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

Alfonso XI, 6
28014 Madrid
www.omie.es

Ref. GuiaConfAccesoSistemasOMIE.docx

Versión 3.00
Fecha: 2024-03-05

ÍNDICE

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 para acceder el uso de certificados de usuario proporcionados por OMIE (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 o navegador. 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.

***Nota**: **EDGE** es el navegador de referencia y OMIE dará soporte sobre el mismo. Pese a que otros navegadores podrían acceder al mercado, no están oficialmente soportados por OMIE al no efectuarse comprobaciones específicas sobre ellos.*

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 10
  - Windows 11 (recomendado)
- Navegador:
  - Microsoft Edge (navegador soportado y de referencia)
- Registro de los certificados a utilizar.
- Instalación del Root CA de OMIE (incluido en el Instalador web de OMIE).
- Fortify app (incluido en el Instalador web de OMIE) para la firma digital de los envíos.

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

2.2 Resolución de pantalla

El web se ha diseñado para una configuración de pantalla 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 (OMIE_Setup_EDGE.zip) 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→Publicaciones).

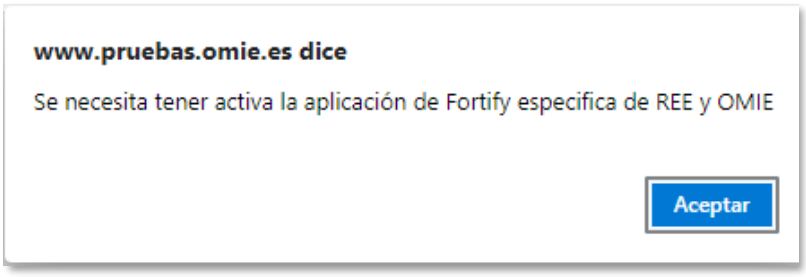
Extraer el archivo del ZIP y ejecutar.

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.

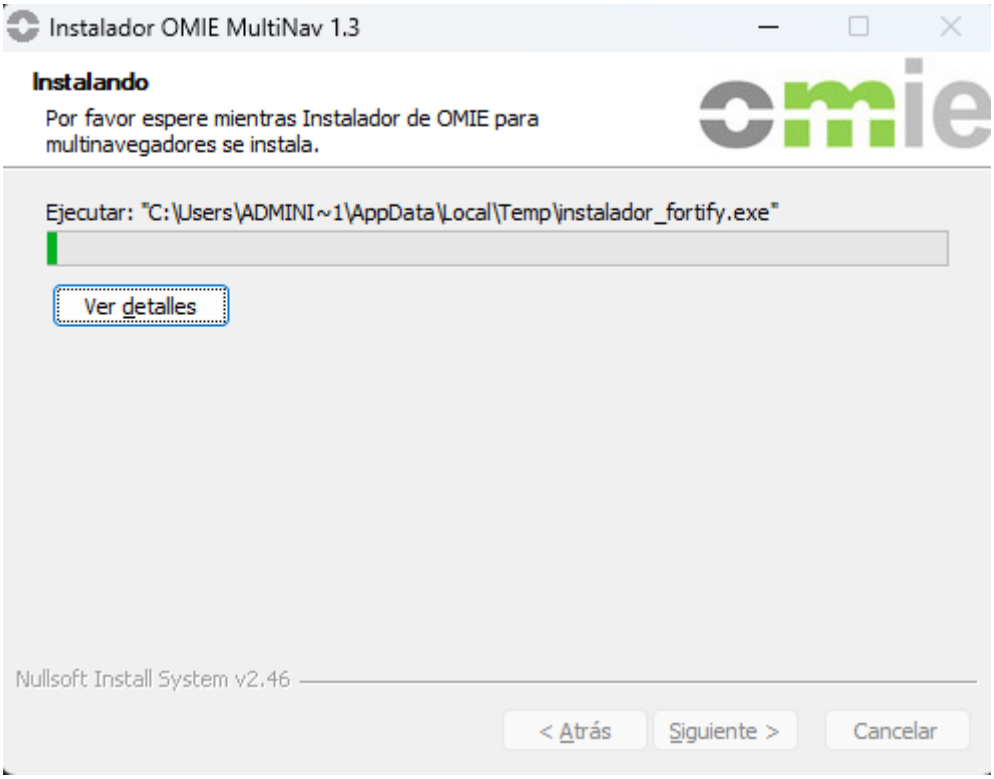
El aspecto del instalador en el arranque es el siguiente:

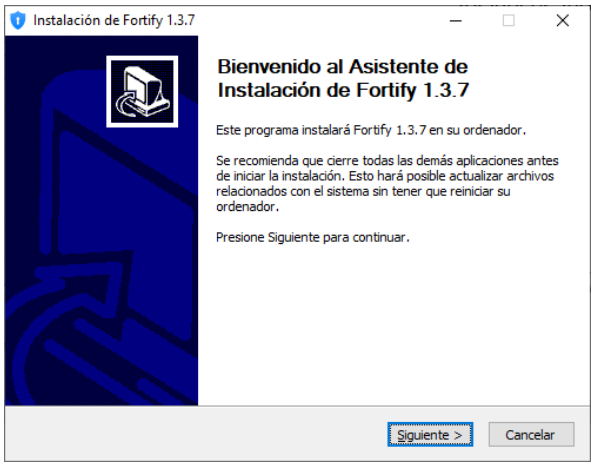
Al pulsar “Siguiente” aparecerá la ventana de selección de las características a instalar. Si el instalador detecta que alguno de los componentes ya está instalado, este aparecerá desmarcado y no se podrá marcar a no ser que primero se desinstale dicho componente:

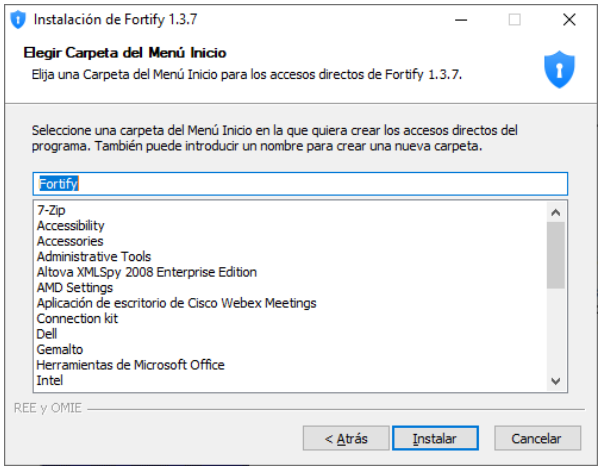
En caso de acceder al Sistema sin tener ninguna versión de Fortify instalada o en ejecución, se mostrará una pantalla en la que se informa de la necesidad de tener instalada la aplicación Fortify.

