



PREGUNTAS FRECUENTES SOBRE LA APLICACIÓN INFORMÁTICA PARA LA SOLICITUD DE SUBVENCIONES DE LA OEPM PARA EL FOMENTO DE SOLICITUDES DE PATENTES Y MODELOS DE UTILIDAD

- [1. ¿Cuáles son los requisitos del sistema para poder ejecutar la aplicación de solicitud de subvenciones?](#)
- [2. ¿Cómo puedo instalar un certificado digital en Microsoft Edge?](#)
- [3. ¿Cómo puedo instalar un certificado digital en Mozilla Firefox?](#)
- [4. ¿Dónde puedo obtener un certificado digital?](#)
- [5. ¿Cómo puedo instalar y ejecutar AutoFirma?](#)
- [6. ¿Cómo puedo llevar a cabo el proceso de firma?](#)
- [7. Al firmar electrónicamente, la página se queda bloqueada con el mensaje “Por favor espere...”](#)
- [8. Al cargar AutoFirma me aparece el mensaje “Aplicación bloqueada por la seguridad de Java”.](#)
- [9. Otros errores al ejecutar el AutoFirma](#)
- [10. ¿Qué significa “Sitio web certificado por una autoridad desconocida”?](#)
- [11. Si soy una persona física que actúa sin representante y no tengo certificado digital, ¿cómo he de adjuntar la solicitud firmada de forma manuscrita?](#)



1. ¿Cuáles son los requisitos del sistema para poder ejecutar la aplicación de solicitud de subvenciones?

Para la ejecución de la aplicación de solicitud de subvenciones es necesario que el ordenador en el que se ejecute cumpla los requisitos técnicos definidos. En resumen, son los siguientes:

- [Adobe Acrobat Reader. XI o superior.](#)

Entorno de ejecución de Java:

- **Se recomienda adoptar la última versión de Java de 32bits**, si no fuese posible usar al menos Java 6u45 o 7u76 de 32bit

Navegador Web:

- [Mozilla Firefox](#)
- [Google Chrome](#)
- [Microsoft Edge](#)

Nota: para usuarios de Firefox 9 o superior y Windows XP o Windows Server 2003: La carga del almacén de claves y certificados de Firefox 9 o superior por parte de AutoFirma necesita que el sistema tenga instalado el entorno de ejecución redistribuible de Microsoft Visual C++ 2005.

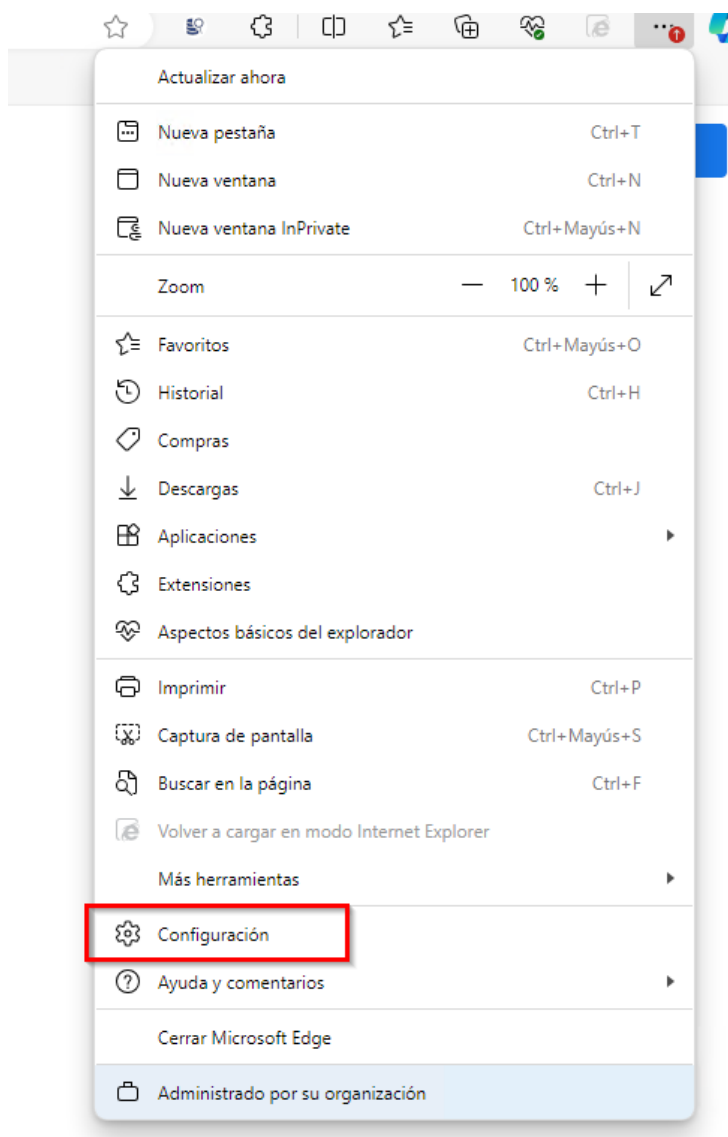
Para las Personas jurídicas y para los representantes que tramiten solicitudes de subvención, se requiere DNI electrónico, Certificado emitido por la FNMT u otro certificado que cumpla con la recomendación UIT X.509.V3 (ISO/IEC 9594-8 de 1997 o posterior) emitidos por un Prestador de Servicios de Certificación que permita la firma electrónica avanzada y que sea reconocido por la Administración Pública ([haga clic aquí para consultar los prestadores con certificados reconocidos por la plataforma @firma](#)).

- Otorgar permisos de ejecución del Java desde el navegador, cuando se vaya a proceder a firmar electrónicamente la solicitud.
- En algunos casos se requerirá el uso de la herramienta AutoFirma. Puede descargarse esta herramienta en la web del [Ministerio de Industria y Turismo](#).

Se puede encontrar más información al respecto en el apartado “Requisitos técnicos” de la aplicación.

2. ¿Cómo puedo instalar un certificado digital en Microsoft Edge?

Abrimos Microsoft Edge, abrimos el menú de Configuración:



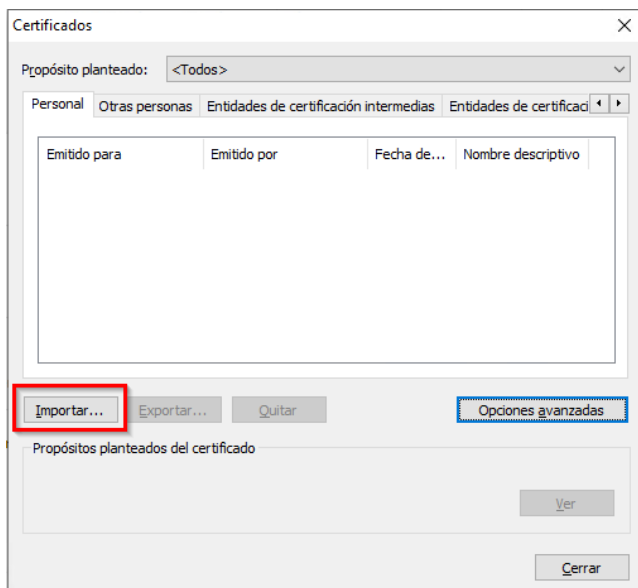
Nos aparecerá una nueva ventana con varias opciones, como la que se muestra en la imagen. Seleccionaremos la opción del menú: "Privacidad, búsqueda y servicios"

Esta imagen muestra la interfaz de configuración de Microsoft Edge, específicamente la sección "Su perfil". En el menú lateral izquierdo, la opción "Privacidad, búsqueda y servicios" está resaltada con un recuadro rojo. El área principal muestra el perfil "Perfil 1" con un botón "Iniciar sesión para sincronizar los datos". Debajo, se listan varias configuraciones del perfil como "Sincronizar", "Microsoft Rewards", "Importar datos de navegador", "Preferencias de perfil" y "Compartir datos de exploración con otras características de Windows". En la parte inferior, se muestra la "Cartera" (Wallet) que almacena información y activos personales.

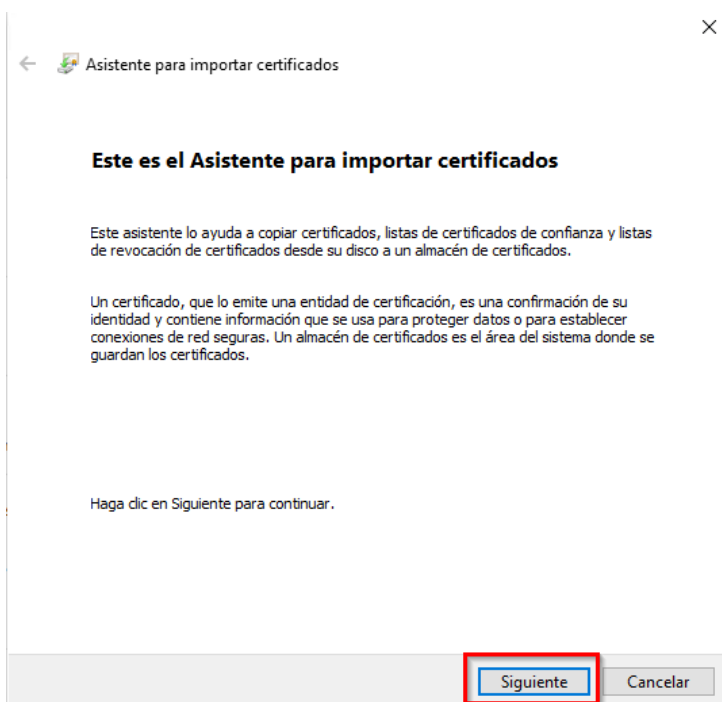
En esta pantalla hacemos scroll hasta la sección de "Seguridad", aquí pulsaremos sobre la opción "Administrar Certificados" para acceder a nuestro contenedor de certificados y poder importar nuestro Certificado.

