MIBGAS
MERCADO IBÉRICO DEL GAS

GUÍA DE CONFIGURACIÓN DEL PUESTO CLIENTE DE ACCESO A LA PLATAFORMA MIBGAS

Fecha: 30/10/2024

Versión 5.3

ÍNDICE

1. INTRODUCCIÓN

La presente guía describe los requisitos en un puesto cliente para el acceso a la Plataforma de MIBGAS y los pasos necesarios para poder configurar correctamente y comenzar a utilizar la Plataforma de Registro y Consultas, la Plataforma de Negociación y la Plataforma de Gestión de Garantías.

Los entornos Web de MIBGAS requieren el uso de certificados digitales de usuario proporcionados por MIBGAS.

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

Ante la posible aparición de problemas, se incluye al final del documento un listado de posibles soluciones a las incidencias con las que se puede encontrar un usuario a la hora de acometer la instalación y configuración de un puesto cliente.

Nota: Las imágenes que se incluyen en el documento son para ayudar a identificar los diferentes pasos de la instalación y se facilitan como ejemplos de pantallas de presentación. Debido a la continua adaptación del software (navegador, instalador, etc.) y de la Plataforma de MIBGAS, las versiones o datos que aparecen en las imágenes pueden no corresponder con la última información disponible.

Nota: Esta versión del documento está adaptada para el acceso a través de navegadores Edge y Chrome a la Plataforma de MIBGAS, Sin embargo, EDGE es el navegador de referencia y MIBGAS dará soporte sobre el mismo. Respecto a Chrome, se permite el acceso al mercado con dicho navegador, pero no está oficialmente soportado por MIBGAS.

2. REQUISITOS PREVIOS

2.1 Componentes principales y versiones

Los principales componentes software necesarios para el uso de la Plataforma de MIBGAS son los siguientes:

- Hardware:
  - PC de sobremesa o portátil.
  - Procesador: Intel Core i5 o i7, 3ª generación.
  - Memoria: 4GB u 8GB de RAM.
  - Disco duro: Mínimo 150GB.
- Sistema operativo:
  - Windows 8 y 8.1
  - Windows 10 (recomendado)
  - Windows 11
- Navegador
  - Microsoft Edge (navegador soportado y de referencia)
  - Google Chrome
- Certificados digitales
  - de usuario a utilizar en el puesto cliente
  - de Entidad Firmante (Root CA) de OMIE

> ***Nota**: Los certificados digitales emitidos para la Plataforma de MIBGAS son en formato software. El uso de certificados en formato tarjeta no está soportado. de tarjetas.*

- Fortify app (incluido en el instalador de MIBGAS) para la firma digital de los envíos.
- Open Web Start (incluido en el instalador de MIBGAS). Necesario para ejecutar el Centro de Descargas y el Módulo de Trading, que al iniciarse la primera vez instalará a su vez la versión necesaria, distribuida por MIBGAS, de la Máquina Virtual Java de Amazon Corretto.

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

2.1.1 Configuración para el módulo de trading del Mercado Organizado

El módulo de Trading del Mercado Organizado del Gas establece una conexión AMQP (https://www.amqp.org/) con el servidor (broker). Esta conexión está además protegida usando SSL (que se establece con el certificado de cliente seleccionado en el arranque de la aplicación).

Para posibilitar la conexión, el cliente debe permitir la conexión al puerto **5671** del servidor, por lo que debe asegurarse de que los Firewall están correctamente configurados y no impidan dicha conexión.

Para más información de puertos, URLs e IPs utilizadas para el acceso a las plataformas de MIBGAS, consultar la presentación Sistema de Emergencia (SIOME) - Mejoras implementadas, también disponible a través del apartado "Otra documentación" de la página de ayuda de la Plataforma de Registro y Consultas de MIBGAS (https://www.market.mibgas.es).

2.1.2 Resolución de pantalla

Para que se pueda visualizar correctamente la Plataforma de MIBGAS el sistema se ha diseñado para una configuración óptima de:

- 1920x1080 pixeles y escala 100%
- 65536 colores.

2.1.3 Configuración de fecha y hora

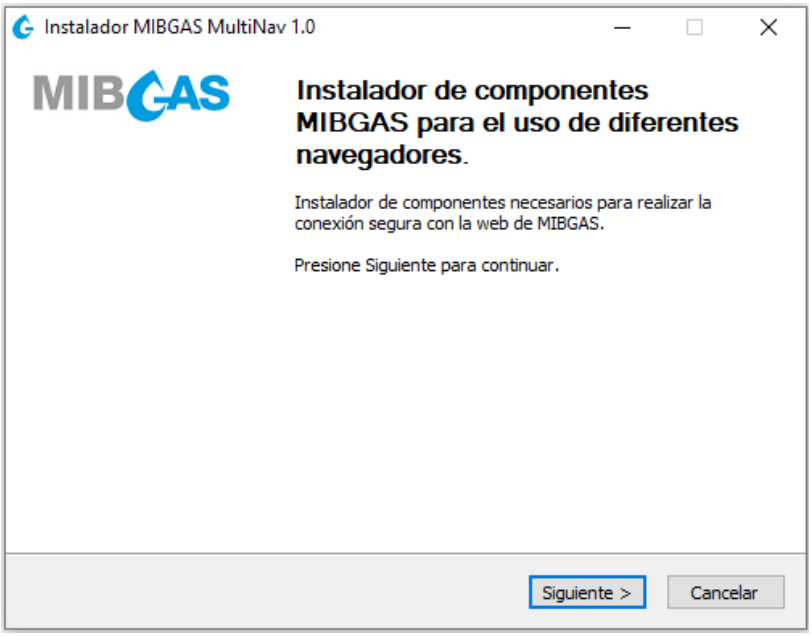
Es necesario ajustar la fecha y hora del equipo desde el que se utilice el Cliente de Trading, de forma que sea correcta y esté sincronizada con un servidor de hora fiable, con objeto de evitar posibles incidencias asociadas a una incorrecta configuración horaria del puesto que accede a las plataformas del Mercado.

