GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

SERPA
Servicios de Prevención Ajenos

Guía de Configuración Previa

ENERO 2020

INDICE

1. INTRODUCCIÓN 3
2. REQUISITOS MINIMOS 4
3. IDENTIFICACION DE USUARIOS 5
3.1. Acceso con AUTOFIRM@ 6
3.2. Acceso con CL@VE 7
3.3. Acceso con Autenticación Centralizada 8
4. CONFIGURACIÓN DEL NAVEGADOR 10
4.1. Internet Explorer 10
4.2. Mozilla Firefox 11
4.3. Google Chrome 14
5. RESOLUCIÓN DE PROBLEMAS 15
5.1. Limpieza de Caché del Navegador 15
INTERNET EXPLORER 15
MOZILLA FIREFOX 16
GOOGLE CHROME 17

1. INTRODUCCIÓN

Para comenzar a utilizar la aplicación SERPA, es necesario llevar a cabo una serie de pasos de configuración previos. En esta guía se detallan:

- Requisitos de uso.
- Diferentes tipos de acceso a la aplicación.
- Ayudas para la configuración y el uso de certificados electrónicos en el navegador.
- Tablas resumen con diferentes comprobaciones a realizar en caso de que la aplicación no funcione correctamente en su navegador.

2. REQUISITOS MINIMOS

Para utilizar SERPA en su ordenador necesitará contar con al menos estos requisitos:

- **Sistema Operativo**
  - Windows 7 SP1 / 8 / 8.1 / 10
- **Navegador web**
  - Internet Explorer 11
  - Mozilla Firefox 45 o superior
  - Google Chrome 46 o superior
  - No es compatible con Microsoft Edge
- **Resolución recomendada de pantalla:** 1920x1080

3. IDENTIFICACION DE USUARIOS

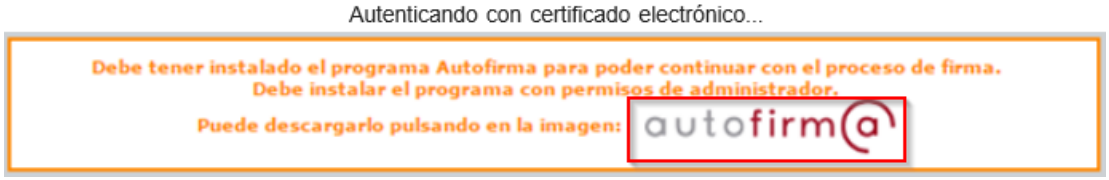
El acceso a la aplicación se realizará a través del portal público de la misma. A continuación se pueden observar el aspecto que presenta dicho portal.

Los usuarios registrados en el sistema pueden realizar el acceso a la aplicación mediante alguna de las siguientes opciones:

3.1. Acceso con AUTOFIRM@

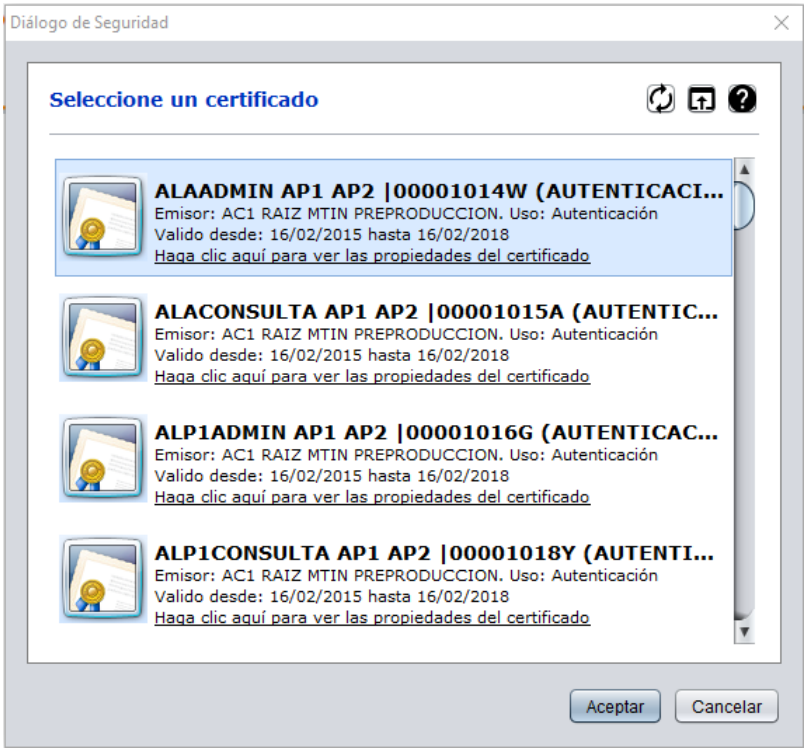
Permite que el usuario se identifique mediante un certificado electrónico disponible en su equipo, mediante la aplicación Autofirm@, que deberá estar instalada previamente en su equipo.

