GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

Formulario de Contacto

Guía de Primeros Pasos

Versión 1.0
MARZO 2020

INDICE

1. IDENTIFICACION Y FIRMA

Para acceder al formulario de contacto es necesario identificarse previamente mediante alguno de los siguientes mecanismos:

- **Autofirma**, que permite utilizar certificados electrónicos o tarjetas inteligentes instaladas en el equipo del usuario.

- **Cl@ve**, que permite utilizar certificados en la nube, de uso compartido para toda la Administracion General del Estado.

2. AUTOFIRMA

Se trata de una aplicación de escritorio, que debe estar instalada previamente en el equipo, y que permite la identificación de los usuarios mediante un certificado electrónico instalado en su equipo o en tarjeta inteligente.

Se permite el uso de cualquier certificado electrónico reconocido, conforme a lo establecido en la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas. En resumen, se permite el uso de certificados electrónicos de las principales Autoridades de Certificación: DNI electrónico, FNMT, CATCERT, IZENPE, ACCV, CAMERFIRMA, ANF, ACA, ANCERT, FIRMAPROFESIONAL, etc.

> **NOTA**: Para garantizar el correcto funcionamiento del certificado de usuario, deberá seguir las instrucciones de configuración e instalación proporcionadas por la Autoridad de Certificación que emitió el certificado o tarjeta inteligente.
>
> Es recomendable revisar que los certificados que vaya a utilizar no estén caducados o revocados, eliminando del almacén de certificados aquellos que no sean válidos, para evitar errores dentro de la aplicación.

2.1.1. Instalación de Autofirma

La última versión de Autofirma puede descargarse de la siguiente página:

> http://firmaelectronica.gob.es/Home/Descargas.html

El asistente de instalación guía a través de unos sencillos pasos. Se recomienda dejar la ruta que se muestra por defecto. En caso de modificar el directorio de instalación por defecto, debe instalarse AutoFirma en un directorio propio y no en uno compartido con más aplicaciones o documentos.

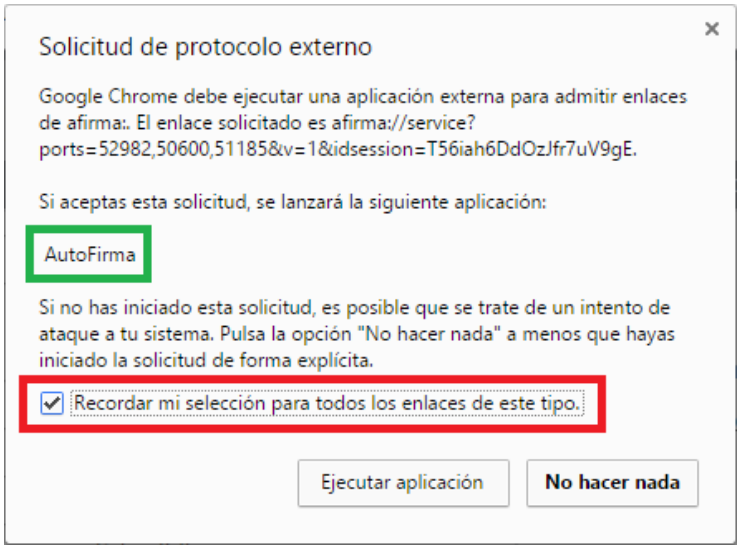
> **NOTA:** La instalación de AutoFirma en Microsoft Windows debe ser realizada siempre por un usuario con permisos de Administrador.

2.1.2. Primer uso de Autofirma

La primera vez que se utiliza Autofirma se muestran varias advertencias de seguridad, que varían en función del navegador utilizado, y que pueden desactivarse fácilmente.