Esta imagen muestra la interfaz de configuración de Microsoft Edge, sección "Seguridad". En el menú lateral izquierdo, la opción "Privacidad, búsqueda y servicios" está resaltada con un recuadro rojo. El área principal muestra varias opciones de seguridad con interruptores de activación/desactivación: "Permitir que Microsoft guarde su actividad de exploración..." (desactivado), "SmartScreen de Microsoft Defender" (activado), "Bloquear aplicaciones potencialmente no deseadas" (activado), "Protección contra errores ortográficos en sitios web" (activado), "Borrar todos los sitios permitidos anteriormente" (botón "Borrar"), y "Usa DNS seguro para especificar cómo buscar la dirección de red de los sitios web" (desactivado). La opción "Administrar certificados" está resaltada con un recuadro rojo.

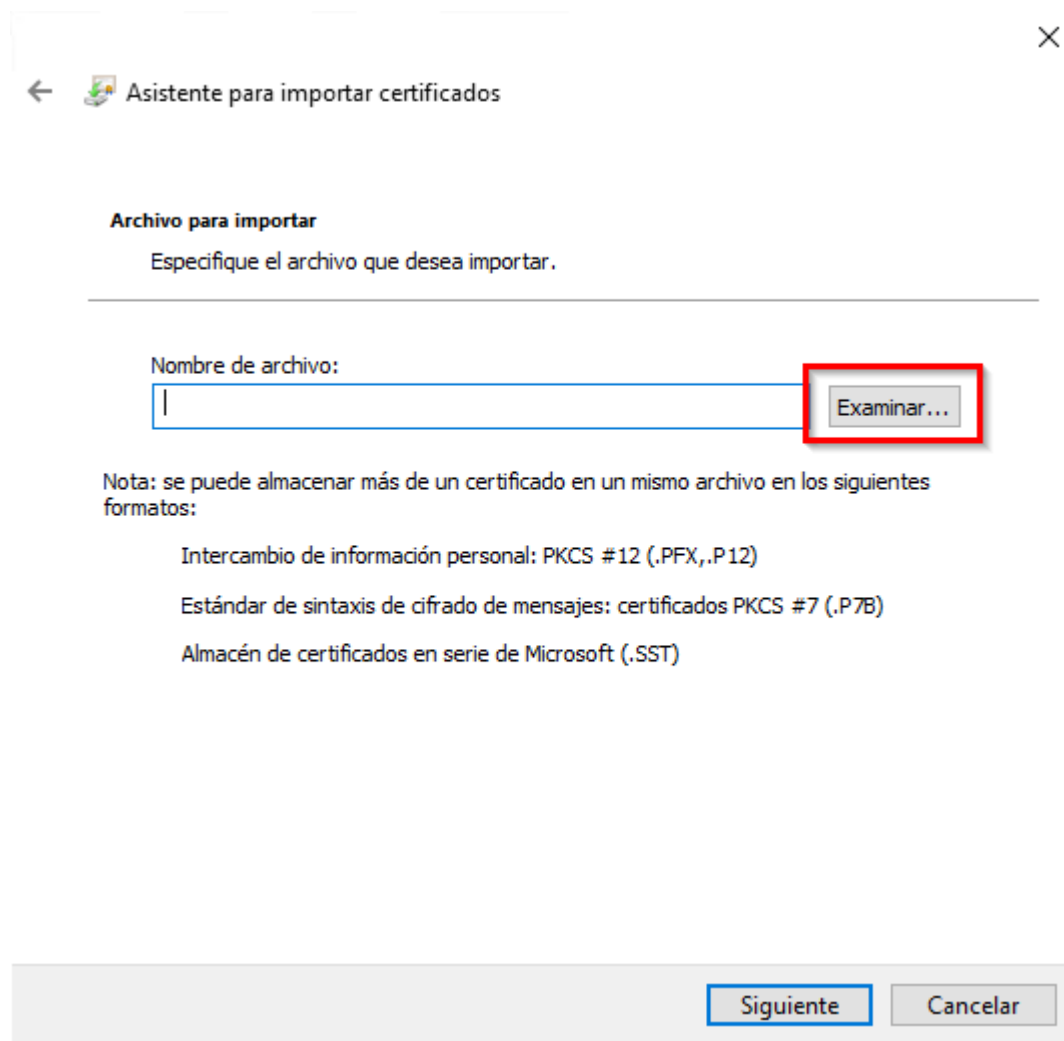
En la ventana que nos aparece tendremos que importar nuestro certificado, para ello pulsamos sobre el botón "Importar...".




Nos aparecerá el asistente para importación de certificados. En la pantalla que se abre pulsamos sobre el botón "Siguiente >" y nos aparecerá la siguiente ventana:



Aquí tendremos que seleccionar nuestro certificado, que bien lo tendremos en un disco o lo habremos descargado de nuestra entidad certificadora. Pulsamos sobre el botón "Examinar..." para poder seleccionar el fichero de nuestro certificado. El tipo de certificado que estamos importando será del tipo "Intercambio de información personal (*.pfx;*.p12)", buscamos nuestro certificado y lo seleccionamos:



←  Asistente para importar certificados

Archivo para importar
Especifique el archivo que desea importar.

Nombre de archivo:

Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:

- Intercambio de información personal: PKCS #12 (.PFX,.P12)
- Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
- Almacén de certificados en serie de Microsoft (.SST)

Si el certificado es válido, el asistente pasará al siguiente paso donde se nos pide una contraseña para protegerlo. También es recomendable marcar la primera opción "Habilitar protección segura de claves privadas." para que el sistema nos avise cada vez que nuestro certificado se utilice.



← Asistente para importar certificados

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

Escriba la contraseña para la clave privada.

Contraseña:

●●●●

Mostrar contraseña

Opciones de importación:

- Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.
- Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.
- Proteger la clave privada mediante security(Non-exportable) basada en virtualizado
- Incluir todas las propiedades extendidas.

Siguiente Cancelar

Pulsamos en "Siguiente >" y el asistente nos preguntará en qué almacén de nuestro contenedor queremos dejar el certificado. Este se ha de dejar en el almacén de certificados "Personal", que será la opción por defecto:

← Asistente para importar certificados

Almacén de certificados
Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.

Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.

- Seleccionar automáticamente el almacén de certificados según el tipo de certificado
- Colocar todos los certificados en el siguiente almacén

Almacén de certificados:

Personal Examinar...

Siguiente Cancelar



Hacemos click sobre el botón "Siguiete >" y pulsamos sobre el botón Finalizar, momento en cual nos advertirá que se está creando un elemento protegido y nos pedirá autorización:

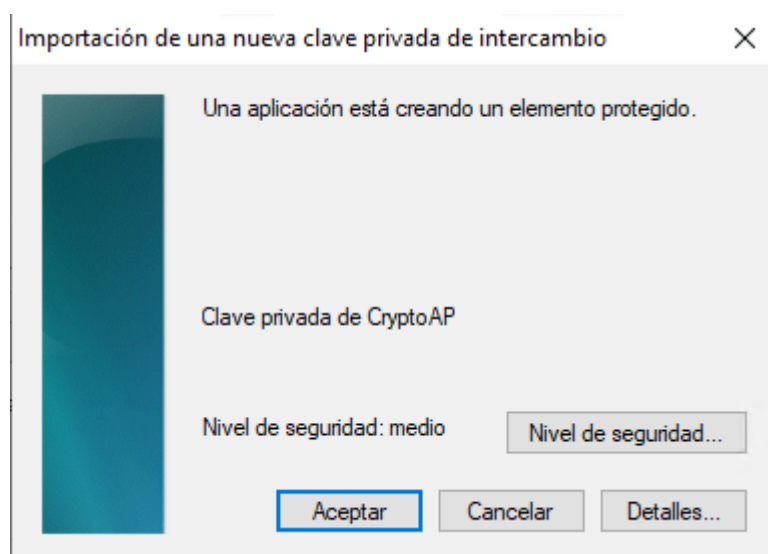
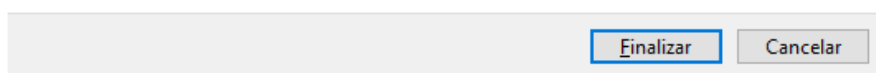


Finalización del Asistente para importar certificados

Se importará el certificado después de hacer clic en Finalizar.

Especificó la siguiente configuración:

Almacén de certificados seleccionado por el usuario	Personal
Contenido	PFX
Nombre de archivo	



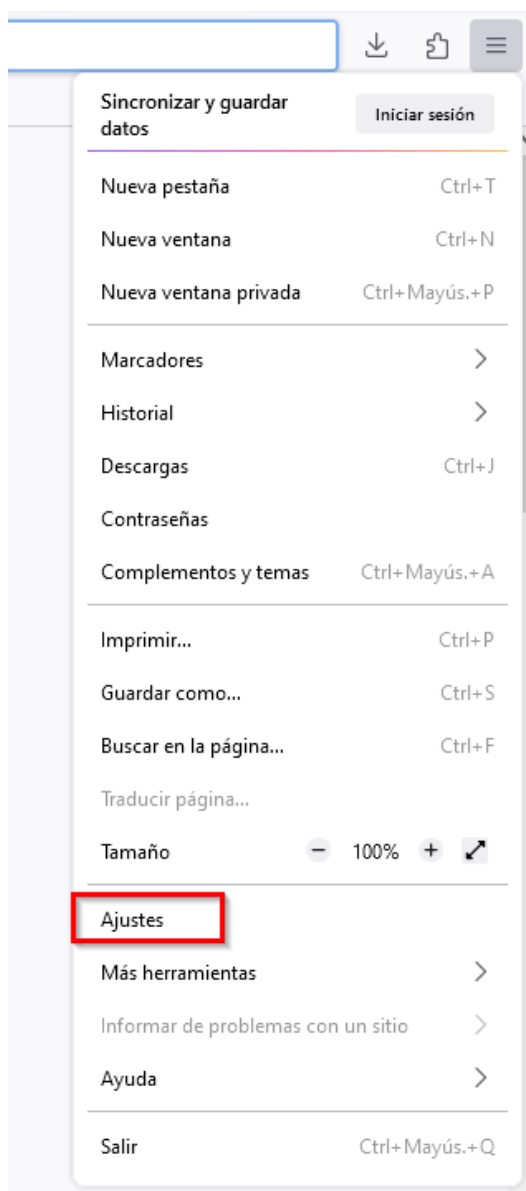


Aceptamos la operación para que se guarde el certificado, el asistente terminará indicándonos que el certificado se importó correctamente.