En caso de que el usuario no tenga instalada la aplicación Autofirm@ deberá seleccionar el enlace para su descarga e instalación.



Al pulsar la opción de “Acceso con autofirm@” se mostrará la pantalla de carga de la aplicación:

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



Se puede obtener información adicional de Autofirm@ pulsando en el logo que aparece en la página principal de la aplicación.

SERPA permite el uso de certificados electrónicos reconocidos, que estén admitidos por la plataforma @Firma del Ministerio de Hacienda y Administraciones Públicas, conforme a lo establecido en la Ley 59/2003 de Firma Electrónica y la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas.

En concreto, SERPA permite el uso de certificados electrónicos emitidos por: FNMT, DNI electrónico, CATCERT, IZENPE, ACCV, CAMERFIRMA, ANF, ACA, ANCERT, FIRMAPROFESIONAL, etc.

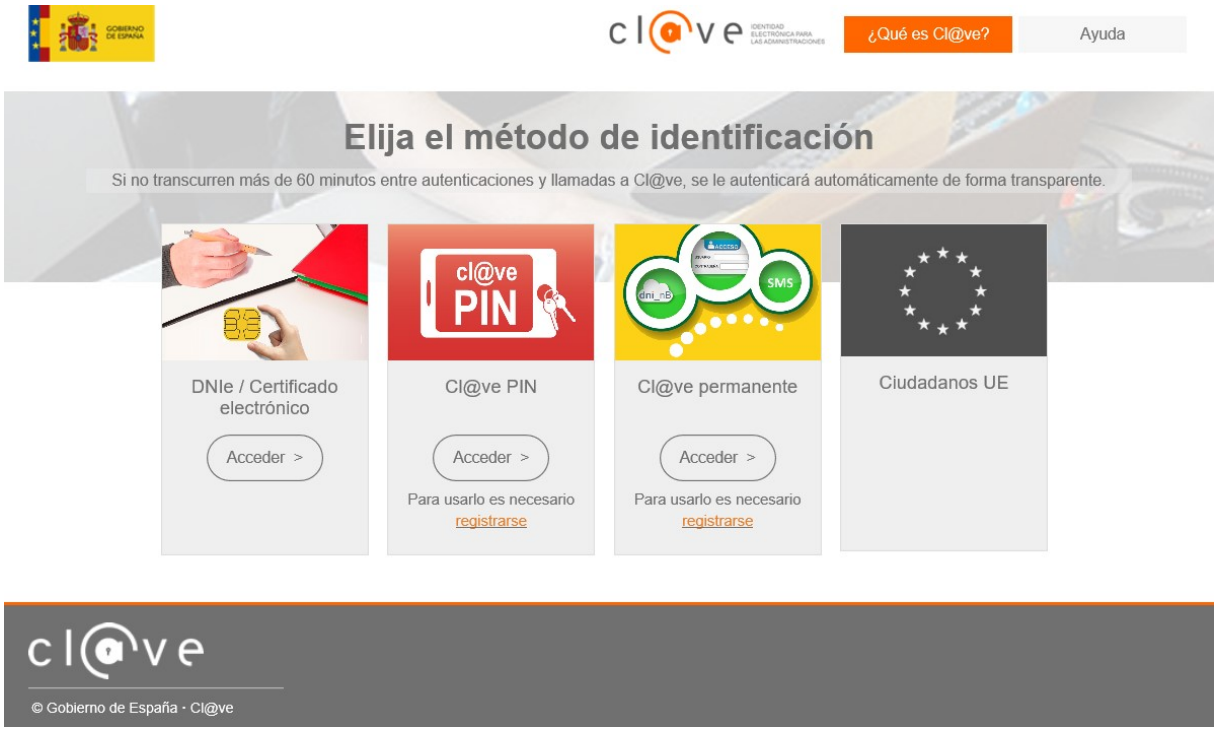
Para garantizar el correcto funcionamiento del certificado de usuario, deberá seguir las instrucciones de configuración e instalación proporcionadas por la Autoridad de Certificación que emitió el certificado o tarjeta inteligente.

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 en la firma dentro de la aplicación.

3.2. Acceso con CL@VE

Permite que el usuario se identifique a través de la plataforma Cl@ve Identificación del Ministerio de Hacienda y Administraciones Públicas, donde debe estar registrado previamente.