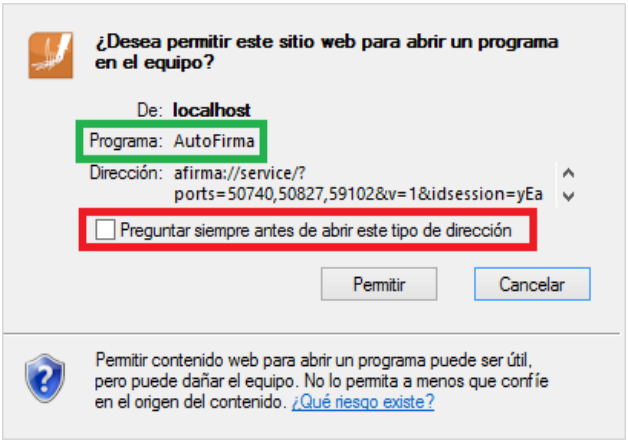
2.1.2.1. Google Chrome

La siguiente ventana se muestra para permitir la llamada a la aplicación Autofirma. Se mostrará cada vez que se realice la identificación de usuario, salvo que se marque la casilla señalada en rojo.



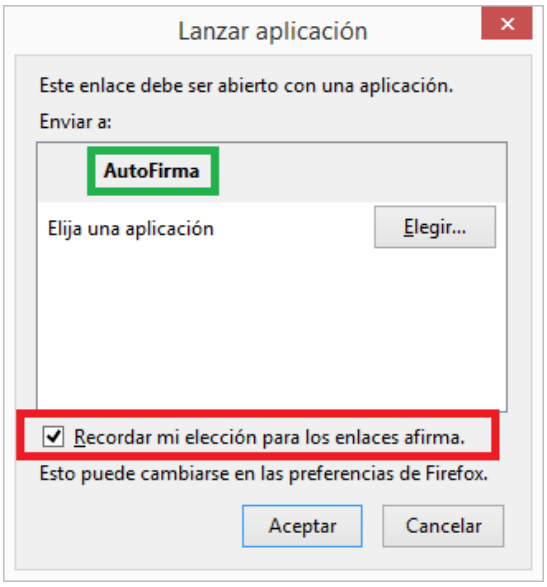
2.1.2.2. Internet Explorer

En Internet Explorer se muestra la siguiente ventana para permitir la llamada a la aplicación Autofirma. Se mostrará cada vez que se utilice, salvo que se desmarque la casilla señalada en rojo.



2.1.2.3. Mozilla Firefox

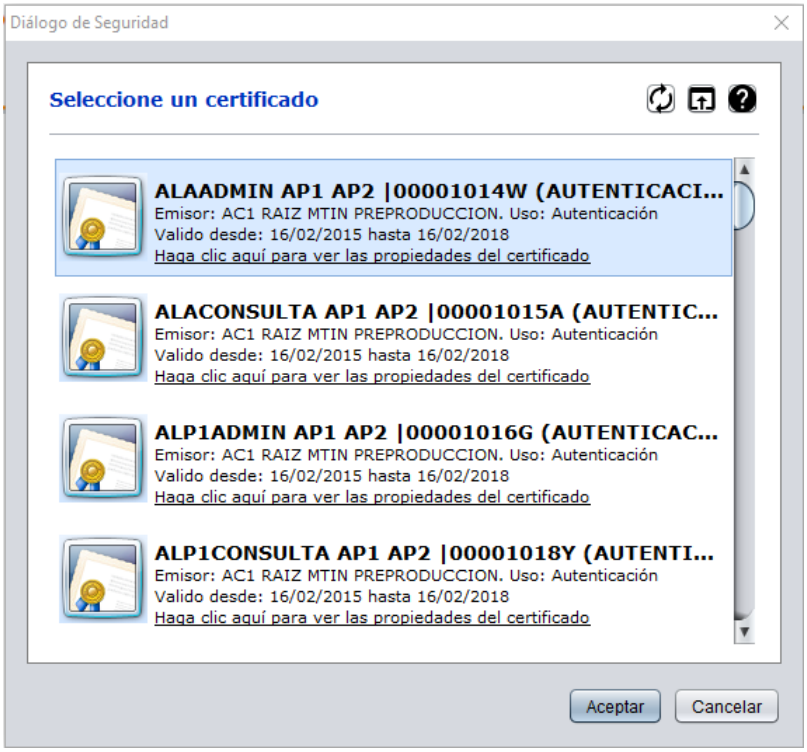
La siguiente ventana se muestra para permitir la llamada a la aplicación Autofirma. Se mostrará cada vez que se utilice, salvo que se marque la casilla señalada en rojo.