Ya tendremos importado nuestro certificado y podremos seleccionarlo cuando nos lo solicite la aplicación de ayudas.

3. ¿Cómo puedo instalar un certificado digital en Mozilla Firefox?

Abrimos Mozilla Firefox, y pulsamos el botón que representa un menú, situado arriba a la derecha, seleccionamos "Ajustes".



Nos aparecerá una nueva ventana con varias opciones, como la que se muestra en la imagen. Seleccionaremos la opción "Privacidad & Seguridad".

General

Inicio

Buscar

Privacidad & Seguridad

Sincronización

Más de Mozilla

Su navegador está siendo administrado por su organización. Buscar en ajustes

General

Inicio

- Abrir ventanas y pestañas anteriores
- Comprobar siempre si Firefox es su navegador predeterminado
- Firefox no es su navegador predeterminado [Convertir en predeterminado...](#)

Importar datos del navegador

Importar marcadores, contraseñas, historial y datos de autocompletado en Firefox. [Importar datos](#)

Pestañas

- Ctrl+Tab pasa por las pestañas en orden de uso reciente
- Abrir enlaces en pestañas en lugar de en ventanas nuevas
- Cuando abra un enlace, imagen o archivo multimedia en una pestaña nueva, cambiar inmediatamente a ella
- Confirmar antes de cerrar múltiples pestañas
- Mostrar miniaturas de las pestañas en la barra de tareas de Windows

En la ventana que se abre nos desplazamos hacia abajo hasta el apartado de Seguridad. Pulsaremos sobre el botón "Ver certificados" para acceder a nuestro contenedor de certificados y poder importar nuestro certificado.



- General
- Inicio
- Buscar
- Privacidad & Seguridad
- Sincronización
- Más de Mozilla

Su navegador está siendo administrado por su organización.

Buscar en ajustes

Seguridad

Protección contra contenido engañoso y software peligroso

- Bloquear contenido peligroso y engañoso [Saber más](#)
- Bloquear descargas peligrosas
- Advertirle sobre software no deseado y poco usual

Certificados

- Consultar a los servidores respondedores OCSP para confirmar la validez actual de los certificados

Ver certificados...

Dispositivos de seguridad...

- Permitir que Firefox confíe automáticamente en los certificados raíz de terceros que se instalen [Saber más](#)

Modo solo-HTTPS

HTTPS proporciona una conexión segura y cifrada entre Firefox y los sitios web que visita. La mayoría de los sitios web admiten HTTPS, y si el modo solo-HTTPS está habilitado, entonces Firefox actualizará todas las conexiones a HTTPS.

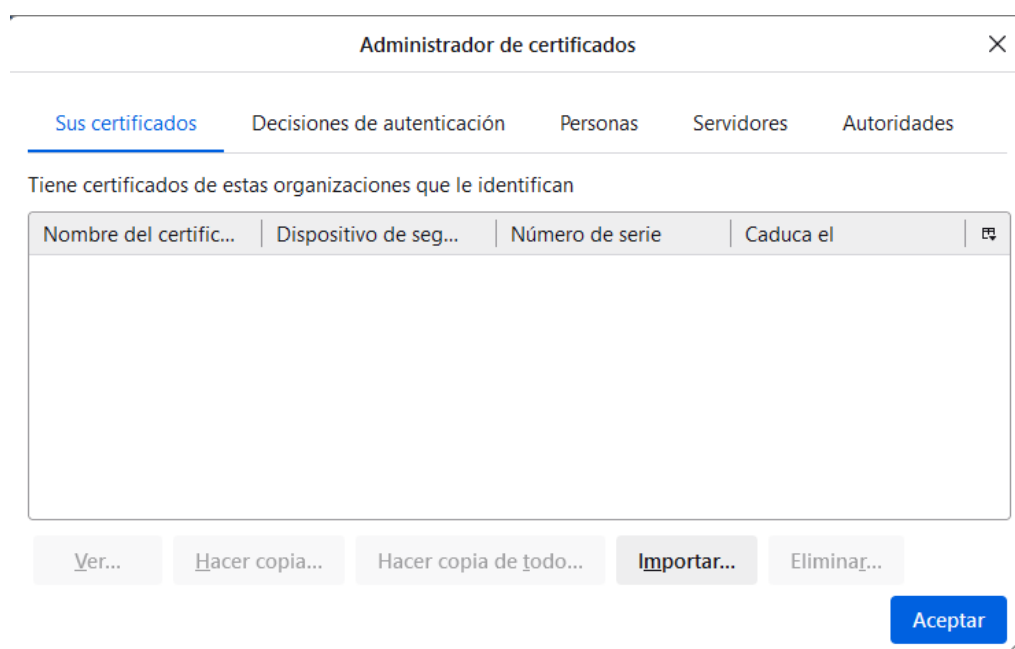
[Más información](#)

- Activar el modo solo-HTTPS en todas las ventanas
- Activar el modo solo-HTTPS solamente en ventanas privadas
- No activar el modo solo-HTTPS

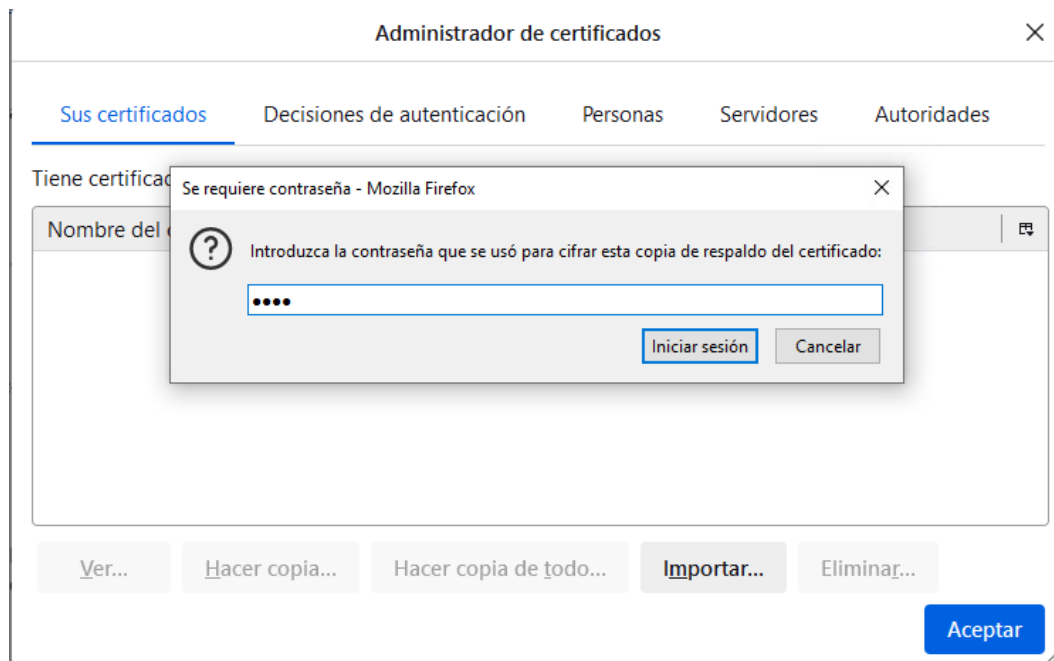
Gestionar excepciones...

Extensiones y temas

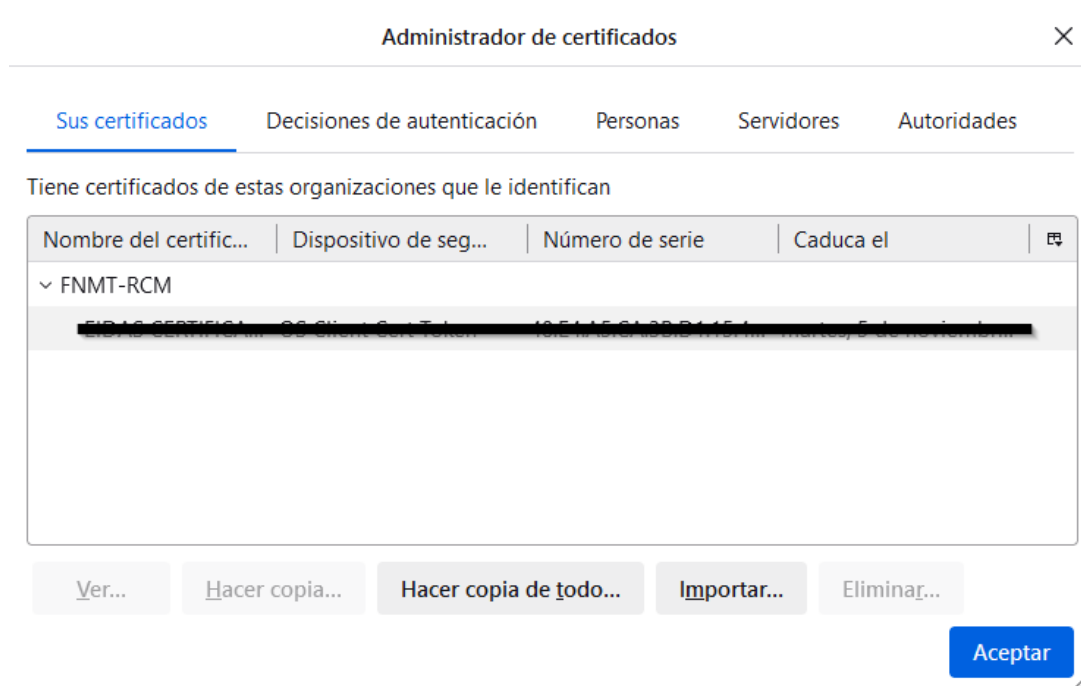
Situándonos en la pestaña “*Sus certificados*” si no tenemos ningún certificado instalado veremos la ventana vacía tal como aparece en la imagen. El siguiente paso será importar nuestro certificado, para ello pulsamos sobre el botón “*Importar...*”. Después seleccionaremos el archivo correspondiente al certificado (habrá que situarse en la carpeta en la que está guardado el archivo) y pulsamos el botón “*Abrir*”.



