



## Sede electrónica

# Requisitos Generales de Configuración del Almacén de Certificados



## Índice

<b>1</b>	<b>Importación de certificado personal.....</b>	<b>3</b>
1.1	Importación del certificado personal en Internet Explorer .....	3
1.2	Importación de certificado personal en Firefox.....	10
<b>2</b>	<b>Importación del certificado de la CA que emite el certificado de firma de código del Componente de Firma. ....</b>	<b>14</b>
2.1	Importación del certificado de CamerFirma con Internet Explorer.....	14
2.2	Importación del certificado de CamerFirma con Firefox. ....	20
2.3	Descarga del certificado de la entidad emisora Camerfirma .....	24
<b>3</b>	<b>Acceso a servidores seguros.....</b>	<b>27</b>
3.1	Acceso a servidores seguros desde Internet Explorer .....	27
3.2	Acceso a servidores seguros desde Firefox.....	30



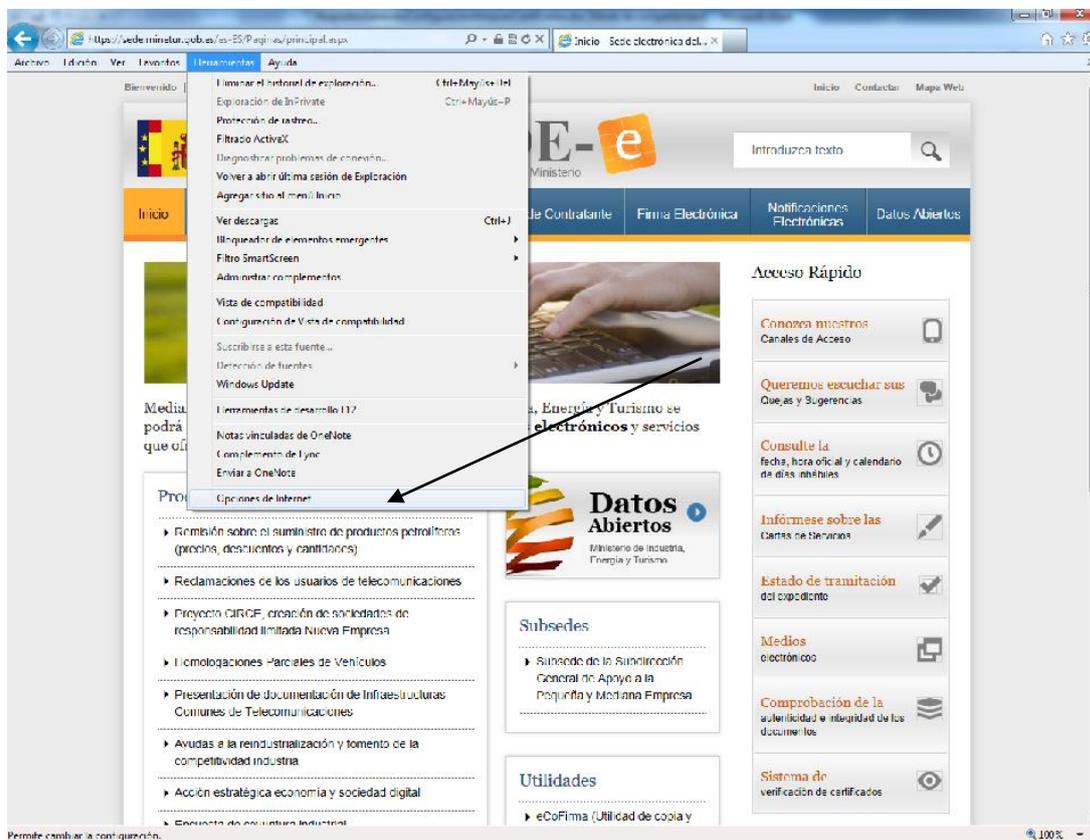
## 1 Importación de certificado personal