Al pulsar la opción de “Acceso con Cl@ve” la aplicación nos redirigirá automáticamente a la plataforma de Cl@ve Identificación:

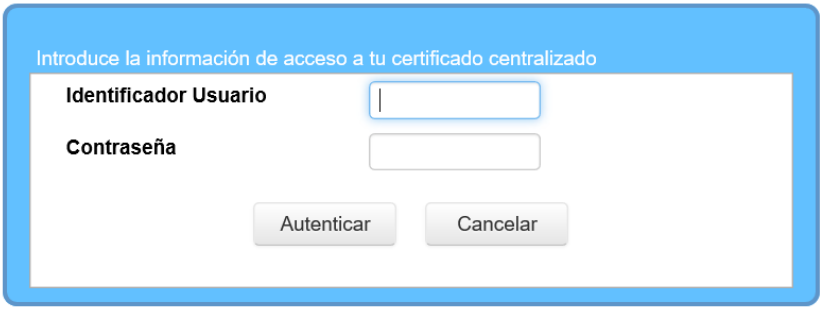


La plataforma Cl@ve permite tres tipos distintos de acceso: con Certificado Electrónico, Cl@ve PIN y/o Cl@ve permanente. Tras seleccionar el método para autenticarse en Cl@ve, la plataforma redirigirá de manera automática de nuevo a la aplicación.

Se puede obtener información adicional de Cl@ve pulsando en el logo que aparece en la página principal de la aplicación.

3.3. Acceso con Autenticación Centralizada

El servicio de Autenticación Centralizada permite a usuarios internos el acceso a la aplicación mediante el uso de un certificado centralizado de empleado público:



Para más información sobre la configuración de este servicio, puede acceder al **Portal de gestión de certificados centralizados**, publicado en la intranet dentro del apartado de Certificados electrónicos.

4. CONFIGURACIÓN DEL NAVEGADOR

Para el correcto funcionamiento de la aplicación, debe revisar y configurar los siguientes puntos en el navegador de Internet que vaya a utilizar.

4.1. Internet Explorer

En Internet Explorer **deben añadirse las siguientes direcciones a la lista de "Sitios de confianza":**

- **Producción**
  - https://expinterweb.mitramiss.gob.es

- **Pruebas**
  - https://preinterweb.mitramiss.gob.es

Si la aplicación siguiera sin funcionar correctamente, revise los siguientes puntos:

Requisito	Opción de menú	Valores
Comprobar certificado de usuario (cadena de confianza)	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"
Activar JavaScript	Herramientas > Opciones de Internet > Pestaña "Seguridad" > Icono "Sitios de confianza" > Botón "Nivel personalizado…" > Opción **Automatización**	"Active scripting": Habilitar

4.2. Mozilla Firefox

Para validar correctamente el certificado de servidor de SERPA, es necesario instalar los siguientes certificados raíz de la FNMT en Firefox:

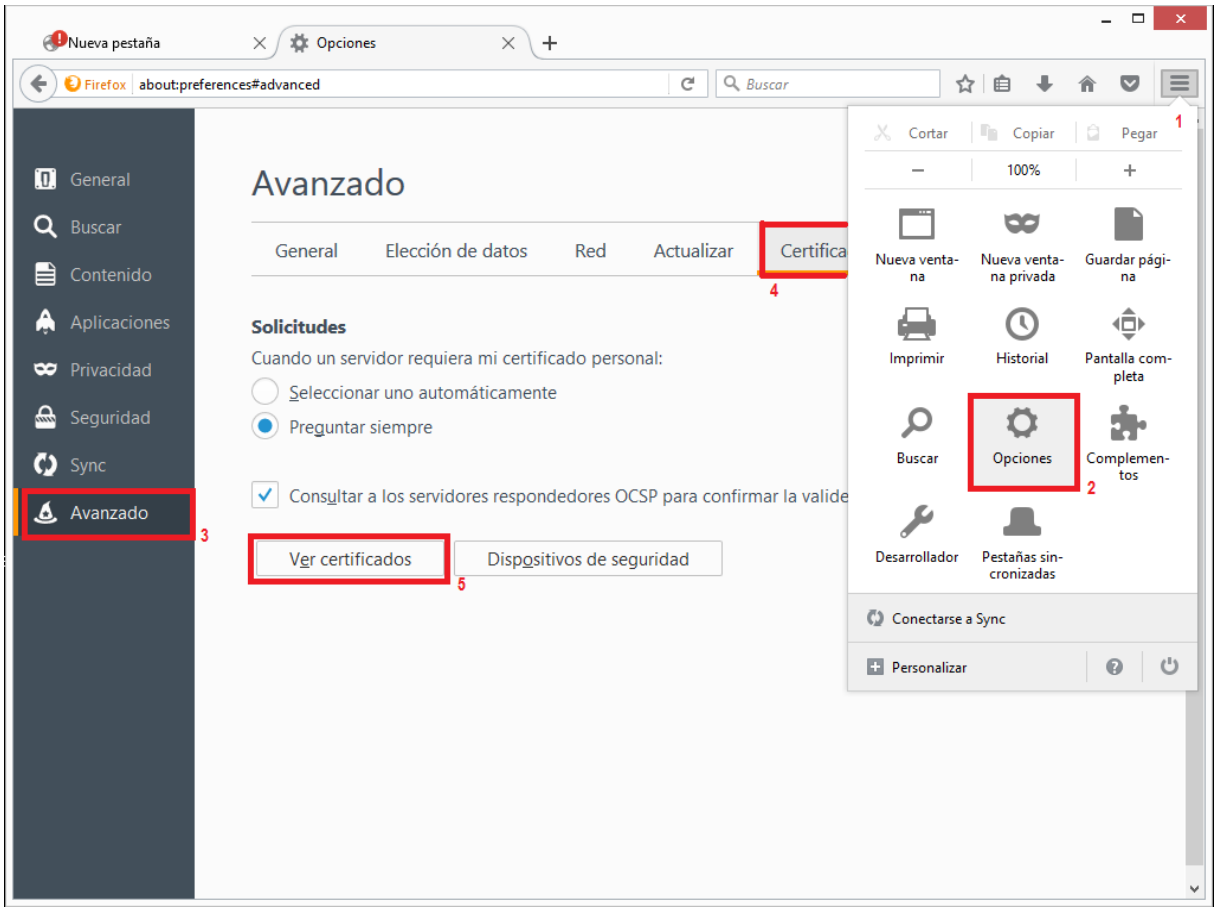
AC Raíz FNMT-RCM:
https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_Raiz_FNMT-RCM_SHA256.cer