Nos pedirá la contraseña de cifrado para el certificado que acabamos de seleccionar:



Si todo ha ido bien podremos ver el certificado ya importado. Si lo seleccionamos y pulsamos el botón “Ver” obtendremos información adicional.





Finalmente, pulsamos el botón “*Aceptar*” y con esto quedará instalado el certificado en nuestro navegador. Ya tendremos importado nuestro certificado y podremos seleccionarlo cuando nos lo solicite la aplicación de ayudas.

4. ¿Dónde puedo obtener un certificado digital?

Existen diferentes prestadores públicos de servicio de certificación nacionales reconocidos por la Administración Pública. Puede consultar el procedimiento a seguir para la obtención visitando su página web. ([haga clic aquí para consultar los prestadores con certificados reconocidos por la plataforma @firma](#)).

5. ¿Cómo puedo instalar y ejecutar AutoFirma?

AutoFirma es una aplicación que permite realizar la firma de forma electrónica a partir de un certificado, es necesario tener instalada la aplicación para poder realizar la firma de forma digital antes de proceder al firmado de los documentos.

Los requisitos mínimos de AutoFirma son:

- **Sistema Operativo**
 - Microsoft Windows 7 o superior.
 - Soportado directamente en 7, 8, 8.1 y 10.
 - En 32 y 64 bits.
 - Linux
 - Guadalinex, Ubuntu.
 - Apple OS X Yosemite o superior.
 - Soportado directamente en Yosemite, El capitán o Sierra.
- **Navegadores Web**
 - Windows
 - Google Chrome 46 o superior.
 - Mozilla Firefox 41.0.1 o superior.
 - Microsoft Internet Explorer 8 o superior.
 - Microsoft Edge v20.
 - Linux
 - Mozilla Firefox 41.0.1 o superior.



- Apple OS X
 - Apple Safari 9.0 superior.
 - Google Chrome 46 o superior.
 - Mozilla Firefox 41.0.1 o superior

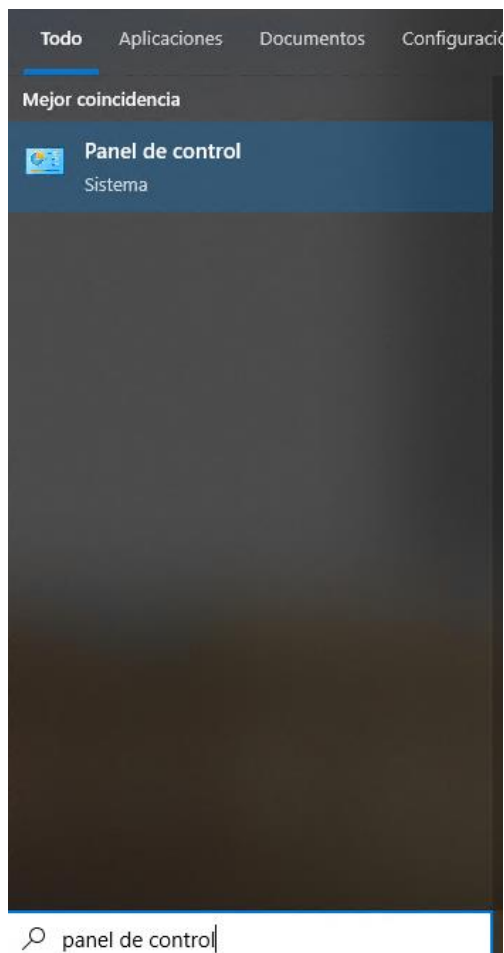
Si cuenta con una versión de Java 1.7 superior a 1.7.0_75 o Java 1.8 superior a 1.8.0_31 por defecto deberá añadir los certificados raíz y de entidades intermedias al almacén de certificados de Java para validar correctamente el certificado SSL del sitio web.

Estos certificados puede descargarlos desde los siguientes enlaces:

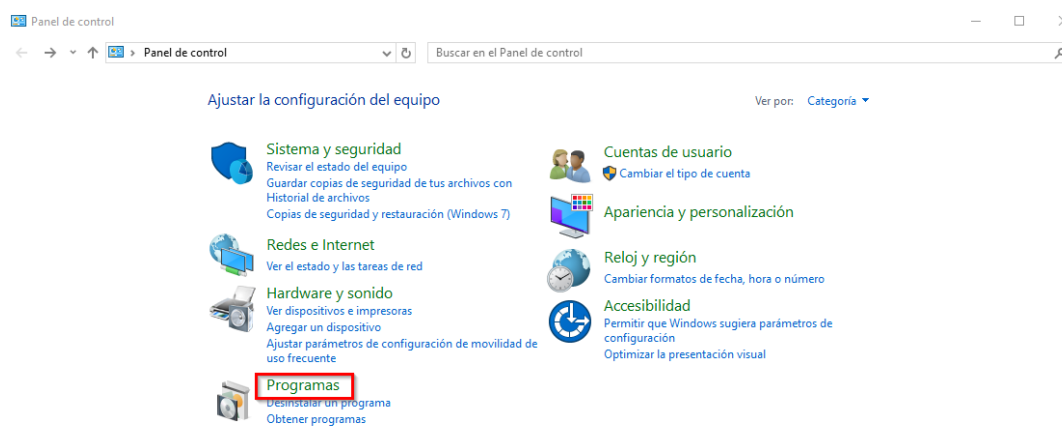
- AC Raíz FNMT RCM:
 - https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_Raiz_FNMT-RCM_SHA256.cer
- AC Componentes Informáticos:
 - https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_Componentes_Informaticos_SHA256.cer



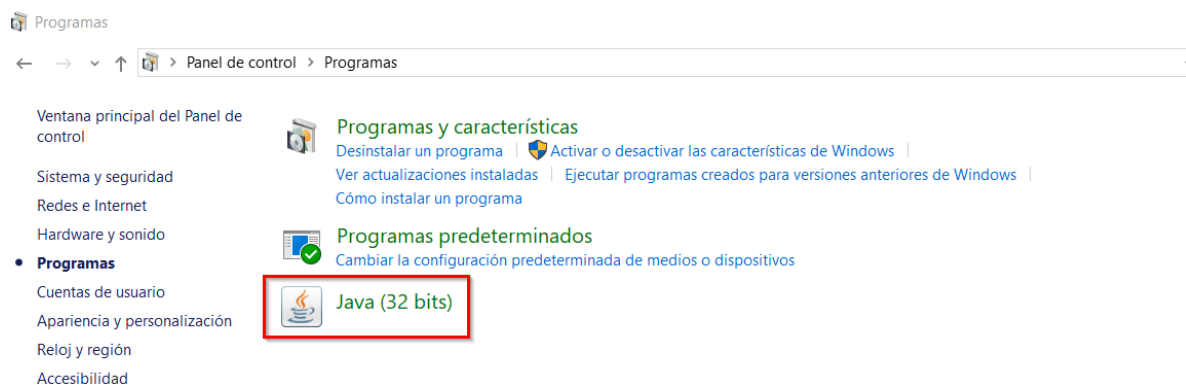
Para añadir los certificados pulse *Inicio* → *Panel de Control*