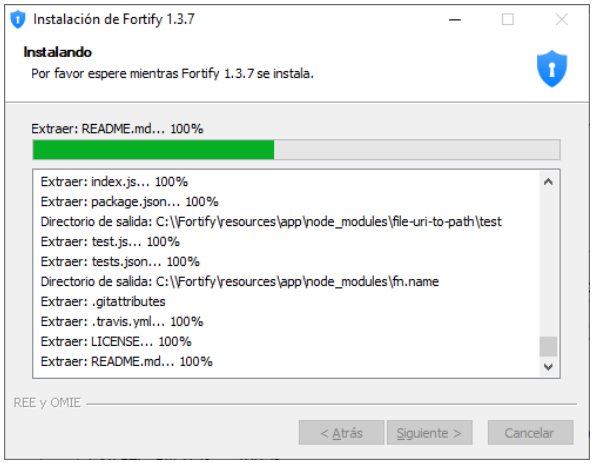


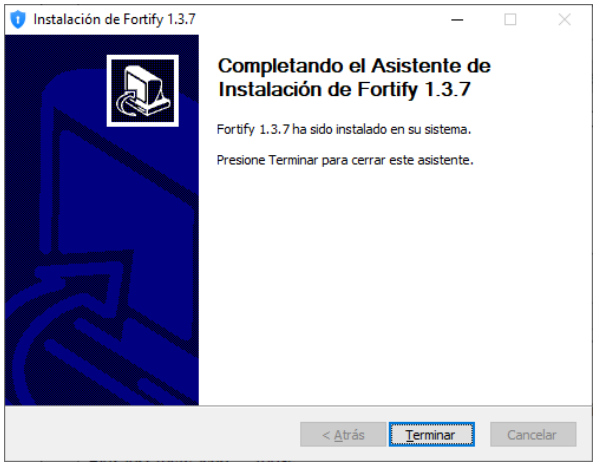
A continuación, aparecerá el instalador de Fortify:


Instalador OMIE MultiNav 1.3
Instalando
Por favor espere mientras Instalador de OMIE para multinavegadores se instala.
omie
Ejecutar: "C:\Users\ADMINI~1\AppData\Local\Temp\instalador_fortify.exe"
Ver detalles
Nullsoft Install System v2.46
< Atrás
Siguiente >
Cancelar


Instalación de Fortify 1.3.7
Bienvenido al Asistente de Instalación de Fortify 1.3.7
Este programa instalará Fortify 1.3.7 en su ordenador.
Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.
Presione Siguiente para continuar.
Siguiente >
Cancelar


Instalación de Fortify 1.3.7
Elegir Carpeta del Menú Inicio
Elija una Carpeta del Menú Inicio para los accesos directos de Fortify 1.3.7.
Seleccione una carpeta del Menú Inicio en la que quiera crear los accesos directos del programa. También puede introducir un nombre para crear una nueva carpeta.
Fortify
7-Zip
Accessibility
Accessories
Administrative Tools
Altova XMLSpy 2008 Enterprise Edition
AMD Settings
Aplicación de escritorio de Cisco Webex Meetings
Connection kit
Dell
Gemalto
Herramientas de Microsoft Office
Intel
REE y OMIE
< Atrás
Instalar
Cancelar

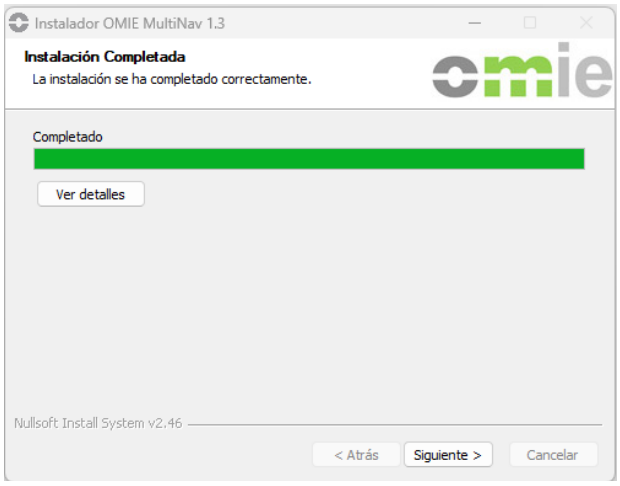

Instalación de Fortify 1.3.7
Instalando
Por favor espere mientras Fortify 1.3.7 se instala.
Extraer: README.md... 100%
Extraer: index.js... 100%
Extraer: package.json... 100%
Directorio de salida: C:\Fortify\resources\app\node_modules\file-uri-to-path\test
Extraer: test.js... 100%
Extraer: tests.json... 100%
Directorio de salida: C:\Fortify\resources\app\node_modules\fn.name
Extraer: .gitattributes
Extraer: .travis.yml... 100%
Extraer: LICENSE... 100%
Extraer: README.md... 100%
REE y OMIE
< Atrás
Siguiente >
Cancelar


Instalación de Fortify 1.3.7
Completando el Asistente de Instalación de Fortify 1.3.7
Fortify 1.3.7 ha sido instalado en su sistema.
Presione Terminar para cerrar este asistente.
< Atrás
Terminar
Cancelar

Nota: *Por las características del instalador de Fortify, la aplicación se instala para todos los usuarios de la máquina, pero sólo arranca automáticamente si el usuario que lo ha instalado es el administrador, aunque cualquier usuario del equipo puede arrancarla (siempre y cuando no haya abierta "en background" la sesión de otro usuario con Fortify arrancado, caso en el que ese usuario debe cerrar su sesión primero).*

En los apartados 3.1 y 4.1 se indican los pasos para verificar el arranque de Fortify y el procedimiento de autorización inicial, una vez se acceda al Web de SIOM.

Con este paso se completa el proceso del instalador de SIOM.



