Castilla-La Mancha
D.G. de Trabajo, Formación y Seguridad Laboral
Consejería de Economía, Empresas y Empleo
Av. de Irlanda 14 - 45071 TOLEDO

indra

FOCO

GESTIÓN DE SOLICITUDES

MANUAL DE USUARIO
ENVÍO DE SOLICITUDES CON FIRMA ELECTRÓNICA

ÍNDICE

1. INTRODUCCIÓN

Este manual tiene como objetivo explicar y guiar al usuario para poder utilizar las nuevas funcionalidades de administración electrónica en FOCO.

Hasta ahora existía la conexión de FOCO con el Registro Electrónico de la Junta de Comunidades de Castilla la Mancha, en el cual se registran las solicitudes de subvención cuando son enviadas por las entidades.

En esta nueva versión se han introducido 2 nuevas patas de la e-administración, por una parte la firma digital (mediante certificados) de documentos en formato PDF y por otro lado el almacenamiento de estos documentos firmados en el Gestor Documental corporativo de la Junta de Comunidades de Castilla la Mancha.

A continuación, se describirán los pasos a seguir por el usuario tanto para adecuar su equipo a los requisitos para el uso de la firma electrónica, como el funcionamiento en FOCO.

2. ADECUACIÓN DEL EQUIPO

Para realizar la firma electrónica de documentos en FOCO es necesario por una parte tener instalado el software de Autofirma proporcionado por portal de administración electrónica del gobierno.

Además de la instalación de Autofirma, se necesita un certificado electrónico válido y que éste sea importado al equipo para su utilización.

A continuación se expone como realizar estas dos operaciones.

2.1. JAVA

Antes de instalar cualquier plataforma, debe asegurarse que tiene instalado java en su equipo, se recomienda utilizar la última versión disponible de java. Es recomendable tener la versión de java actualizada ya que en cada versión se incorporan mejoras y correcciones de seguridad. La última versión de java disponible actualmente es la 8 en la revisión 131. **https://www.java.com/es/download/**

En la URL anterior, podrá descargar e instalar la última versión disponible de java, además, existe un enlace denominado ¿Tengo Java? Donde podrá comprobar si está instalado en su ordenador.

2.2. INSTALACIÓN DE AUTOFIRMA

La aplicación Autofirma es necesaria para realizar la firma, ya que la ésta se realiza a través de un miniapplet proporcionado por el Ministerio de Hacienda y Administraciones Públicas (MINHAP) y, en general, los navegadores actuales no permiten la utilización de Applets por sus problemas de seguridad, es por esto, que al no poder ejecutar dicho applet, se despliega la aplicación Autofirma.

Si no está instalada esta aplicación en su equipo no podrá realizar la firma con los navegadores que no permiten la ejecución de applets.

Para descargar esta aplicación debe conectarse a la URL **http://firmaelectronica.gob.es/Home/Descargas.html** y descargar la versión que más se adecúe a su sistema, está disponible para Windows 32 Bits, Windows 64 Bits, Linux y Mac.

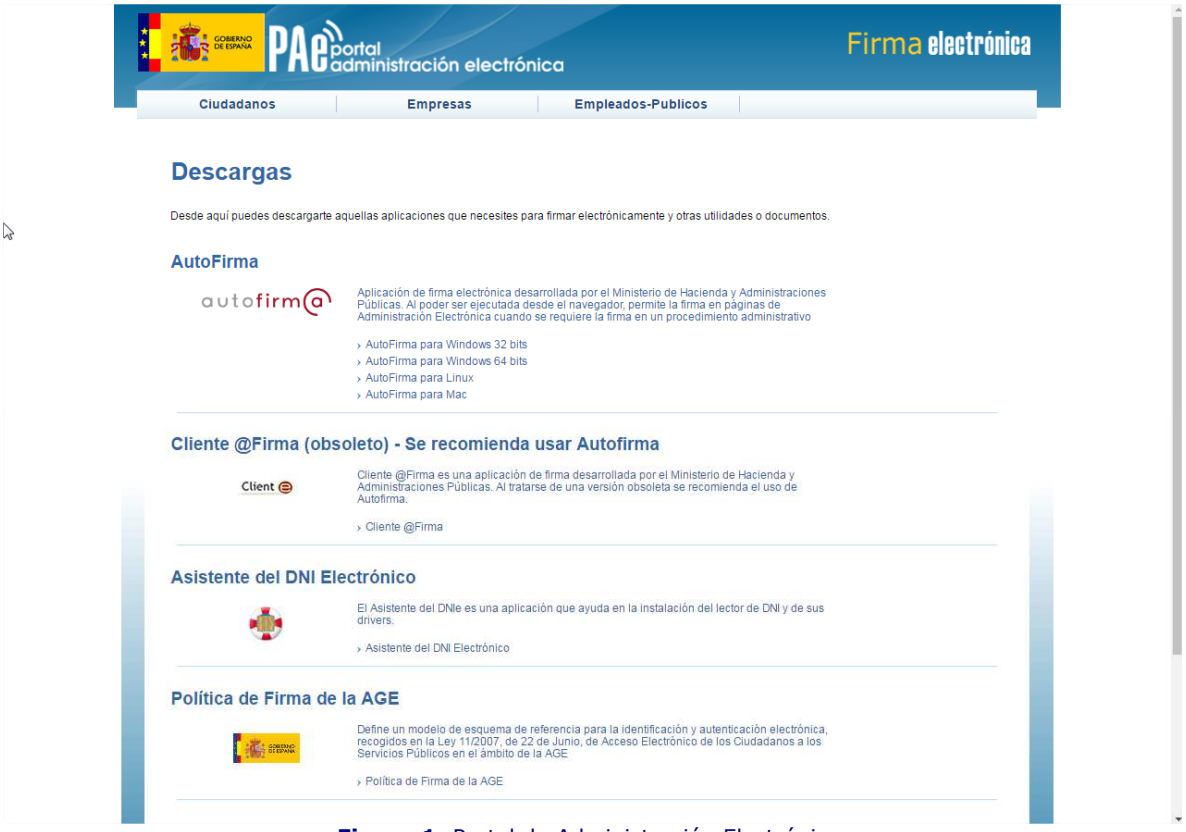

Figura 1: Portal de Administración Electrónica.