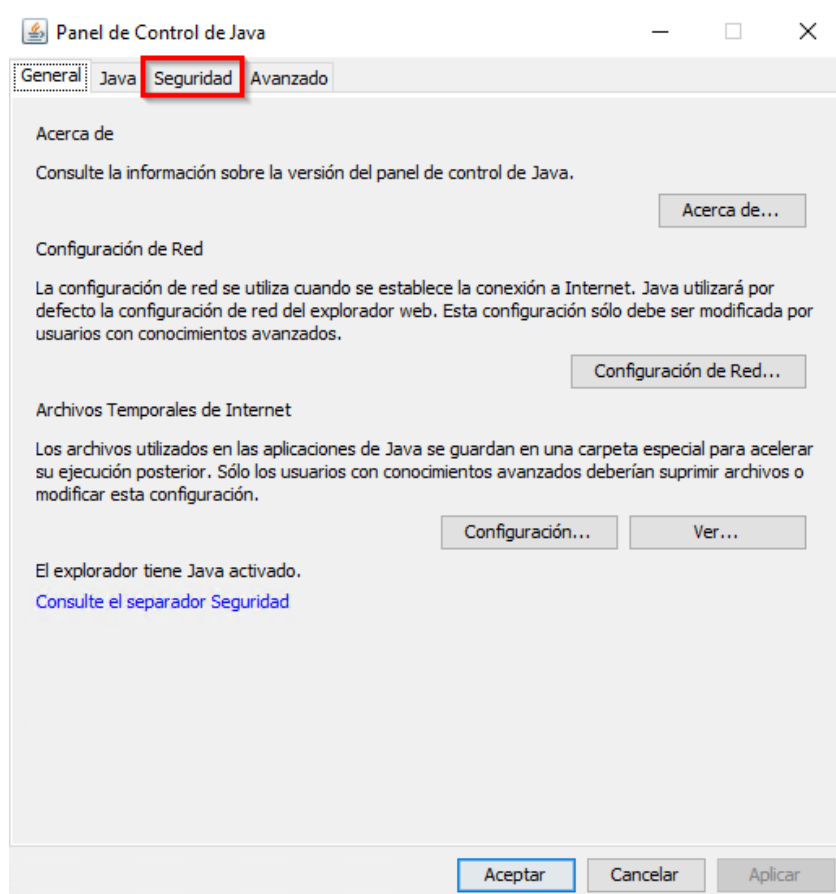
Programas

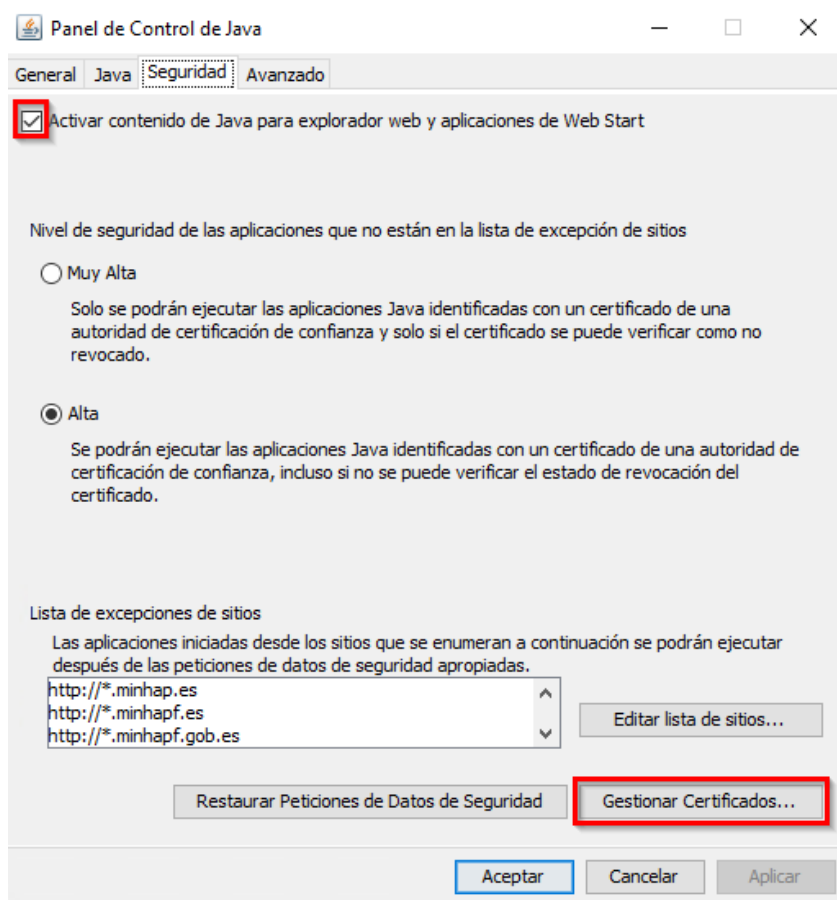


Java

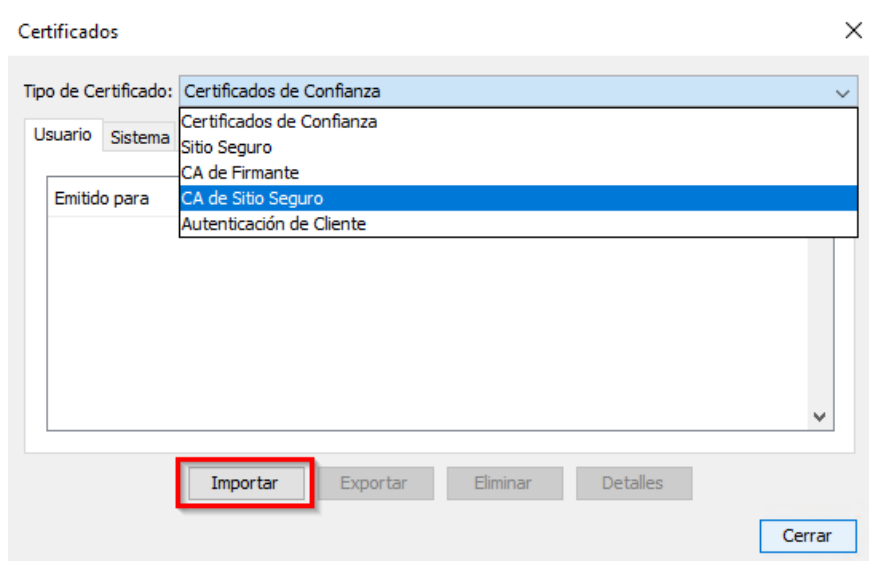


A continuación, haga clic en la pestaña “Seguridad” → botón “Gestionar Certificados...” tal como se muestra en la siguiente imagen.

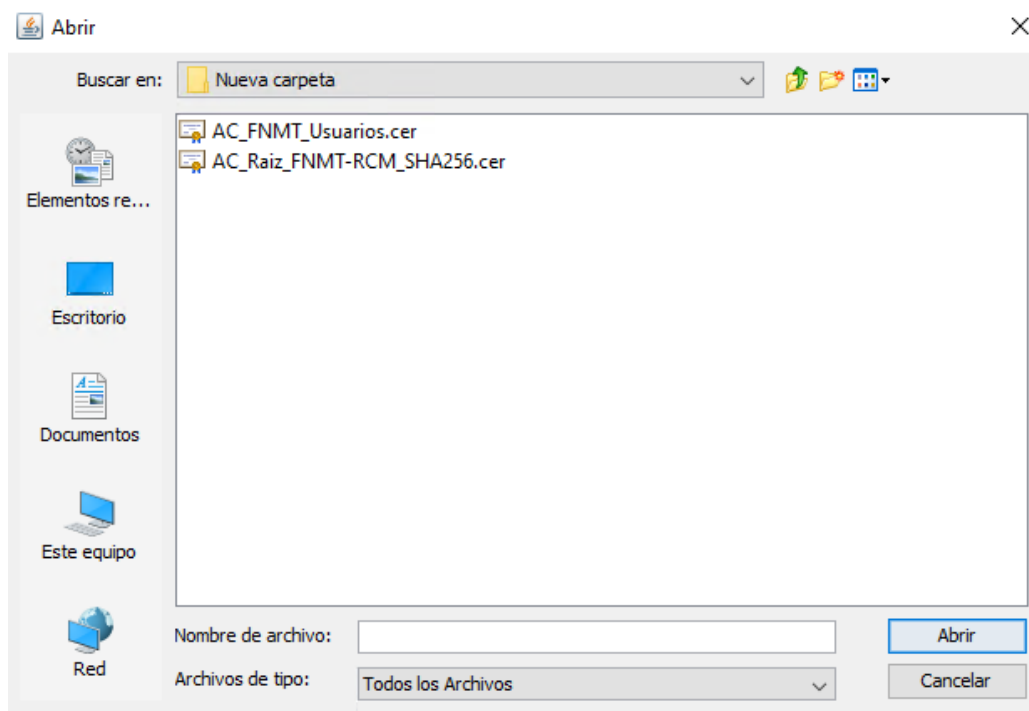




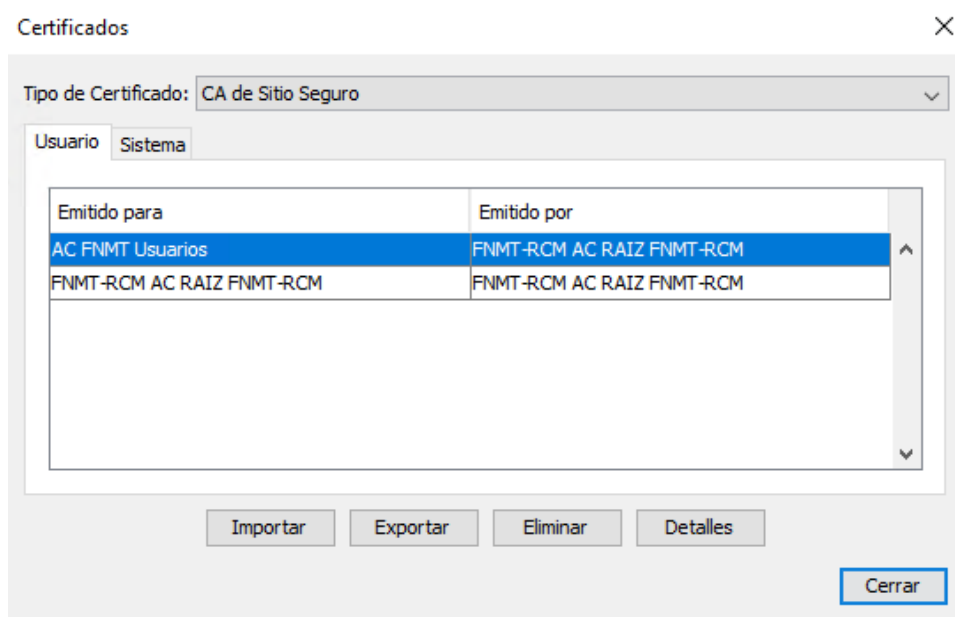
Una vez hecho esto, seleccione en el desplegable: “Sitio Seguro”.