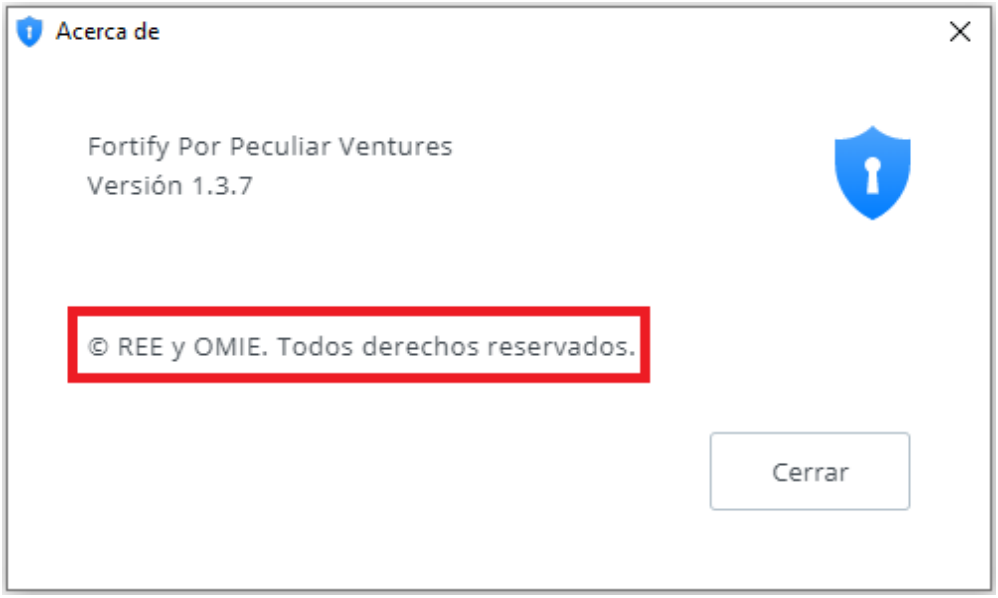
Nota: *Se recomienda un reinicio del equipo a continuación, a fin de comprobar si Fortify arranca al inicio. Ver punto 3.1 de la guía.*

3.1 Comprobación de arranque de Fortify

Para comprobar que Fortify está en ejecución, diríjase al área de notificación de la barra de tareas de Windows, donde deberá aparecer este icono  .

> ***Nota:*** *En caso de duda se recomienda reiniciar primeramente el equipo y comprobar si, tras inicio, el icono aparece. En caso de tratarse de un usuario con privilegios de administrador (caso de Administrador local o de un único usuario en el equipo) deberá iniciarse por defecto. En caso contrario, se recomienda seguir los pasos indicados en el punto 3.2.*

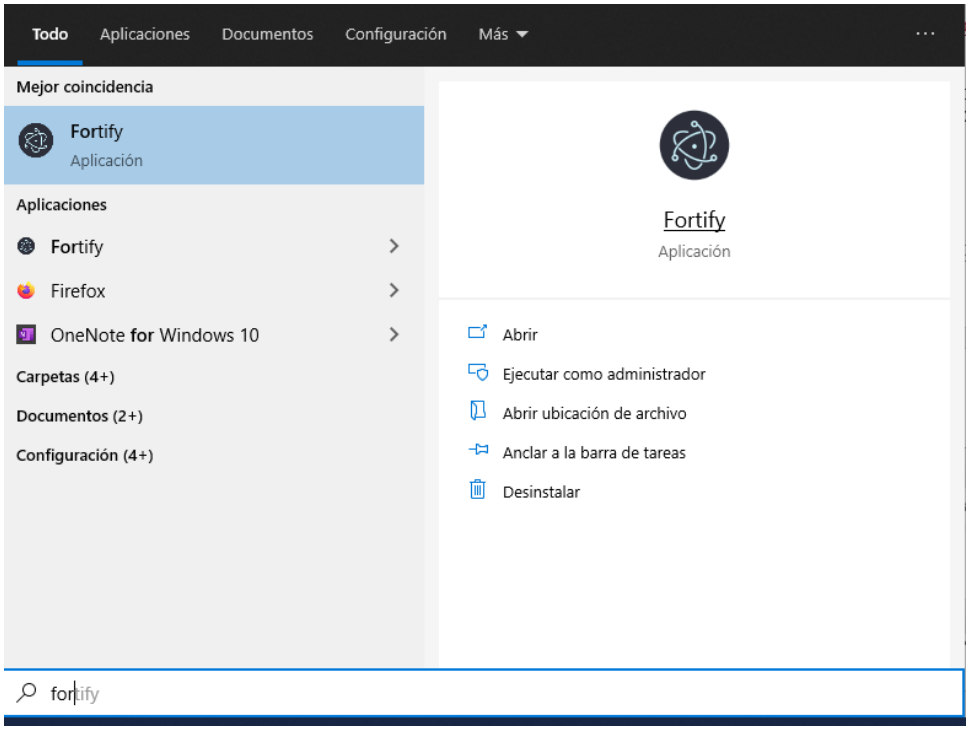
Puede comprobar que se trata de la versión autorizada por REE y Omie haciendo click con el botón derecho para mostrar la ventana 'Acerca de', donde deberá aparecer el mensaje que se resalta en la imagen:



En caso de no encontrar el icono antes mencionado en el área de notificación, como sería el caso si se ha cerrado la aplicación, puede arrancar manualmente la aplicación de la siguiente manera:

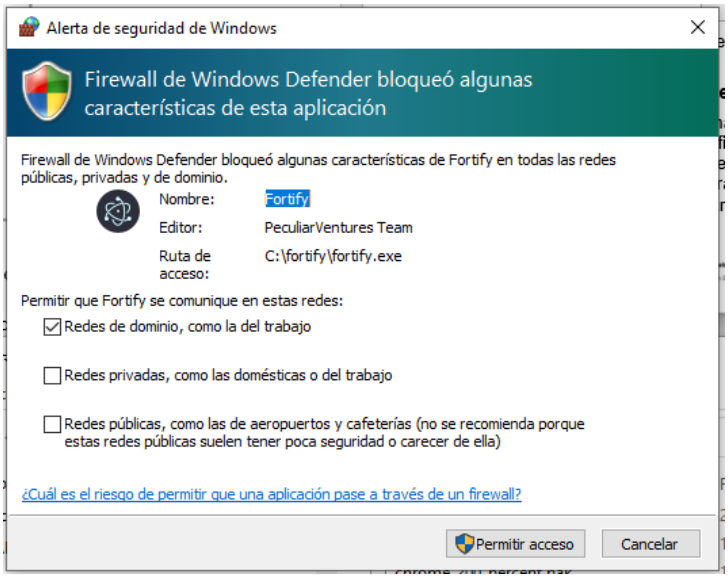
1. Utilizando el buscador de Windows, escriba Fortify en el cuadro de texto

Si la aplicación está instalada, aparecerá disponible para ejecutarla, de manera similar a la mostrada en la imagen:



2. En el caso de que la aplicación no aparezca en la búsqueda, acceder a la ruta *C:\Fortify* y localizar el ejecutable *Fortify.exe*.

