



Guía de Configuración del Puesto de Acceso a los Sistemas de Información de OMIE

Alfonso XI, 6
28014 Madrid
F(+34) 91 524 03 96
www.omie.es

Ref. GuiaConfAccesoSistemasOMIE.docx

Versión 2.16
Fecha: 2021-01-12

ÍNDICE

1	INTRODUCCIÓN	3
2	REQUISITOS PREVIOS	4
2.1	COMPONENTES PRINCIPALES Y VERSIONES	4
2.1.1	<i>Navegador Internet Explorer</i>	4
2.1.2	<i>Resolución de pantalla</i>	4
3	UTILIZACIÓN DEL INSTALADOR DEL PUESTO CLIENTE	5
4	CONFIGURACIÓN MANUAL DEL PUESTO CLIENTE	8
4.1	CONFIGURACIÓN JAVA	8
4.2	INSTALACIÓN DEL LECTOR DE TARJETAS (SÓLO PARA CERTIFICADOS EN TARJETA)	9
4.3	REGISTRO DE CERTIFICADOS DE USUARIO	9
4.3.1	<i>Certificados en tarjetas inteligentes</i>	9
4.3.2	<i>Certificados software</i>	12
4.4	CONFIGURACIÓN DEL APPLLET DE FIRMA	14
5	PROBLEMAS FRECUENTES	16
5.1	APARECEN MENSAJES DE ERROR EN LA INSTALACIÓN DE LOS APPLETS	16
5.2	EL PIN DE LA TARJETA TARDA MUCHO EN SER SOLICITADO, O EL NAVEGADOR QUEDA BLOQUEADO EN ESE MOMENTO	17
5.3	APARECE AL “ERROR DE CERTIFICADO” AL ACCEDER AL SISTEMA	18
5.4	EL SERVIDOR NO PERMITE EL ACCESO AL SISTEMA	18
5.5	USO DE NAMESPACES EN LOS DOCUMENTOS XML (SÓLO PARA EL WEB DEL MERCADO)	19
5.6	BLOQUEO DE VENTANAS EMERGENTES	20
5.7	AVISO AL DESCARGAR FICHERO	22
5.8	PROBLEMA AL ARRANCAR EL CENTRO DE DESCARGAS (SÓLO PARA EL WEB DEL MERCADO)	22
5.9	PROBLEMA AL ENTRAR AL WEB SIN NINGÚN JAVA INSTALADO	24
5.10	INSTALACIÓN INCORRECTA DEL ROOT CA DE OMIE.	25
5.11	SE ABREN DOS VENTANAS DEL CENTRO DE DESCARGAS (SÓLO PARA EL WEB DEL MERCADO).	26
5.12	SE OBTIENE UN MENSAJE DE VERSIÓN DE NAVEGADOR NO SOPORTADA (SÓLO PARA EL WEB DEL MERCADO).	27
5.13	ERROR AL ENVIAR UNA OFERTA POR FICHERO.	27

1 INTRODUCCIÓN

La presente guía describe los requisitos en un puesto cliente para el acceso a los Sistemas de Información de OMIE y los pasos necesarios para comenzar a utilizar los entornos Web del Sistema de Información del Mercado de Electricidad (en adelante SIOM).

Los entornos Web de SIOM requieren el navegador *Internet Explorer* de *Microsoft* y el *Plug-in* de *Java* para la ejecución de componentes *Java* en el navegador. Asimismo, para el acceso a los mismos es necesario el uso de certificados de usuario proporcionados por OMIE tanto en soporte de tarjeta inteligente como en soporte fichero (certificado software).

Para la configuración del puesto cliente se hará uso del Instalador del Puesto cliente para acceso a los Sistemas de Información de OMIE. Mediante la utilización de este instalador facilitado por OMIE, se automatiza el proceso de instalación, minimizando las actuaciones manuales que tengan que ser realizadas.

No se incluyen apartados para la instalación de componentes hardware y software estándar, como sistema operativo, navegador, o la instalación hardware del lector de tarjetas. No obstante, se detallan en los apartados siguientes los requisitos necesarios en cuanto a versiones, y algunos detalles de configuración de los mismos para un correcto funcionamiento. Para la instalación básica de los productos es necesario remitirse a las guías de instalación o ayuda de los mismos.

2 REQUISITOS PREVIOS

2.1 Componentes principales y versiones

Los principales componentes software y hardware necesarios para el uso de los entornos Web de SIOM son los siguientes:

- Sistema operativo:
 - Windows 7
 - Windows 8 / 8.1
 - Windows 10 (recomendado)
- Navegador Microsoft Internet Explorer
 - Versiones 10 y 11 (recomendado), todas de 32 bits

Nota: En Windows 8, existen dos experiencias de exploración, una optimizada para dispositivos táctiles y la ya conocida de Internet Explorer para el escritorio. La primera no está soportada en el sistema debiendo utilizar la opción de escritorio.

- Máquina Virtual Java
La información más actualizada sobre la última versión de la Máquina Virtual recomendada y homologada para el acceso a los Webs de SIOM se encuentra en el Web Público de OMIE (www.omie.es), en el apartado “Documentación Técnica” dentro de “Sistema de Contratación”.
- Lector de tarjetas (sólo para certificados en tarjeta)
- Registro de los certificados a utilizar.
- Instalación del Root CA de OMIE.

A continuación, se describen con más detalle estos requisitos, junto con opciones de configuración adicionales.

2.1.1 Navegador Internet Explorer

El navegador Internet Explorer para el acceso a los Webs de SIOM debe ser siempre la versión de 32 bits (aunque el sistema operativo sea de 64 bits).

2.1.2 Resolución de pantalla

El web se ha diseñado para una configuración óptima de **1280x1024 pixels y 65536 colores**.

Como configuración máxima de pantalla, se recomiendan las siguientes:

- Resolución 1366x768 y tamaño de Fuente mediana (125%)
- Resolución 1600x900 y tamaño de Fuente mediana (125%)

3 UTILIZACIÓN DEL INSTALADOR DEL PUESTO CLIENTE

El instalador facilitado por OMIE automatiza el proceso de instalación, minimizando las actuaciones manuales que tengan que ser realizadas. Dicho instalador puede descargarse desde el Web Público de OMIE (www.omie.es).

En caso de acceder al Sistema sin tener ninguna versión de insta de 32 bits instalada, se mostrará una pantalla en la que se informa de la necesidad de ejecutar el instalador y se facilita el acceso a la página correspondiente del Web Público.



Se ha detectado que no existe ~~ninguna versión~~ de Java de 32 bits instalada en este equipo. Por favor descargue y ejecute el [Instalador OMIE](#) y vuelva a intentar entrar en la Web despues de cerrar el navegador.

No installed 32 bit Java version has been detected in this workstation. Please, download and execute the [OMIE Automatic Installer](#), close your browser and try to log in the Web again.

INSTALADOR

— INSTALADOR WEB

Descárguese desde aquí el Instalador OMIE para facilitar la instalación y configuración del puesto de agente para el acceso al Web del Mercado de Electricidad.

El programa Instalador ofrece las siguientes funcionalidades: Verificación mínima de requisitos, instalación opcional de la JVM, copia de los componentes propios del Web del Mercado de Electricidad, configuración de la JVM, configuración de las Opciones de Internet del Sistema y comprobación de la instalación del software GemSAFE.

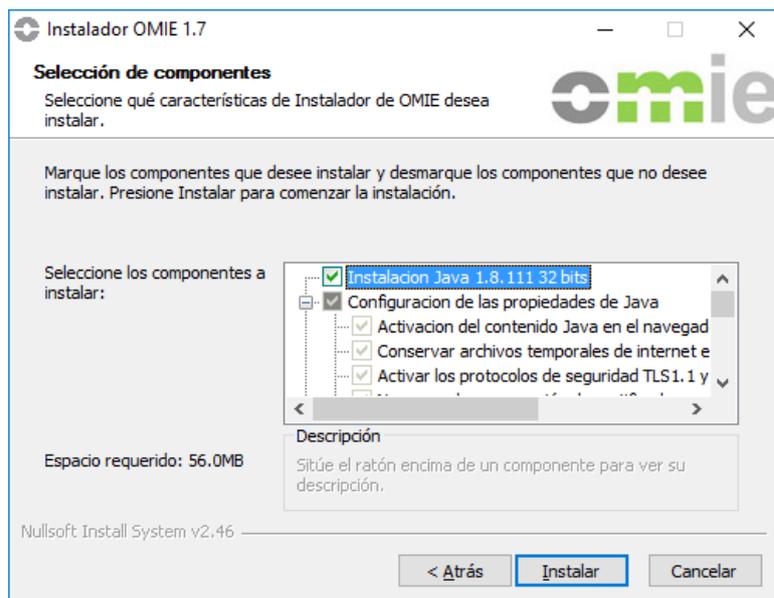
[files/omiesetup_32.exe](#)

El aspecto del instalador en el arranque es el siguiente:



Nota: Si el usuario activo en el equipo no tiene permisos de administración, aparecerá previamente la ventana de introducción de credenciales de un usuario administrador.