Pulse el botón *“Importar”*, y seleccione el certificado que ha descargado previamente. Es necesario seleccionar *“Todos los archivos”* para que se muestre el certificado.

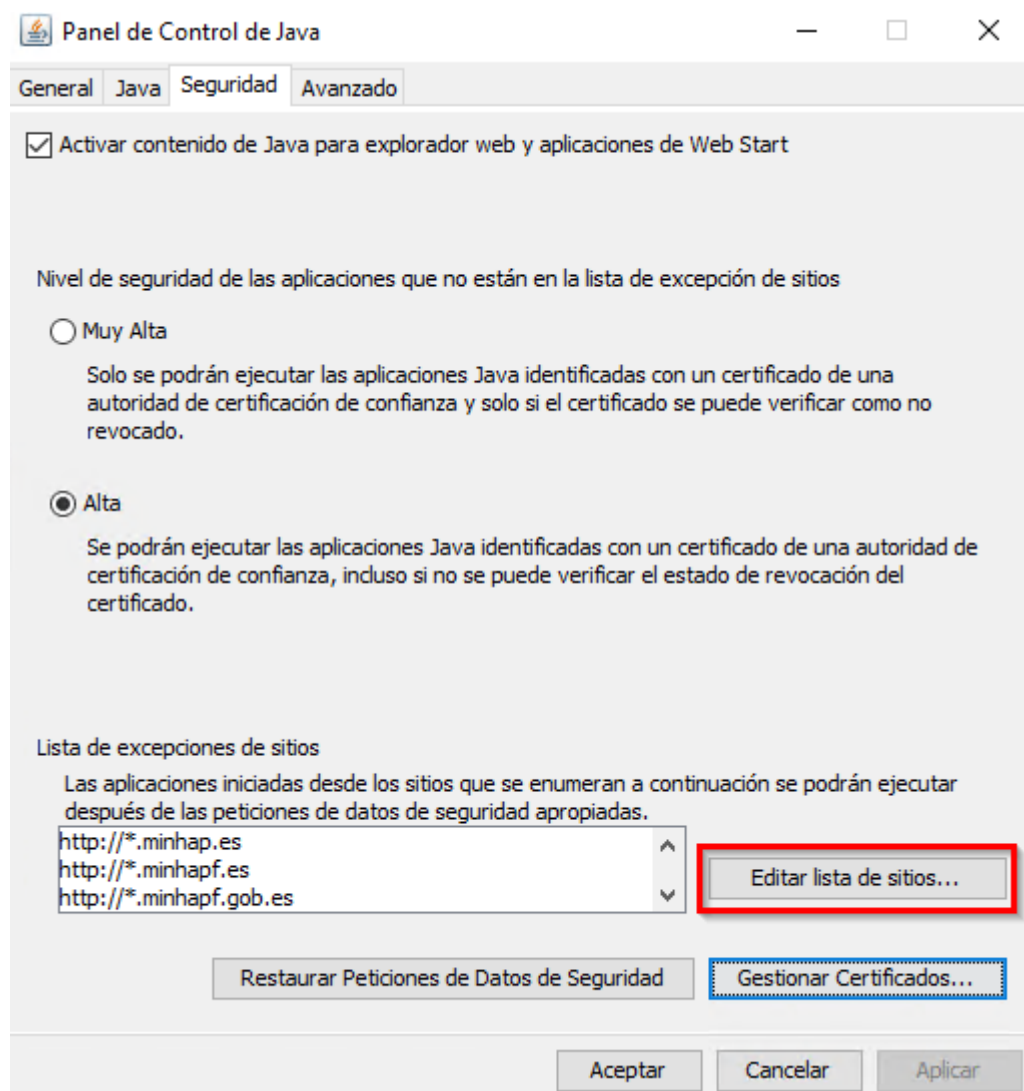


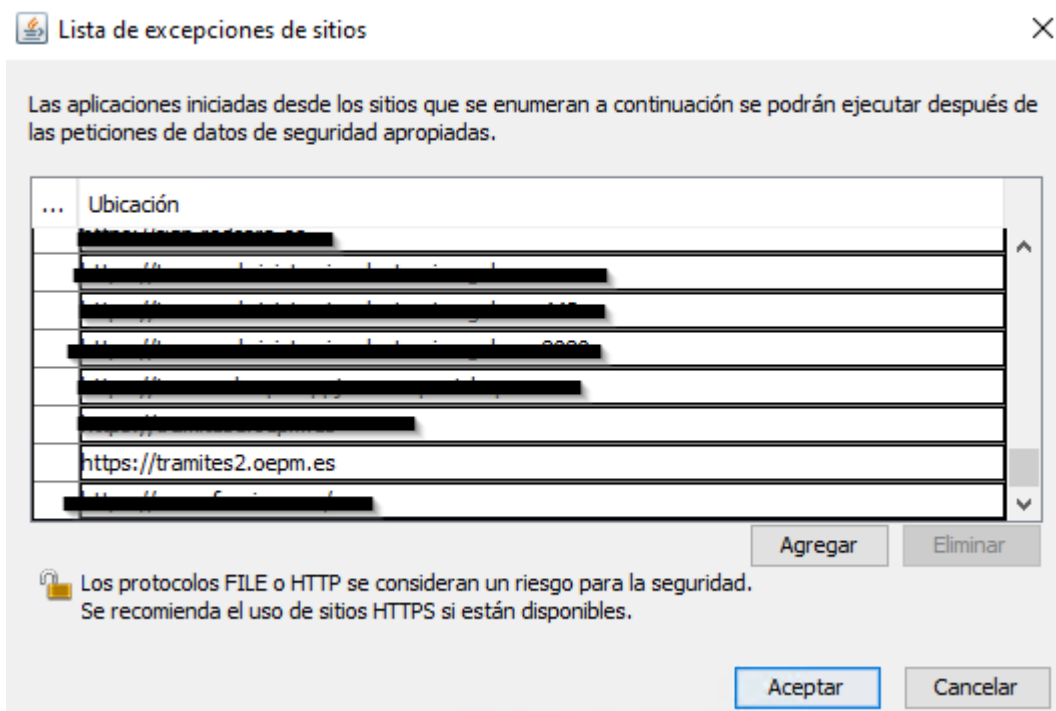
Repita esta operación para ambos certificados. Una vez importados debería visualizarlos en el almacén.





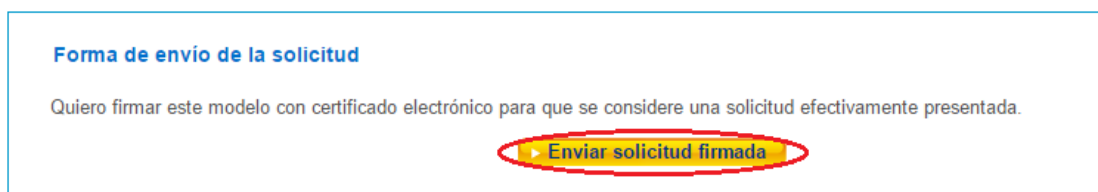
Cierre la ventana anterior. Finalmente deberá editar la lista de sitios confiables en la pantalla de Seguridad pulsando el botón “Editar lista de sitios...” y agregando la url “https://tramites2.oepm.es” a la lista de sitios de confianza:





IMPORTANTE: En caso de que no realice estos pasos previos de configuración, es posible que se encuentre con alguno de los errores contemplados en apartados posteriores de este documento.

El proceso de ejecución de AutoFirma comienza tras seleccionar la opción “*Presentar*” y pulsar el botón que le permite enviar la solicitud firmada de forma electrónica, en función del tipo de solicitante le aparecerá una u otra de las siguientes pantallas. Es posible que la transición a la siguiente pantalla dure unos segundos, por favor, tenga paciencia.





Forma de envío de la solicitud

<p>Quiero firmar este modelo con mi certificado electrónico para que se considere una solicitud electrónicamente presentada.</p> <p>Enviar solicitud firmada de forma electrónica</p>	<p>Quiero imprimir el modelo, firmarlo de manera manuscrita y adjuntarlo por la pantalla de inicio para que se considere una solicitud efectivamente presentada.</p> <p>Enviar solicitud sin firmar de forma electrónica</p>
--	---

6. ¿Cómo puedo llevar a cabo el proceso de firma?

Para ello deberemos pulsar el botón “Firmar solicitud”.

Firmar Solicitud

Esta solicitud sólo se puede firmar con el certificado digital del solicitante: D./Dña. Ciudadano Activo con DNI:92920000T

Antes de firmar la solicitud es conveniente que revise el siguiente documento que contiene la información que usted va a firmar:

[Documento para revisar antes de firmar.](#)

A continuación, y si es la primera vez que lleva a cabo este proceso, le aparecerá una nueva ventana solicitándole permisos.

¿Abrir AutoFirma?