En el primer arranque de Fortify es posible que pida permisos para el Firewall de Windows:



Dejar marcado "*Redes de dominio, como la del trabajo*" y hacer clic en "Permitir acceso". Windows solicitará credenciales de administrador.

Activar LOGs de Fortify:

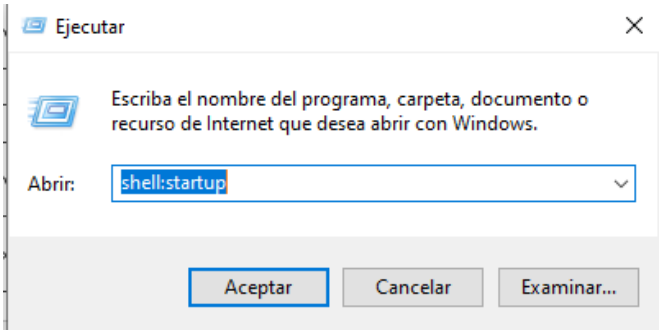
Hacer clic con el botón derecho en el icono de Fortify  , en los iconos ubicados al lado de la Fecha/Hora de Windows y seleccionar “Settings”.

Clic en “GESTIONAR LOG” y desplazar el botón a la derecha para que se vea como muestra la captura superior derecha. Cerrar la ventana con la “X”

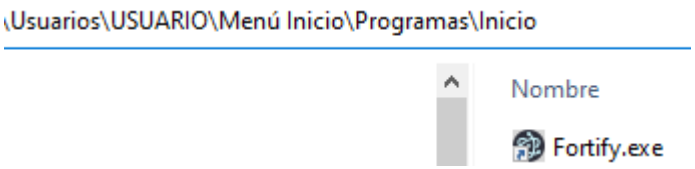
3.2 Pasos adicionales para un usuario sin privilegios de administración

Si Fortify no arranca automáticamente para un usuario, como sería el caso de un usuario sin privilegios de administrador, puede añadirse un acceso directo al Fortify.exe en la carpeta de inicio. De esta forma se ejecutará cada vez que el usuario inicie la sesión en Windows. Para ello:

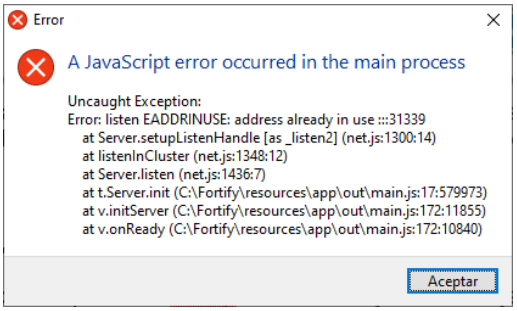
1. Ejecutar el siguiente comando: *shell:startup*



2. Se abrirá una ventana con la carpeta de Inicio del usuario. Crear aquí el **acceso directo al Fortify.exe** (muy importante, **crear un acceso directo**, **no una copia del ejecutable**):



Si un usuario deja en un equipo la sesión abierta con Fortify arrancado, y otro usuario inicia la sesión en el mismo equipo, Fortify mostrará el error Javascript EADDRINUSE y no funcionará:



En ese caso, es necesario que el primer usuario cierre su sesión o, al menos, cierre Fortify. Como alternativa también puede reiniciar el equipo.

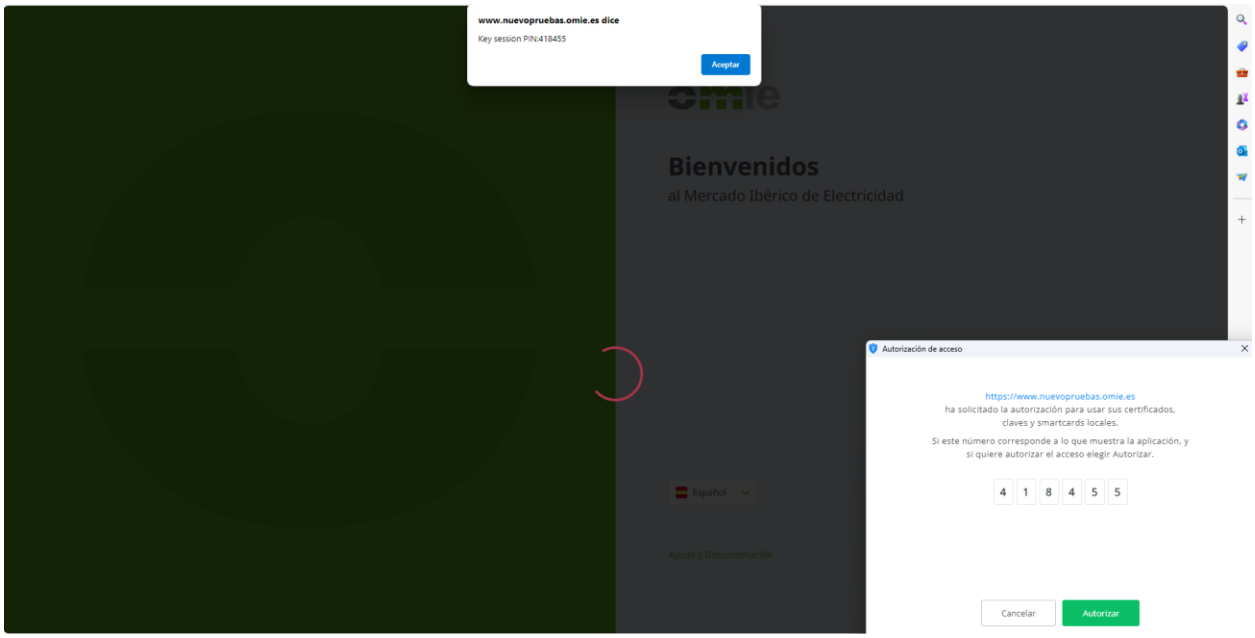
> ***Nota:*** *El mismo error puede replicarse si el usuario con privilegios de administrador realiza el paso de poner un acceso directo a Fortify en su carpeta de Inicio, en cuyo caso para revertirlo debe retirar el acceso directo del directorio anterior.*

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 Autorización inicial de Fortify

En la primera entrada al sistema por cada navegador, la aplicación Fortify solicitará autorización de acceso al almacén de certificados y asociar el certificado seleccionado a la URL de la Web de Mercado y al navegador que se esté usando. Para ello, aparecerá la pantalla que se muestra a continuación, en la que deberá comprobarse que el código que se muestra en ambas ventanas es el mismo, y deberán aceptarse ambas.