Al pulsar “Siguiente” aparecerá la ventana de selección de las características a instalar:

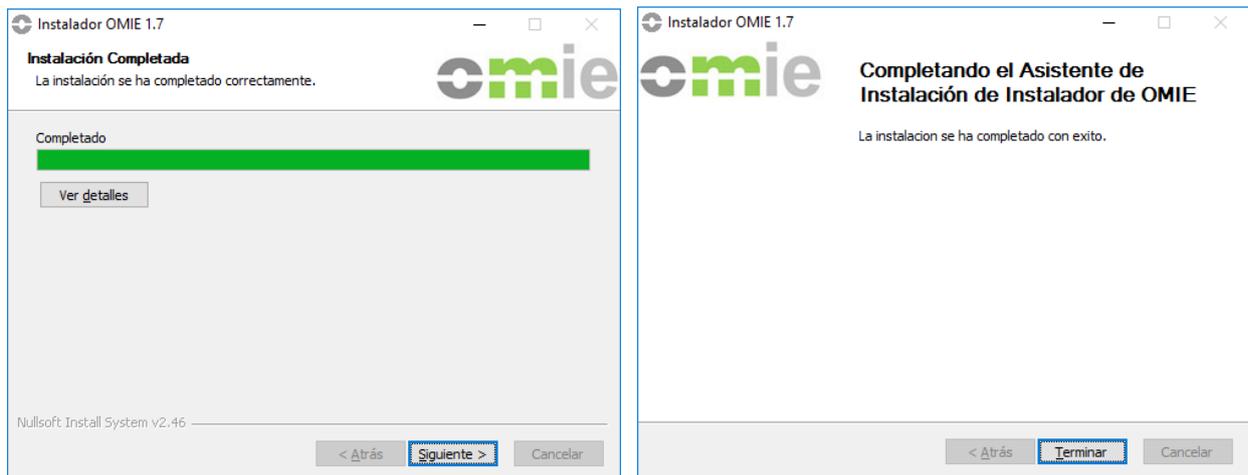


Dependiendo de la versión de la Máquina Virtual Java de 32 bits instalada en el equipo, la instalación de la versión incluida en el instalador será opcional, pudiendo el usuario desactivar esta opción. El resto de las opciones corresponden a elementos de configuración de la máquina virtual y del navegador Internet Explorer, que no pueden ser desactivados. Tras pulsar en “Instalar”, se aplicarán los cambios.

Si se ha seleccionado la instalación de la Máquina Virtual, se ejecutará en primer lugar el instalador de la misma.



Una vez finalizada dicha instalación, se continuará con el resto de características del instalador OMIE.



Nota: En caso de haber necesitado utilizar credenciales de administrador, los cambios de configuración se aplicarán tanto para el usuario administrador como para el usuario con el que se inició la sesión en el Sistema Operativo.

4 CONFIGURACIÓN MANUAL DEL PUESTO CLIENTE

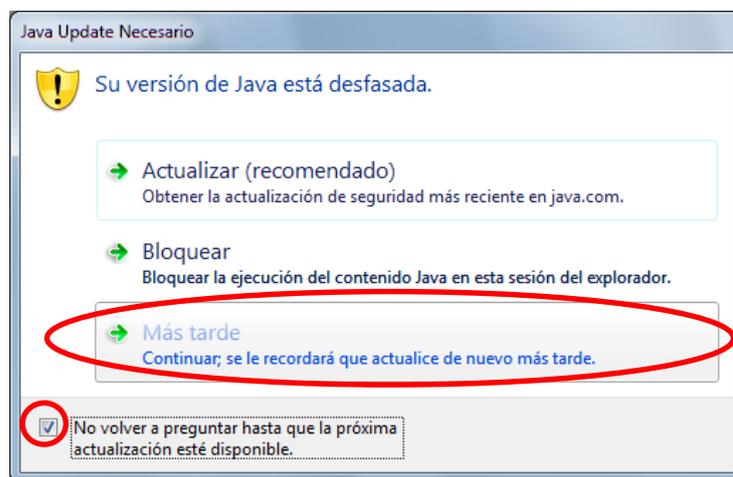
En este apartado se dispone de información adicional, que podría necesitarse para la correcta configuración del puesto cliente.

4.1 Configuración Java

En caso de no tener una versión válida, la forma de actualizar a la versión adecuada es desinstalar la versión instalada y acceder al Web de OMIE. Desde aquí, y según se describe en el capítulo 3, se realizará la instalación de la JVM correcta a través del Instalador OMIE (para poder realizar esta instalación, el usuario conectado al sistema operativo debe tener permisos de Administración.).

La desinstalación de la versión actual debe realizarse desde la opción de “Programas y características” del Panel de Control de Windows, seleccionando la entrada “J2SE Runtime Environment” o “Java ...” con la versión correspondiente, y pulsando el botón “Quitar”.

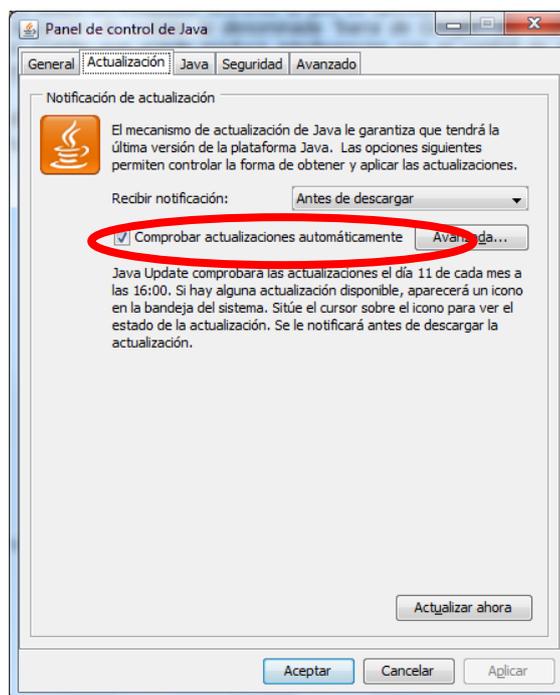
Al acceder al Web, puede aparecer una alerta indicando que existe una nueva versión Java disponible, bajo el texto “Su versión de Java está desfasada.” Para que no vuelva a aparecer el mensaje, pulsamos la casilla de abajo “No volver a preguntar hasta que la próxima actualización esté disponible”, y a continuación pulsamos “Más tarde”.



No se recomienda la opción de actualizar la versión, pues las nuevas versiones publicadas deben ser primero homologadas para uso en el sistema.

Este mensaje puede volver a aparecer cuando se publique una nueva versión de la máquina virtual.

Por otro lado, ante la posibilidad de que Oracle libere una nueva versión de JRE que aún no estuviese certificada para su uso en SIOM, es conveniente desactivar la actualización automática de la JVM. Esto se configura desactivando la siguiente casilla del Panel de Control:



4.2 Instalación del Lector de Tarjetas (Sólo para Certificados en Tarjeta)

Para el acceso a los Webs de SIOM es necesario disponer de un certificado de seguridad personal X.509, que OMIE emite bien en soporte de tarjeta inteligente Gemplus, o mediante un fichero. En caso de utilizar certificados en soporte de tarjeta, es necesario disponer de un lector de tarjetas inteligentes.

El usuario puede utilizar cualquier lector compatible con el estándar PC/SC, sobre el cual debe instalarse el software Gemplus. En la '**Guía de Instalación del software de Gemplus para acceso a SIOM**', que se proporciona como documento separado, se detallan los pasos a seguir. Es necesario tener instalado el lector y poder utilizar la tarjeta de seguridad con Internet Explorer para seguir con los pasos siguientes de configuración del puesto.

En el caso de querer instalar un lector de tarjetas GemPCTwin será necesario instalar los drivers específicos de ese tarjetero una vez hayamos instalado el software de Gemplus.