3. UTILIZACIÓN DEL INSTALADOR DEL PUESTO CLIENTE

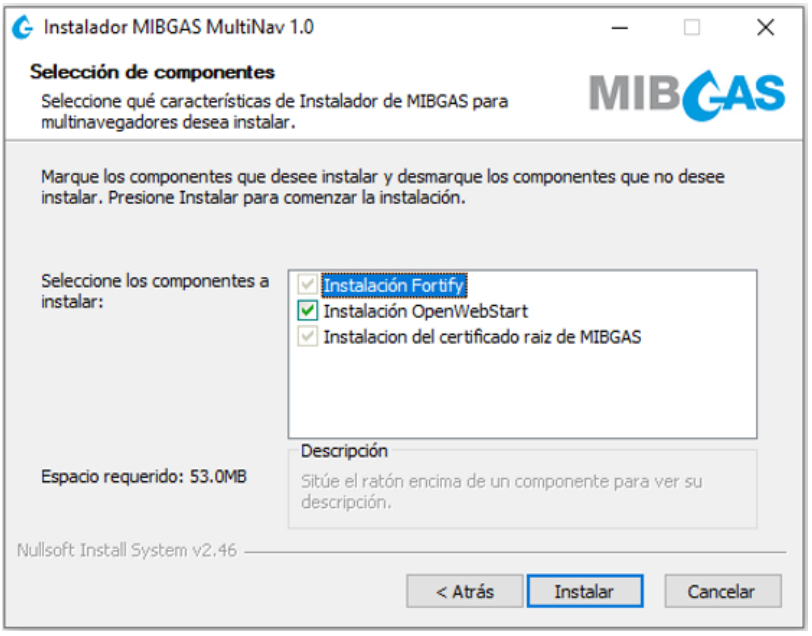
El instalador facilitado por MIBGAS automatiza el proceso de instalación, minimizando las actuaciones manuales que tengan que ser realizadas. Dicho instalador puede descargarse desde el Web Público de MIBGAS (http://www.mibgas.es).

Dado que el instalador realiza cambios de configuración en el perfil del usuario de Windows, debe ejecutarse desde la sesión del usuario con la que queremos operar en la Plataforma de MIBGAS. Si el usuario con el que ejecutemos el instalador no tiene permisos de administración, aparecerá previamente la ventana de introducción de credenciales de un usuario administrador.

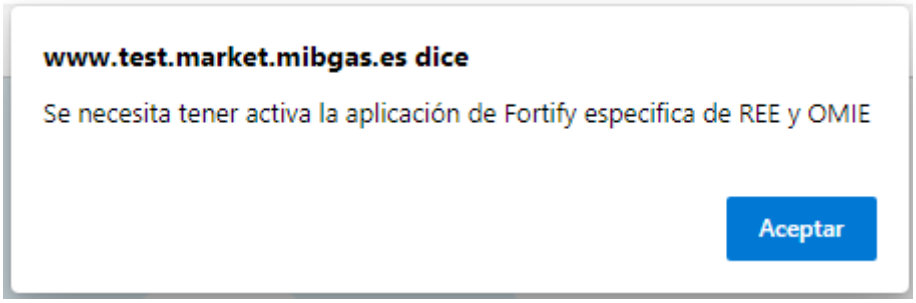
El aspecto del instalador en el arranque es el siguiente:



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

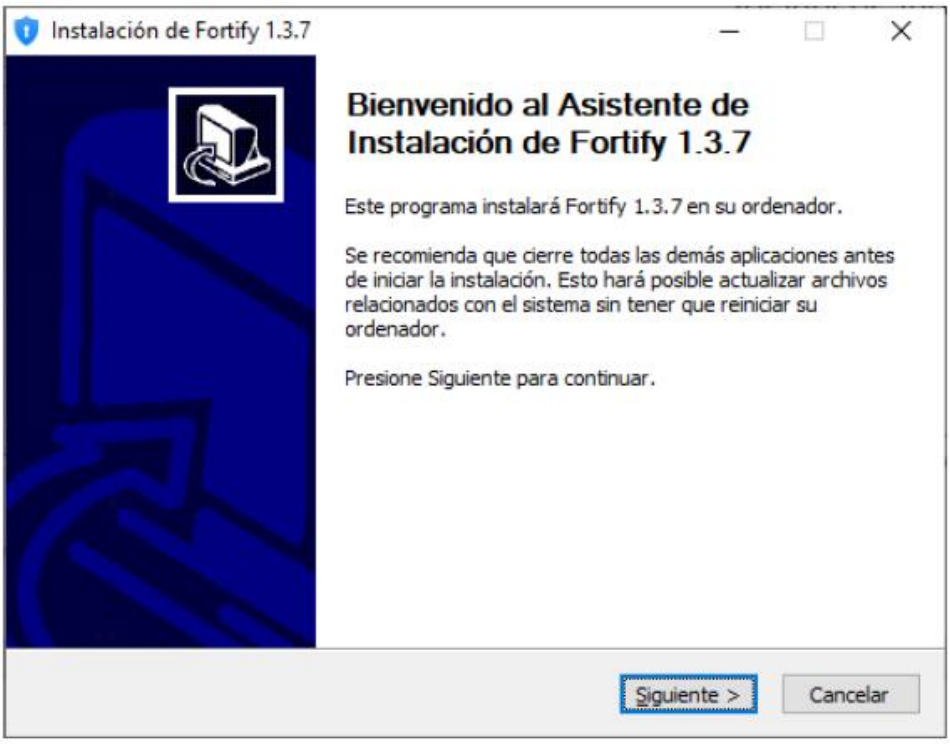


En caso de acceder al Sistema sin tener ninguna versión de Fortify instalada o en ejecución, se mostrará una pantalla en la que se informa de la necesidad de tener instalada la aplicación Fortify.



La instalación de OpenWebStart es necesaria si se va a utilizar el Módulo de Trading o el Centro de Descargas. Las opciones corresponden a elementos necesarios, que no pueden ser desactivados. Tras pulsar en "Instalar", se aplicarán los cambios.

A continuación, aparecerá el instalador de Fortify:

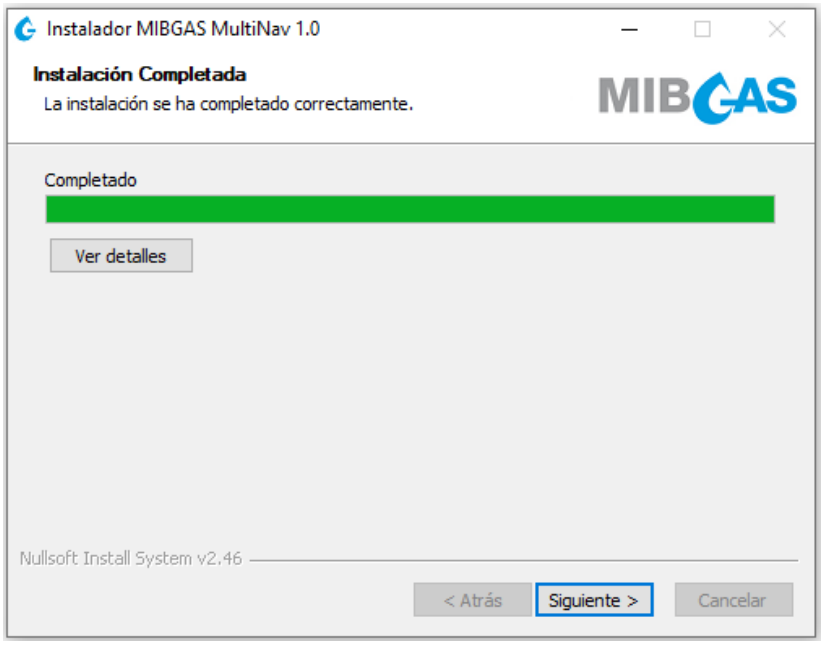


Nota: Por las características del instalador de Fortify, la aplicación se instala para todos los usuarios de la máquina, pero sólo arranca automáticamente si el usuario que lo ha instalado es el administrador, aunque cualquier usuario del equipo puede arrancarla (siempre y cuando no haya abierta "en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

En los apartados 4.2 y 4.3 se indican los pasos para verificar el arranque de Fortify y el procedimiento de autorización inicial, una vez se acceda a la Plataforma de MIBGAS.