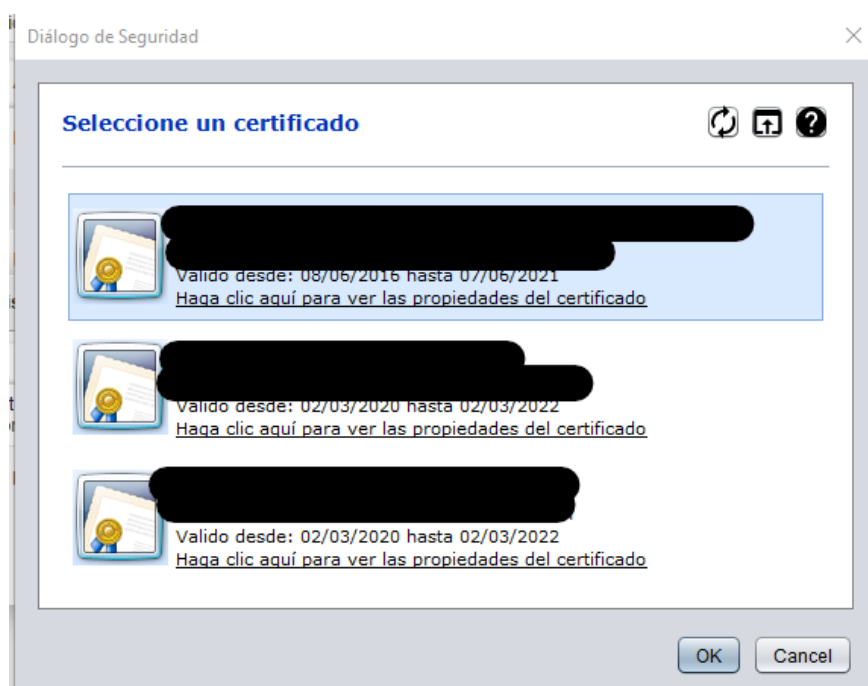
<http://pruebainterno2.oepm.local> quiere abrir esta aplicación.

Abrir AutoFirma

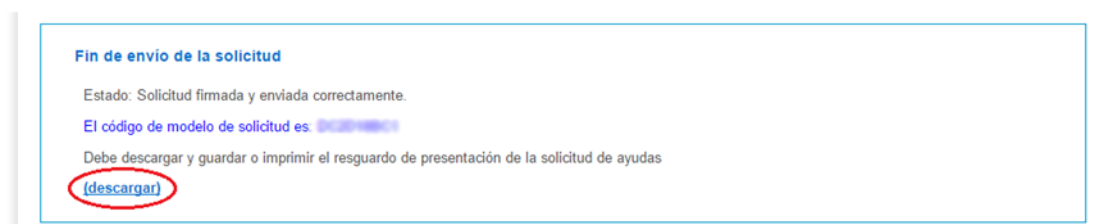
Cancelar



Justo después de esta ventana con el logo de AutoFirma aparecerá una ventana en la que se nos solicitará seleccionar el certificado que usaremos para firmar, tan solo se debe seleccionar el certificado y pulsar en “OK”.

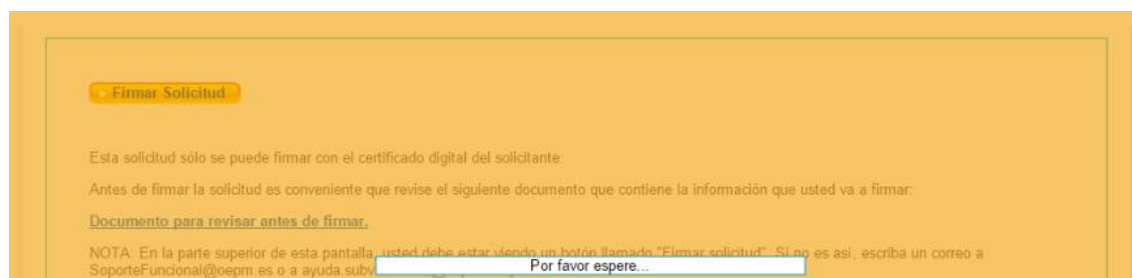


Tras esto debería pasar a una página desde la que poder descargar el resguardo firmado por la OEPM, dándose por finalizado el envío.



7. Al firmar electrónicamente, la página se queda bloqueada con el mensaje “Por favor espere...”

Cuando trate de firmar la solicitud de manera electrónica, le aparecerá la siguiente pantalla.

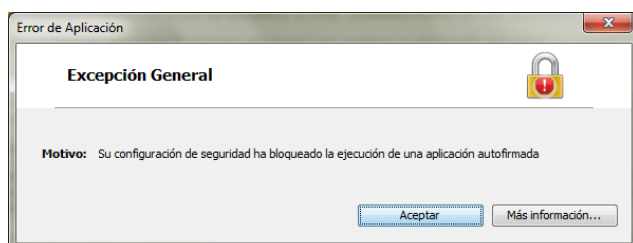


El mensaje “Por favor espere...” debería aparecer no más de unos segundos o tal vez un minuto en función de la velocidad a la que se cargue AutoFirma. Si la página se queda bloqueada, mostrando continuamente este mensaje, o le aparece una pantalla de error.

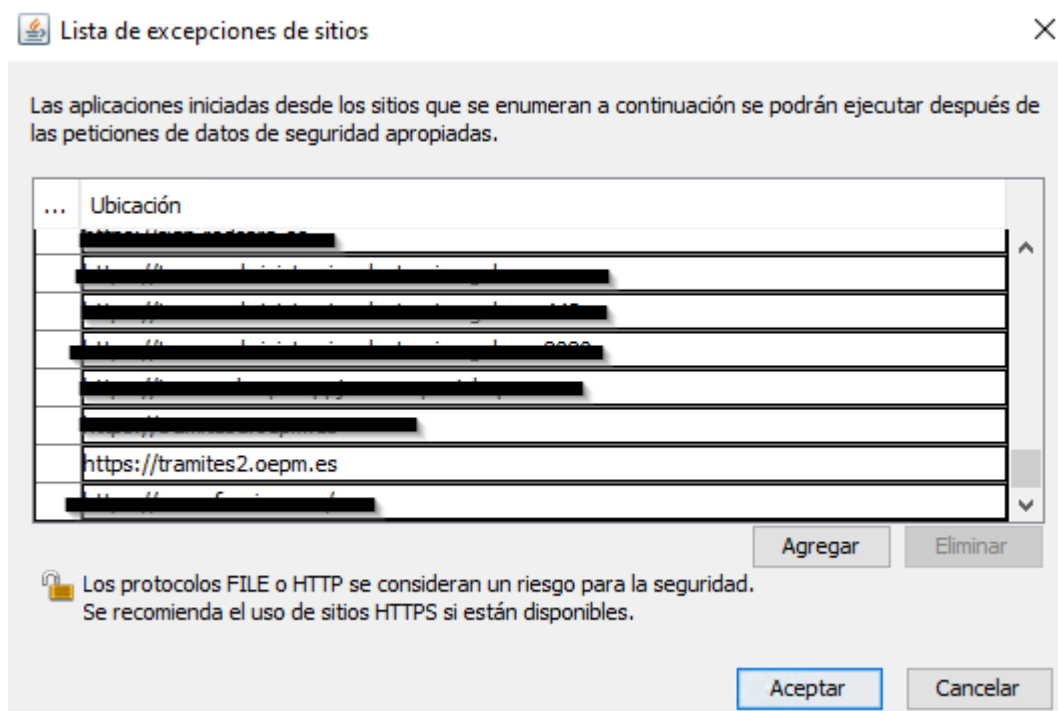
Lo más probable es que AutoFirma no haya podido cargarse por no estar correctamente instalado. Para instalarlo puede seguir los pasos que se indican en el apartado [¿Cómo puedo instalar y ejecutar el AutoFirma?](#)

8. Al cargar AutoFirma me aparece el mensaje “Aplicación bloqueada por la seguridad de Java”.

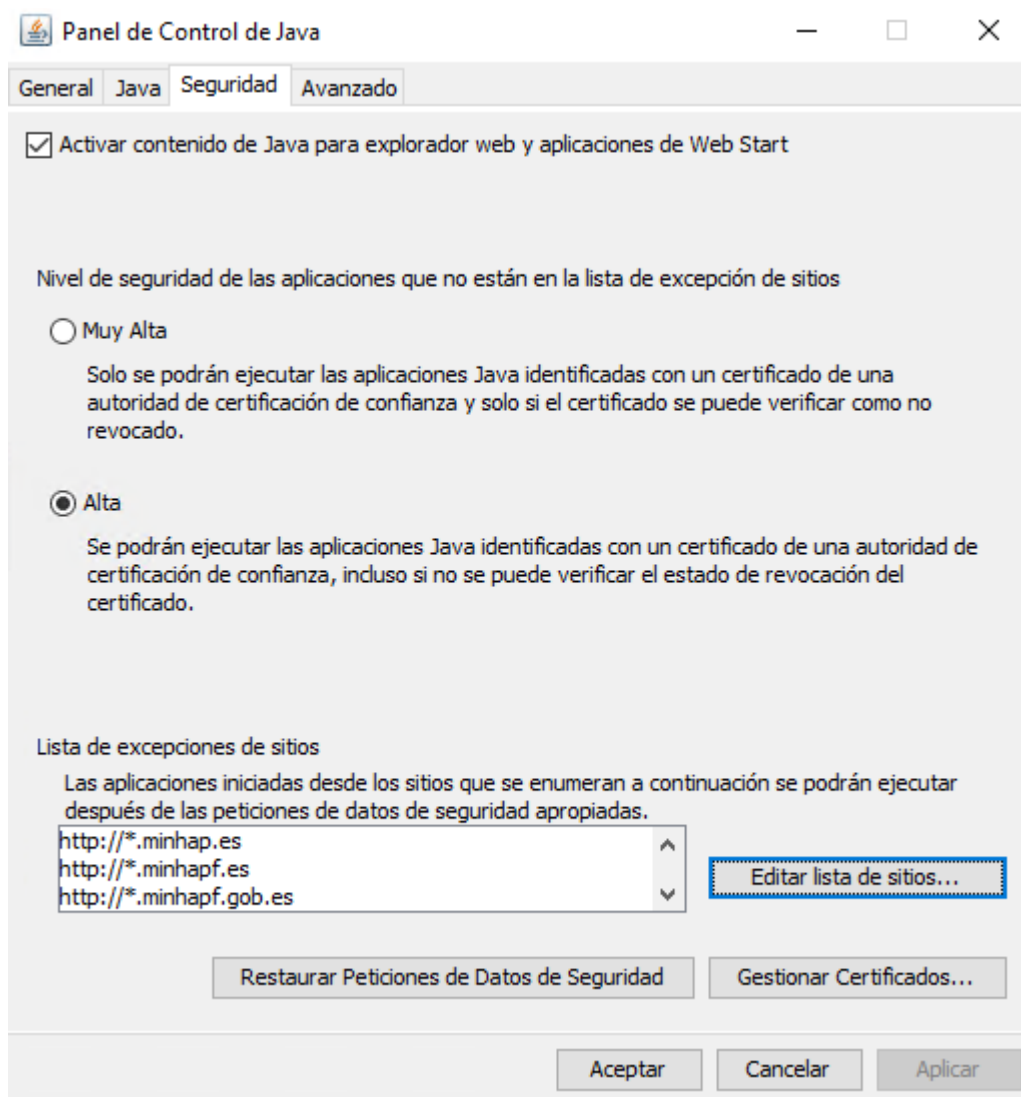
Este caso puede producirse para las versiones de Java 1.7.0_51 y superiores; debe pulsar el botón “Aceptar”, al hacerlo, le aparecerá el siguiente mensaje. Pulse de nuevo “Aceptar”.