2.1.3. Carga de Autofirma

Una vez dados los permisos necesarios para la ejecución de Autofirma, se mostrará la siguiente pantalla de carga cada vez que se utilice:

, y a continuación se solicitará al usuario un certificado válido:



El certificado seleccionado será el utilizado para identificar al usuario mediante su NIF.

NOTA: Autofirma no almacena ningún tipo de información personal del usuario, ni hace uso de cookies ni ningún otro mecanismo para la gestión de datos de sesión. Autofirma sí almacena trazas de su última ejecución a efectos de ofrecer soporte al usuario si se encontrase algún error. Estas trazas de ejecución no contienen ningún tipo de información personal y la aplicación no facilita de ninguna forma el acceso a estos datos almacenados.

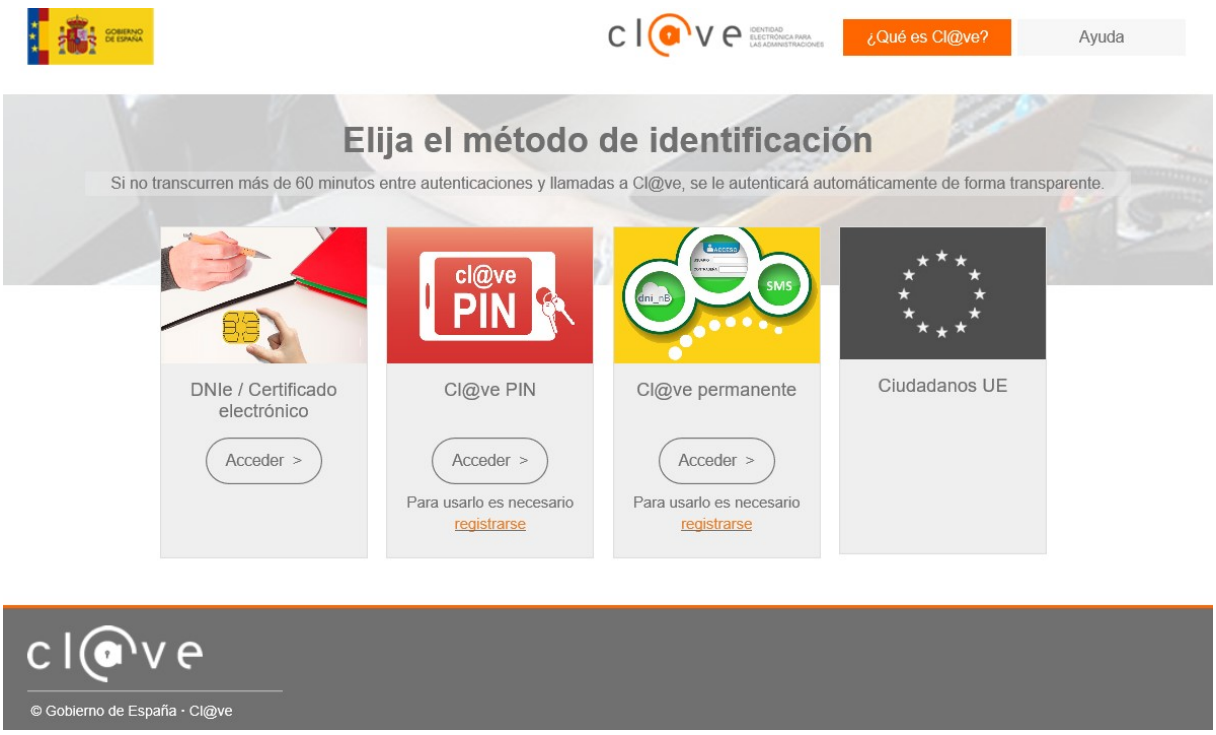
3. CL@VE

Cl@ve es la plataforma común del Sector Público Estatal para la identificación y firma electrónica mediante el uso de credenciales almacenadas de manera segura en la nube (no están almacenadas en el equipo del usuario).

