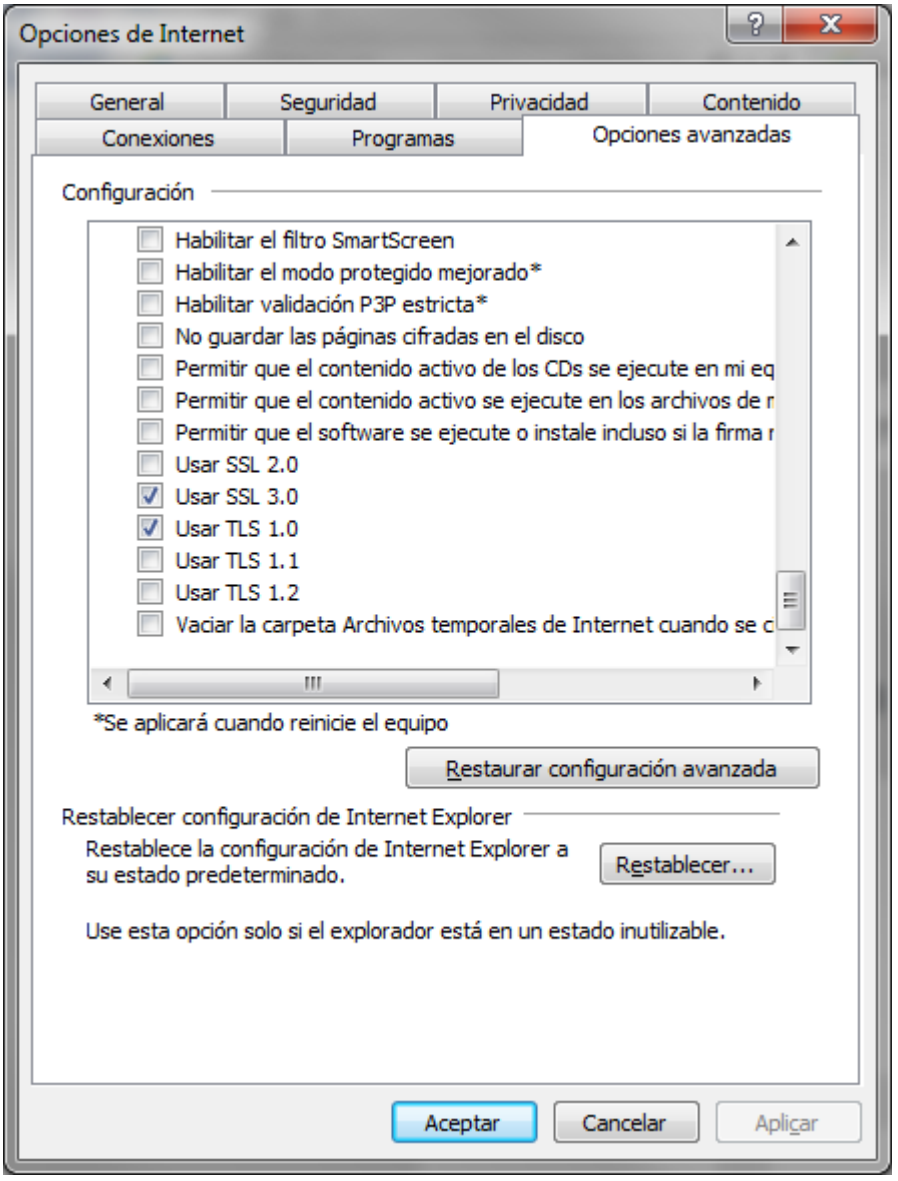
4. Pulsar en “Aceptar” o “Cerrar” en todas las ventanas abiertas

5. Realizar el mismo proceso para el certificado AC APE.

A partir de Internet Explorer 10, se deben activar las opciones de SSL y TLS en:

Herramientas | Opciones de desarrollo | Opciones avanzadas | Seguridad|

Se deben activar las opciones Usar SSL 3.0 y Usar TLS 1.0 como en la siguiente imagen:



NOTA: El certificado raíz de la FNMT se instala automáticamente en el caso de que se tenga instalado un certificado personal emitido por la FNMT. En el caso de dicho certificado raíz no se encuentre instalado puede descargarse de la Web de la FNMT: www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

e importarlo desde Internet Explorer | Herramientas | Opciones de Internet | Contenido | Certificados | Entidades Emisoras Raíz de Confianza | Importar. El nuevo certificado de Sede Electrónica se basa también en una Autoridad de certificación subordinada AC APE. Por lo que para ver correctamente los contenidos de la Sede, deberá asegurarse de que también está instalado. El certificado se instalará posteriormente al de raíz de la FNMT y se puede descargar desde este enlace: Descarga Certificado Autoridad subordinada AC APE.