A continuación, si se ha elegido la opción correspondiente, se instalará OpenWebStart de forma desatendida (no presentará ninguna pantalla al usuario) para todos los usuarios.

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



Nota: *Se recomienda un reinicio del equipo a continuación, a fin de comprobar si Fortify arranca al inicio. Ver punto 4.2 de la guía.*

Finalizada la ejecución del instalador del puesto cliente, para poder acceder al sistema es necesario registrar el certificado digital de usuario según se describe en el apartado 5.

En caso de problemas en el acceso tras la configuración automática del puesto, verificar los apartados 6 (Actuaciones ante problemas) y 0 (Verificaciones ante problemas en instalación) de la presente guía.

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. VERIFICACIONES ANTE PROBLEMAS EN INSTALACIÓN

Todos los ajustes incluidos en este punto son realizados automáticamente por el instalador como se describe en el capítulo 3, pero se incluyen a continuación como ayuda en caso de necesitar realizar manualmente alguna configuración.

4.1 Certificado de Entidad Firmante (Root CA de OMIE)

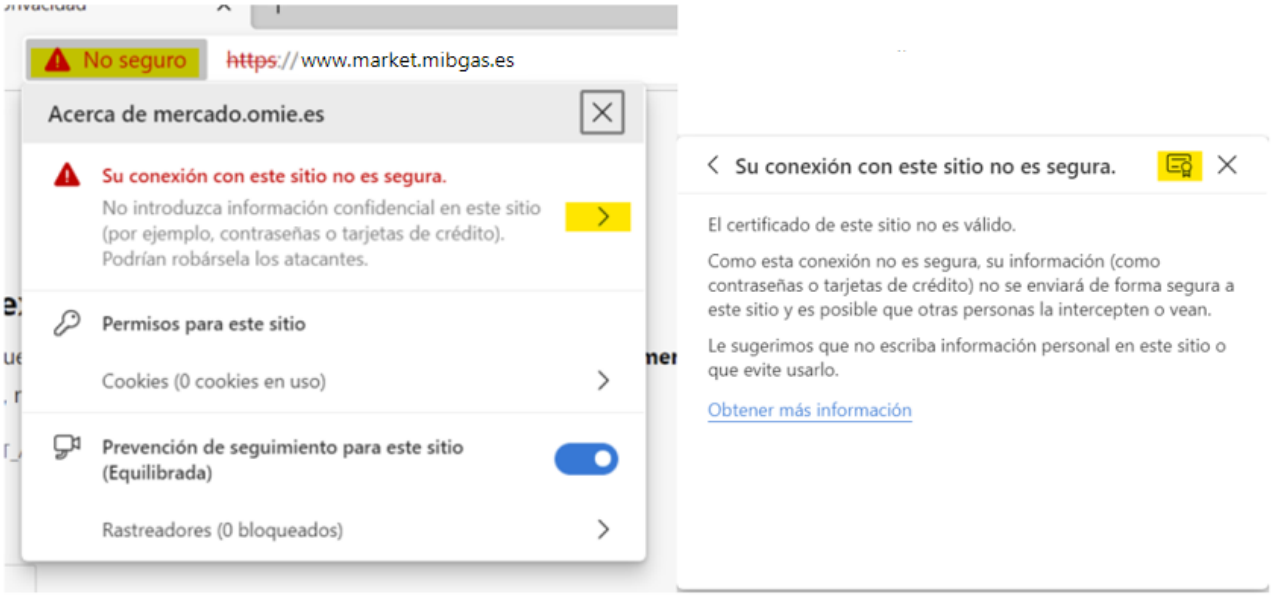
Un requisito imprescindible para la correcta instalación de componentes propios de los Webs de la Plataforma de MIBGAS es tener instalado en el navegador el certificado de Entidad Firmante OMIE CA. Los pasos de la instalación del certificado OMIE CA se detallan a continuación.

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

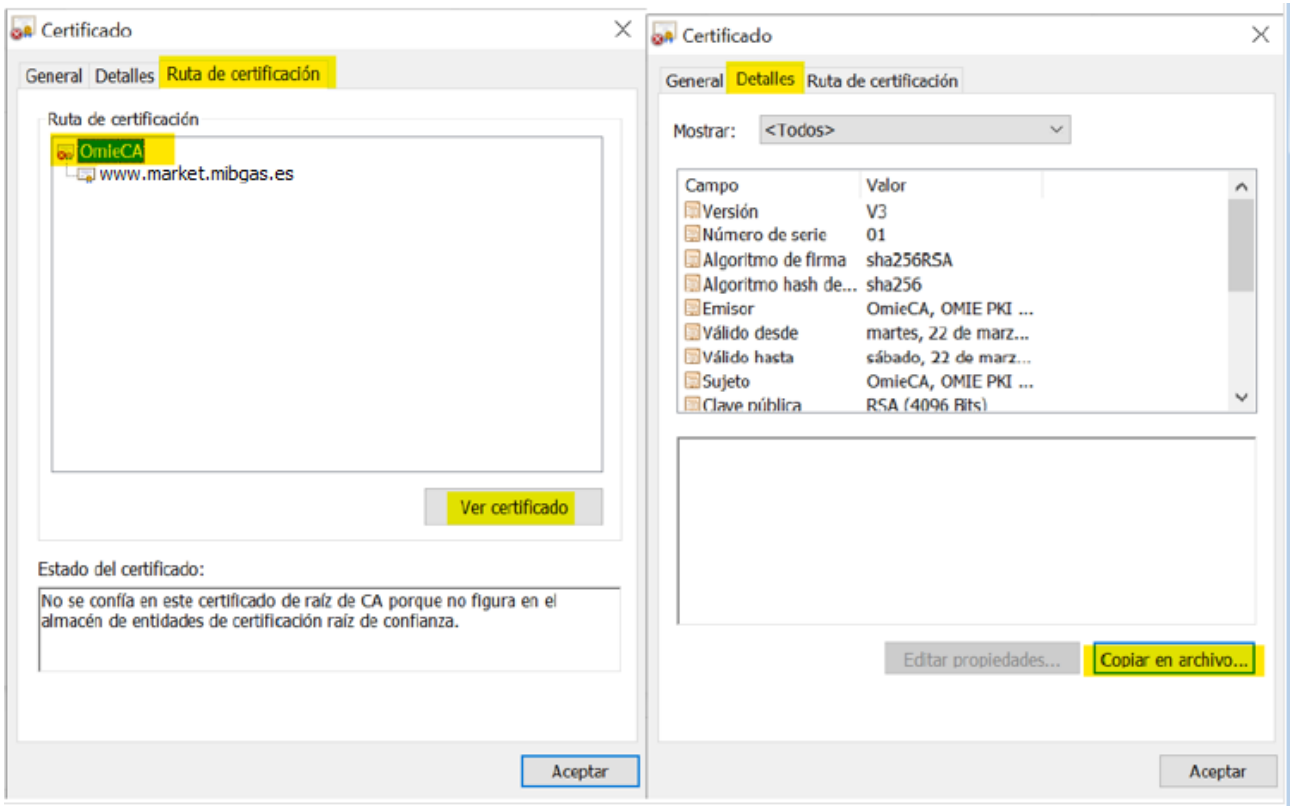
Este paso sólo es necesario si por cualquier motivo (en general políticas de dominio/seguridad de la organización), el registro del Certificado Raíz de OMIE falla o este es eliminado del almacén de certificados de Windows tras, por ejemplo, el reinicio del equipo.