Al tratarse de servicios en la nube, no es necesaria configuración previa del equipo del usuario para su utilización.

3.1. Cl@ve Identificación

Al pulsar la opción de acceso con Cl@ve la aplicación redirige automáticamente a la plataforma Cl@ve Identificación:



Podrá utilizarse cualquiera de los siguientes mecanismos de identificación:

- **DNIe / Certificado Electrónico**: de manera similar al Cliente @Firma, permite el uso de certificados electrónicos o tarjetas inteligentes disponibles localmente en el equipo del usuario

- **Cl@ve PIN**: está basado en el uso de un código elegido por el usuario y un PIN comunicado al teléfono mediante la app Cl@ve PIN o con un mensaje SMS.

  Es muy sencillo ya que no es necesario recordar una contraseña de forma permanente. Además, su validez es limitada en el tiempo, lo que hace que sea más seguro.

  Es obligatorio registrarte previamente en el sistema.

- **Cl@ve permanente**: es un sistema de identificación diseñado para personas que necesitan acceder frecuentemente. Se basa en el uso de un código de usuario, su DNI o NIE, y de una contraseña que se establece en el proceso de activación.

  Es obligatorio registrarse previamente en el sistema.

Tras seleccionar el método de identificación a utilizar, la plataforma Cl@ve redirigirá de manera automática al servicio correspondiente.

NOTA: Para obtener más información sobre la plataforma Cl@ve, y realizar el registro previo obligatorio, debe visitar la siguiente página: http://clave.gob.es

4. CONFIGURACIÓN DEL NAVEGADOR

Si el formulario de contacto no funciona correctamente revise los siguientes puntos en la configuración del navegador de Internet que esté utilizando.

4.1. Google Chrome

Requisito	Opción de menú	Valores
Activar JavaScript	Configuración > "Mostrar opciones avanzadas…" > (Privacidad) botón "Configuración de contenido…" > **Javascript**	Seleccionar: Permitir que todos los sitios ejecuten JavaScript (recomendado)
Comprobar certificado de usuario *(si no se utiliza Cl@ve)*	Configuración > "Mostrar opciones avanzadas" > (HTTP/SSL) botón "Administrar certificados…" > Pestaña "Personal" > Botón "Ver" > Pestaña "**Ruta de certificación**"	"Estado del certificado" debe ser: "Certificado válido"

4.2. Internet Explorer

Requisito	Opción de menú	Valores
Activar JavaScript	Herramientas > Opciones de Internet > Pestaña "Seguridad" > Icono "Sitios de confianza" > Botón "Nivel personalizado…" > Opción **Automatización**	"Active scripting": Habilitar
Comprobar certificado de usuario *(si no se utiliza Cl@ve)*	Herramientas > Opciones de Internet > Pestaña "Contenido" > Botón "Certificados" > Pestaña "Personal" > Seleccionar certificado > Botón "Ver" > Pestaña "**Ruta de certificación**"	El estado del certificado debe ser: "Certificado válido"
Sitios confianza	Herramientas > Opciones de Internet > Pestaña "Seguridad" > Icono "Sitios de confianza" > Botón "Sitios"	Agregar la siguiente dirección: https://expinterweb.empleo.gob.es/formugab