Para poder realizar firmas digitales el usuario tendrá que tener cargado en el almacén el certificado con el que desee realizar la firma. En caso de encontrarse el certificado en una tarjeta criptográfica no será necesaria la importación. Si se trata de un certificado software, es decir, dispone de un fichero con el certificado, se podrá importar según se indica a continuación:

### 1.1 Importación del certificado personal en Internet Explorer

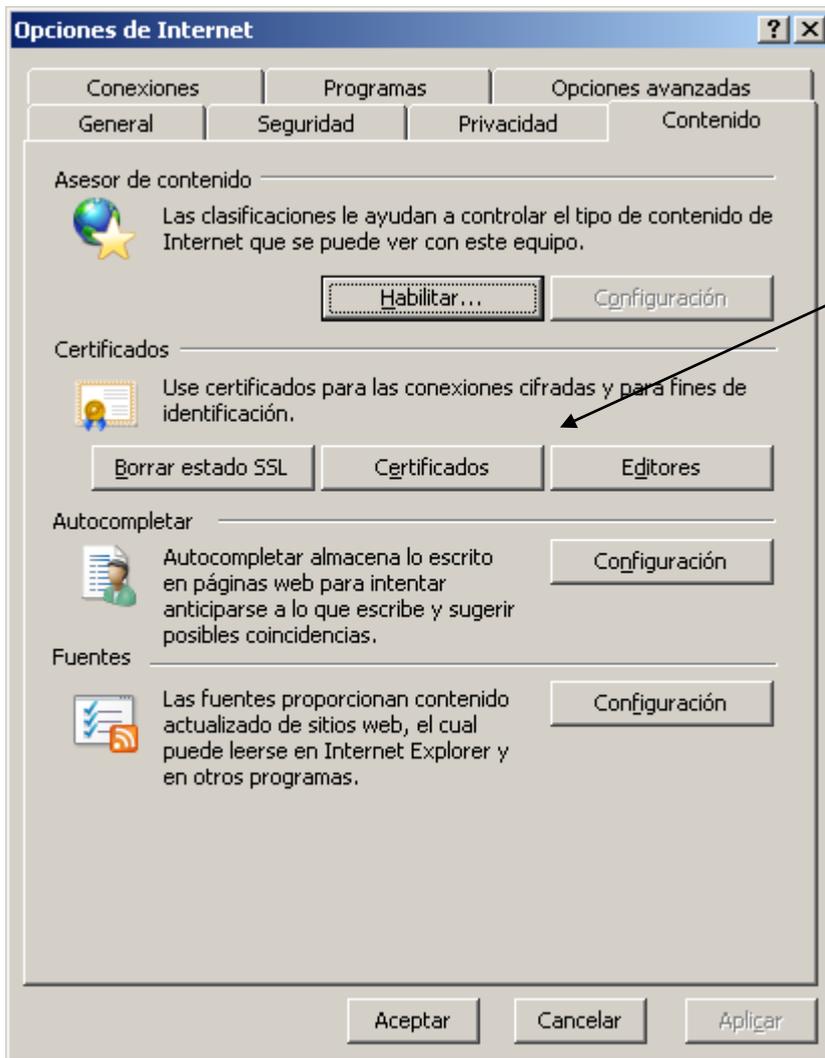
Para importar un certificado en Internet Explorer puede seguir los siguientes pasos.

Acceder al menú *Herramientas-Opciones de Internet*.





Pulsar en la pestaña *Contenido* y a continuación en el botón *Certificados*.



Pulsar el botón *Importar*:



**Certificados** [?] [X]

Propósito planteado: <Todos>

Personal | Otras personas | Entidades emisoras de certificados intermedias | Entidades emi [◀] [▶]

Emitido para	Emitido por	Fecha de...	Nombre descriptivo

Importar... | Exportar... | Quitar | Avanzadas...