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:

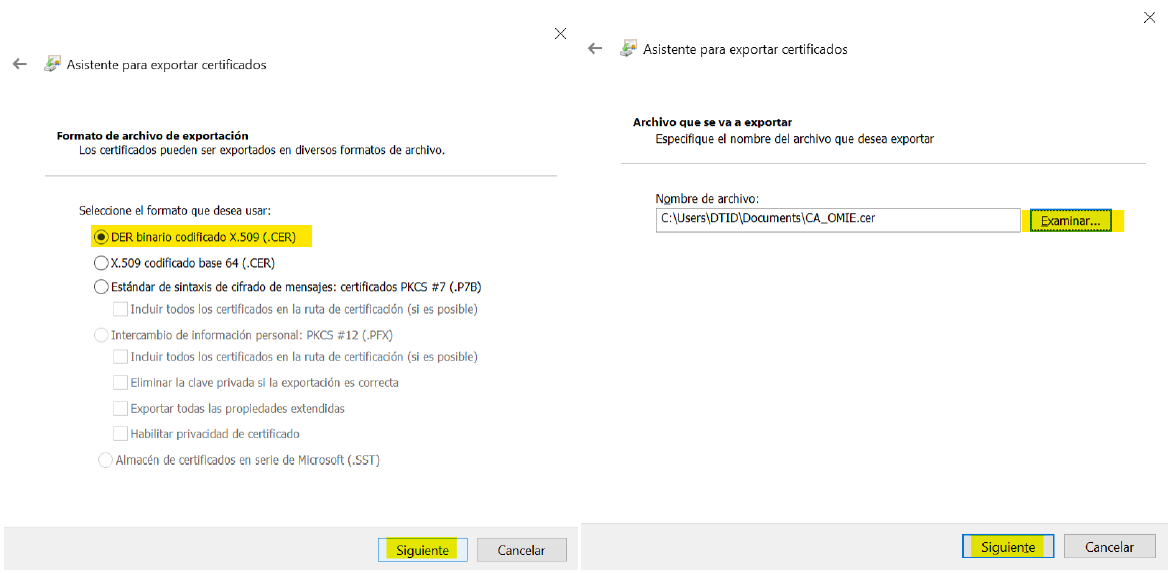
El primer paso será conseguir una copia de este certificado raíz. Para ello:



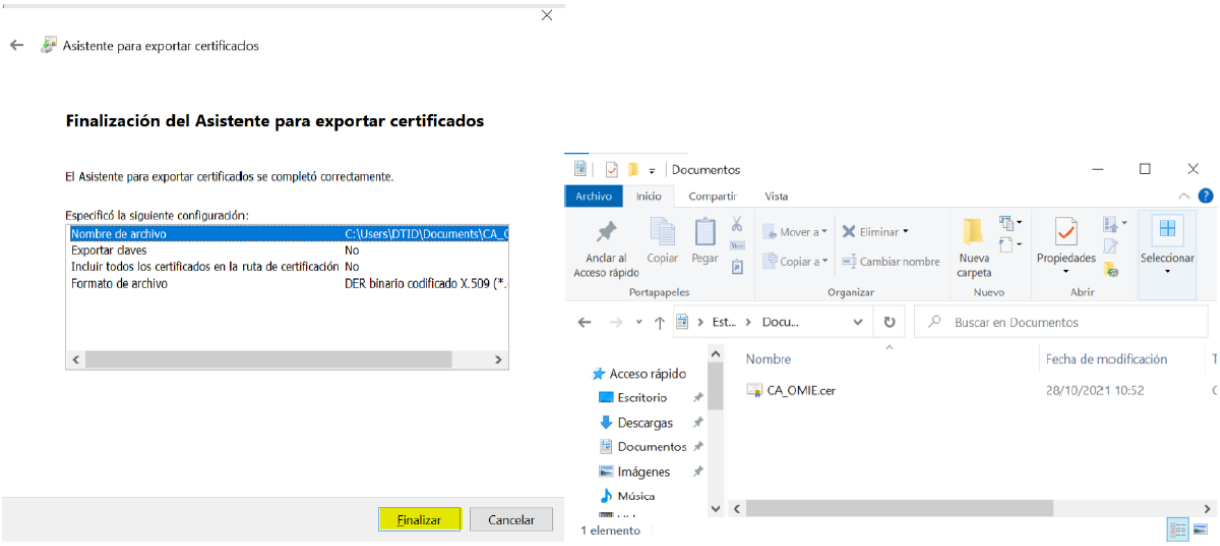
- Clic en la advertencia “No seguro” y en el símbolo “>”.
- Clic en el símbolo de certificado



- 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.