4.3. Mozilla Firefox

4.3.1. Certificados FNMT

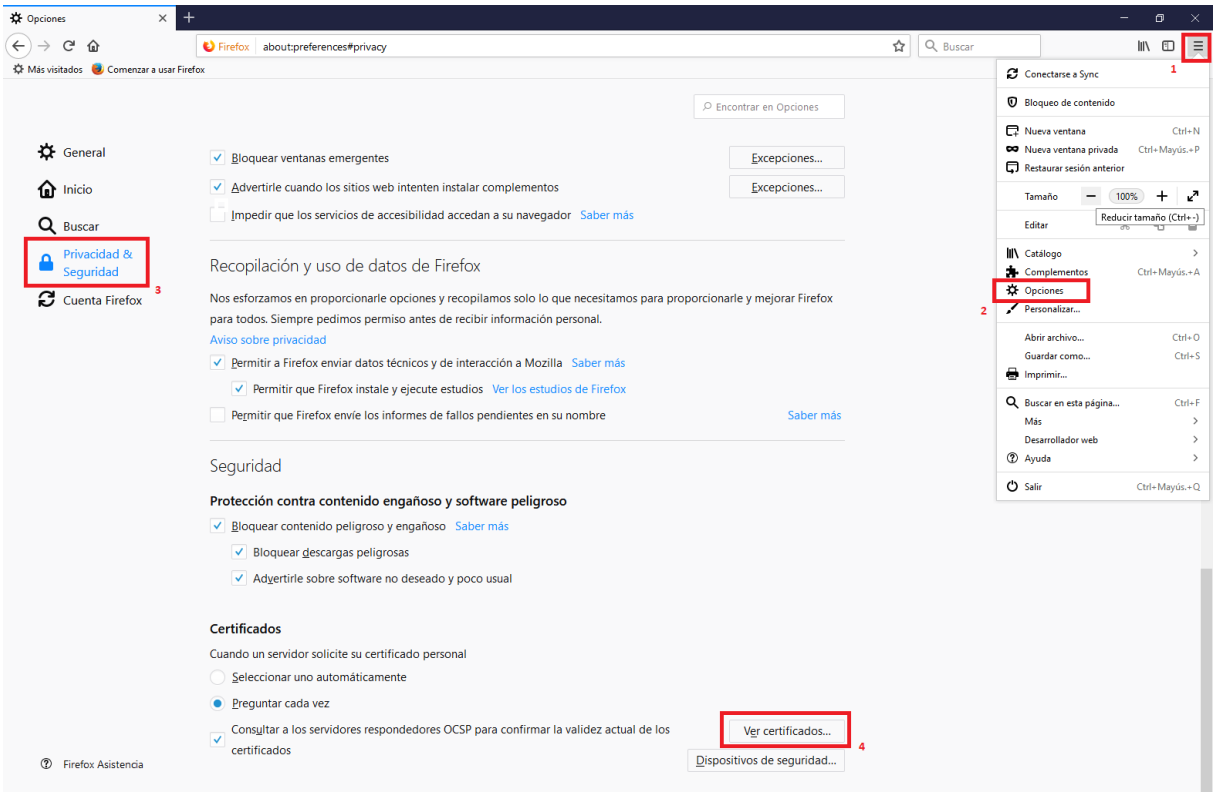
En Firefox, si se va a utilizar un certificado de la FNMT para identificarse, es necesario instalar previamente en el navegador los siguientes certificados raíz:

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

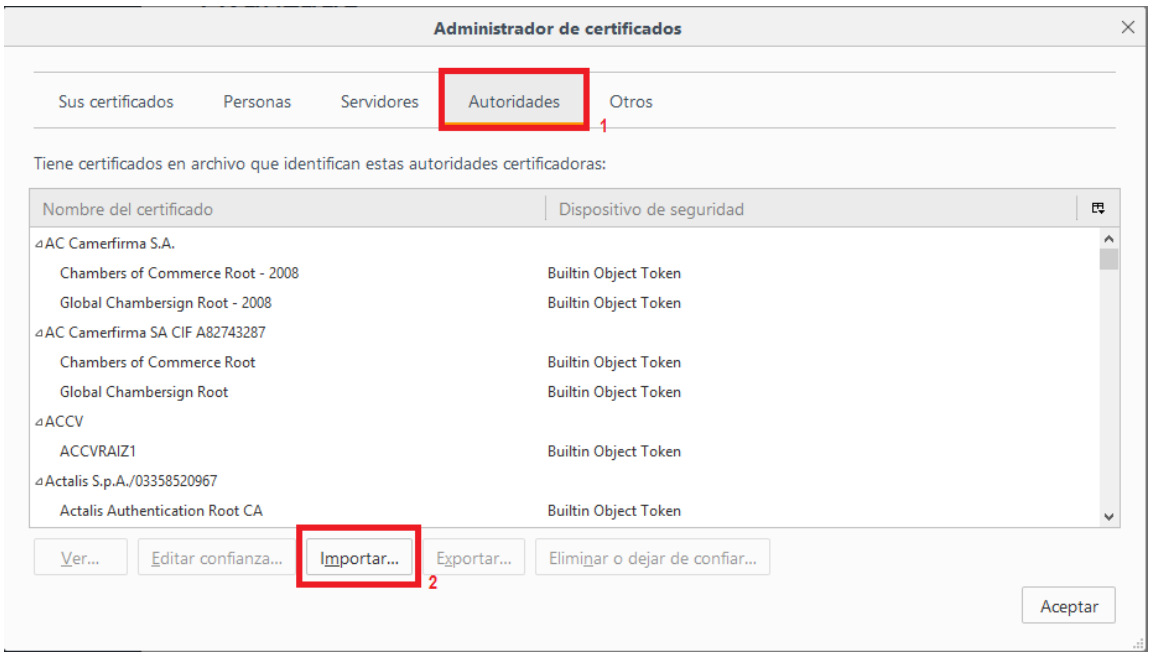
AC Componentes Informáticos:
https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_Componentes_Informaticos_SHA256.cer

Una vez descargados en el equipo, deben seguirse los siguientes pasos para su instalación en Firefox.

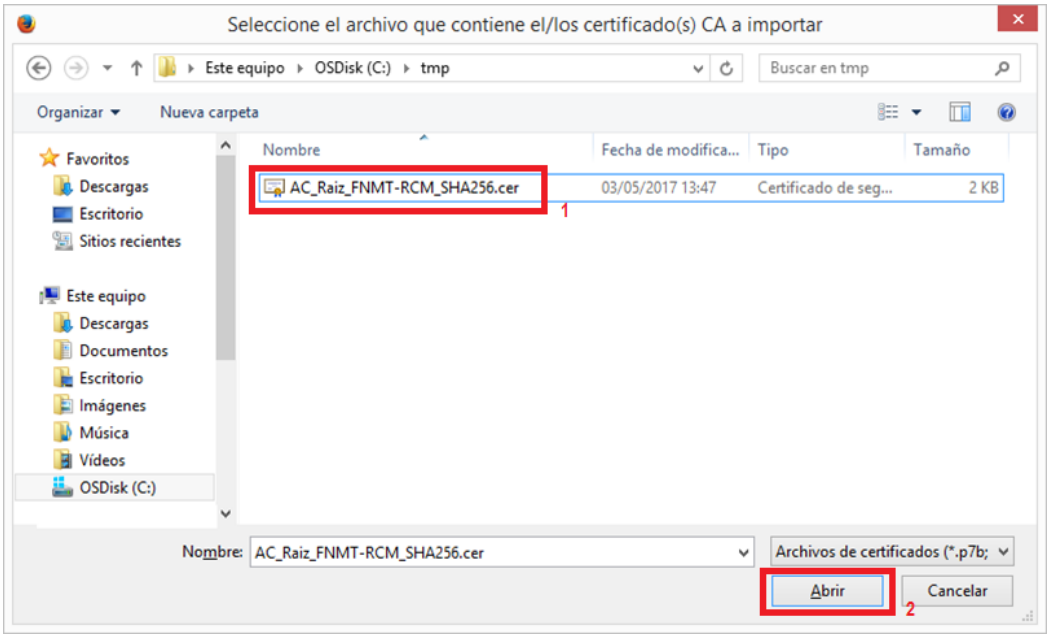
- Abrir el navegador Firefox y acceder a *Opciones* → *Privacidad & Seguridad* → *Certificados* → *Ver certificados…*