3.2. La versión de la máquina virtual de Java no es la correcta.

Si la versión de la máquina virtual de Java no es la adecuada, no es posible ejecutar en applet de firma y se presenta al usuario una pantalla de error o un mensaje.

Es posible que la pantalla muestre algún tipo de error comentando una posible solución. Cada uno de estos errores se indica en los apartados 3.4 - 3.7.

Si se abre la consola de java (seleccionando en la opción *Abrir Consola* al pulsar el botón derecho sobre el icono de java – taza de café - situado a la derecha en la barra de herramientas de Windows, normalmente en la parte inferior de la pantalla) se accederá al resultado de ejecución del applet:

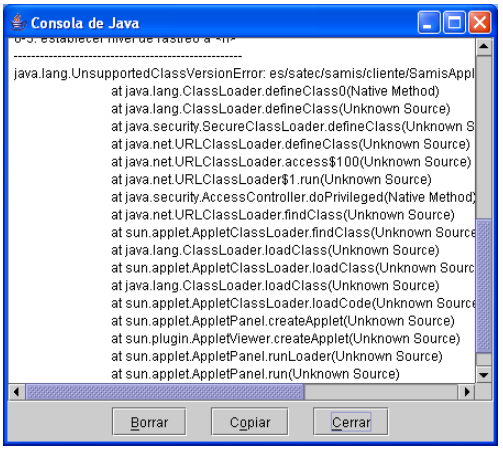


Figura 6.- Mensaje de error relativo a la versión de la máquina virtual de Java (consola de Java)

3.3. Aparece ventana de advertencia sobre la firma digital del applet.

Puede que al iniciar el proceso de firma aparezca una ventana similar a la siguiente

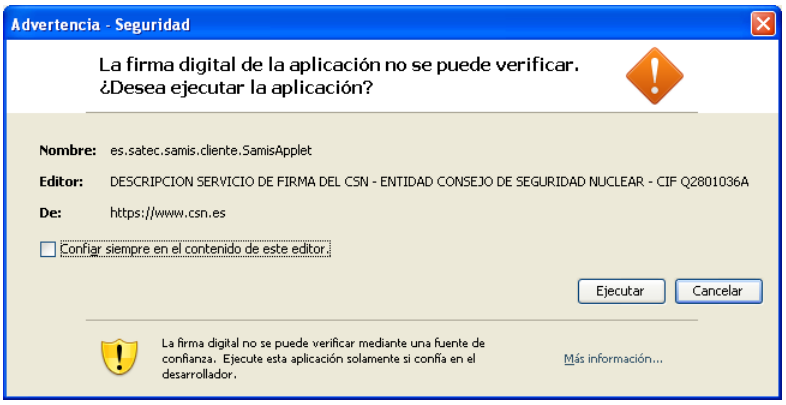


Figura 7.- Mensaje de aviso de certificado de confianza

El applet de firma es una aplicación firmada digitalmente con un certificado emitido por la FNMT. En este caso, se está informado al usuario de que dicho certificado no está almacenado como un certificado de confianza. Si desea que esta ventana no vuelva a aparecer, deberá hacer clic en el casilla que indica que se confía siempre en el contenido de este editor pulsar el botón “Ejecutar”. En caso de que se quiera que esta ventana aparezca siempre no marcar la casilla y pulsar el botón “Ejecutar”

3.4. No funciona con versiones inferiores a 1.6.0_31.

Con versiones inferiores de Java a la 1.6.0_31, es posible que el proceso de firma bloquee el ordenador, o muestre una pantalla como la siguiente:

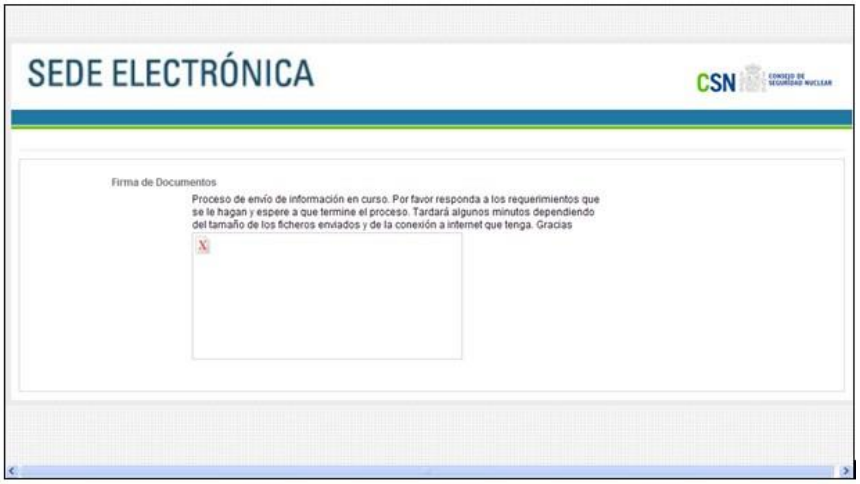


Figura 8: Pantalla de error por versión muy antigua

Este error se soluciona siguiendo el paso 2.3 para descargar una versión de Java más moderna y compatible.

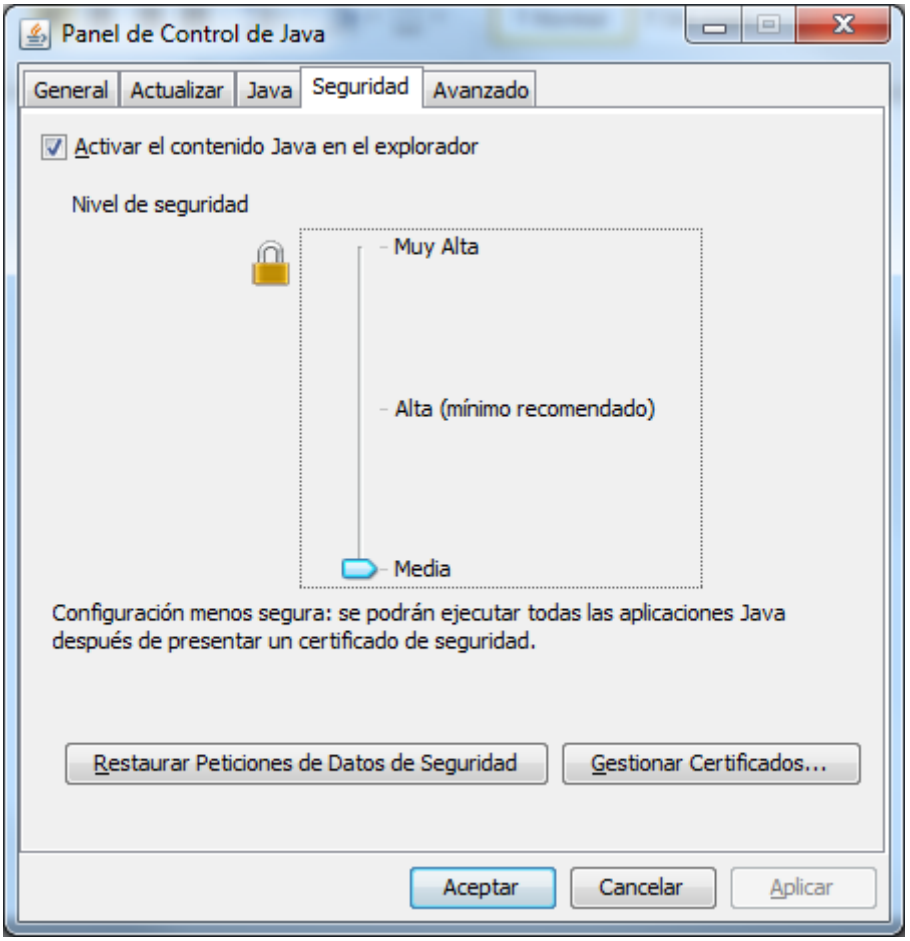
3.5. Ejecutar Applet de firma con la versión 1.7.0_51 o superior de Java.