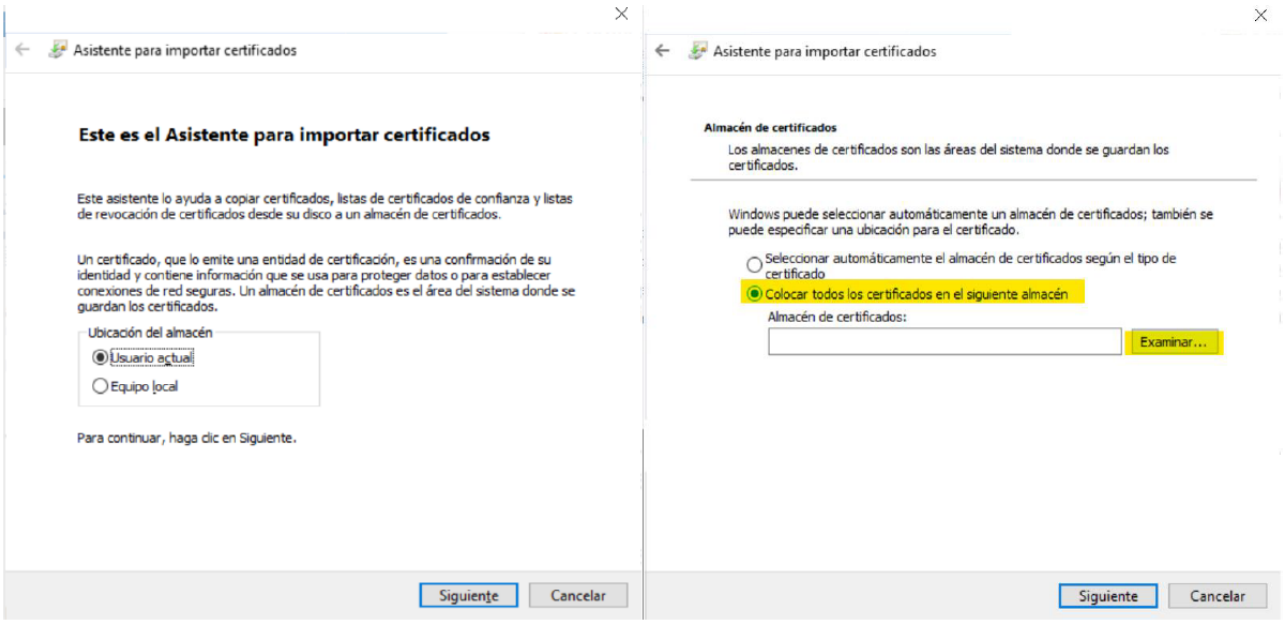


- Clic en “Finalizar”.

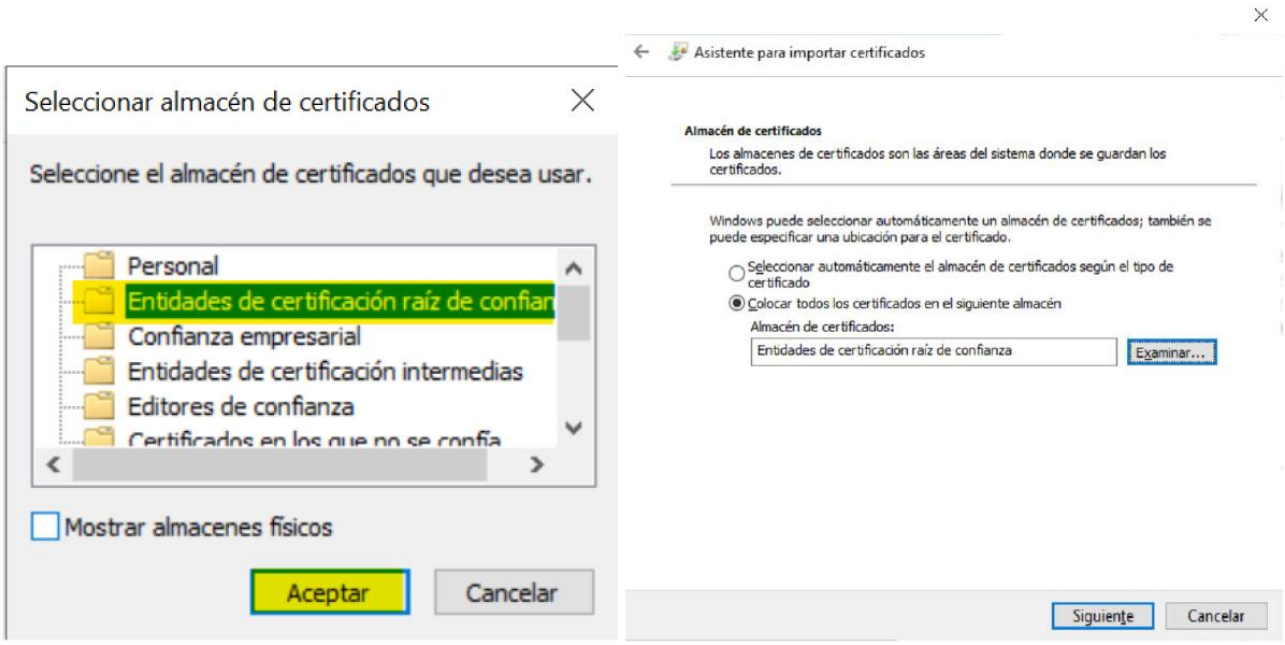
A partir de este punto dispondremos del certificado Raíz de OMIE para poder importarlo o configurarlo en políticas de dominio.

La importación en un equipo se haría siguiendo estos pasos:

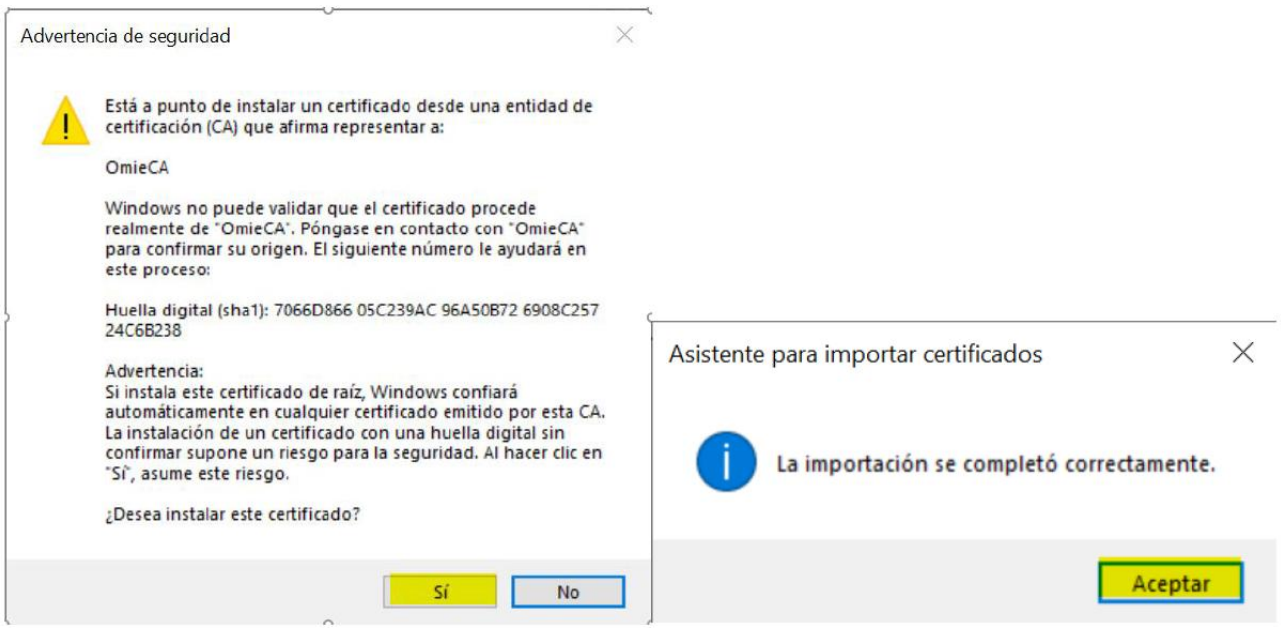
- Doble clic en el fichero creado anteriormente (en el ejemplo CA_OMIE.cer).
- En la ventana que aparece, clic en botón “Instalar certificado …”