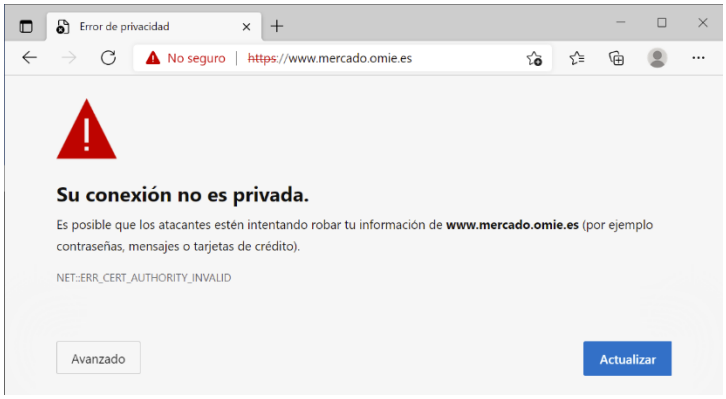
4.2 Registro del certificado ROOT CA de OMIE

El ROOT CA de OMIE es instalado en Edge por el instalador del puesto cliente. Además, por políticas de dominio que se aplican en el puesto del agente, la instalación de este certificado podría fallar durante la instalación.

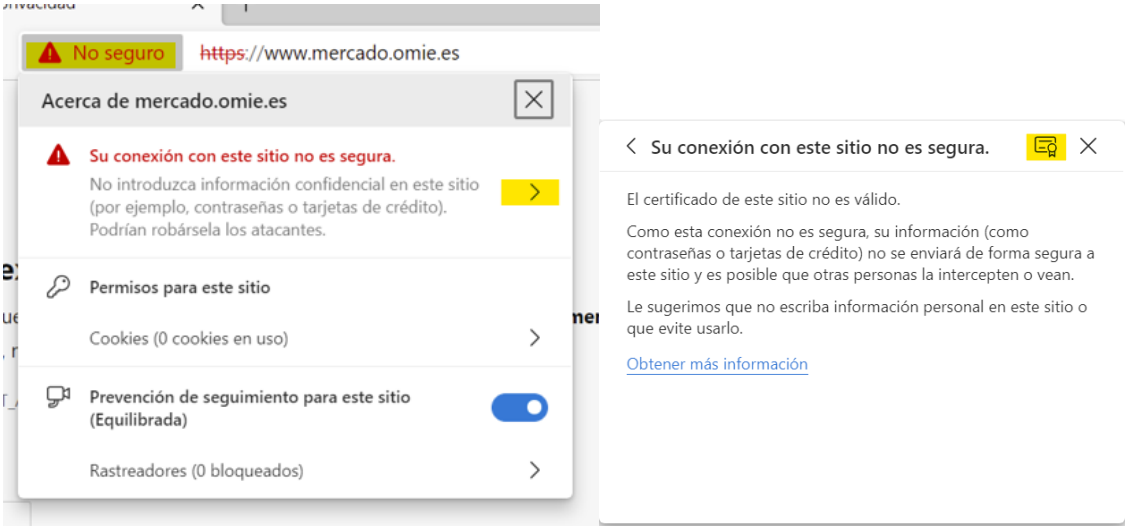
4.2.1 Registro del ROOT CA en EDGE (sólo en caso de problemas).

Este paso sólo es necesario si por cualquier motivo (en general políticas de dominio/seguridad de la organización), el registro del Certificado Raíz de OMIE falla o este es eliminado del almacén de certificados de Windows tras, por ejemplo, el reinicio del equipo.

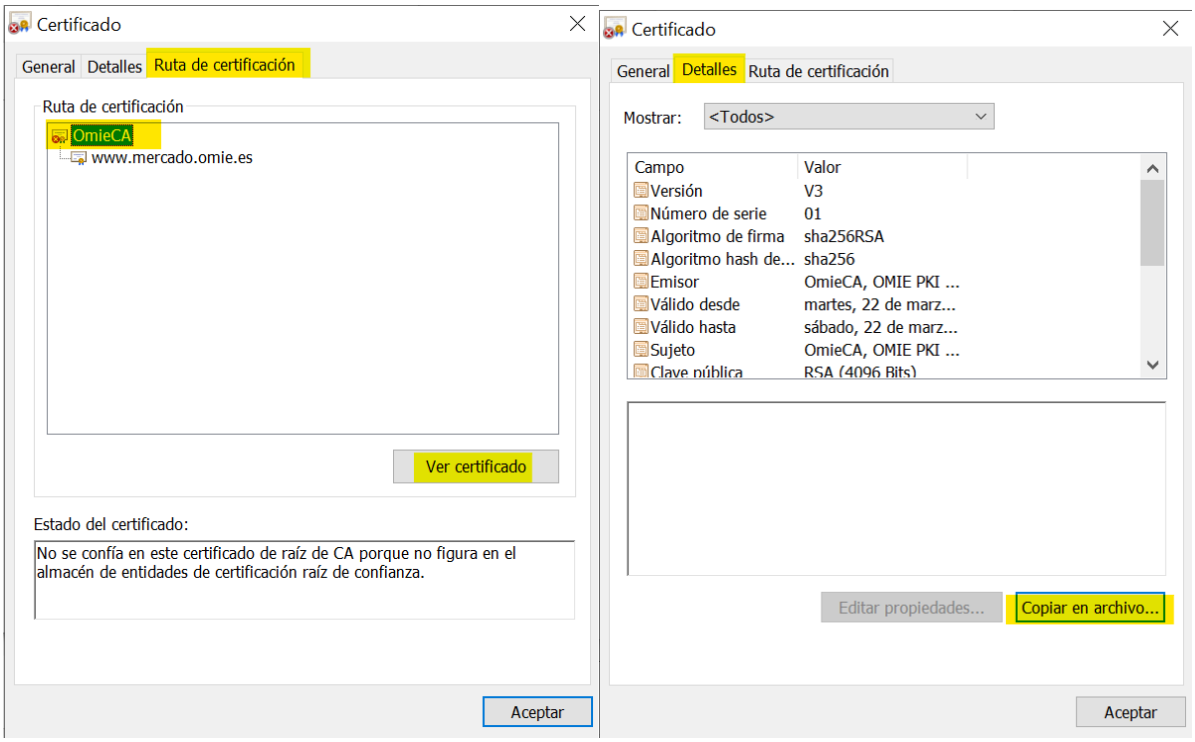
En el caso de que no se tenga instalado el certificado ROOT CA de OMIE, al intentar entrar al Web de Mercado se obtendrá un aviso como este:



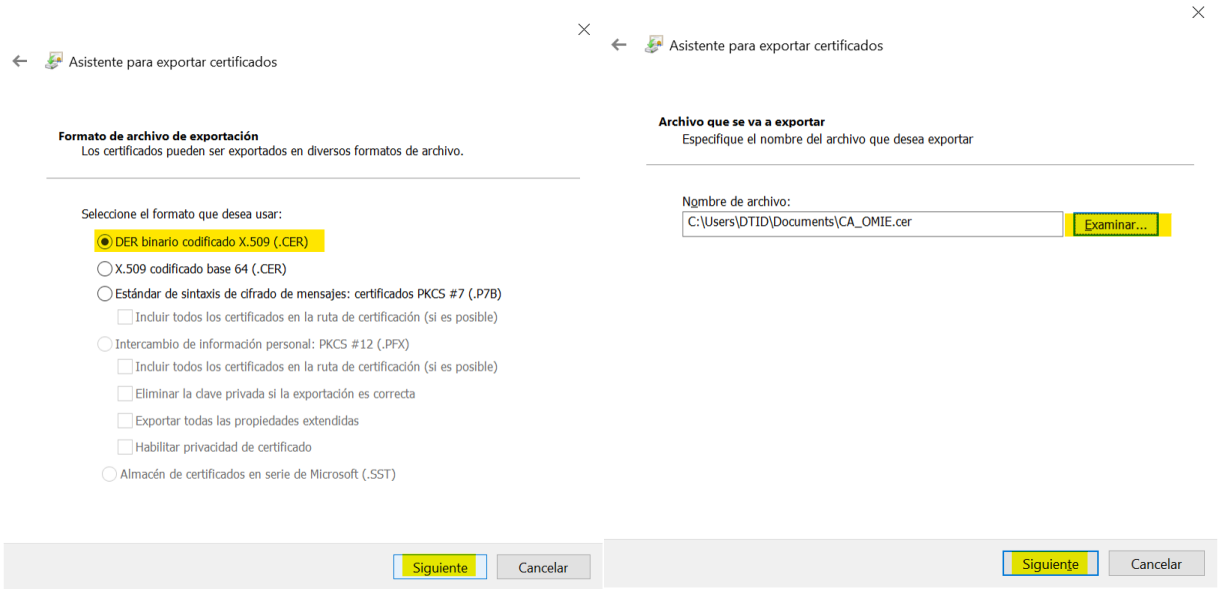
El primer paso será conseguir una copia de este certificado raíz. Para ello:



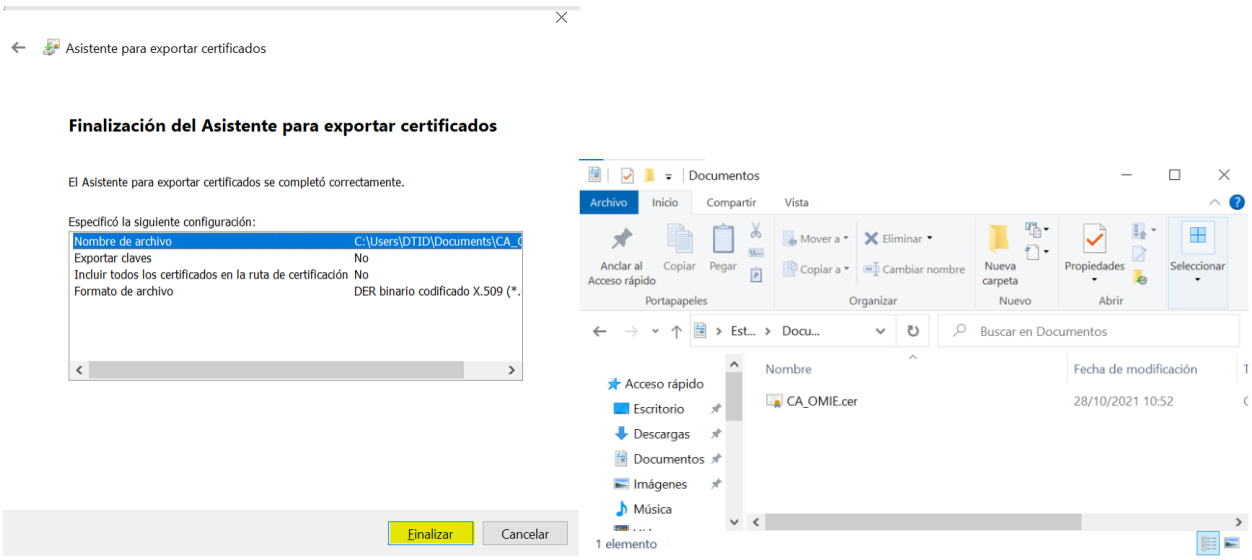
- Clic en la advertencia “No seguro” y en el símbolo “>”.
- Clic en el símbolo de certificado .



- Clic en “Ruta de Certificación”, en la entrada “OmieCA” y en “Ver certificado”.
- Clic en “Detalles” y en “Copiar en archivo”.



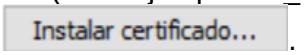
- Seleccionar “DER binario…” y clic en “Siguiente”
- Clic en “Examinar”, buscar la ruta donde queramos guardar el certificado y darle un nombre al fichero (por ejemplo, CA_OMIE.cer) y clic en Siguiente.



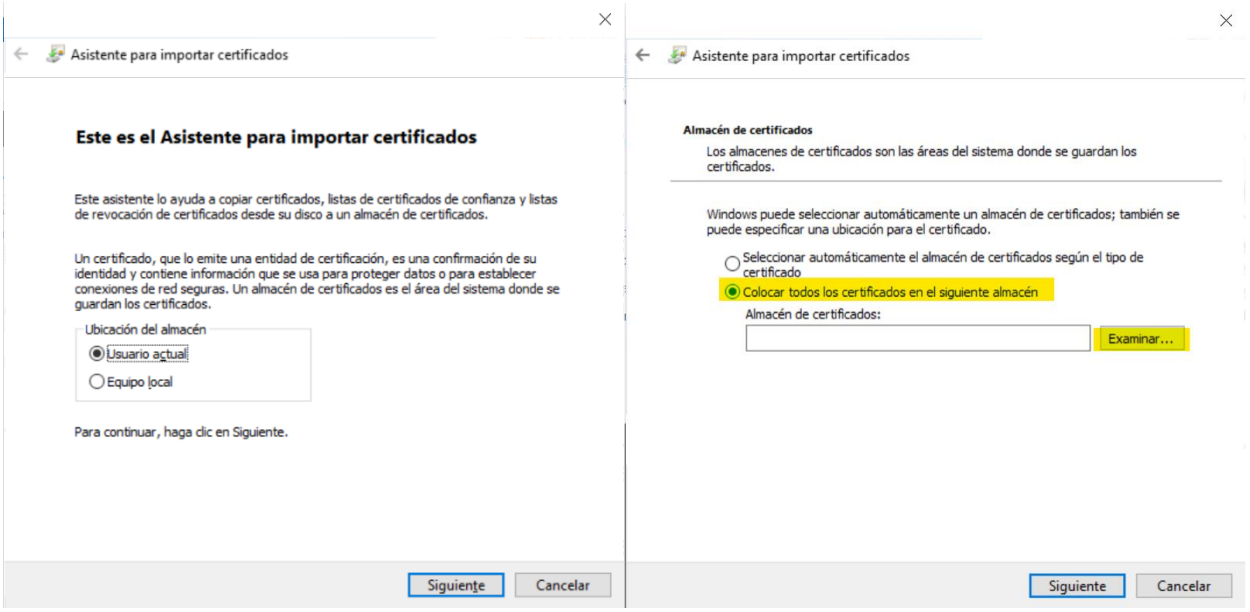
- Clic en “Finalizar”.