Se descargará un fichero de extensión zip que contiene a su vez 2 ficheros:

- Un PDF con el manual de instalación de la aplicación.
- Un fichero de instalación de la aplicación.

Para instalar el software, descomprima dicho fichero descargado y siga los pasos que se indican en el manual en formato PDF.

2.3. IMPORTAR CERTIFICADO

La firma electrónica de un documento, se realizará con un certificado digital, estos certificados están emitidos por entidades emisoras, como puede ser la FNMT y nos identifica a la hora de firmar un documento.

Estos certificados digitales se deben importar a un almacén de certificados, en el presente documento se expondrán diferentes posibilidades para importar los certificados, los certificados importados en el almacén por defecto del sistema podrán utilizarse con los navegadores Internet Explorer, Google Chrome o Safari, mientras que para Mozilla Firefox la importación se hace en su propio almacén y debe hacerse desde el propio navegador.

Para la utilización de la firma, se recomienza actualizar el navegador a la última versión tanto por temas de compatibilidad como por temas de seguridad. Actualmente, es compatible y está testado para Internet Explorer 11, Mozilla Firefox 53.0, Google Chrome 58.0 y Safari para Windows 5.1.7.

Además de esto, puede visitar las preguntas frecuentes sobre la importación y eliminación de certificados que ofrece la sede electrónica de la FNMT, esta página contiene mucha información útil acerca de los certificados: **https://www.sede.fnmt.gob.es/preguntas-frecuentes/exp-imp-y-elim-de-certificados**

2.3.1. EJECUTANDO EL FICHERO CON EL CERTIFICADO EN WINDOWS

Alojar el fichero con el certificado en una ruta conocida por el usuario y hacer doble click sobre dicho fichero, en ese momento se ejecutará el asistente de importación de certificados:

Figura 2: Pantalla inicial del asistente para la importación de certificados

En la pantalla de la figura anterior, pulsar el botón **Siguiente**, se mostrará una pantalla donde se indica la ruta completa del fichero ejecutado:

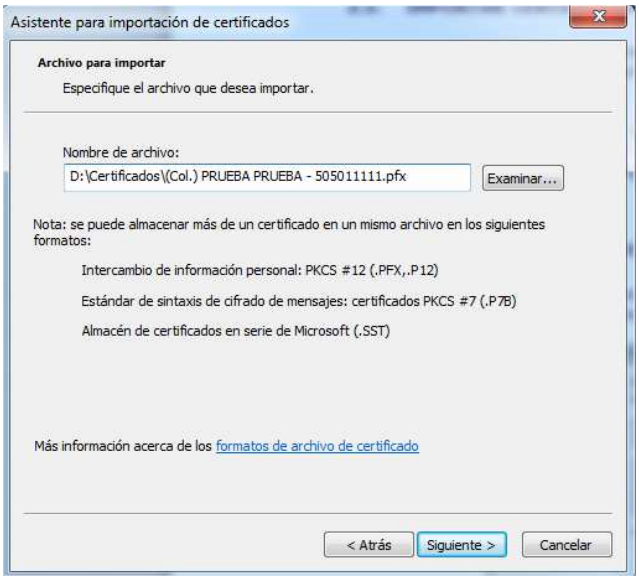

Figura 3: Pantalla donde se muestra el fichero ejecutado.

En la pantalla de la figura anterior, pulsar el botón **Siguiente**, se mostrará la pantalla para la introducción de la contraseña del certificado:

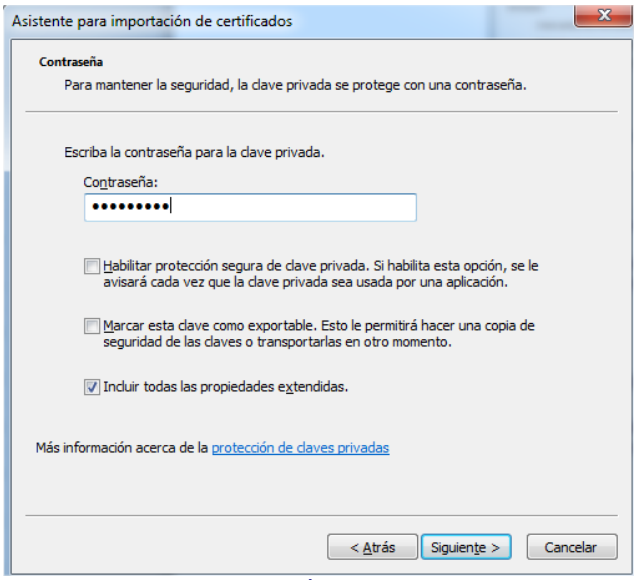

Figura 4: Pantalla de introducción de la contraseña del certificado.