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

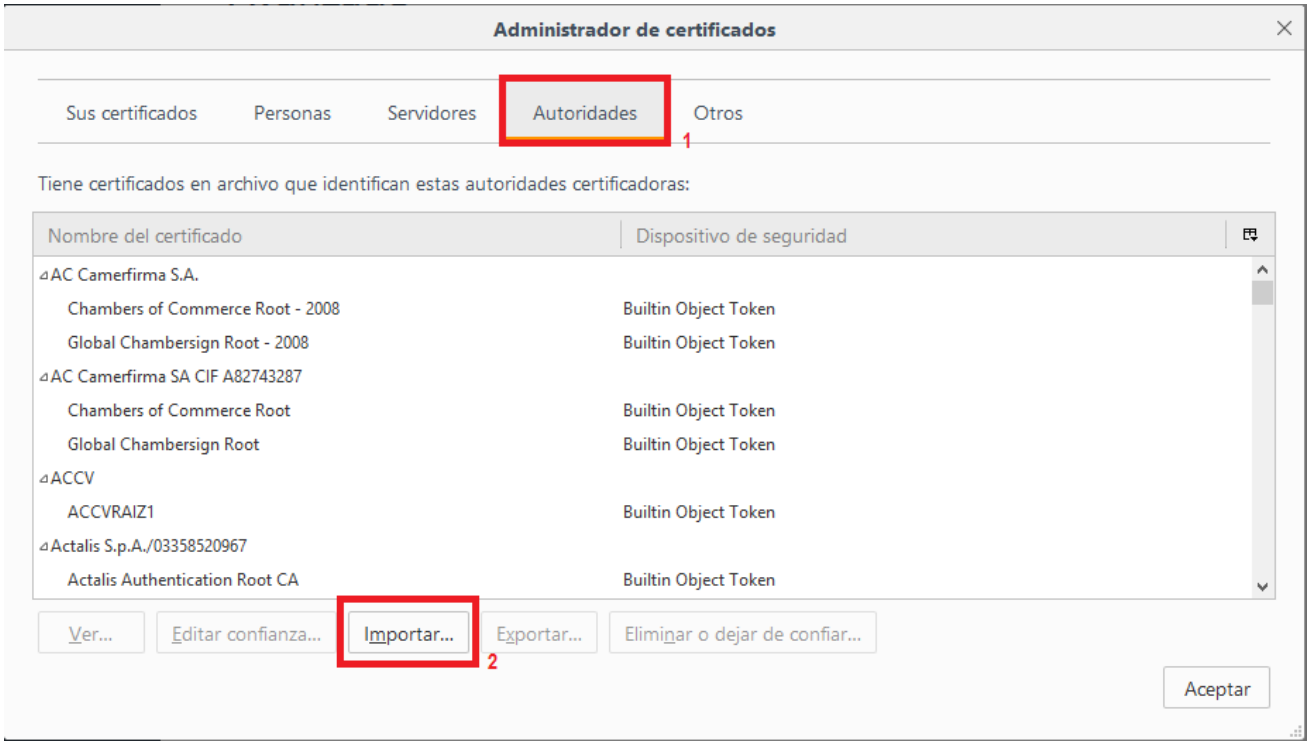
Una vez descargados los certificados en el equipo, deben seguirse estos pasos para su instalación en Firefox:

- Abrir Firefox y acceder a:

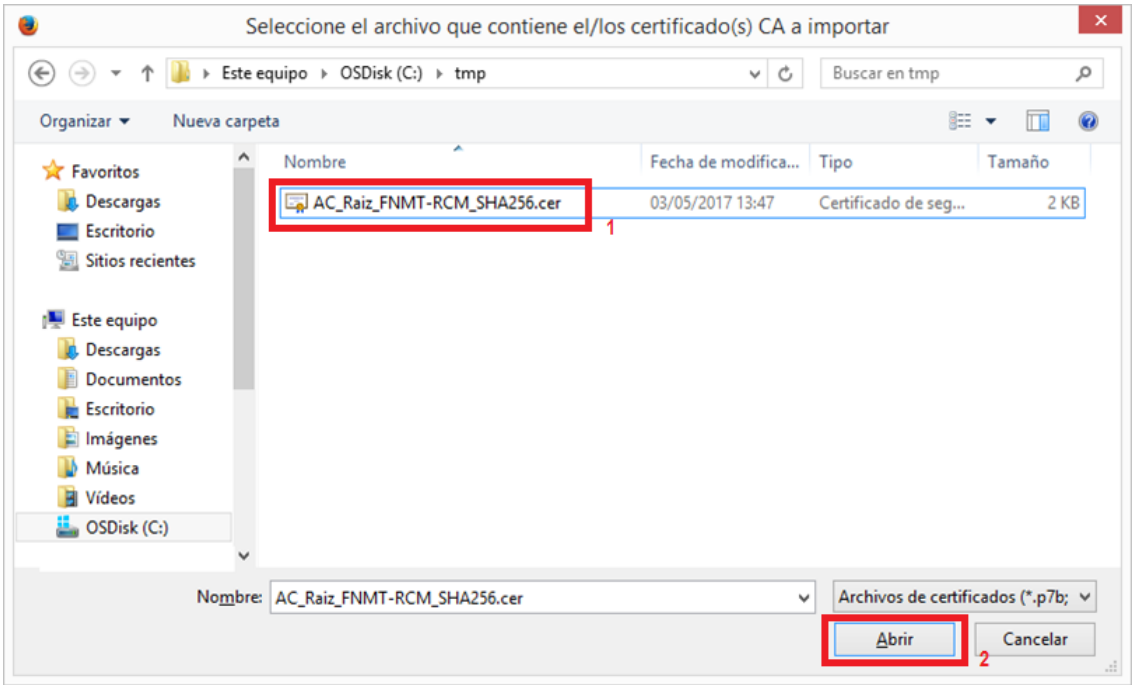
  Herramientas → Opciones → Avanzado → Cifrado o Certificados → Ver certificados



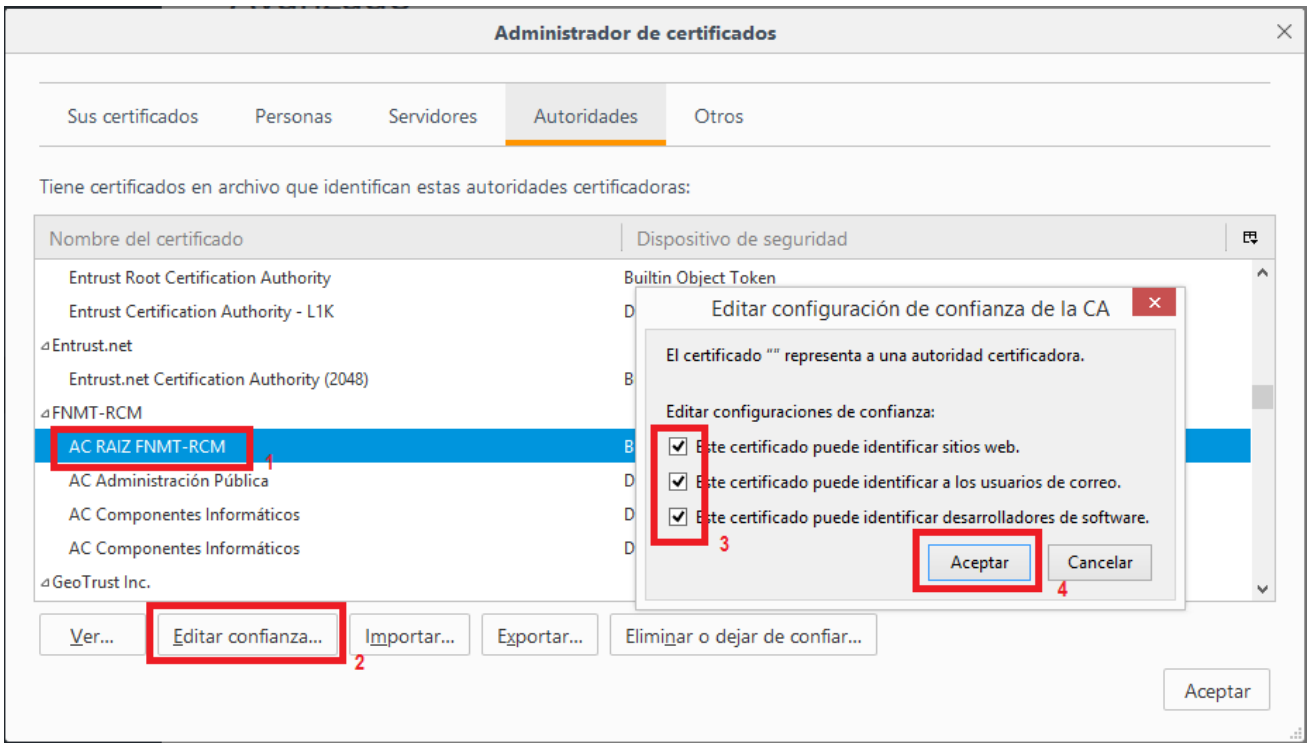
- Seleccionar la pestaña Autoridades y pulsar el botón Importar.