4.3 Registro de Certificados de Usuario

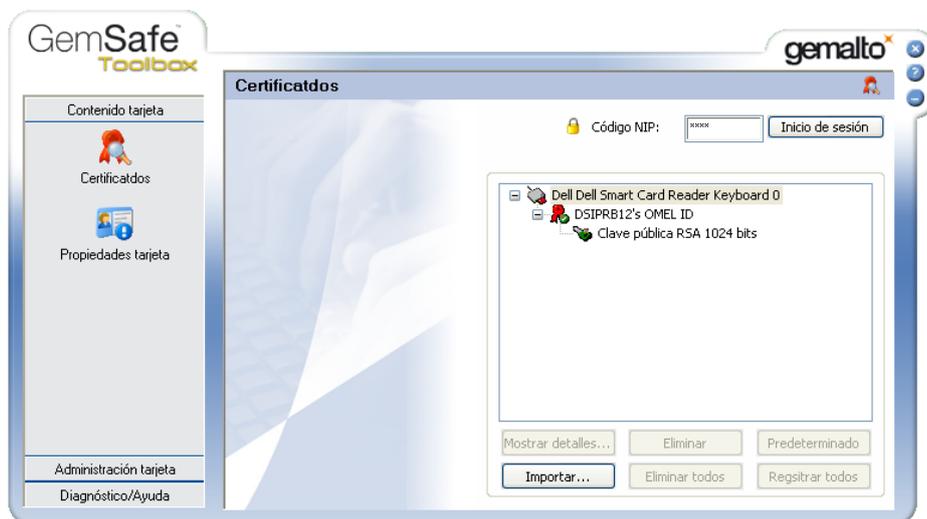
4.3.1 Certificados en tarjetas inteligentes

A la hora de utilizar por primera vez una nueva tarjeta de seguridad en un puesto de usuario, debe tenerse en cuenta que **es necesario registrar en Windows el certificado** entregado en la tarjeta para que pueda ser utilizado desde el navegador (es un requerimiento de Internet Explorer). La forma de registrar un certificado de usuario es mediante el software del lector de Tarjetas, tal como sigue:

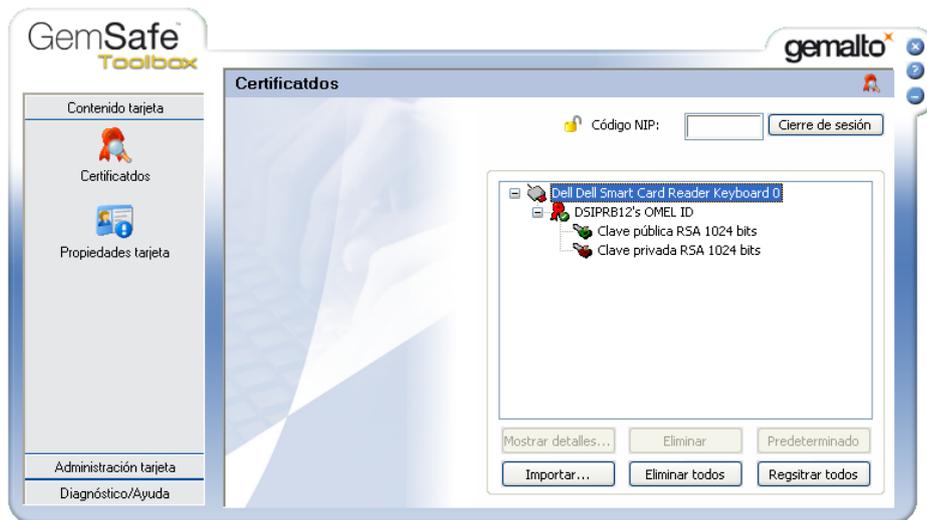
Introducir la tarjeta en el lector y arrancar el programa *GemSafe Toolbox* desde Windows:



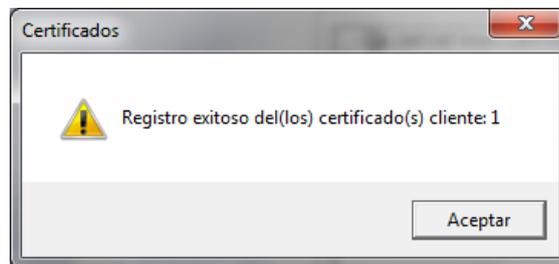
Pulsamos en *Contenido tarjeta* → *Certificados* e introducimos el PIN de la tarjeta en el apartado *Código NIP*. Pulsamos el botón *Inicio de sesión* para iniciar sesión:



Para registrar el certificado, hay que seleccionar el icono del tarjetero y a continuación pulsar el botón *Registrar todos*:



Tras unos segundos, aparece la siguiente pantalla donde indica que el certificado ha sido registrado.



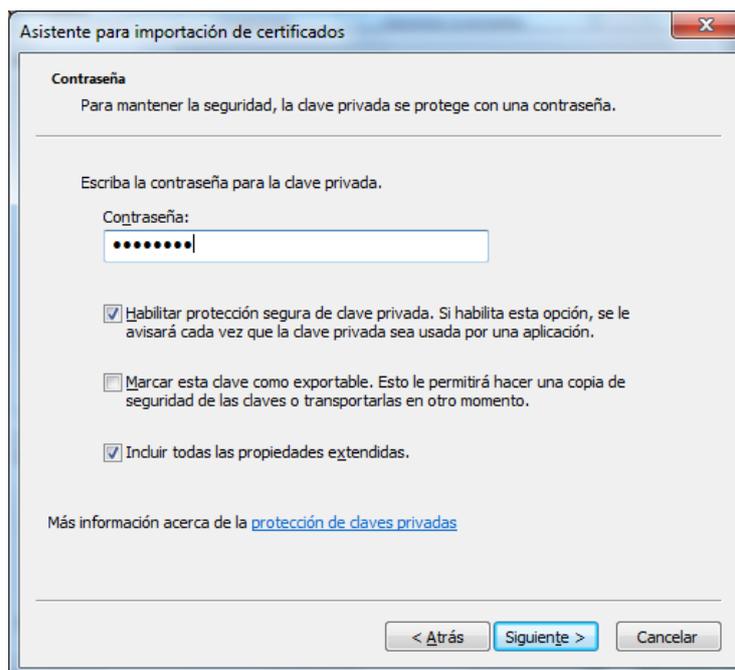
Se pulsa *Aceptar* y el proceso de registro del certificado concluye.

4.3.2 Certificados software

Los certificados en soporte de fichero, o certificados software, se entregan en formato “.p12” (estándar PKCS #12). Para registrar certificados entregados en este formato, deben seguirse los pasos que se describen a continuación.

Descargar el fichero “.p12” en un directorio accesible desde el puesto en que se va a registrar el certificado. Seleccionar el fichero y activarlo con “doble click” (este proceso también puede iniciarse desde el navegador, en “*Herramientas / Opciones de Internet / Contenido / Certificados / Importar*”).

Seguir los pasos que aparecen en pantalla, utilizando las opciones por defecto, hasta llegar a la siguiente pantalla:

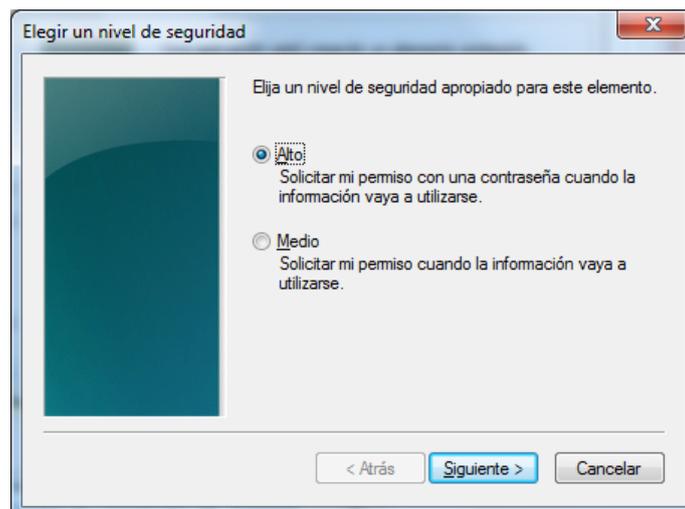


Introducir la contraseña de la clave privada, facilitada por OMIE, y marcar la casilla “*Habilitar protección segura de claves privadas*”.