- 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 “Finalizar”



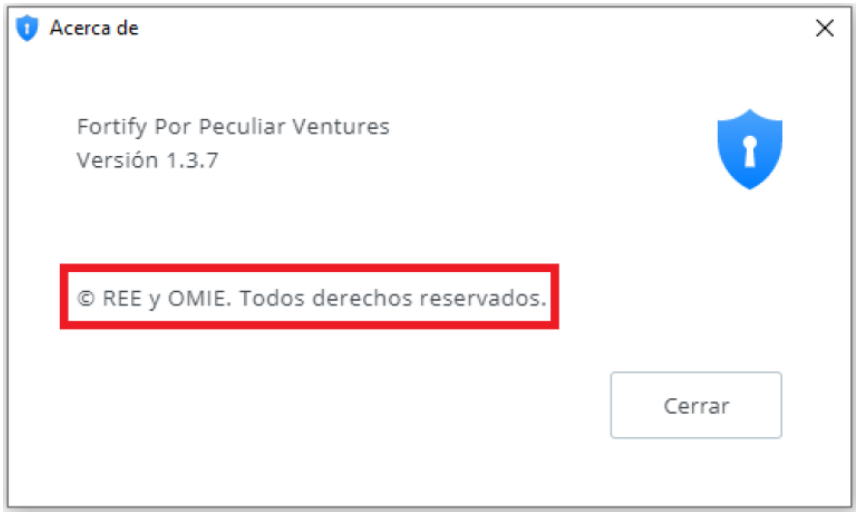
- Hacer clic en “Si”.
- Hacer clic en “Aceptar”

Con esto ya no se obtendría el error indicado al principio de este punto al entrar en el Site de la Plataforma de MIBGAS.

4.2 Comprobación de arranque de Fortify

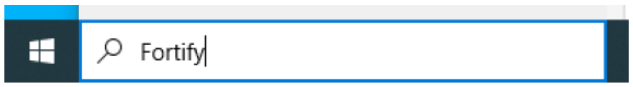
Para comprobar que Fortify está en ejecución, diríjase al área de notificación de la barra de tareas de Windows, donde deberá aparecer este icono: 

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:

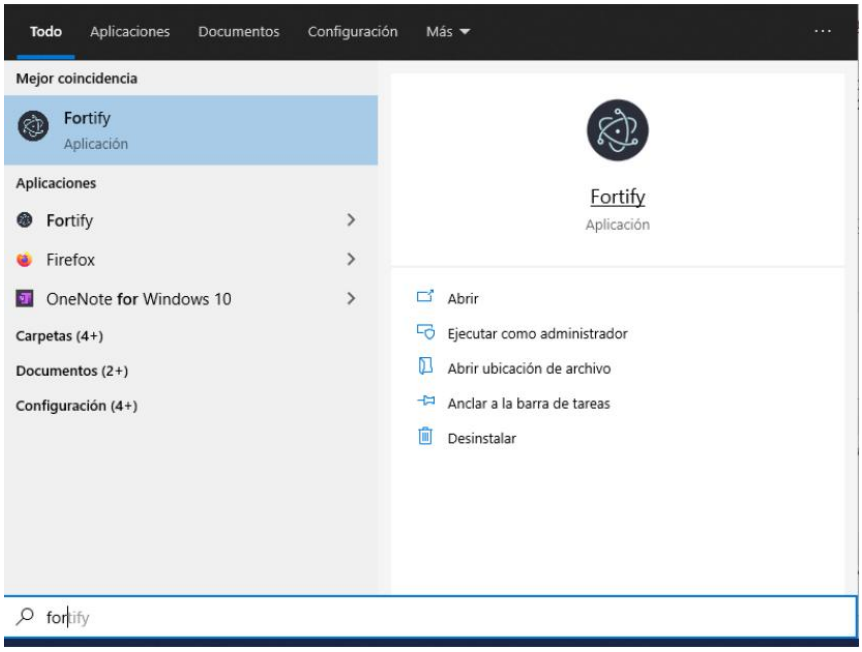


En caso de no encontrar el icono antes mencionado en el área de notificación, puede arrancar manualmente la aplicación de la siguiente manera:

- Utilizando el buscador de Windows, escriba Fortify en el cuadro de texto:



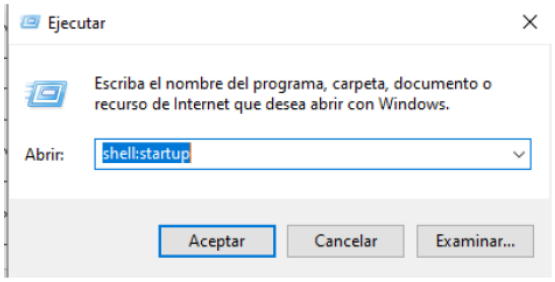
- Si la aplicación está instalada, aparecerá disponible para ejecutarla, de manera similar a la mostrada en la imagen.



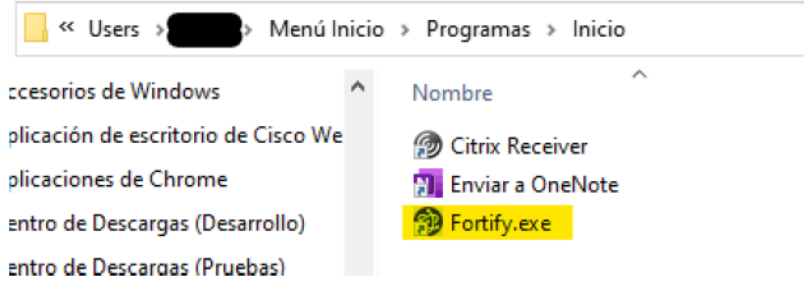
- En el caso de que la aplicación no aparezca en la búsqueda, acceder a la ruta C:\Fortify.