En la pantalla de la figura anterior, introducir la contraseña y pulsar el botón **Siguiente**, se mostrará la pantalla de selección del almacén de certificados:

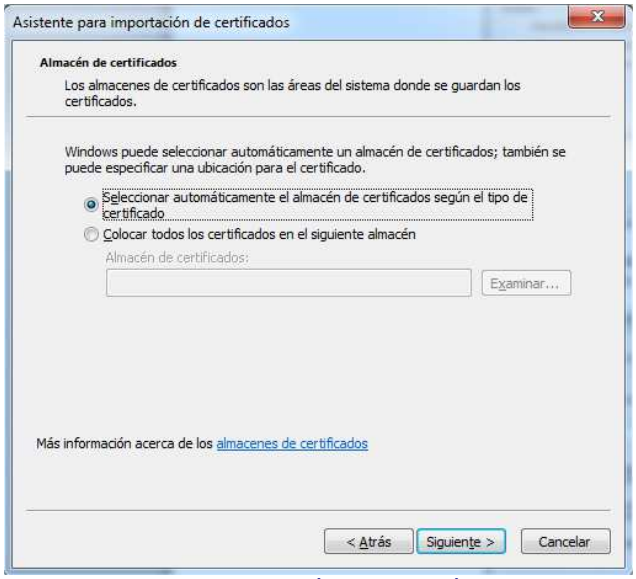

Figura 5: Pantalla de selección del almacén de certificados

Dejar marcada la opción "*Seleccionar automáticamente el almacén de certificados según el tipo de certificado*" de manera que el propio sistema operativo lo alojará en el almacén correcto, pulsar el botón **Siguiente** y se mostrará la pantalla de finalización del asistente:

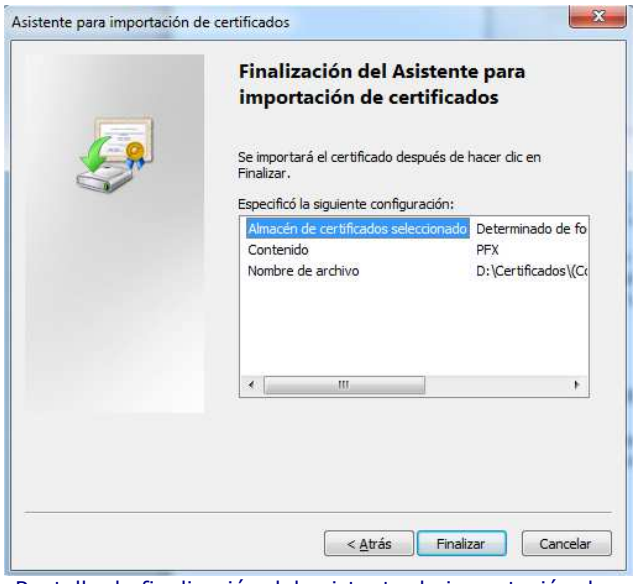

Figura 6: Pantalla de finalización del asistente de importación de certificados

La pantalla de la figura anterior, nos mostrará un resumen para finalizar el proceso de importación, para ello debemos pulsar el botón **Finalizar**, en ese momento el certificado quedará importado en el almacén de certificados personal del sistema y estará disponible para realizar la firma con los navegadores Internet Explorer, Google Chrome o Safari.

2.3.2. INTERNET EXPLORER

Para importar un certificado con internet explorer, en el menú superior, pulsar la opción Herramientas -> Opciones de internet y acceder a la pestaña contenidos.

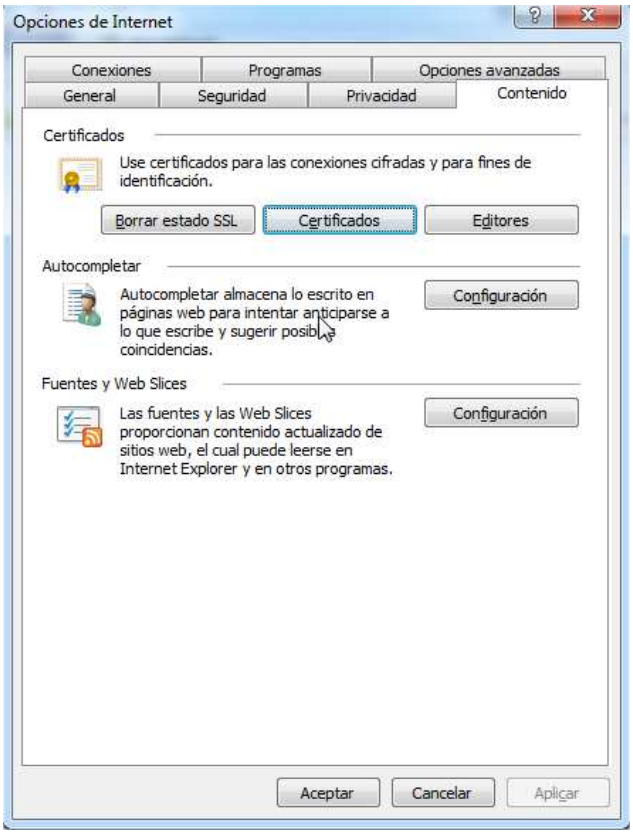

Figura 7: Pantalla de acceso en Internet Explorer

Una vez en la pantalla de la figura anterior, en el apartado **Certificados,** pulsar el botón **Certificados,** Se mostrará la pantalla donde se muestran los certificados instalados en el equipo, pulsando en la pestaña personal, veremos los importados por el usuario:

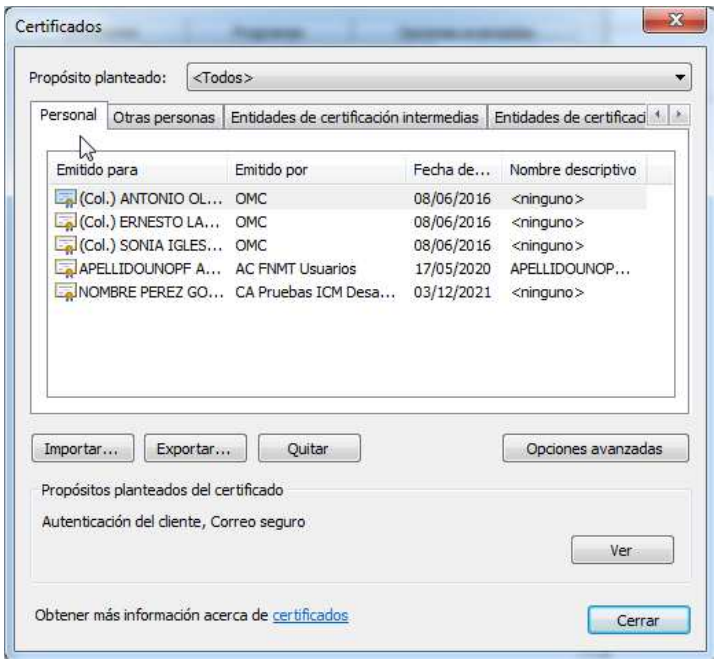

Figura 8: Certificados Importados

Una vez en la pantalla de la figura anterior, en el apartado **Certificados,** pulsar el botón **Certificados,** Se mostrará la pantalla donde se muestran los certificados instalados en el equipo, pulsando en la pestaña personal, veremos los importados por el usuario tal y como se muestra en la pantalla de la figura anterior.

Para importar un certificado, se debe pulsar el botón **Importar**, en ese momento se mostrará la pantalla del asistente de importación de certificados tal y como se muestra en la **Figura 2**, el proceso será el mismo que el explicado en el punto **Ejecutando el Fichero con el Certificado en Windows**, con la salvedad de que en la pantalla de la **Figura 3**, debe seleccionar el fichero pulsando el botón **Examinar**, para facilitar la búsqueda del certificado y que aparezca correctamente en la pantalla de búsqueda, seleccionar como tipo de fichero la opción **Intercambio de información personal (*.pfx, *.p12)** que son los certificados empleados para la identificación de una persona u organización:

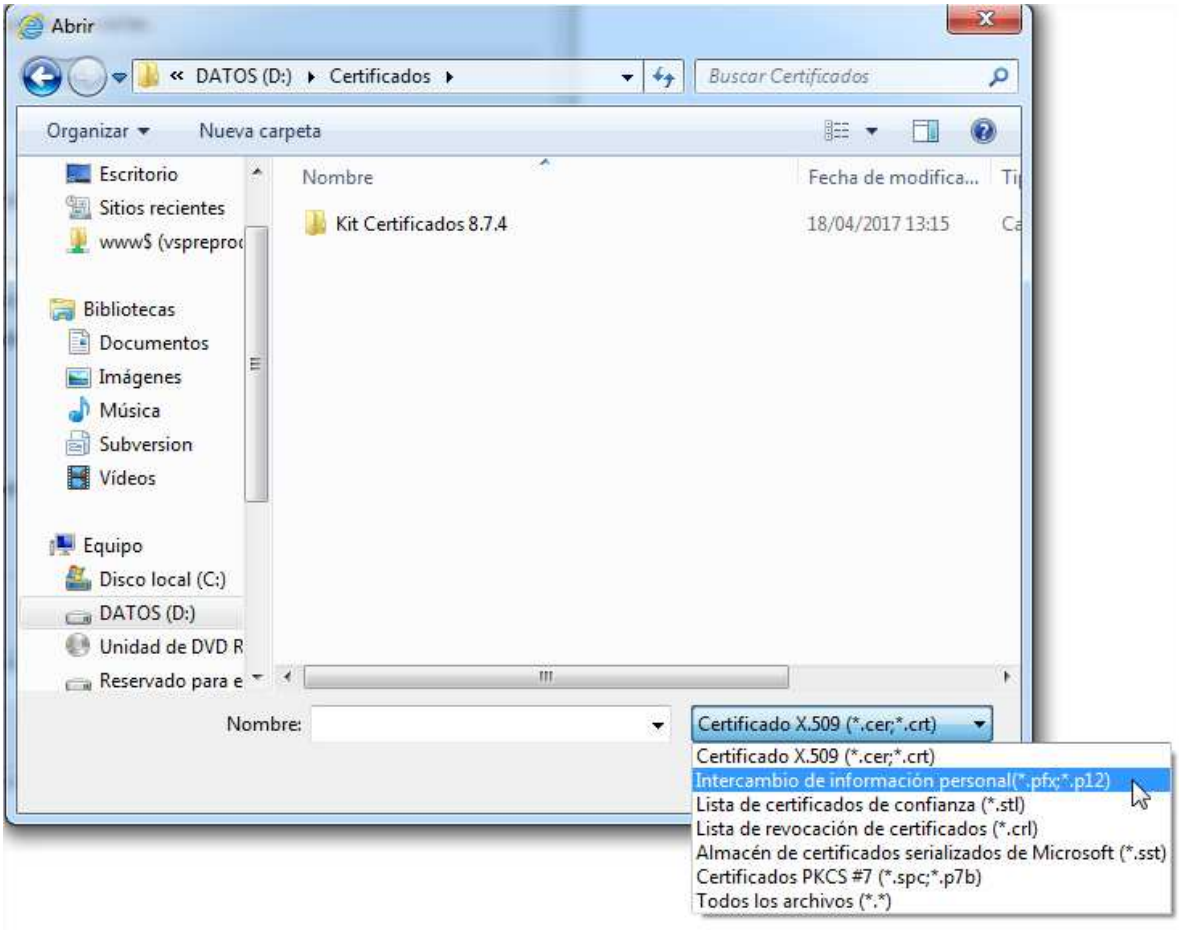

Figura 9: Selección del tipo de fichero a buscar.