Continuar con las opciones por defecto hasta la pantalla siguiente:

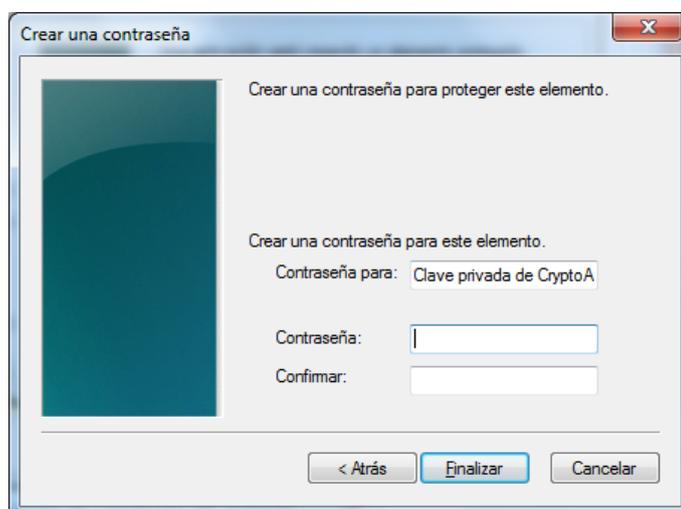


Pulsar en “Nivel de seguridad...”:

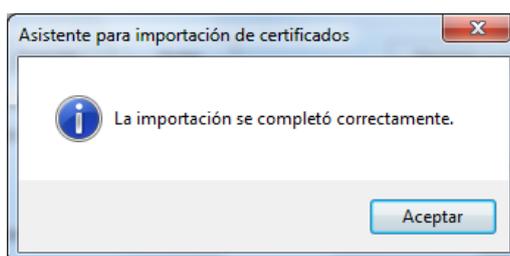


En esta pantalla puede seleccionarse un nivel de seguridad “Medio” o “Alto” para configurar el comportamiento del sistema al utilizar el certificado cuando se accede SIOM o se realiza la firma de un envío de información. En el caso de nivel “Medio”, el navegador mostrará únicamente un aviso para que el usuario confirme el acceso a la clave privada. En el caso de nivel “Alto”, el navegador solicitará además una contraseña de acceso a dicha clave privada.

Se recomienda seleccionar el nivel “Alto” y elegir una contraseña a utilizar a modo de PIN para el acceso al sistema y la firma de datos a enviar. En tal caso, al pulsar en “Continuar”, se mostrará la siguiente pantalla en la que se podrá escribir y confirmar la contraseña elegida.

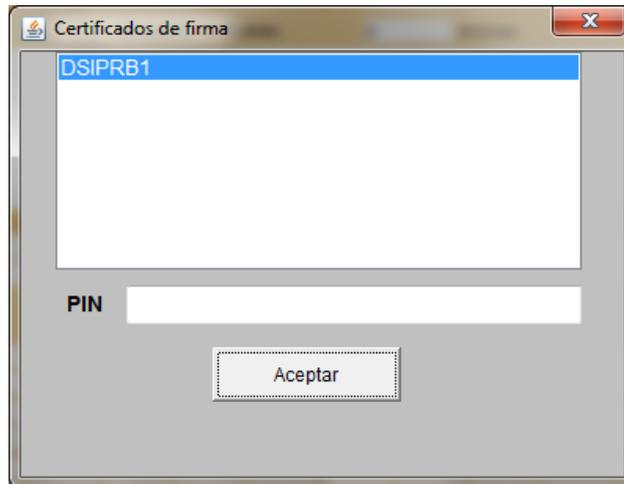


Tras pulsar en “Finalizar”, y posteriormente en “Aceptar”, se mostrará el mensaje que indica el final del proceso.

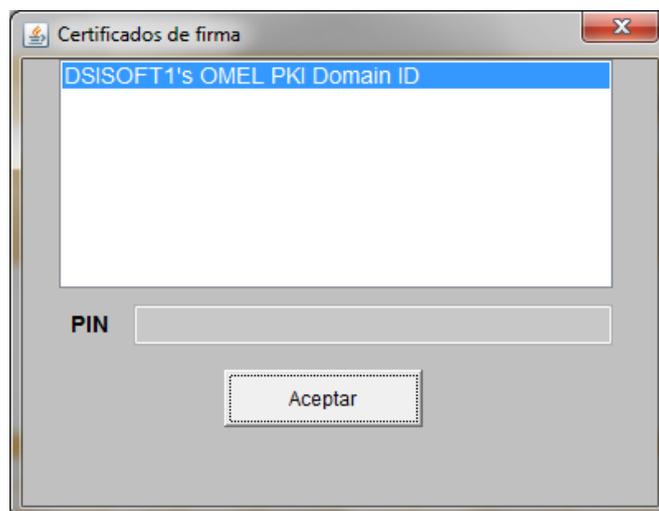


4.4 Configuración del Applet de Firma

El 'Applet de Firma' es el componente Java utilizado para realizar envíos de información firmados digitalmente a OMIE. El aspecto gráfico de este, cuando se ha de realizar cualquier envío firmado es el siguiente:



El Applet muestra el certificado a utilizar para realizar la firma digital del envío, que será el mismo utilizado en la conexión al Sistema. Asimismo, se incluye una casilla para el PIN del certificado para el caso de que se trate de un certificado en tarjeta inteligente. Si se ha utilizado un certificado software, la casilla estará desactivada, y será el propio navegador el que solicite posteriormente confirmación de uso del certificado, con o sin *password*, de acuerdo al nivel de seguridad elegido al registrarlo.



Este 'Applet' dispone de un fichero de configuración ubicado en 'C:\OMEL\ConfAppletFirma.xml'. El 'Applet', por defecto establece una configuración inicial en caso de no existir dicho fichero, creándolo para posterior modificación del usuario. En la primera instalación del puesto este fichero no se creará hasta que se haya entrado a la página principal del Web

El contenido de dicho fichero es el siguiente:

```
<?xml version='1.0'?>
<!--
    NOTA : Cualquier cambio en este fichero se tendrá en cuenta a
           partir del próximo reinicio del navegador.
-->
<ConfAppletFirma>
  <Seguridad>
    <PINTimeout>0</PINTimeout>
  </Seguridad>
  <Log>

  <DirEnviosFirmados>c:\omel\EnviosFirmados</DirEnviosFirmados>
  </Log>
</ConfAppletFirma>
```

Dentro de este fichero se establecen dos parámetros configurables:

- **PINTimeout:** Tiempo de expiración de PIN. Este tiempo expresado en minutos, establece el tiempo máximo que espera el 'Applet' entre envío firmado, para pedir de nuevo el PIN al usuario. Si desde el último envío firmado no ha pasado el tiempo máximo definido, no se volverá a pedir el PIN al usuario. El valor '0' indica que siempre se pedirá el PIN al usuario. Este parámetro tiene un valor máximo establecido en 30 minutos. Si se pone un valor superior a este, por defecto se utilizará el tiempo de 30 minutos.
- **DirEnviosFirmados:** Directorio destino de los envíos firmados. En este directorio se irá creando una estructura de subdirectorios con todos los envíos firmados que el usuario haya realizado con el 'Applet', organizados por tipos de envíos ("OfertasMD", "Desagregaciones", "OfertasSubastas", "ReclamacionesSubastas" etc.). En caso de especificarse un directorio no existente, el 'Applet' lo creará automáticamente. Si no se pudiera crear dicho directorio, el directorio destino sería el definido por defecto por el 'Applet', que es '**c:\omel\EnviosFirmados**'.

Cualquier cambio en este fichero se tendrá en cuenta en la próxima ejecución del navegador.

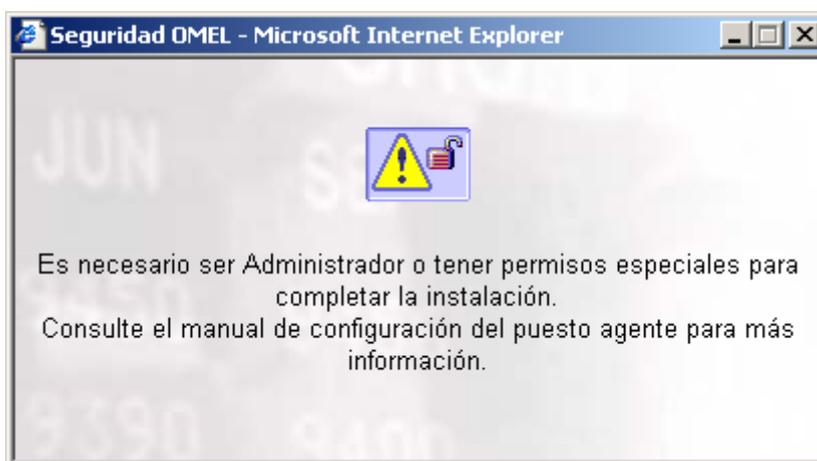
5 PROBLEMAS FRECUENTES

5.1 Aparecen mensajes de error en la instalación de los applets

Cuando se da alguna de las siguientes situaciones:

- el usuario que hace la primera instalación no tiene privilegios de Administrador,
- el Administrador no dio permisos de actualización de componentes a Usuarios Avanzados, y un Usuario Avanzado realiza la entrada al sistema cuando OMIE ha incluido una actualización de versiones de Applets,
- un Usuario Normal realiza la entrada al sistema cuando OMIE ha incluido una actualización de versiones de Applets,

la ventana principal del navegador se cerrará automáticamente, y se obtendrá el siguiente mensaje:

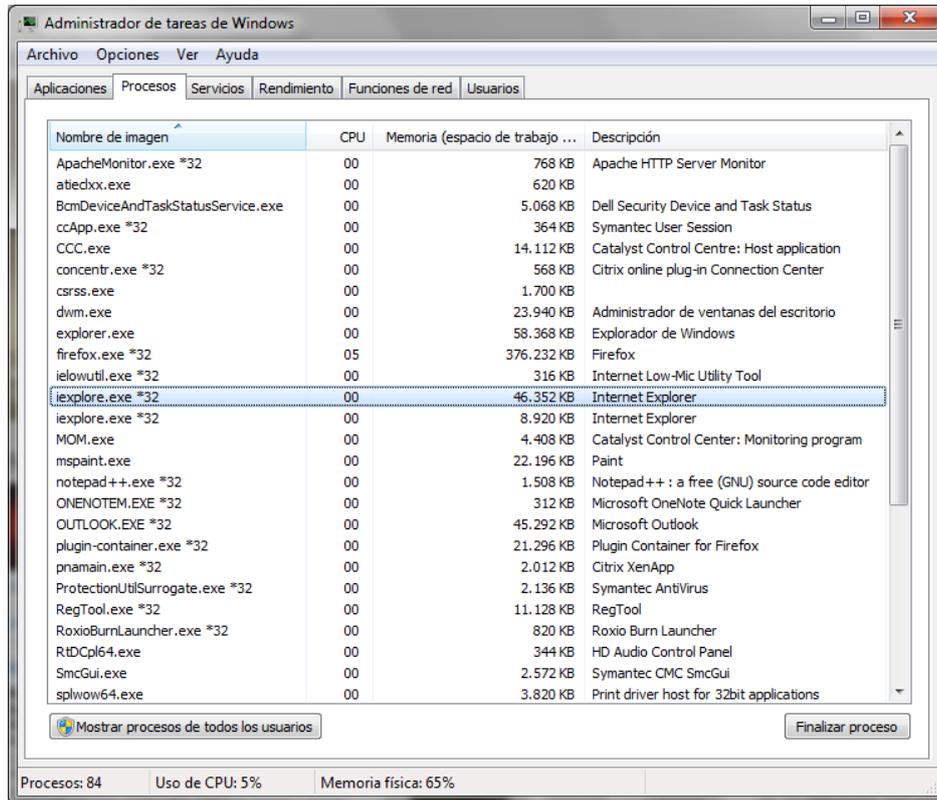


Para evitar esto, debe realizarse la entrada al sistema con un usuario con privilegios de Administrador, o de Usuario Avanzado si el Administrador dio permisos a los Usuarios Avanzados para realizar actualizaciones posteriores.

5.2 El PIN de la tarjeta tarda mucho en ser solicitado, o el navegador queda bloqueado en ese momento

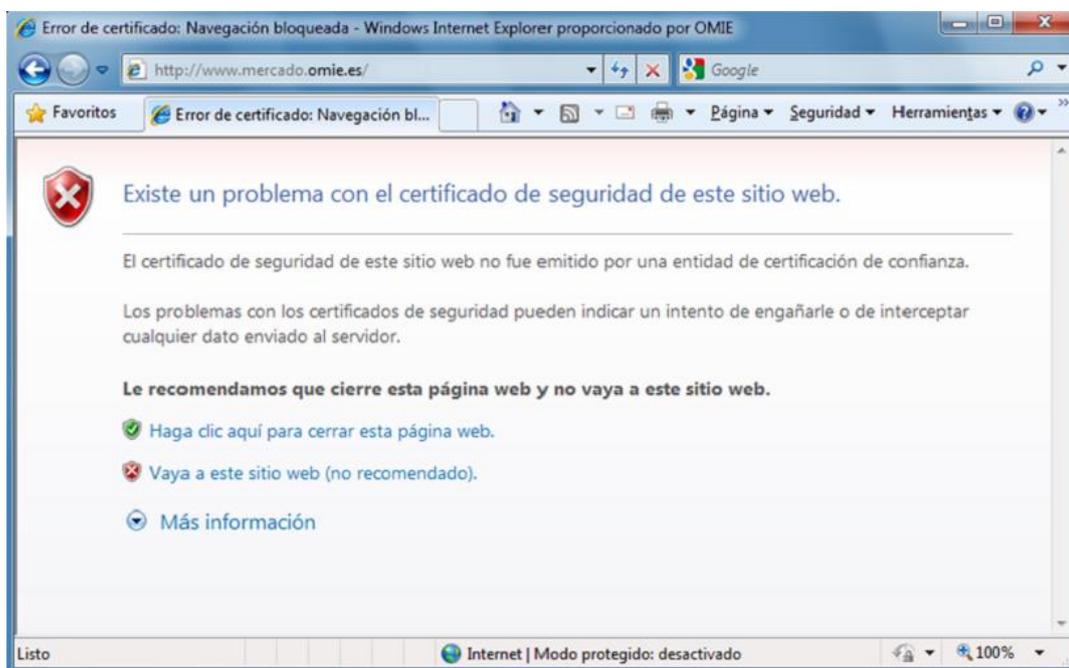
Este problema puede deberse a que existen otras sesiones de Internet Explorer abiertas. Para solucionar este problema, se deben cerrar todas las sesiones del navegador, y repetir la entrada al sistema.

Si el problema persiste, debe comprobarse si existen procesos activos en el Administrador de Tareas del sistema, bajo el nombre *IEXPLORE.EXE*, como muestra la imagen. En tal caso, estos procesos deben cerrarse manualmente desde el Administrador de Tareas (mediante el botón "Terminar proceso", antes de reintentar el acceso al sistema.



5.3 Aparece al “Error de certificado” al acceder al sistema

Tal como se explica en el apartado **¡Error! No se encuentra el origen de la referencia.**, esta ventana aparece cuando no se ha registrado el certificado de Entidad Firmante OMIE CA en el navegador.



Esto puede ocurrir, aunque ya se haya registrado anteriormente dicho certificado, si se utiliza un usuario del Sistema Operativo que no haya entrado antes al Web de SIOM o bien por una actualización de la rootCA en SIOM.

Para solucionar este problema, deben seguirse los pasos descritos en el presente documento, a partir del apartado **¡Error! No se encuentra el origen de la referencia.**, así como revisar las opciones de configuración del navegador para ese usuario, tal como se describe en el apartado 4.2.

5.4 El servidor no permite el acceso al sistema

Si se detectan errores del tipo “*No se puede mostrar la página*” o “*Access Forbidden*”, puede ser debido a que se está utilizando un navegador que no soporta encriptación de 128 bits.

Para verificar el nivel de encriptación soportado por el navegador que se está utilizando, pueden seguirse los pasos que se describen en el apartado 4.2.

Actualmente, las versiones de navegador que pueden descargarse de Microsoft incorporan el nivel de encriptación necesario. El problema puede deberse a que se está utilizando una versión antigua, u obtenida cuando se distinguía entre versiones con o sin encriptación fuerte por temas legales internacionales. Por tanto, el problema se resuelve instalando una versión actualizada del navegador.

5.5 Uso de Namespaces en los documentos XML (sólo para el Web del Mercado)

Cuando se envíen documentos XML que no incluyen la especificación correcta del *namespace*, ya sea a través del navegador como a través de WebServices, se obtendrá un mensaje de error. En el caso del envío a través del navegador, se obtendrá una ventana con el siguiente mensaje:

**Ha habido un error de parseado del documento:
El fichero XML no tiene el 'namespace' correcto 'http://www.omel.es/Schemas'**

Para que un documento XML enviado a OMIE tenga el *namespace* correcto, su cabecera debe incluir el contenido que se muestra en el siguiente ejemplo:

```
<MensajeOfertasMD xmlns="http://www.omel.es/Schemas">
  <IdMensaje v="OfertasMD-2004-10-05"/>
  <FechaMensaje v="2004-10-04T09:19:43-00:00"/>
  <IdRemitente v="AGENT"/>
  ...
</MensajeOfertasMD>
```

El error producido en caso de utilizar la interfaz Web Services, tomando en ejemplo de envío de ofertas al Mercado Diario, sería el siguiente, en el que se indica que el servidor no sería capaz de encontrar el elemento '*MensajeOfertasMD*' asociado al correspondiente *Namespace*, dentro del documento enviado:

```
AxisFault
  faultCode:
    {http://xml.apache.org/axis/}Server.userException
  faultString:
    org.xml.sax.SAXParseException:
      No se ha encontrado la declaración del elemento 'MensajeOfertasMD'.
```

El *namespace* se utiliza para eliminar conflictos de nomenclatura entre documentos XML que pueden compartir las mismas etiquetas con propósitos diferentes. Con el fin de evitar posibles conflictos en un futuro, en SIOM2 se ha optado por aplicar los estándares de forma estricta y exigir la especificación del *namespace*.