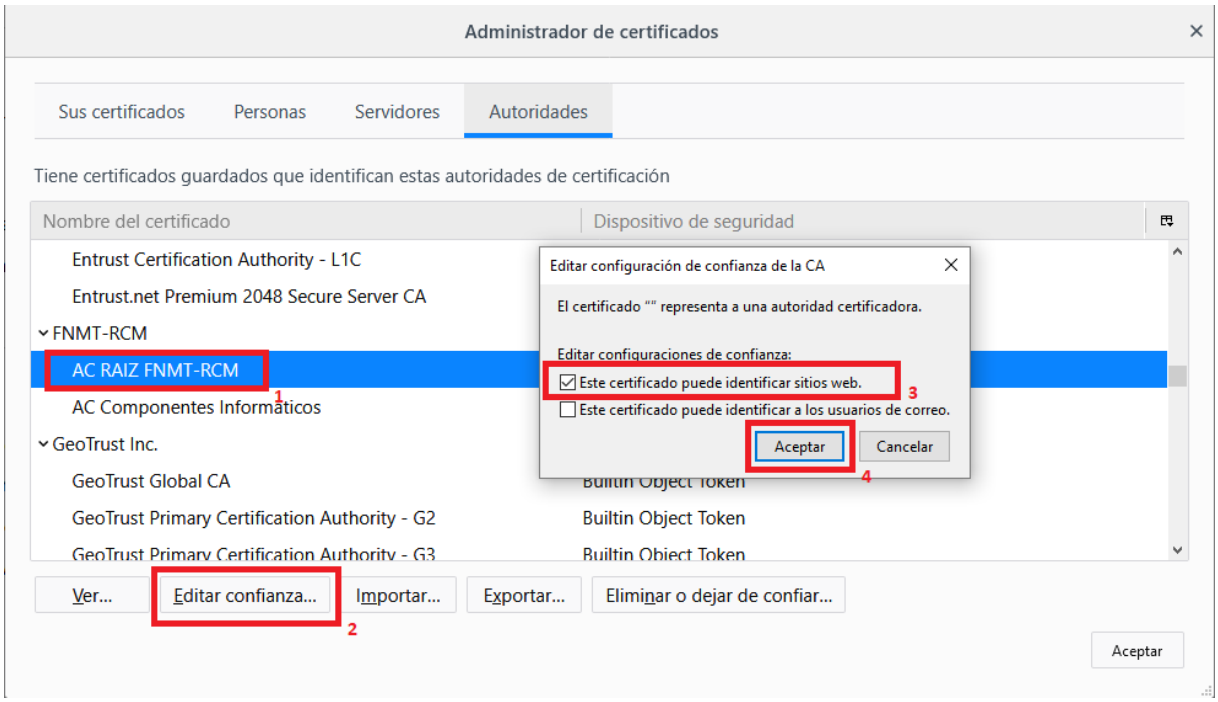
- Seleccionar la pestaña Autoridades y pulsar el botón Importar.



- Seleccionar la ubicación del certificado “AC Raíz FNMT-RCM” y pulsar el botón Abrir.



- Una vez importado el certificado, comprobar que está marcada la confianza para identificar sitios web.



- Realizar los mismos pasos para el certificado “AC Componentes Informáticos”.

Si la aplicación no funciona correctamente en este navegador, revise los siguientes puntos:

Requisito	Opción de menú	Valores
Activar JavaScript	Escribir en la barra de direcciones “about:config” > Pulsar “Enter” > Pulsar "¡Tendré cuidado, lo prometo!" > Modificar opción “javascript.enabled” > Pulsar "Recargar esta página"	javascript.enabled = true
Comprobar certificado de usuario *(si no se utiliza Cl@ve)*	Herramientas > Opciones > Pestaña “Avanzado” > Pestaña “Certificados” > Botón “Ver Certificados” > Pestaña “Sus certificados” > Seleccionar certificado > Botón “Ver” > Pestaña General	El estado del certificado debe ser “Verificado”