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



- Marcar las casillas correspondientes a los diferentes propósitos y pulsar el botón Aceptar.



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

Si la aplicación continúa sin funcionar correctamente, revise los siguientes puntos:

Requisito	Opción de menú	Valores
Comprobar certificado de usuario (cadena de confianza)	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”
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

4.3. Google Chrome

Si la aplicación no funciona correctamente en Google Chrome, debe revisar los siguientes puntos:

Requisito	Opción de menú	Valores
Comprobar certificado de usuario (ruta de certificación)	Configuración > "Mostrar opciones avanzadas" > (HTTP/SSL) botón "Administrar certificados…" > Pestaña "Personal" > Botón "Ver" > Pestaña "**Ruta de certificación**"	"Estado del certificado" debe ser: "Certificado válido"
Desactivar el bloqueo de elementos emergentes	Configuración > "Mostrar opciones avanzadas…" > (Privacidad) botón "Configuración de contenido…" > **(Pop-ups)** No permitir que ningún sitio muestre pop-ups > botón "Administrar Excepciones"	Agregar: **Producción** [*.]expinterweb.mitramiss.gob.es **Pruebas** [*.]preinterweb.mitramiss.gob.es
Activar JavaScript	Configuración > "Mostrar opciones avanzadas…" > (Privacidad) botón "Configuración de contenido…" > **Javascript**	Seleccionar: Permitir que todos los sitios ejecuten JavaScript (recomendado)