Con versiones de Java de la 1.7.0_51 en adelante, es posible que el proceso de firma se bloquee por motivos de seguridad de Java. Para ello es necesario bajar la seguridad de Java desde el Panel de Control así:

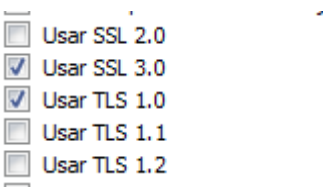
Abrir el Panel de Control

En Java → Pestaña Seguridad

Bajar el Nivel de Seguridad de **Alta** a **Media** y Aceptar.

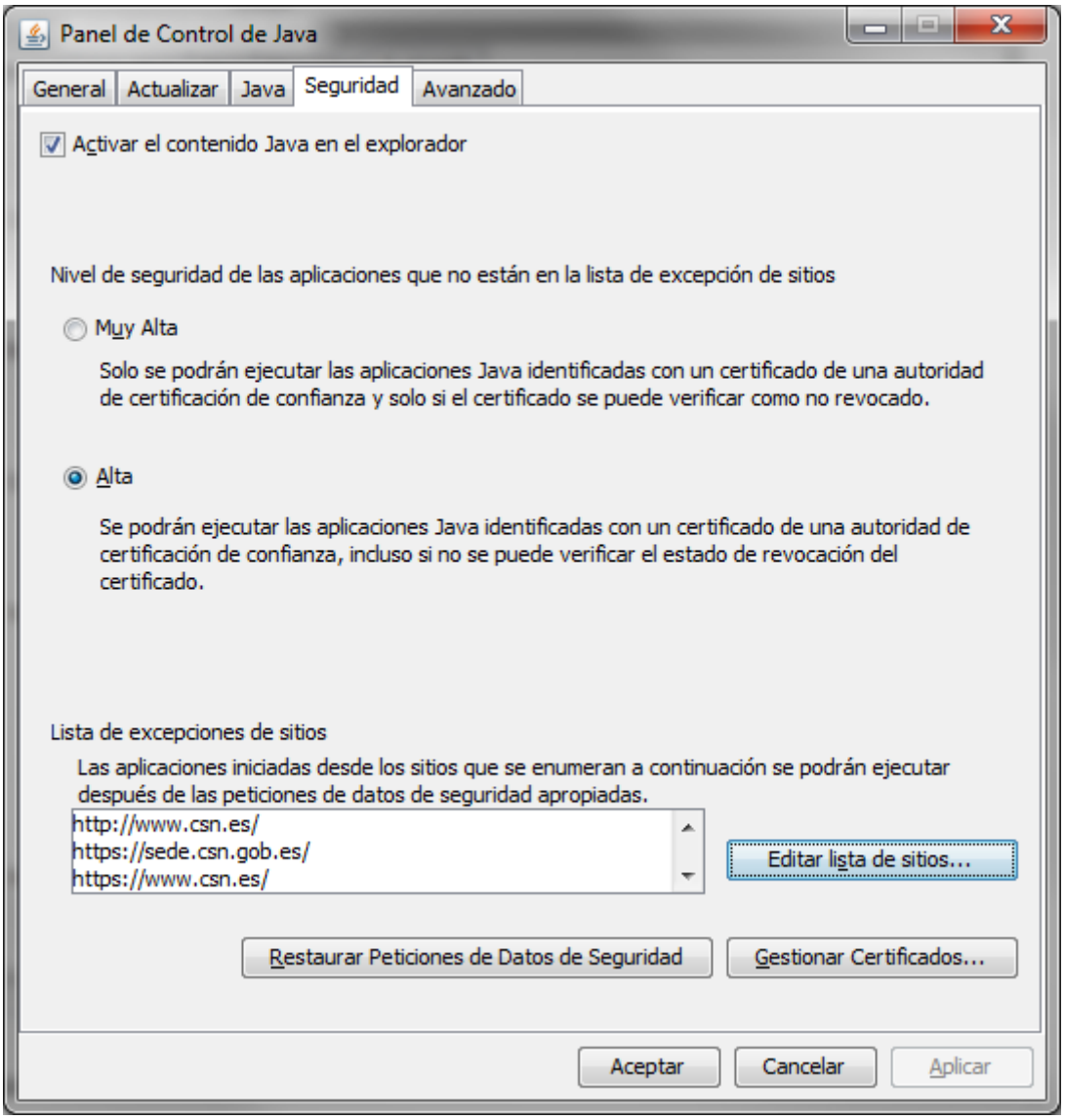


En la última pestaña de 'Avanzado', abajo del todo, en Valores de seguridad avanzada, únicamente marcamos el SSL 3.0 y TLS 1.0, como se muestra a continuación (TLS 1.1 y TLS 1.2 tienen que estar desmarcados):



3.6. Ejecutar Applet de firma con la versión 1.8.0_… de Java.

Si se tiene instalada la versión 1.8.0_... de Java, cualquier actualización de la versión 1.8, no permite bajar la seguridad a media desde el panel de control, así que la dejamos en Alta y es necesario añadir estas urls del CSN en la lista de excepciones de sitios seguros.