Una vez seleccionado el certificado a importar, el proceso es el mismo que el expuesto en el apartado **Ejecutando el Fichero con el Certificado en Windows**.

2.3.3. GOOGLE CHROME

Para importar un certificado en el navegador Google Chrome debe acceder a la configuración de dicho navegador y pulsar el enlace *Mostrar configuración avanzada…* En el apartado HTTPS/SSL pulsar el botón **Administrar certificados**.

Se mostrará la pantalla de la **Figura 8,** donde se muestran los certificados importados. En dicha pantalla, pulsar el botón el botón **Importar**, en ese momento se mostrará la pantalla del asistente de importación de certificados tal y como se muestra en la **Figura 2**, el proceso será el mismo que el explicado en el punto **Ejecutando el Fichero con el Certificado en Windows**, con la salvedad de que en la pantalla de la **Figura 3**, debe seleccionar el fichero pulsando el botón **Examinar**, para facilitar la búsqueda del certificado y que aparezca correctamente en la pantalla de búsqueda, seleccionar como tipo de fichero la opción **Intercambio de información personal (*.pfx, *.p12)** que son los certificados empleados para la identificación de una persona u organización tal y como se muestra en la **Figura 9**.

2.3.4. MOZILLA FIREFOX

El caso de Mozilla Firefox es un poco especial, como hemos visto tanto Internet Explorer como Google Chrome utiliza el almacén de certificados del sistema, pero en el caso de Mozilla Firefox la importación de certificados se realiza sobre su propio almacén de certificados, con lo que si queremos utilizar alguno de los navegadores anteriores y Mozilla Firefox indistintamente debemos importar el certificado en ambos almacenes.

Para importar el certificado en Mozilla Firefox, se debe acceder a las opciones del navegador, ir a la opción **Avanzado** y a la pestaña **Certificados**:

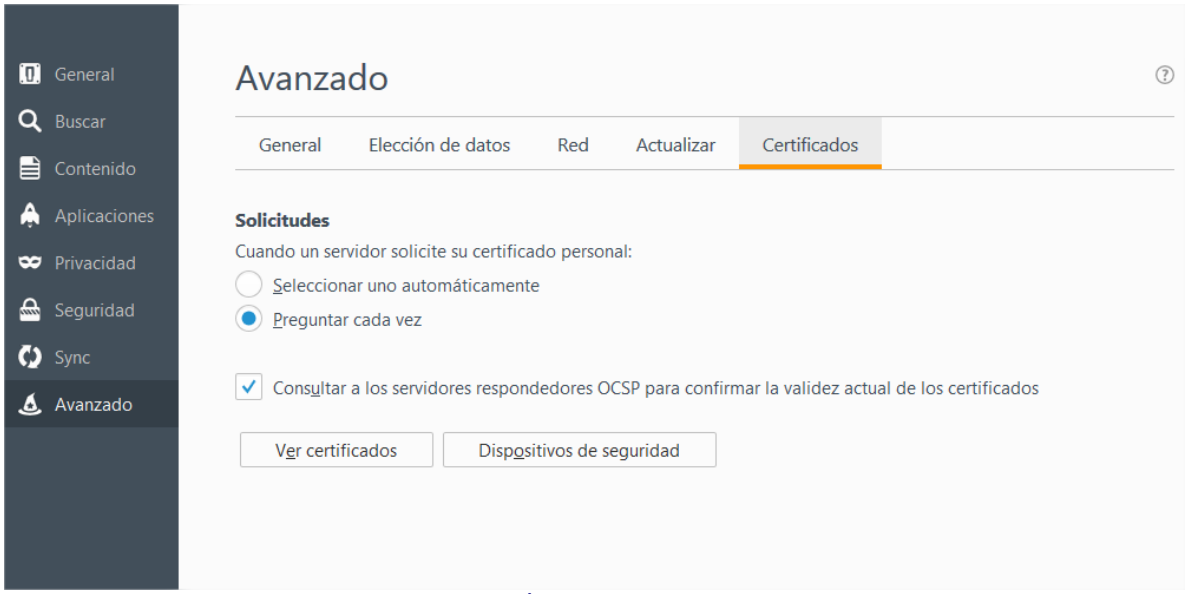

Figura 10: Configuración de Certificados de Mozilla Firefox.