A continuación se muestran dos ejemplos de documentos con conflicto de nomenclatura:

Documento con información bursátil:

```
<table>
  <value>
    <ticker>TLR3</ticker>
    <last>18.23</last>
  </value>
</table>
```

Documento con información de un producto:

```
<table>
  <name>Mesa de cafe Americana</name>
  <width>80</width>
  <length>120</length>
</table>
```

Si estos dos tipos de documentos son agregados en un solo documento, existirá un conflicto de elementos, ya que ambos documentos contienen un elemento del tipo *<table>*.

El uso de *Namespaces* soluciona este tipo de problemas, asignando un espacio de nombres a un conjunto de etiquetas. Los *Namespaces* se suelen definir en el elemento raíz del documento XML, asignando así este *Namespace* a todos los elementos incluidos los hijos. A continuación se muestran los documentos XML anteriores corregidos incorporando su *Namespace*:

Documento con información bursátil:

```
<table xmlns="http://www.mibolsa.com/tabla">
  <value>
    <ticker>TLR3</ticker>
    <last>18.23</last>
  </value>
</table>
```

Documento con información de un producto:

```
<table xmlns="http://www.muebles.es/Catalogo">
  <name>Mesa de cafe Americana</name>
  <width>80</width>
  <length>120</length>
</table>
```

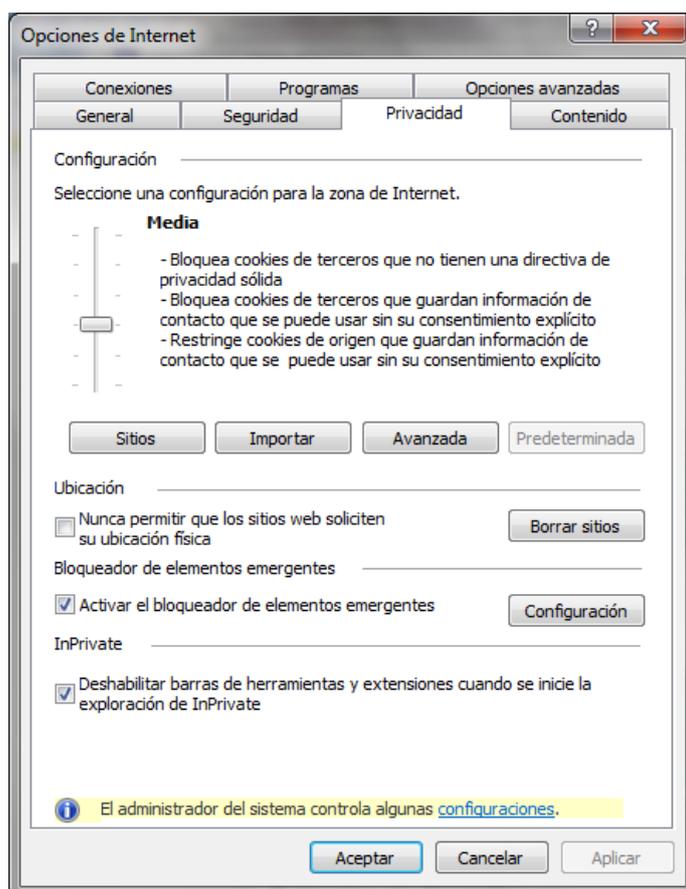
Debido a esto, todos los documentos XML enviados a OMIE y recibidos de OMIE tendrán establecido su correcto *namespace* para impedir posibles conflictos.

5.6 Bloqueo de ventanas emergentes

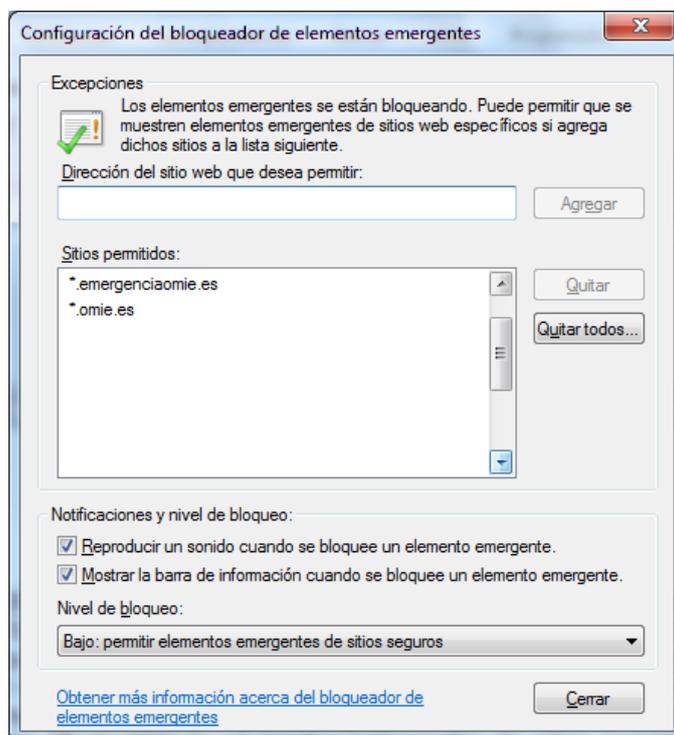
El procedimiento de instalación de componentes de los Webs de SIOM utiliza ventanas emergentes en la ejecución de algunos de sus pasos (ver apartado 4.2). En caso de que la aparición de ventanas emergentes está bloqueada en el navegador, dicha instalación no se ejecutará correctamente, impidiendo la operación en el Web.

La configuración del bloqueo de ventanas se realiza en

Herramientas → Opciones de Internet → Privacidad → Bloqueador de elementos emergentes

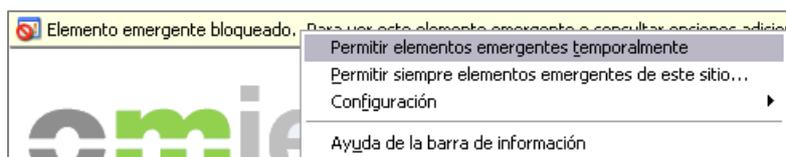


Si la opción “*Bloquear elementos emergentes*” está activada, no se podrá acceder correctamente a SIOM. Para solucionar este problema, debe desactivarse esta opción, o bien especificar que los Servidores Web de OMIE sí pueden abrir ventanas emergentes. Para ello, debe pulsarse el botón “*Configuración...*”, y en la caja de texto “*Dirección del sitio Web que desea permitir*” escribir “**.omie.es*” y pulsar “*Agregar*”. Con objeto de poder acceder sin problemas al entorno de emergencias, esta operación debe repetirse asimismo para “**.emergenciaomie.es*”. Además, deberá indicarse como “*Nivel de filtro*” la opción “*Bajo: permitir elementos emergentes de sitios seguros*” (ver captura a continuación).

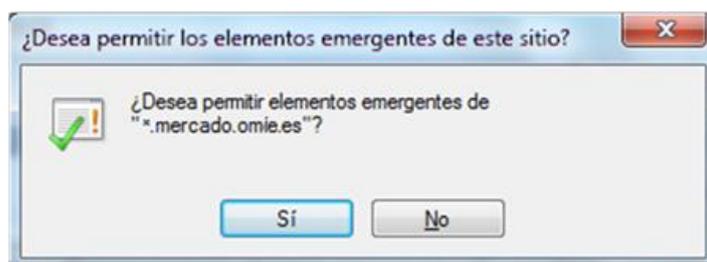


De esta forma, podrá accederse sin problemas a todos los servidores Web de OMIE.

En caso de que se hayan bloqueado las ventanas emergentes, y no se hayan permitido las de OMIE, aparecerá la siguiente línea de aviso en el navegador, con las siguientes opciones al pulsar en ella:



Si se elige la opción “*Permitir siempre elementos emergentes de este sitio...*” aparecerá la siguiente ventana de confirmación (ejemplo para el Web “http://www.mercado.omie.es”):



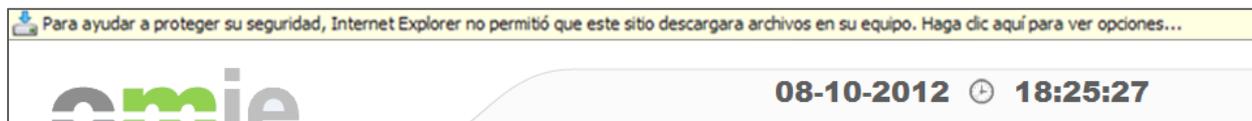
Al pulsar “*Sí*” quedará desactivado el bloqueo de ventanas emergentes para ese servidor, y podrá reintentarse la entrada al mismo.