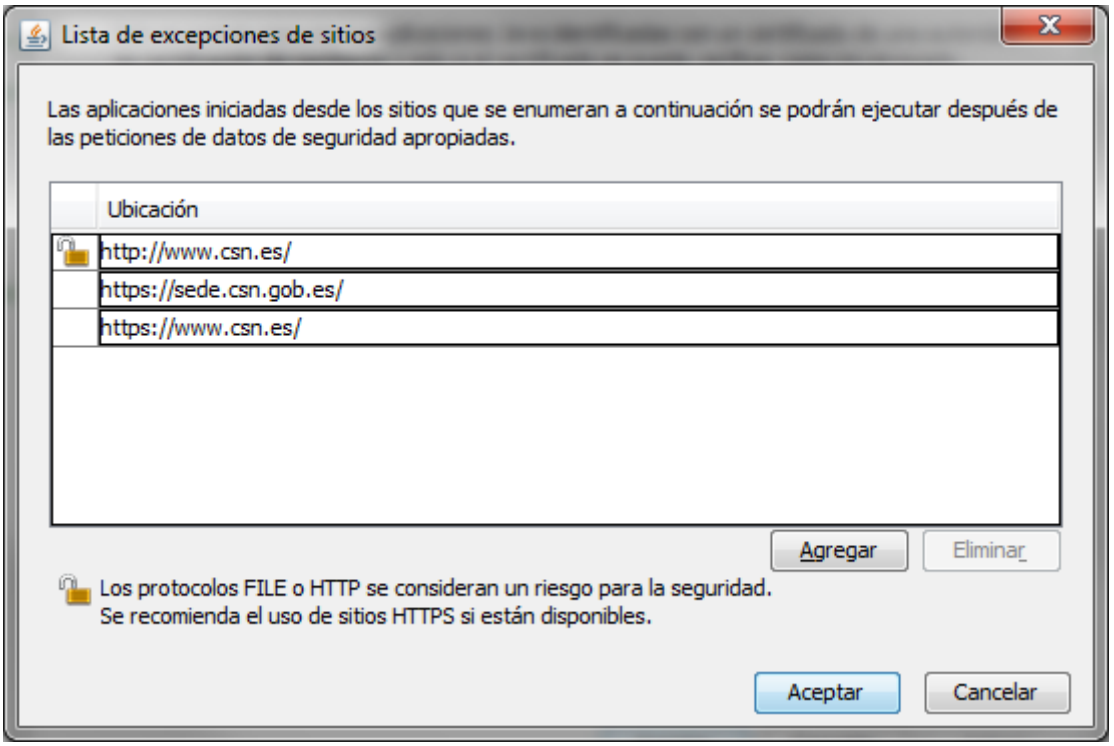


Para añadirlas pulsamos el botón ‘Editar lista de sitios…’, y se abre la siguiente ventana en la que hay que añadir las siguientes urls, pulsando ‘Agregar’ con cada una:

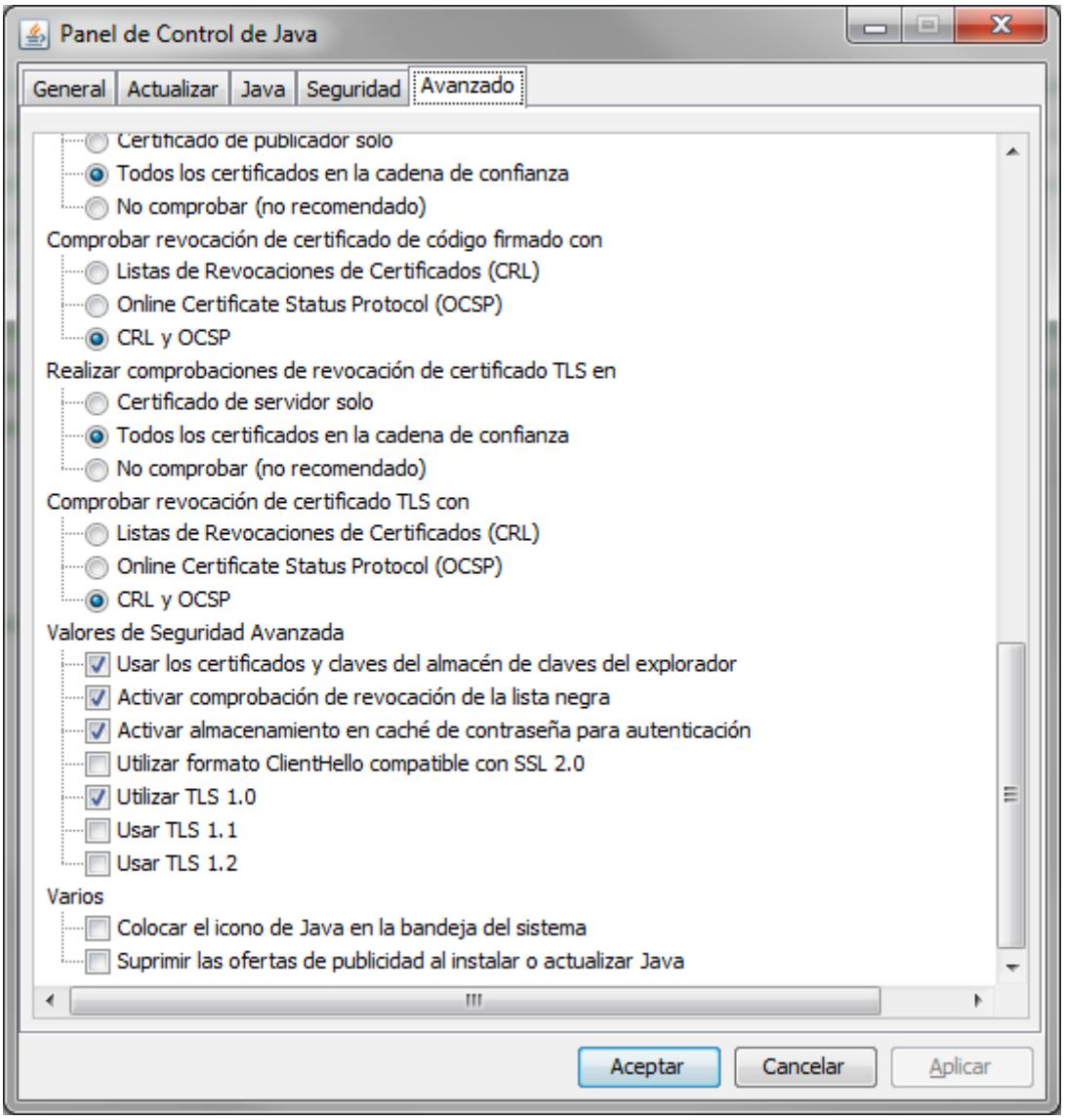
http://www.csn.es/

https://sede.csn.gob.es/

https://www.csn.es/



Por último, en la última pestaña de ‘Avanzado’, ahora tampoco está la opción de SSL 3.0, así que únicamente marcamos el TLS 1.0, como se muestra a continuación (TLS 1.1 y TLS 1.2 tienen que estar desmarcados):



3.7. No se ejecuta el Applet de firma con las versiones de Java de 64 bits.

Para poder ejecutar el applet de firma (y en general cualquier applet) hay que tener instalada una versión compatible de Java, **de 32 bits, aunque el equipo sea de 64 bits**.

Desde la web oficial de Oracle, de descargas de java, para Windows, el instalable está en el apartado ‘Windows x86’, y se suele llamar ‘jre-(versión)-windows-i586.exe’.

4. Comprobar versión de Java instalada y activa.

A lo largo de este documento se citan varias versiones de Java y su compatibilidad con el Applet, y es posible que en alguna ocasión no se sepa cuál es la versión instalada.