En la pantalla de la figura anterior, pulsar el botón **Ver Certificados**, se abrirá una ventana donde se muestran los certificados importados en el almacén propio de Mozilla Firefox:

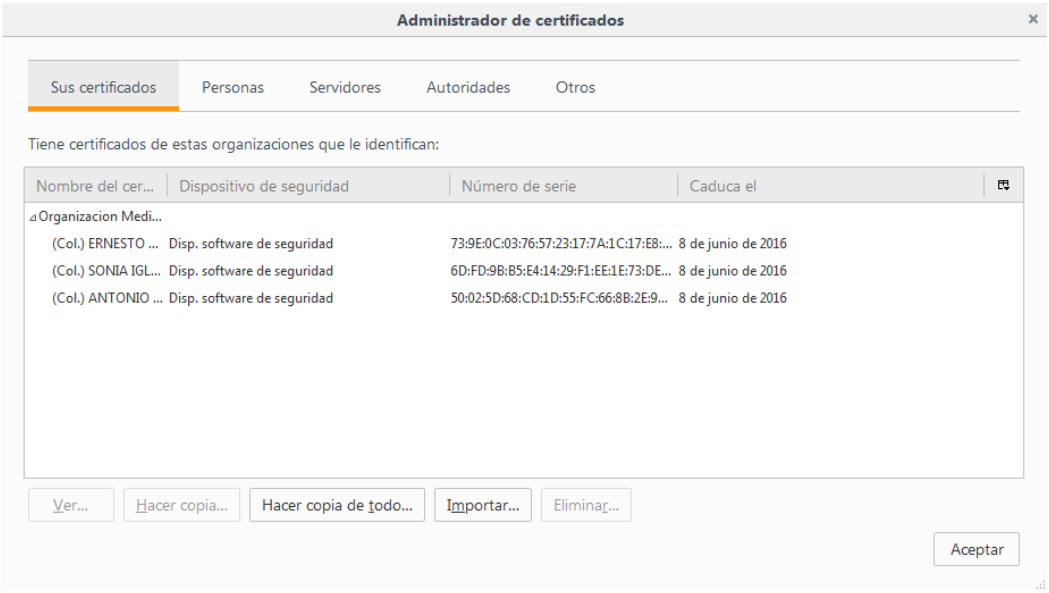

Figura 11: Pantalla con los certificados instalados en Mozilla Firefox

Para importar un nuevo certificado, pulsar el botón **Importar**, se abrirá una pantalla para de selección del certificado:

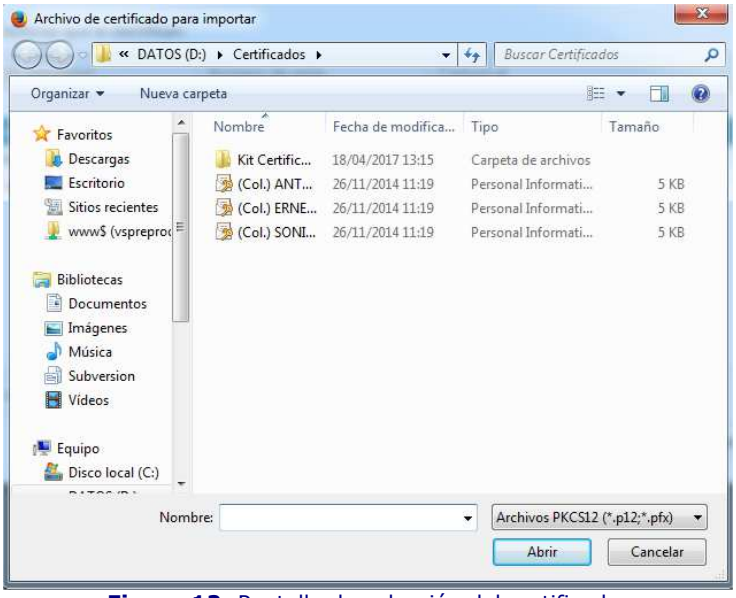

Figura 12: Pantalla de selección del certificado.

En la pantalla de la figura anterior, navegar a la carpeta donde está el certificado, seleccionarlo y pulsar el botón abrir, se mostrará una ventanita para introducir la contraseña del mismo:

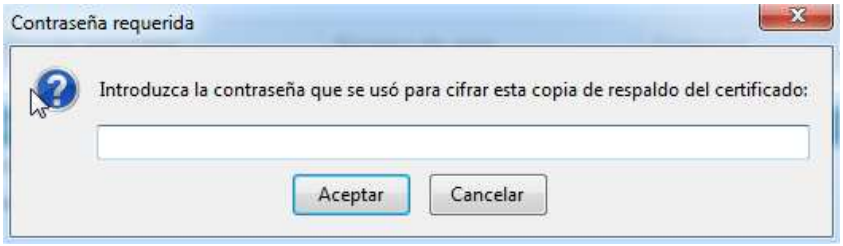

Figura 13: Introducción de la contraseña del certificado

En la pantalla de la figura anterior, introducir la contraseña y pulsar el botón **Aceptar,** se si todo va bien se mostrará un mensaje indicando que se ha importado correctamente el certificado y ya puede ser utilizado para firmar electrónicamente documentos en Mozilla Firefox.

2.3.5. MAC OS X

Si es usuario de MAC OS X de Apple, los certificados se importarán al llavero que el usuario estime conveniente, para ello debe hacer doble click en el fichero que contiene el certificado y se abrirá una ventana para seleccionar el llavero correspondiente, una vez seleccionado, continúe con el proceso y le solicitará la contraseña del certificado, una vez introducida, continuar y el certificado estará disponible para hacer la firma.

Ejecutando "Acceso a Llaveros" y seleccionando el llavero correspondiente en la opción Mis Certificados podremos ver el certificado importado.

2.4. CONFIGURACIÓN DEL NAVEGADORES

Como ya se ha comentado, se recomienda tener instalado las últimas versiones de los navegadores, tanto por temas de compatibilidad como por temas de seguridad. Actualmente, es compatible y está testado para Internet Explorer 11, Mozilla Firefox 53.0, Google Chrome 58.0 y Safari para Windows 5.1.7.