A partir de este punto dispondremos del certificado Raíz de OMIE para poder importarlo o configurarlo en políticas de dominio.

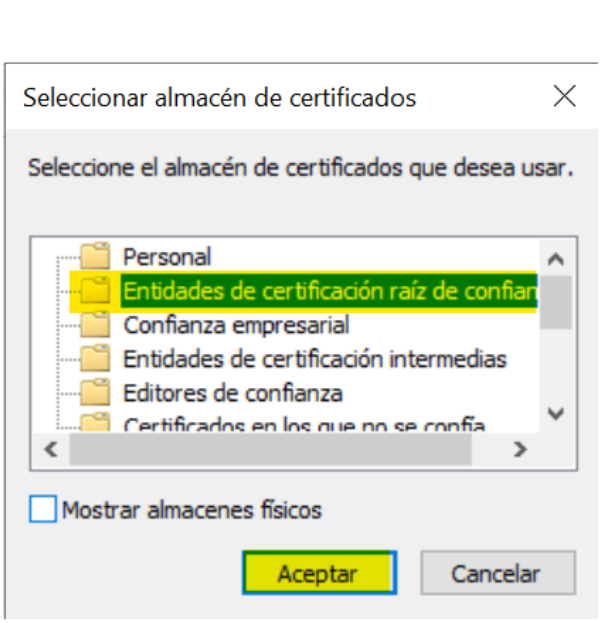
La importación en un equipo se haría siguiendo estos pasos:

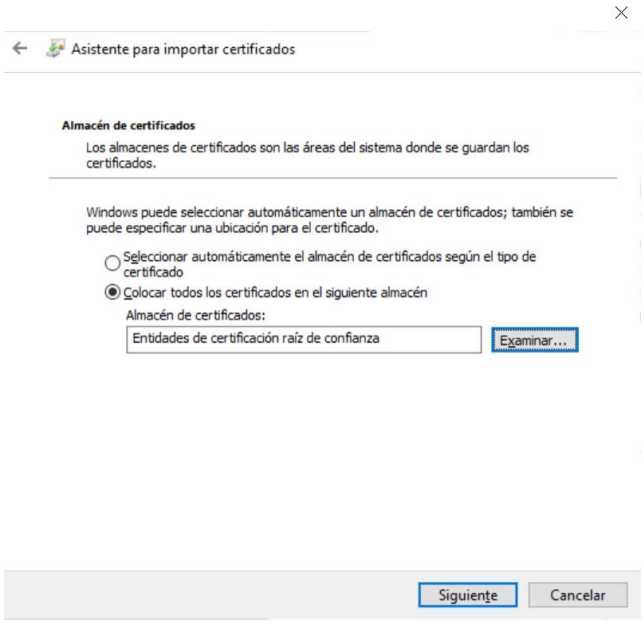
- Doble clic en el fichero creado anteriormente (en el ejemplo CA_OMIE.cer).
- En la ventana que aparece, clic en botón 

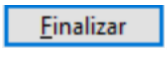
.



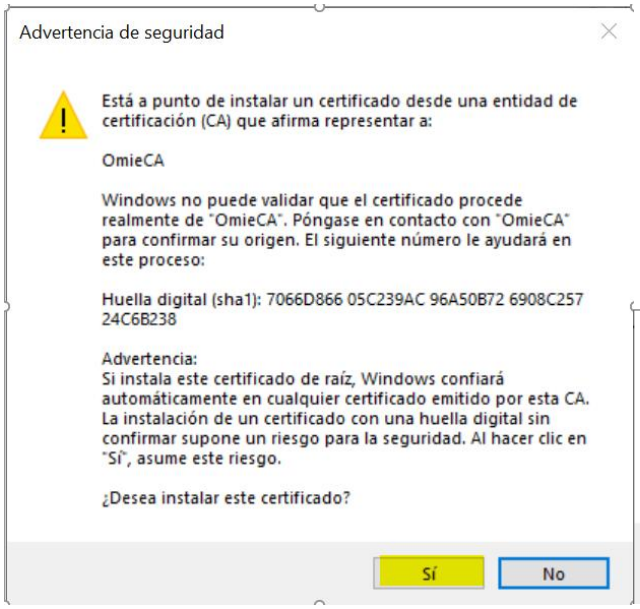
- Seleccionar una de las dos opciones. En el caso de seleccionar “Equipo local” se requerirán credenciales de Administrador. Clic en “Siguiente”.
- **PASO CRÍTICO**: Seleccionar “Colocar todos los certificados en el siguiente almacén”.

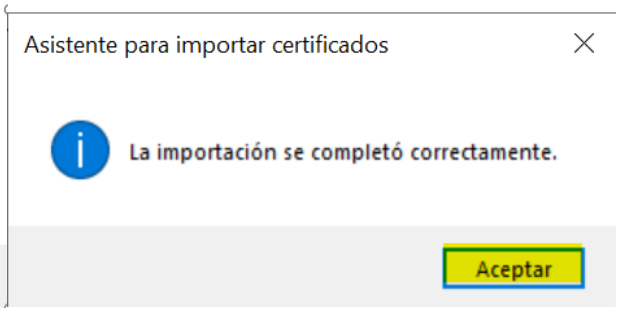




- **PASO CRÍTICO**: Seleccionar “Entidades de certificación raíz de confianza”. Clic en “Aceptar”
- Clic en “Siguiente”
- En la siguiente ventana, clic en 

.





- Hacer clic en “Si”.
- Hacer clic en “Aceptar”

Con esto ya no se obtendría el error indicado al principio de este punto al entrar en el Web de Mercado de OMIE.