Para saber las versiones de Java que hay instaladas y la que está activa, hay que realizar los siguientes pasos:

Entrar en el Panel de control del sistema y pulsar sobre el icono Java (32 bits). Tras esto aparecerá una ventana como la siguiente:

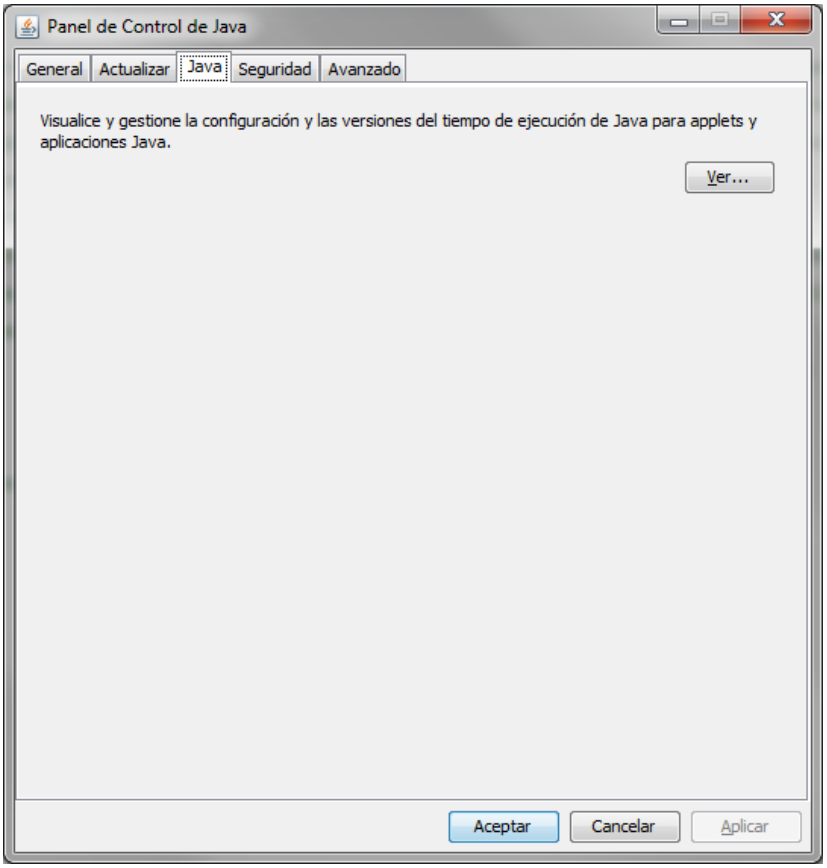


Figura 17: Ventana del Panel de Control de Java

Una vez abierta la ventana hay que pulsar sobre la pestaña Java y a continuación sobre el botón **Ver**…con lo que aparecerá una ventana como la siguiente:

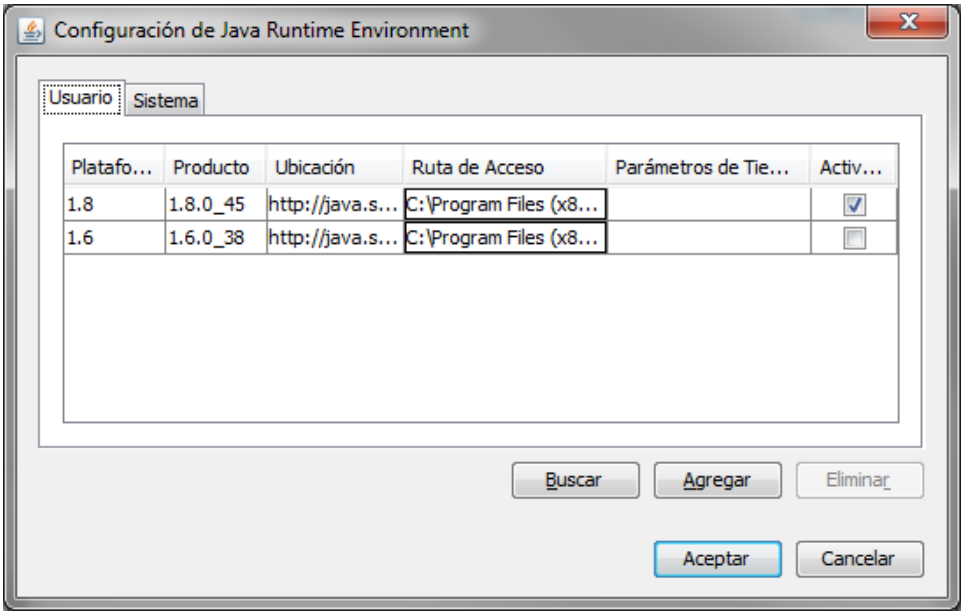


Figura 18: Ventana de versiones de Java instaladas y habilitadas

En esta ventana se indican todas las versiones instaladas y cuál de ellas es la que está

activada.