En los citados navegadores, el único con el que podrían ejecutarse los applets para la firma sería en Internet Explorer 11. Para no encontrar problemas el dominio *.jccm.es no debe estar agregado a la vista de compatibilidad del navegador, para saber si está o no agregado, debe ir a la opción Herramientas -> Configuración de vista de compatibilidad

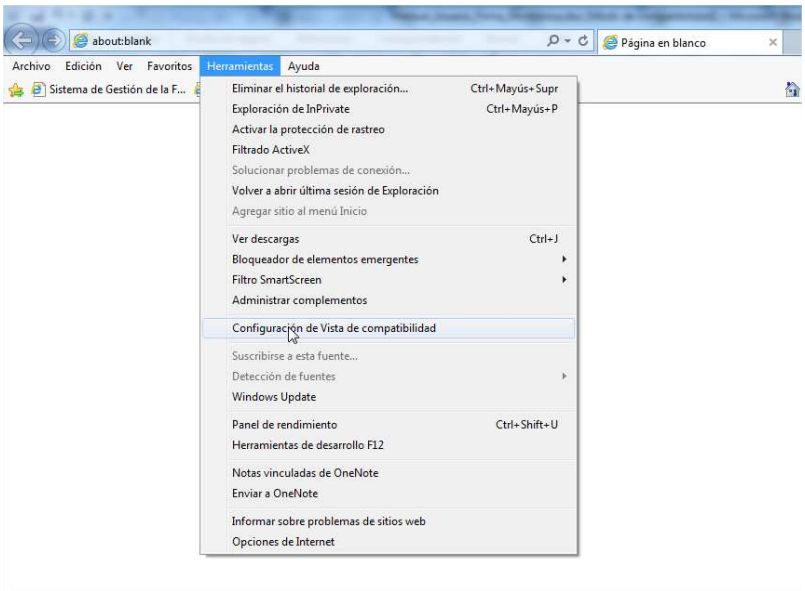

Figura 14: Acceso a la configuración de la vista de compatibilidad

En ese momento se mostrará la siguiente figura:

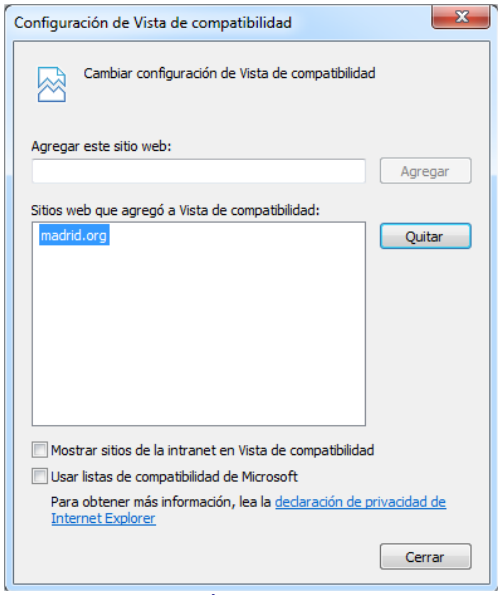

Figura 15: Configuración de la vista de compatibilidad

En la figura anterior, hay que asegurarse que no está jccm.es en la lista "Sitios web que agregó Ha visto de compatibilidad".

3. ADMINISTRACIÓN ELECTRÓNICA EN FOCO

En la nueva versión implantada, tanto la firma electrónica como la utilización del Gestor Documental están incluidas en el Mantenimiento de Solicitudes de Modalidad II.

Todos los elementos de administración electrónica presentes en FOCO están integrados en el proceso de envío de solicitudes.

Hasta ahora, al enviar una solicitud el proceso que se realizaba era:

1. Registrar la solicitud.
2. Actualizar el estado de la solicitud a Enviada.
3. Notificar el envío mediante correo electrónico.

A partir de la implantación de los nuevos elementos de administración electrónica el proceso quedará de la siguiente manera:

1. Registrar la solicitud.
2. Actualizar el estado de la solicitud a Pendiente de Firma.
3. Firma electrónica del PDF mediante Certificado.
4. Comprobación del Certificado.
5. Subida al Gestor Documental del Documento.
6. Actualizar el estado de la solicitud a Enviada.
7. Notificar el envío mediante correo electrónico.

En todo este proceso, el usuario solo tendrá que intervenir para pulsar el botón **Enviar y** para seleccionar el certificado con el que firmará, el resto lo hará el sistema automáticamente.

A continuación se especifica cómo realizar el envío y las diferentes fases por las que irá pasando y mensajes que puede recibir el usuario.

1. Lo primero que debe realizar el usuario es realizar una búsqueda de solicitudes, seleccionar una en estado GRABADA y pulsar el botón **Enviar** y aceptar la confirmación.
2. El sistema comprobará que los datos de la solicitud y acción están completos y son correctos, si no es así, se mostrará un mensaje al usuario y no se realizará ninguna operación.
3. Si las comprobaciones son correctas, se realiza el registro electrónico y se cambia la solicitud a estado PENDIENTE DE FIRMA, en ese momento se mostrará un mensaje indicando al usuario que la solicitud se ha registrado y ha pasado a estado pendiente de firma y que proceda a realizar la firma.
   Si se produce algún problema a la hora de registrar la solicitud en el Registro de la JCCM, se notificará al usuario y la solicitud permanecerá en estado GRABADA.
4. En ese momento, el sistema generará internamente la solicitud de subvención en formato PDF, dependiendo del navegador y la configuración del usuario podrá saltar el applet o Autofirma para realizar la firma, tanto en un caso como el otro, se mostrará una pantalla con los certificados disponibles para hacer la firma.
   Si se ejecutara autofirma el navegador le pedirá permiso para ejecutarla y se mostrará la siguiente pantalla:

Figura 16: Pantalla de lanzamiento de Autofirma

Mientras que si se ejecuta el applet el navegador le pedirá varios permisos para su ejecución:

Figura 17: Permisos para ejecutar el applet para la firma.