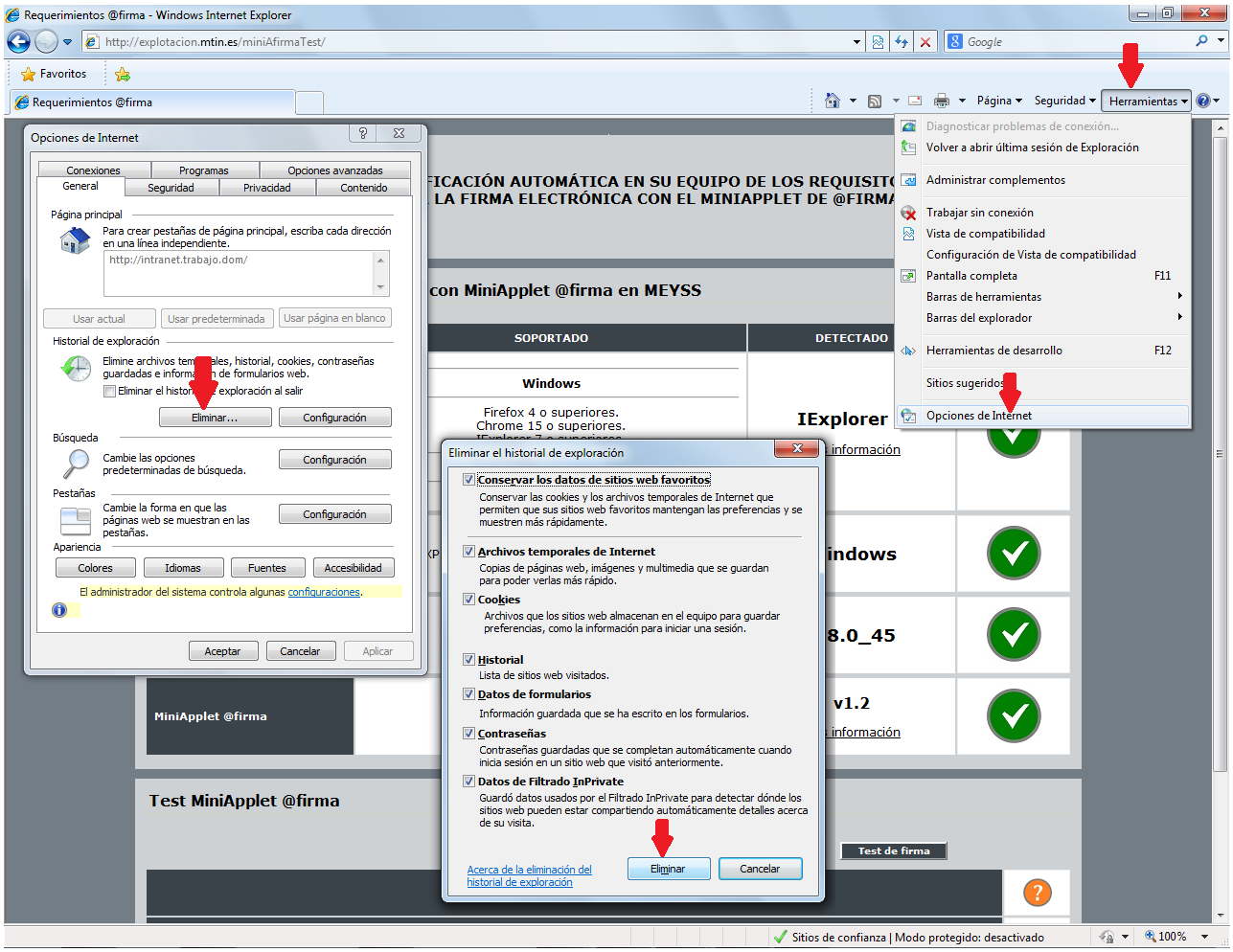
5. RESOLUCIÓN DE PROBLEMAS

5.1. Limpieza de Caché del Navegador

En algunas ocasiones, para que la aplicación funcione correctamente, es necesario limpiar la caché del navegador.