Propósitos planteados del certificado

Ver

Cerrar

Se abrirá el Asistente de Importación. Pulsar *Siguiente*:

**Asistente para importación de certificados** [X]



### Éste es el Asistente para importación de certificados

Este asistente le ayuda a copiar certificados, listas de confianza de certificados y listas de revocaciones de certificados desde su disco a un almacén de certificados.

Un certificado, que se emite por una entidad emisora de certificación, es una confirmación de su identidad y contiene información que se utiliza para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Haga clic en *Siguiente* para continuar.

< Atrás | Siguiente > | Cancelar



Pulsar el botón *Examinar* para buscar la ubicación del fichero con el Certificado:

**Asistente para importación de certificados**

**Archivo para importar**

Especifique el archivo que desea importar.

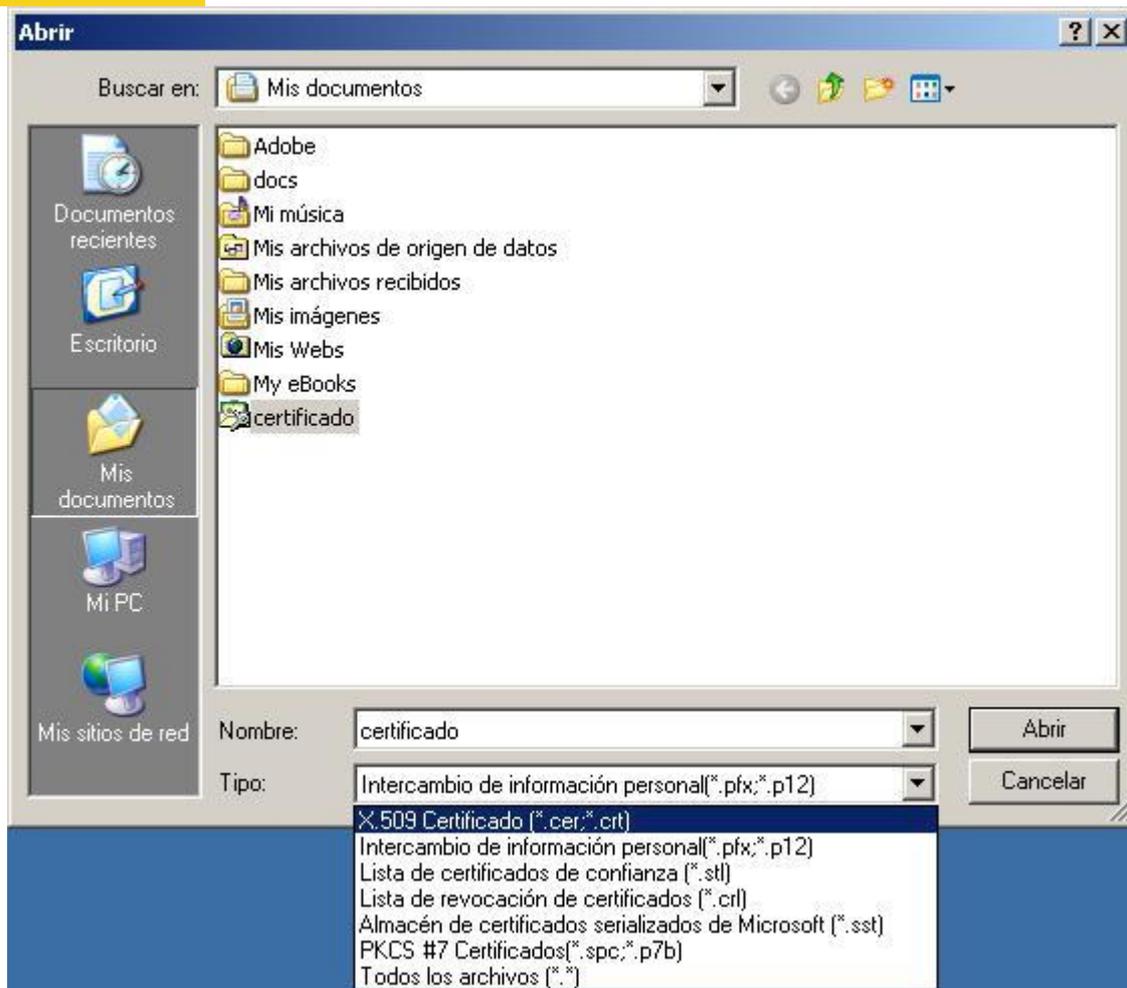
Nombre de archivo:

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)

< Atrás    Siguiete >    Cancelar

En la caja *Tipo* elegir Intercambio de información personal.



Seleccionar el archivo y pulsar el botón *Abrir*.

Pulsar el botón *Siguiente*:



**Asistente para importación de 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)

< Atrás    Siguiete >    Cancelar

Introducir la contraseña y seleccione la casilla Marcar como exportable:

**Asistente para importación de certificados**

**Contraseña**  
Para mantener la seguridad, la clave privada se protege con una contraseña.

Escriba la contraseña para la clave privada.

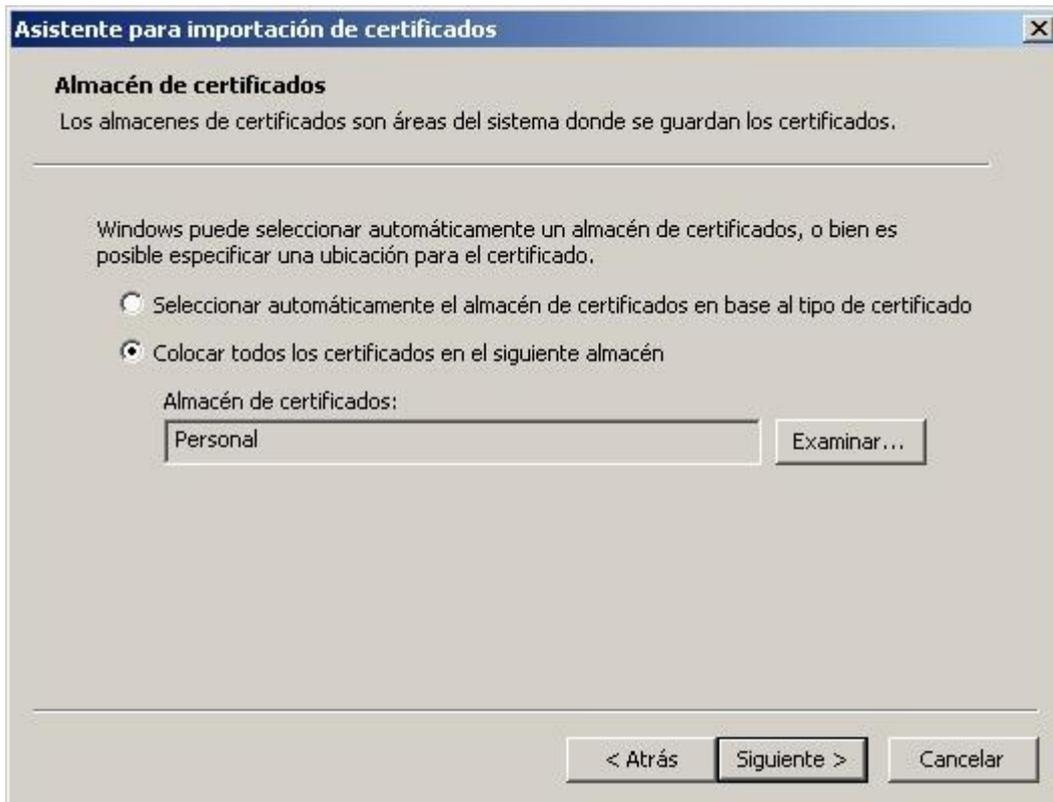
Contraseña:

Habilitar protección segura de claves privadas. 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.