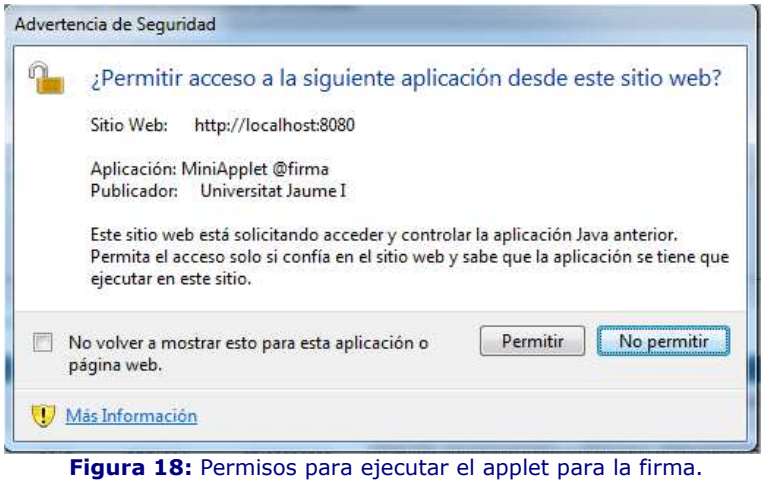

Figura 18: Permisos para ejecutar el applet para la firma.

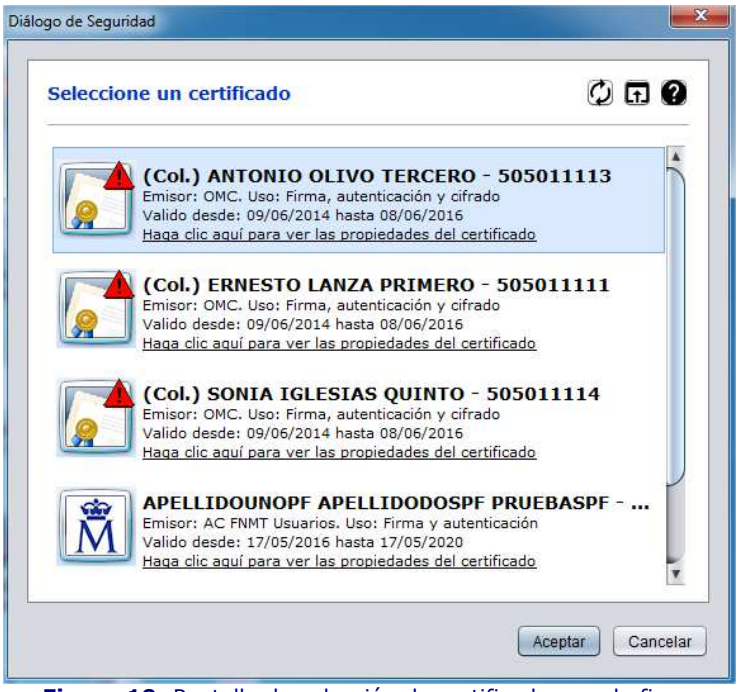

Figura 19: Pantalla de selección de certificado para la firma.

Si el navegador no permite la ejecución de applets y no tiene instalado Autofirma, se notificará esta situación al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
Si no hay ningún certificado instalado, se notificará esta situación al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
Si se produce algún otro error inesperado, se notificará el error al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.

5. Una vez seleccionado el certificado para realizar la firma, se realizará la firma del pdf interno generado y se mostrará un mensaje al usuario indicando que una vez firmado el documento se procederá a hacer comprobaciones y la subida del fichero al Gestor Documental.
6. Se comprobará que el certificado es válido para la firma.
   Si el servicio de validación del certificado no estuviera disponible, se notificará el problema al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
   Si no fuera válido, se notificará el problema al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
7. Se comprobará que la firma realizada también es válida
   Si el servicio de validación de la firma no estuviera disponible, se notificará el problema al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
   Si no fuera válida, se notificará el problema al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
8. Si el certificado y la firma son válidos, se procede al almacenamiento del PDF de la solicitud de subvención en el Gestor Documental.
   Si el servicio del Gestor Documental no está disponible, se notificará el problema al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.
   Si se produce un error al almacenar en el Gestor Documental, se notificará el problema al usuario y la solicitud quedará registrada y en estado PENDIENTE DE FIRMA.

9. Se cambia el estado de la solicitud a ENVIADA.
10. Se envían los correos de notificación de envío de la solicitud.

Como puede observarse, en el proceso de envío no solo interviene FOCO, sino que se intervienen otros sistemas de la JCCM y del MIHAP, por lo que el uso de sistemas externos a FOCO conlleva el riesgo de que estos sistemas no estén disponibles en un momento puntual, de ahí que como se observa en el proceso, se notifiquen los problemas al usuario, la solicitud permanezca en estado PENDIENTE DE FIRMA y se debe comenzar de nuevo el proceso de firma.

En el momento que una solicitud se queda en estado PENDIENTE DE FIRMA, el usuario en cualquier momento puede volver a ejecutar el proceso desde la firma del documento, para ello solo debe realizar una búsqueda y selección de dicha solicitud en estado PENDIENTE DE FIRMA y pulsar el botón **Firmar**, se desencadenará el proceso de envío pero desde el **paso 4** del listado anterior, siendo el resultado el mismo que el del envío.