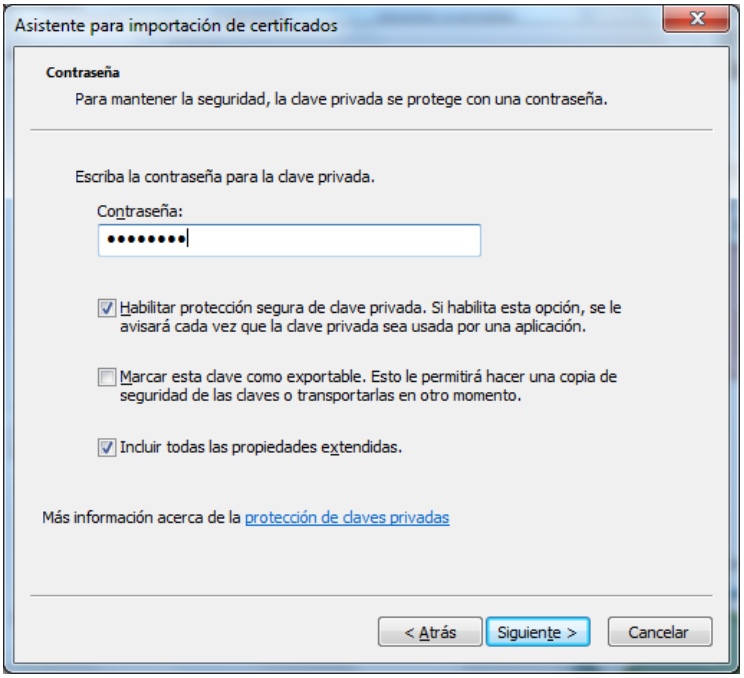
4.3 Registro de Certificados de Usuario

4.3.1 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".

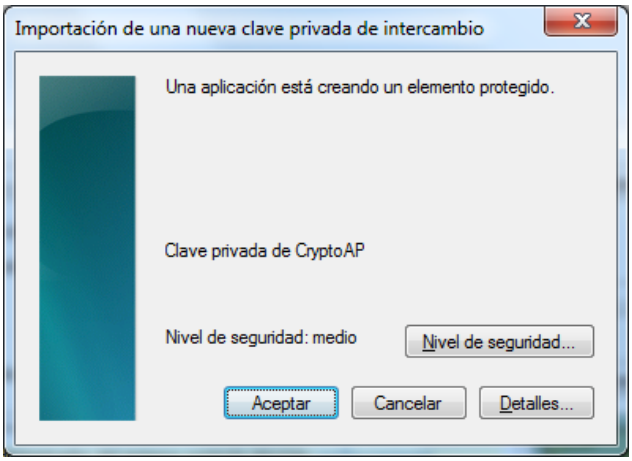
Para una configuración más segura se recomienda seguir los pasos que aparecen en pantalla, utilizando las opciones por defecto hasta llegar a la siguiente pantalla (por defecto la primera opción de "Habilitar protección segura" estará desmarcada):



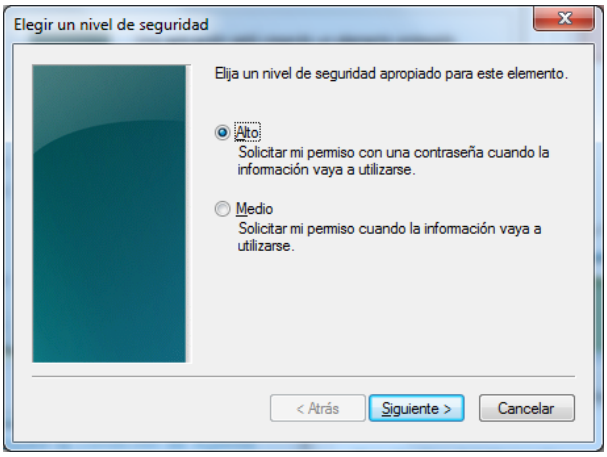
Introducir la contraseña de la clave privada, facilitada por OMIE, y marcar la casilla "*Habilitar protección segura de claves privadas*".

> ***Nota***: *Si elige no marcar la casilla, continúe hasta la siguiente ventana y marque Finalizar.*

Continuar con las opciones por defecto hasta la pantalla siguiente:



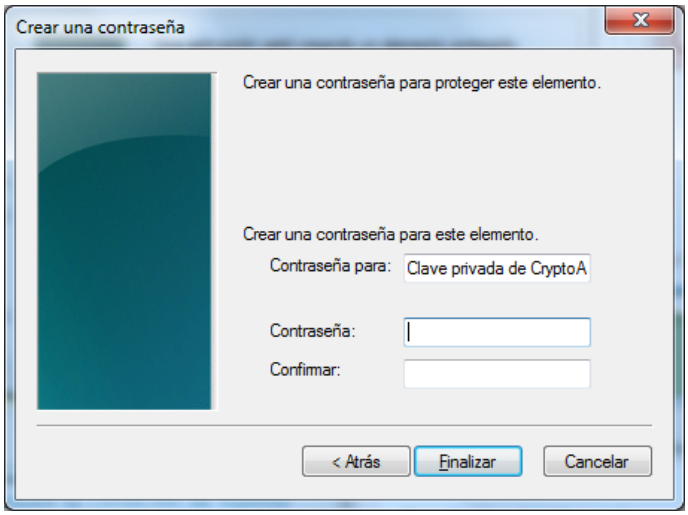
Pulsar en “Nivel de seguridad…”:



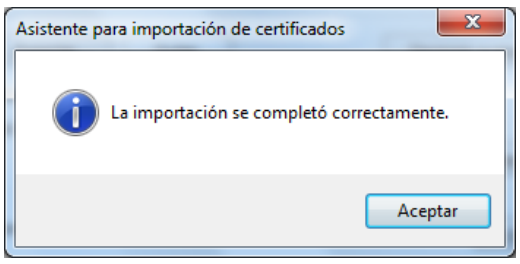
En esta pantalla puede seleccionarse un nivel de seguridad “Medio” o “Alto” para configurar el comportamiento del sistema al utilizar el certificado cuando se accede SIOM o se realiza la firma de un envío de información.

- 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 elegir e introducir 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 (no será conocida por OMIE).



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



5 PROBLEMAS FRECUENTES

Si en algún momento se produce un error no contemplado en esta guía, tienen como referencia el documento "Preguntas frecuentes (FAQs) sobre la Configuración del Puesto de Acceso a los Sistemas de Información de OMIE" (OMIE | Publicaciones: Documentación Técnica).