Para evitar este error debe añadir los siguientes sitios a la lista de excepciones de Java. Para ello, diríjase a: *Inicio* → *Panel de Control* → *Programas* → *Java* → *pestaña "Seguridad"* → *botón "Editar lista de sitios..."*. A continuación le aparecerá una pantalla en la que debe introducir los sitios <https://tramites.oepm.es> y <https://tramites2.oepm.es> de manera que obtenga el siguiente resultado:



Pulse *"Aceptar"* y volverá a la pestaña de seguridad de Java, ya con las excepciones añadidas.



Para realizar el proceso de firma le recomendamos que salga de la aplicación de solicitud de ayudas, y vuelva a cargar su solicitud indicando de nuevo su código de modelo y NIF.

9. Otros errores al ejecutar el AutoFirma

Si se encuentra con algún problema, por favor compruebe que ha realizado correctamente todo lo indicado en el apartado [¿Cómo puedo instalar y ejecutar AutoFirma?](#) En caso de que haya seguido de manera adecuada todos los pasos y el error persista, por favor, contacte con SopORTEFuncional@oepm.es

10. ¿Qué significa “Sitio web certificado por una autoridad desconocida”?

Es posible que el navegador muestre un mensaje de aviso al acceder a la página principal de la aplicación web de solicitud de subvenciones 2024 **ayudas 2023**. Firefox muestra el siguiente mensaje:



Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **pruebatramites.oepm.es**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

[¡Sácame de aquí!](#)

► **Detalles técnicos**

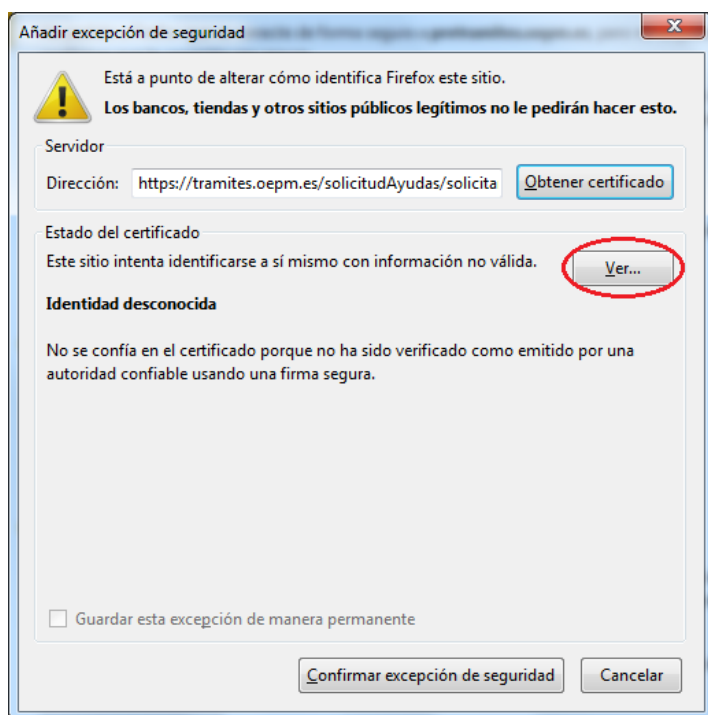
▼ **Entiendo los riesgos**

Si sabe lo que está haciendo, puede obligar a Firefox a confiar en la identificación de este sitio. **Incluso aunque confíe en este sitio, este error puede significar que alguien esté interfiriendo en su conexión.**

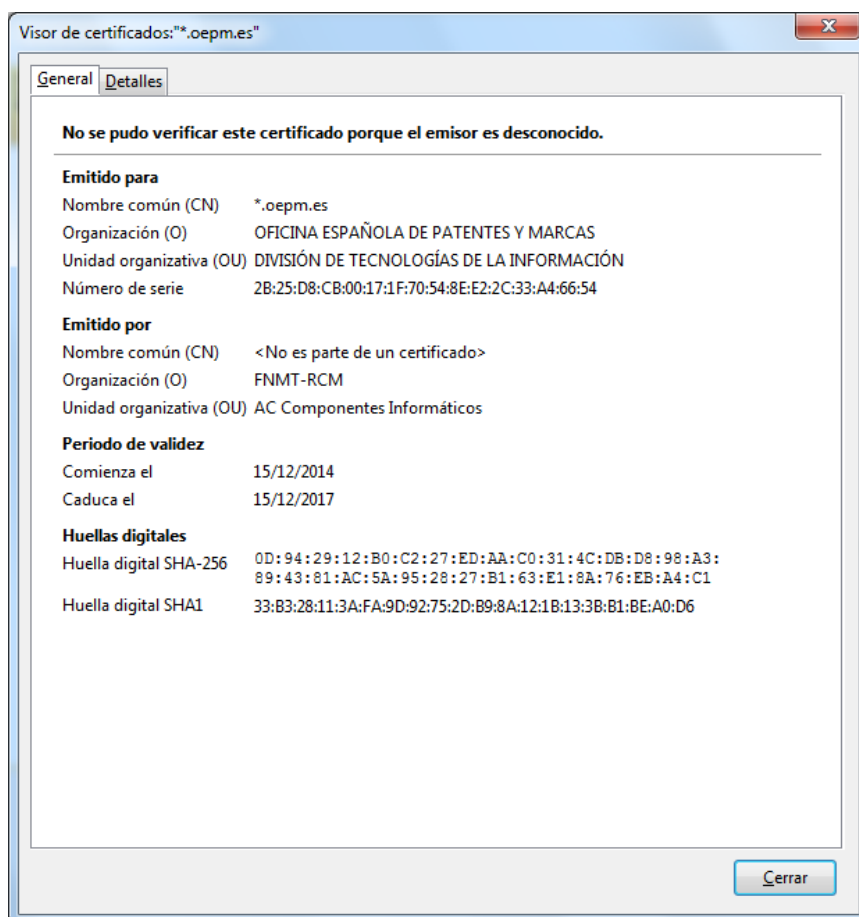
No añada una excepción a menos que sepa que hay una razón seria por la que este sitio no use identificación confiable.

[Añadir excepción...](#)

Si pulsa sobre “*Entiendo los riesgos*” y a continuación en el botón el botón, “*Añadir excepción...*”, se le mostrará la siguiente pantalla.

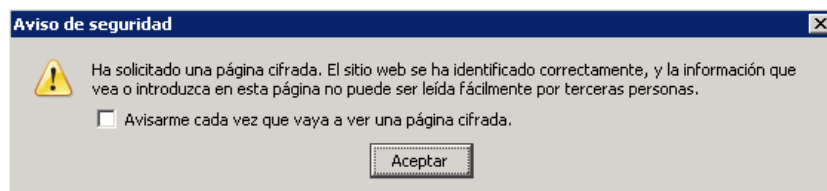


El motivo es que su navegador no reconoce la entidad *.OEPM.ES. Puede comprobar que dicha identidad es confiable pulsando “Ver...”. Al examinar el certificado asegúrese de que contiene la información que muestra la siguiente imagen.



Una vez comprobada la información anterior, y cerrado el Visor de certificados, puede indicar a su navegador que acepta el certificado pulsando aceptar.

Es posible que a continuación le aparezca un mensaje que le avisa de que la información introducida en la aplicación viajará cifrada, pulse "Aceptar".



11. Si soy una persona física que actúa sin representante y no tengo certificado digital, ¿cómo he de adjuntar la solicitud firmada de forma manuscrita?

En el caso de que una persona física sin representante enviará la solicitud sin firmar electrónicamente, tras imprimir el formulario de solicitud, firmarlo manuscritamente y escanearlo, debería seguir los siguientes pasos para completar la solicitud de ayuda:

En primer lugar, dirigirse a la página de inicio de la aplicación de solicitud de ayudas y pulsar sobre el vínculo “*Soy persona física que actúa sin representante. He completado la solicitud con firma manuscrita y deseo adjuntar la solicitud firmada*”.

A continuación, introducir el código de modelo, el NIF del solicitante de la ayuda y el archivo que contiene la solicitud firmada de forma manuscrita y pulsar el botón “*Firmar Solicitud*”.

Si los datos introducidos son correctos aparecerá la página de fin de envío de la solicitud desde la que descargar el acuse de recibo de la solicitud de ayuda. Cuando se haya descargado el documento puede pulsarse el hipervínculo “*Salir*”.



Fin de envío de la solicitud

Estado: Solicitud firmada y enviada correctamente.

El código de modelo de solicitud es: [0123456789](#)

Debe descargar y guardar o imprimir el resguardo de presentación de la solicitud de ayudas

[\(descargar\)](#)