Sin embargo, se recomienda el primer procedimiento descrito en este apartado, por el que permite el acceso a todos los servidores de OMIE con una sola operación.

Por otro lado, el bloqueo de las ventanas emergentes puede activarse de otras formas, como por ejemplo instalando herramientas que, entre otras funciones, permiten bloquear dichas ventanas. Es el caso de las “barras” de *MSN* o *Google* (entre otras). En caso de tener instalada alguna de estas herramientas, es necesario configurarla de manera que no se bloqueen, al menos, las ventanas emergentes de los Webs de OMIE (“*.omie.es” y “*.emergenciaomie.es”). Consúltese para ello la documentación proporcionada por dichas herramientas.

5.7 Aviso al descargar fichero

Si se intenta descargar un fichero (por ejemplo, descarga de la petición o la respuesta en la consulta de transacciones firmadas), puede ocurrir que se muestre un aviso como el siguiente:



Aunque se indique que se desea descargar el fichero, el navegador mostrará la página de bienvenida del Web.

Para solucionar este problema, debe revisarse las opciones mínimas de configuración del navegador (tal como se indica en el apartado 4.2):

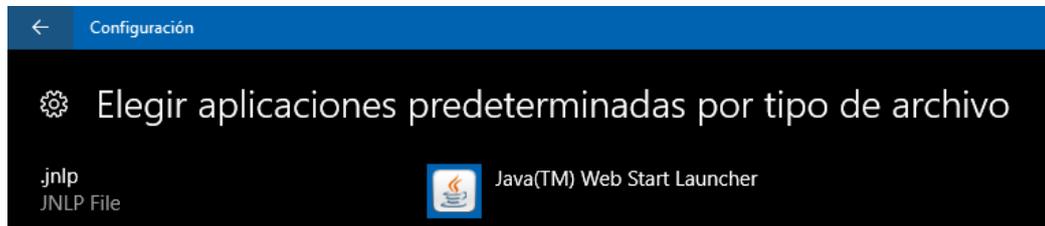
Herramientas / Opciones de Internet / Seguridad / Internet [o la zona en la que esté la web] / Nivel Personalizado / Descargas / Pedir intervención del usuario automática para descargas de archivo/ Habilitar.

De esta forma, al solicitar la descarga de un fichero, no se mostrará el mensaje de aviso, y aparecerá únicamente el diálogo estándar que permite abrirlo o guardarlo en disco.

5.8 Problema al arrancar el Centro de Descargas (sólo para el Web del Mercado)

Como el Centro de Descargas hace uso del Java Web Start, para una correcta ejecución del mismo, se debe establecer la extensión .jnlp a dicho programa, siguiendo las indicaciones siguientes, para que el Centro de Descargas arranque automáticamente.

Configuración → Aplicaciones → Aplicaciones predeterminadas → Elegir aplicaciones predeterminadas por tipo de archivo.



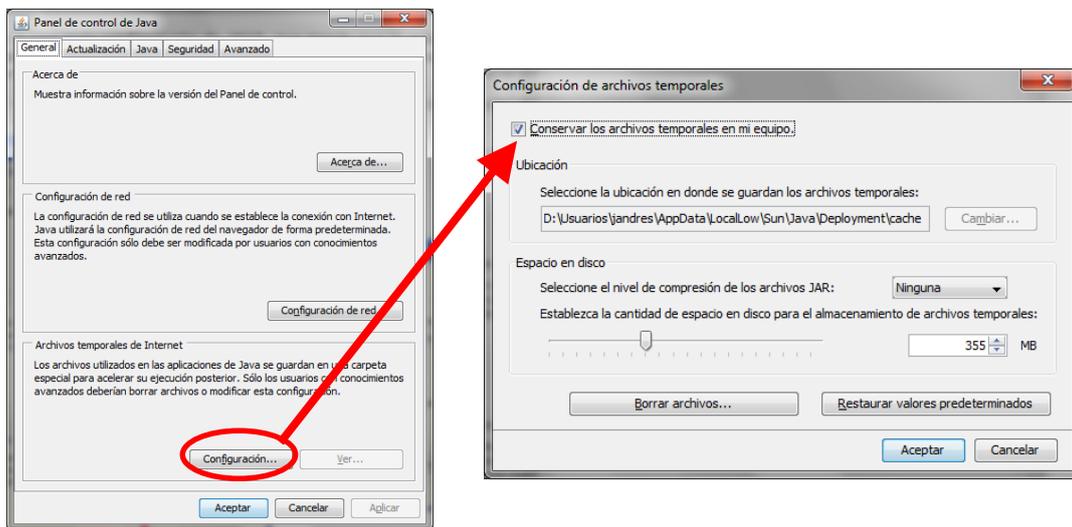
Por otro lado, en algunos casos tras arrancar “Centro de Descargas” puede aparecer la siguiente excepción:



Este error se debe a una mala configuración de JAVA, que impide que la aplicación arranque. Para solucionar este problema se deberá cambiar la configuración desde el panel de control.

Dicha configuración se encuentra en:

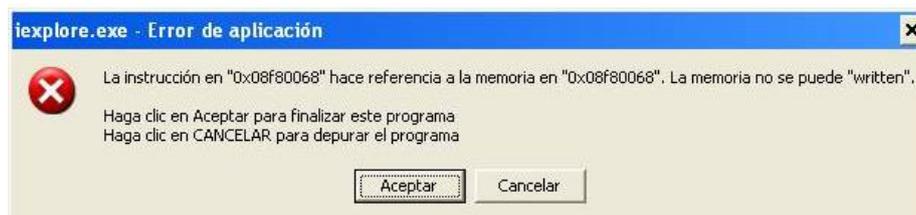
Panel de Control → Java → General → Archivos temporales de Internet → Configuración



Una vez allí, activamos el check “Conservar los archivos temporales en mi equipo”.

5.9 Problema al entrar al WEB sin ningún Java instalado

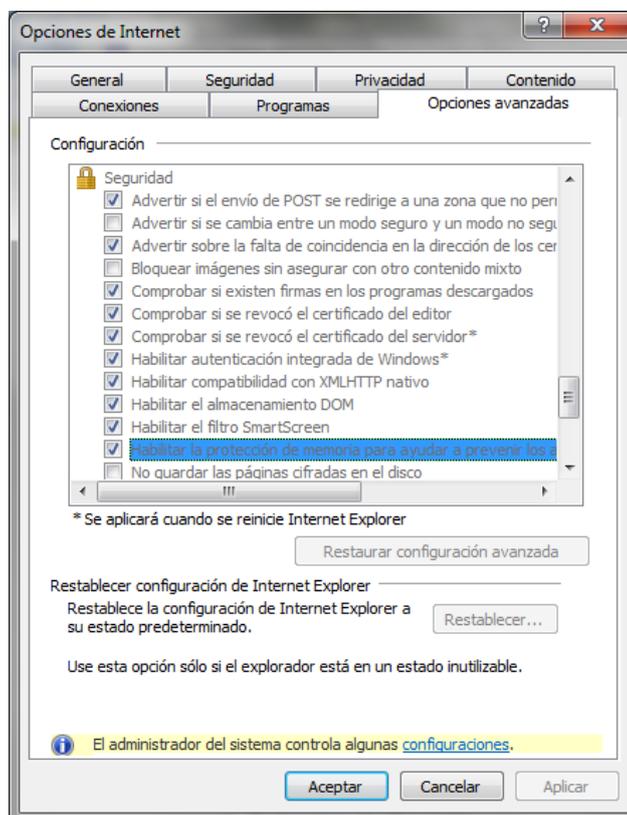
En algunos casos, al entrar en el Web sin tener ningún JRE de Java instalado, nos aparece el siguiente error:



Este error es debido a un mecanismo de seguridad incorporado en Explorer para evitar la ejecución de código malicioso (*"Data Execution Prevention"*). En la instalación de la JRE, al igual que en otras extensiones del navegador, puede producirse este problema si dichas extensiones no están actualizadas para ser compatibles con dicho mecanismo.

Si se desea realizar la instalación desde el Web, se puede desactivar esta comprobación de la siguiente manera:

Herramientas → *Opciones de Internet* → *Opciones avanzadas* → *Seguridad*



Deshabilitar la casilla *"Habilitar la protección de memoria para ayudar a prevenir los ataques en línea"*, reiniciar el navegador y repetir la entrada al sistema. Se recomienda reactivar esta casilla después de la instalación.