Una vez activada la versión de Java compatible con el applet, hay que ir pulsando sobre el botón aceptar en todas las ventanas para guardar los cambios.

5. Resolución de problemas en el Formulario de Solicitud.

5.1. Carga mal la ruta al anexar un documento a la solicitud en Internet Explorer.

Se ha detectado que una vez se selecciona el fichero y se pulsa Abrir en Internet Explorer, la ruta que carga en el cuadro a la izquierda del botón Examinar, no se corresponde con la seleccionada. Para solventar este problema debemos acudir a la opción de menú Herramientas > Opciones de Internet. Dentro de la pestaña Seguridad pulsaremos, con la zona Internet remarcada, sobre el botón Nivel Personalizado. En la ventana que se muestra a continuación aparecen una serie de opciones con su configuración actual. Iremos hasta la opción denominada: **Incluir la ruta de acceso al directorio local cuando se carguen archivos a un servidor** y marcamos **Habilitar**. Después Aceptar hasta completar la configuración.

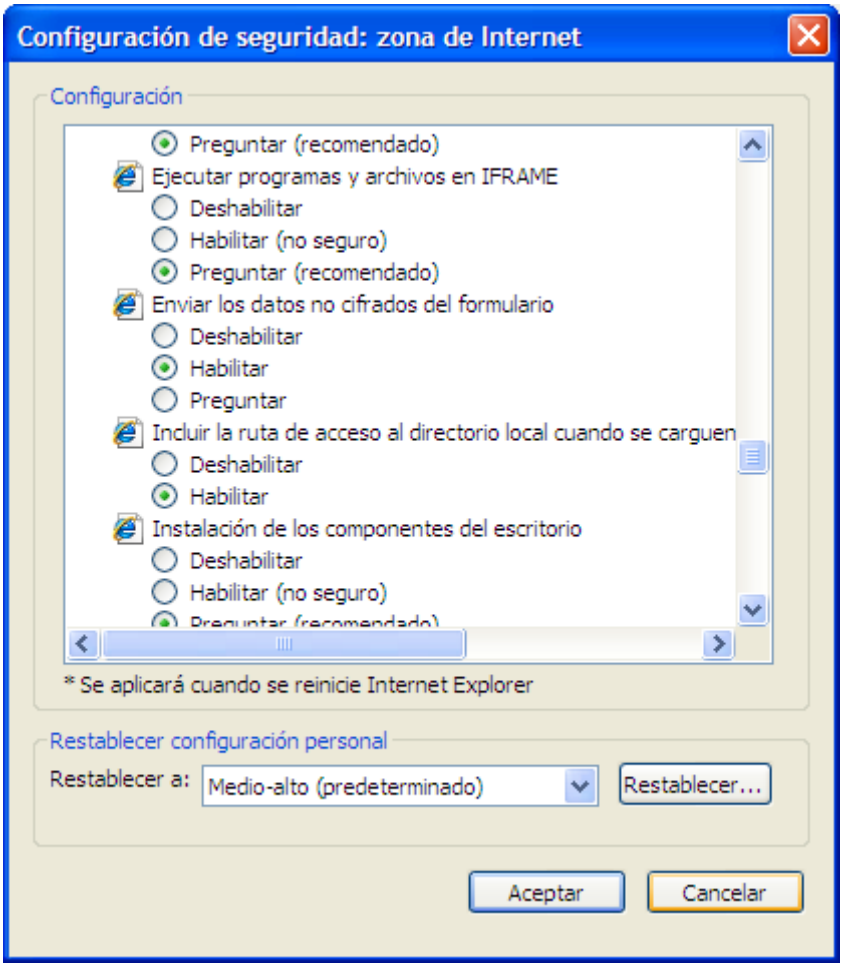


Figura 15.- Marcamos "Habilitar en Incluir la ruta de acceso al directorio local" cuando se

carguen…

6. Google Chrome y Mozilla Firefox (Incompatible con applets Java).

En ambos navegadores en sus últimas versiones no están soportados los applets, debido a esto no puede ejecutarse código java desde el navegador del cliente y no puede ejecutarse más que en Internet Explorer el componente de firma que tenemos.