Si Fortify no arranca automáticamente para ese usuario, 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:

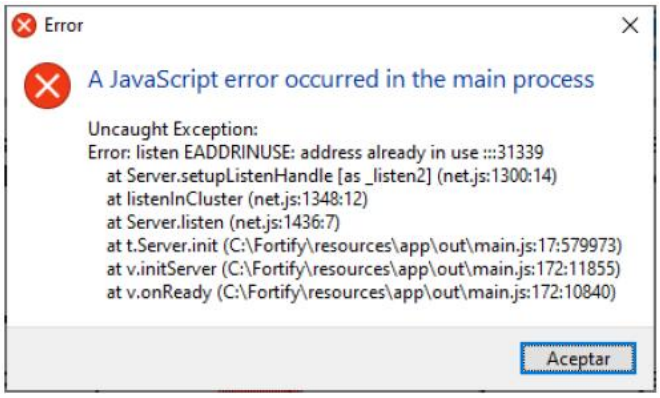
- Ejecutar el siguiente comando: *shell:startup*



- 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):

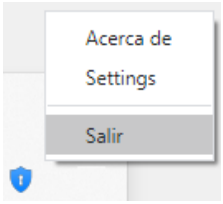


Si un usuario deja en un equipo la sesión abierta con Fortify arrancado, y otro usuario inicia la sesión en el mismo equipo, Fortify dará error y no funcionará:



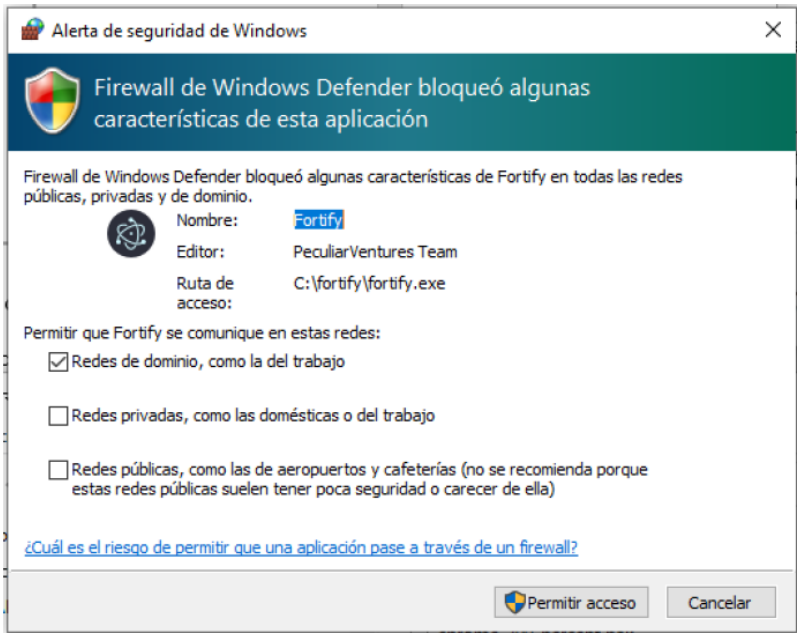
En ese caso, es necesario que el primer usuario cierre su sesión o, que el usuario que tiene el error cierre Fortify, finalizando el proceso, y lo vuelva a abrir. Se puede cerrar el Fortify:

- A través del icono ubicado en el área de notificaciones (al lado del reloj de Windows)



- Forzando el cierre de los procesos fortify.exe con el Administrador de Tareas de Windows.

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.

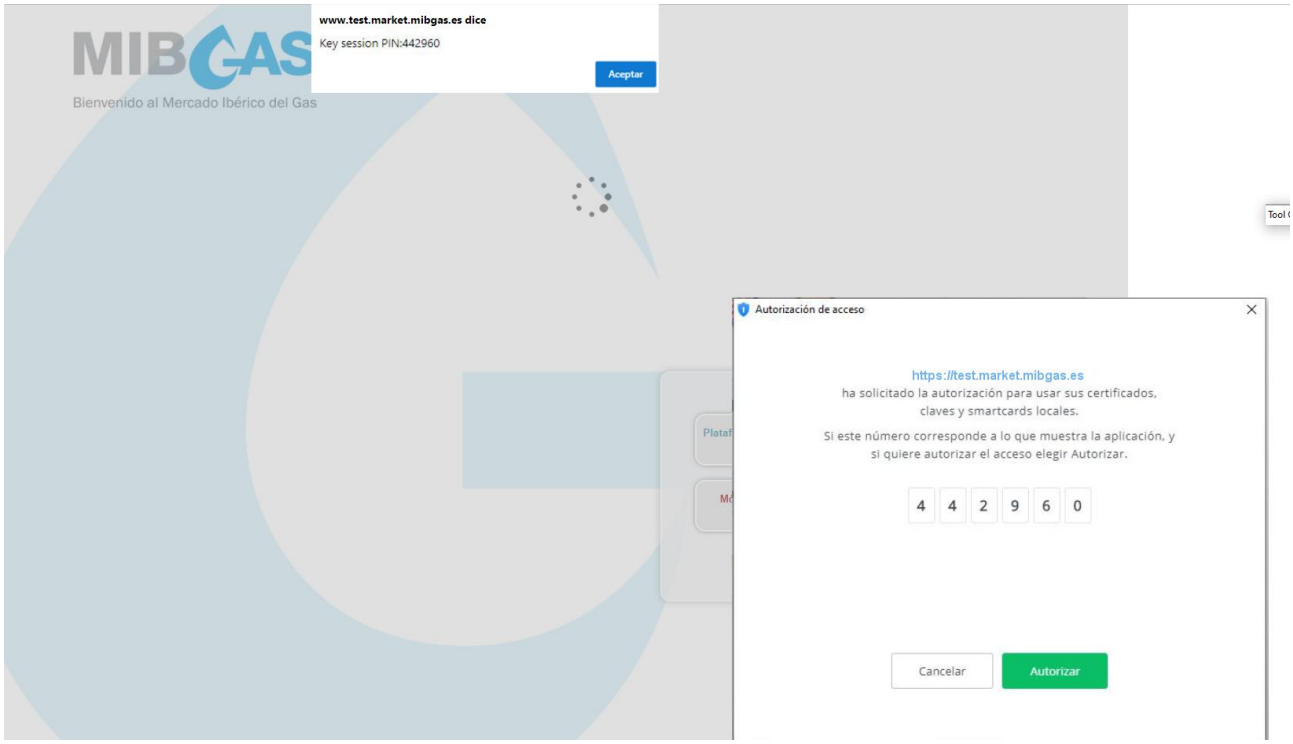
Activar LOGs de Fortify:

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”.