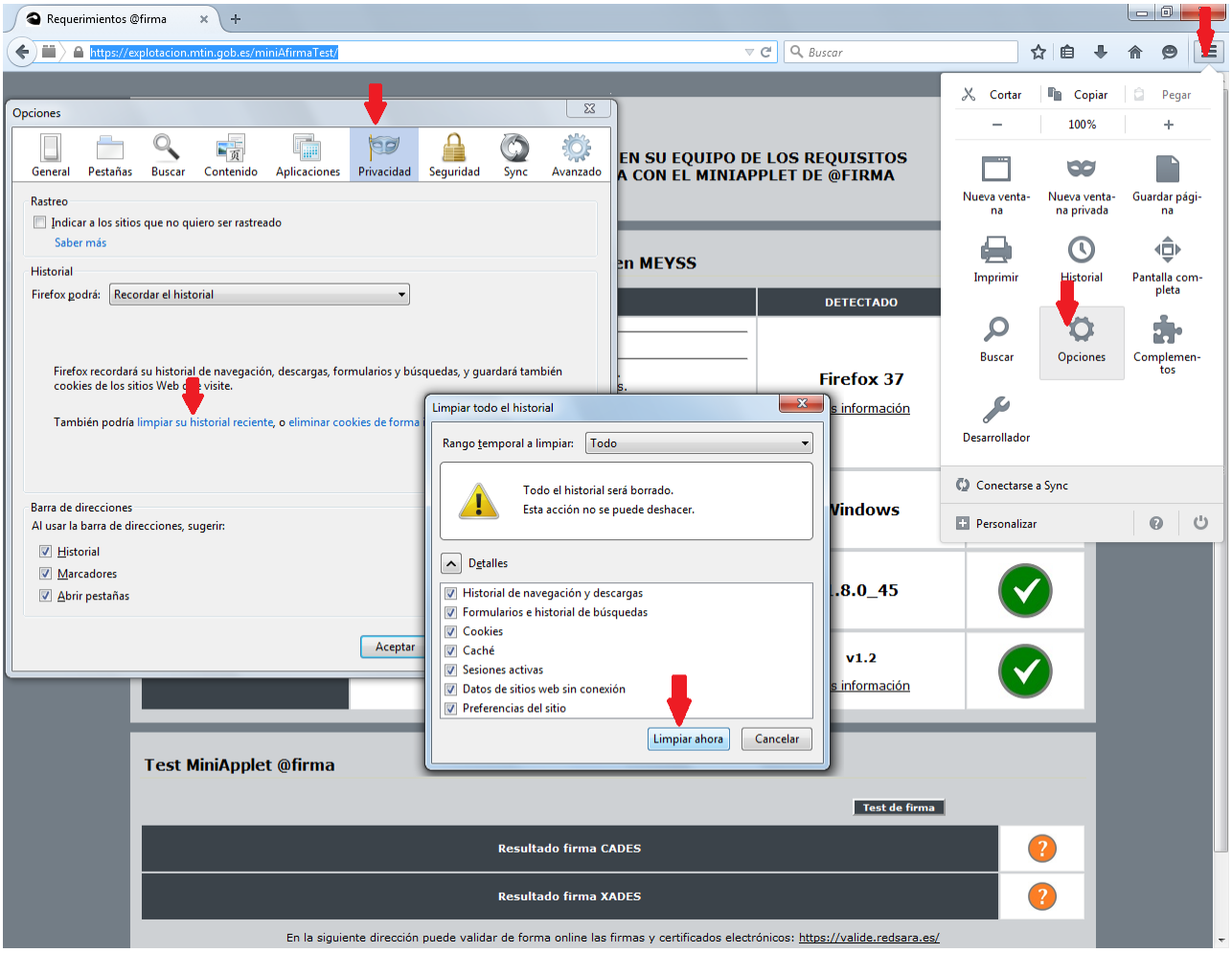
INTERNET EXPLORER

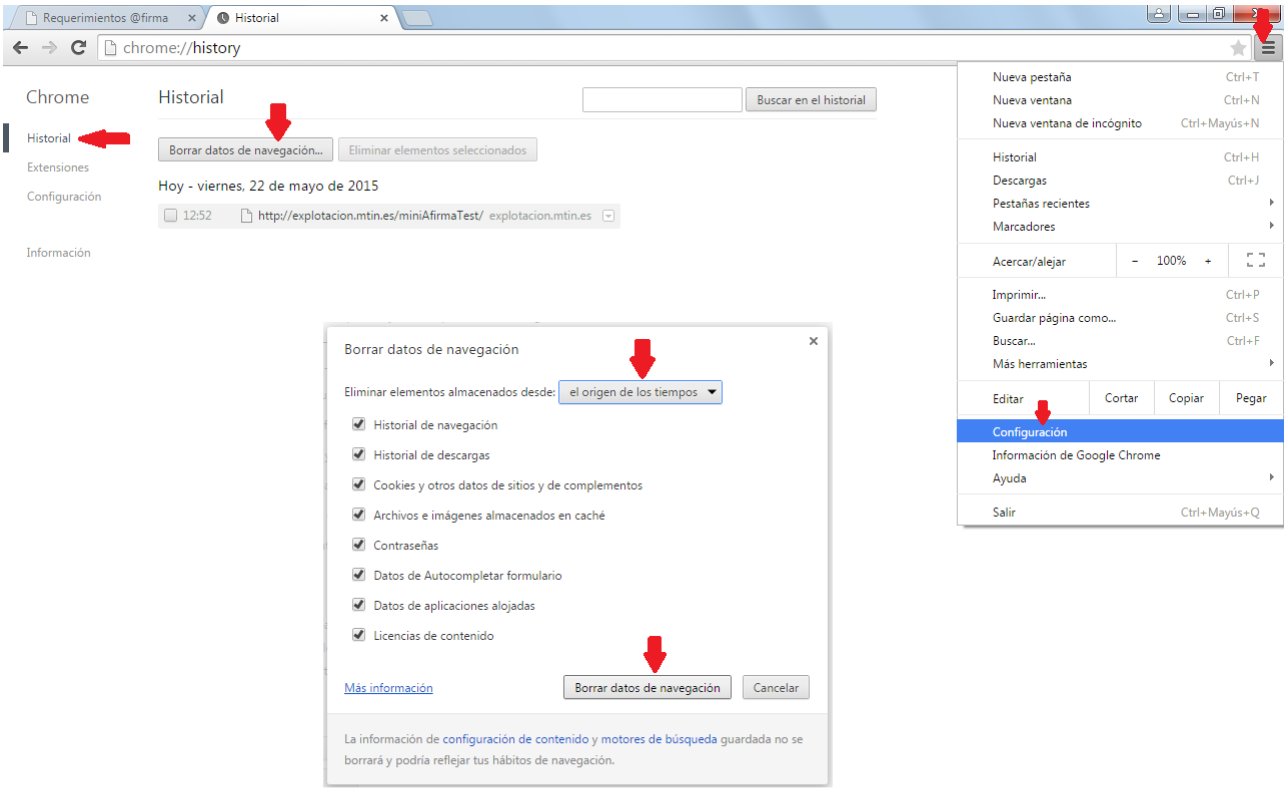
Herramientas → Opciones de Internet → Eliminar… → Seleccionar todo → Eliminar



MOZILLA FIREFOX

Menú → Opciones → Privacidad → limpiar su historial reciente → Limpiar ahora



GOOGLE CHROME

Menú → Configuración → Historial → Borrar datos de navegación → desde el origen de los tiempos → Borrar datos de navegación