Otra alternativa es descargar Java desde su propia página Web;

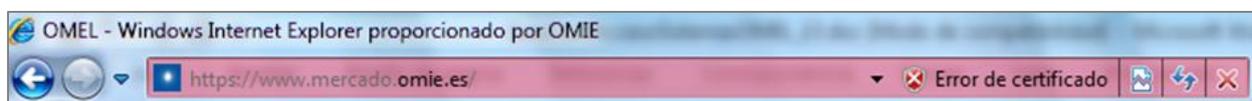
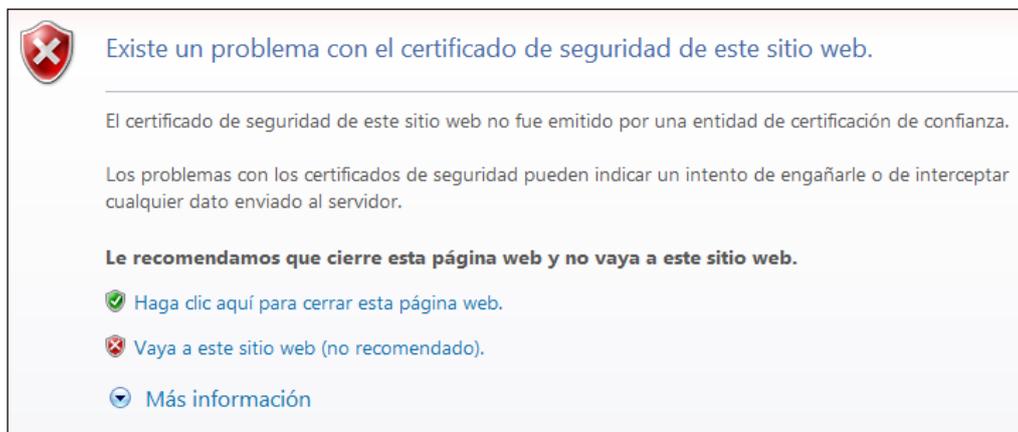
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

Descargar la versión "JRE" compatible del aplicativo.

Una vez descargado realizar la instalación como se detalla en el punto 3.1 y a continuación entrar de nuevo en el Web.

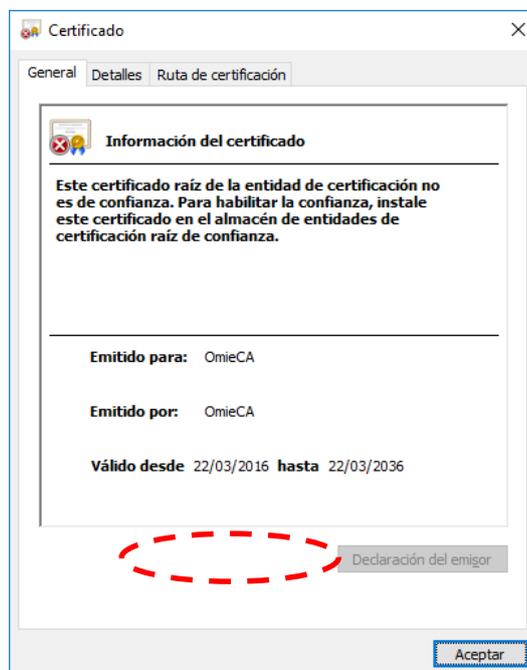
5.10 Instalación incorrecta del ROOT CA de OMIE.

Puede darse el caso de que, después de haber instalado el ROOT CA de OMIE, siga apareciendo la advertencia de seguridad, y el error de certificado:



Este problema puede ser debido a que el certificado ROOT CA de OMIE no ha sido instalado en el almacén de certificados correcto (puesto que si se siguen las opciones por defecto que ofrece el navegador, el certificado puede quedar instalado en el almacén "Entidades de certificación intermedias", en lugar de en "Entidades de certificación raíz de confianza").

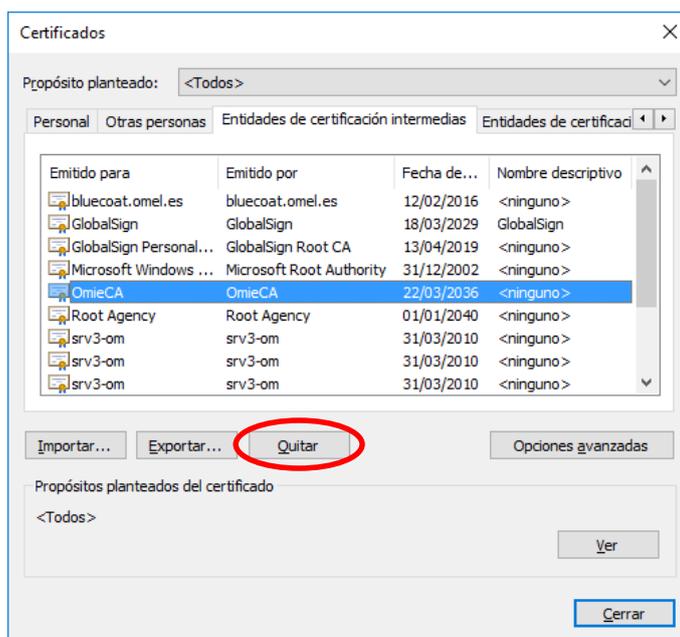
Además, en esta situación no es posible instalarlo de nuevo en el almacén adecuado, puesto que si se siguen los pasos descritos en el apartado 4.6, no aparece el botón de "Instalar certificado". Esto se debe a que el certificado ya está instalado en un almacén.



Por tanto, la solución consiste en desinstalar primero el certificado. Para ello, debe accederse desde el navegador a:

Herramientas → *Opciones de Internet* → *Contenido* → *Certificados* → *Entidades de certificación intermedias*

En este punto, se debe seleccionar el certificado “OmieCA” y pulsar en “Quitar”:



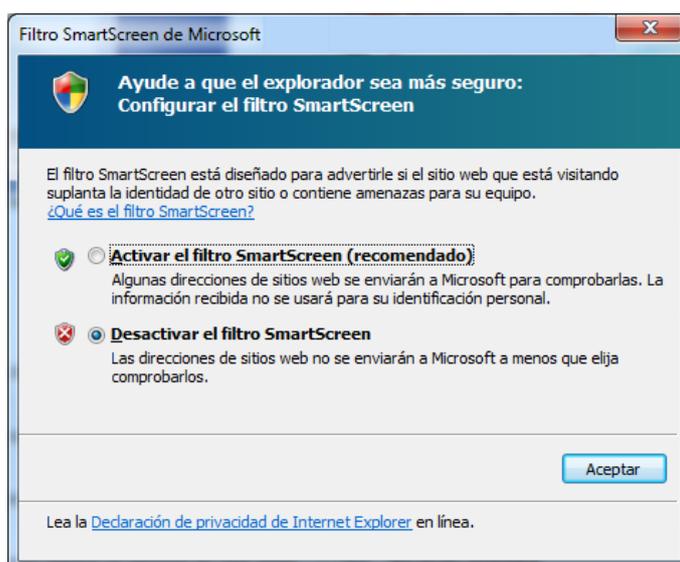
Tras confirmar la operación, el certificado se habrá desinstalado. A partir de ese momento, deben seguirse de nuevo los pasos que se describen en el apartado 4.6 para la correcta instalación del ROOT CA de OMIE.

5.11 Se abren dos ventanas del Centro de Descargas (sólo para el Web del Mercado).

En algunas ocasiones, al ejecutar el Centro de Descargas desde el Web del Mercado, ésta se ejecuta dos veces (se abren dos ventanas de la Descarga Automática, por lo que se solicita el certificado de conexión también dos veces).

Este problema se ha detectado con Internet Explorer 9 al tener activado el “Filtro SmartScreen”. Para solucionar este problema es necesario desactivar este filtro. El “Filtro SmartScreen” puede encontrarse en:

Herramientas → Filtro SmartScreen → Desactivar el filtro SmartScreen...



5.12 Se obtiene un mensaje de versión de navegador no soportada (sólo para el Web del Mercado).

Si se utiliza Internet Explorer 8, puede obtenerse el siguiente mensaje:



Esto es debido a que se está ejecutando el navegador en “Vista de compatibilidad”.

Para solucionar este problema, deben seguirse las instrucciones de configuración de la vista de compatibilidad que se describen en el apartado 4.2.

5.13 Error al enviar una oferta por fichero.

Al enviar una oferta por fichero, puede aparecer el siguiente mensaje imposibilitando el envío



Para corregirlo, seguir el apartado 4.2, el punto “Revisión de opciones mínimas”.

Herramientas / Opciones de Internet / Seguridad / Internet [o la zona en la que esté la web] / Nivel Personalizado / Miscelánea / Incluir la ruta de acceso al directorio local cuando se carguen archivos a un servidor / Habilitar.