4.3 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.

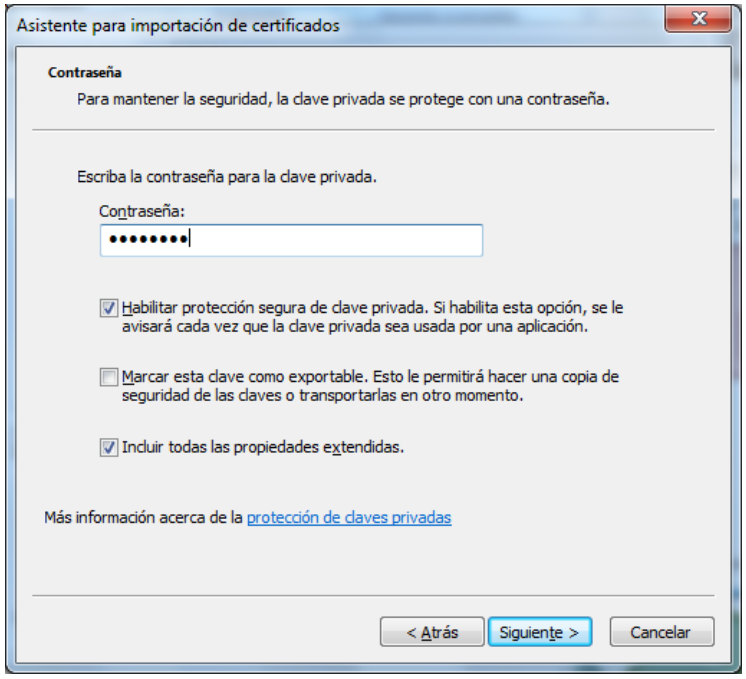


5. REGISTRO DE CERTIFICADOS DIGITALES DE USUARIO

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.

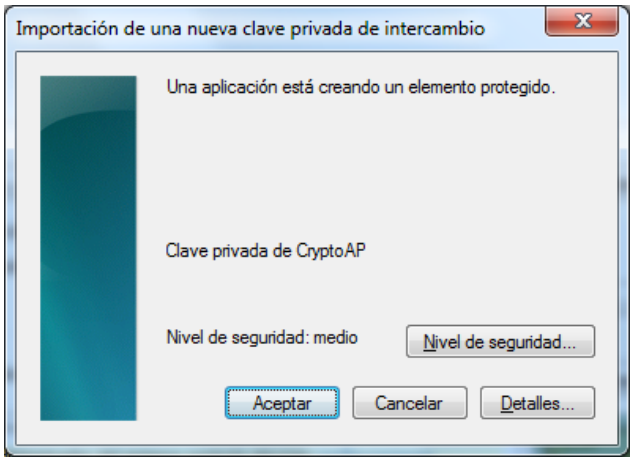
Descargar el fichero ".p12" en un directorio accesible desde el puesto en que se va a registrar el certificado. Seleccionar el fichero y activarlo con "doble click" (este proceso también puede iniciarse desde el navegador, en "*Herramientas/Opciones de Internet/Contenido/Certificados/ Importar*").

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

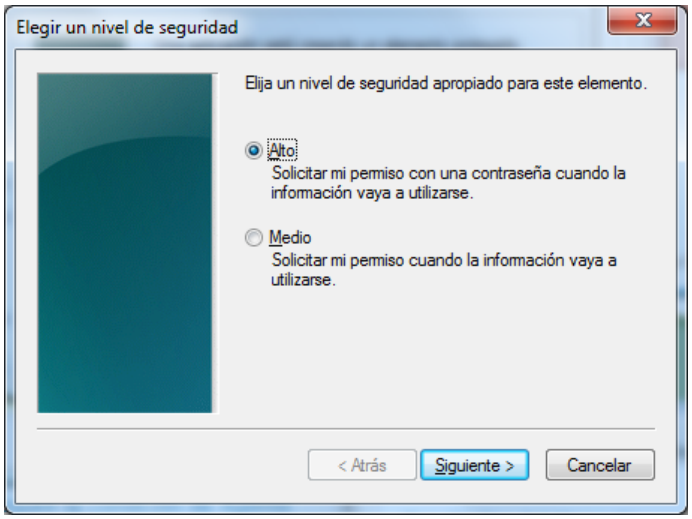


Introducir la contraseña de la clave privada, facilitada por MIBGAS, y marcar la casilla "*Habilitar protección segura de claves privadas*".

Continuar con las opciones por defecto hasta la pantalla siguiente:

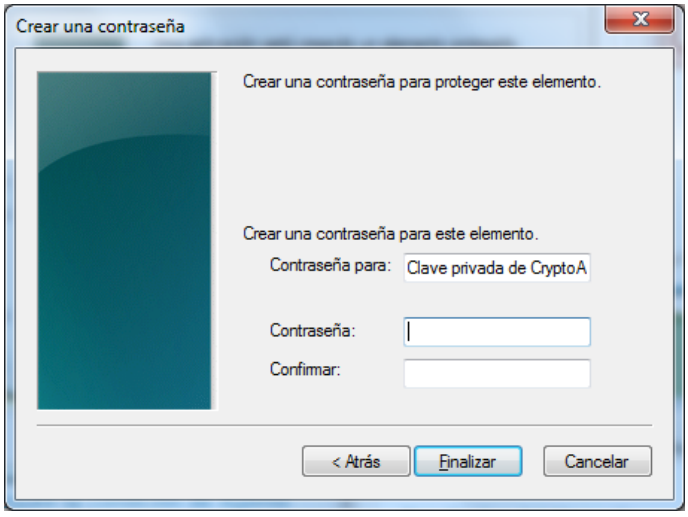


Pulsar en "Nivel de seguridad...":

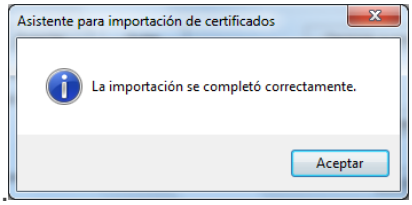


En esta pantalla puede seleccionarse un nivel de seguridad "Medio" o "Alto" para configurar el comportamiento del sistema al utilizar el certificado cuando se accede al Web o se realiza la firma de un envío de información. En el caso de nivel "Medio", el navegador mostrará únicamente un aviso para que 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.



6. ACTUACIONES ANTE POSIBLES PROBLEMAS

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*" ubicado en https://www.mibgas.es