< Atrás    Siguiete >    Cancelar

Pulsar el botón *Siguiete*:

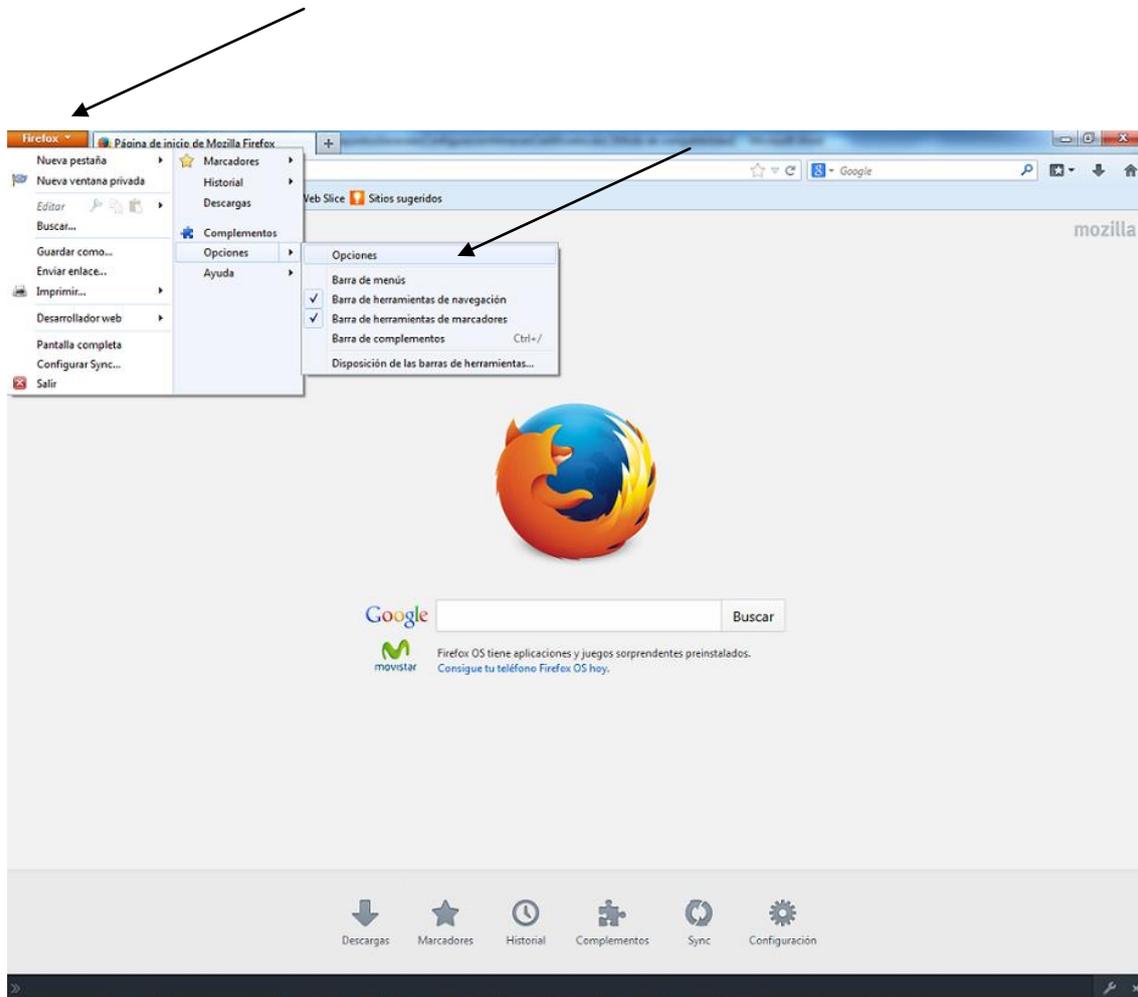


Para terminar de importar el certificado pulsar Finalizar:

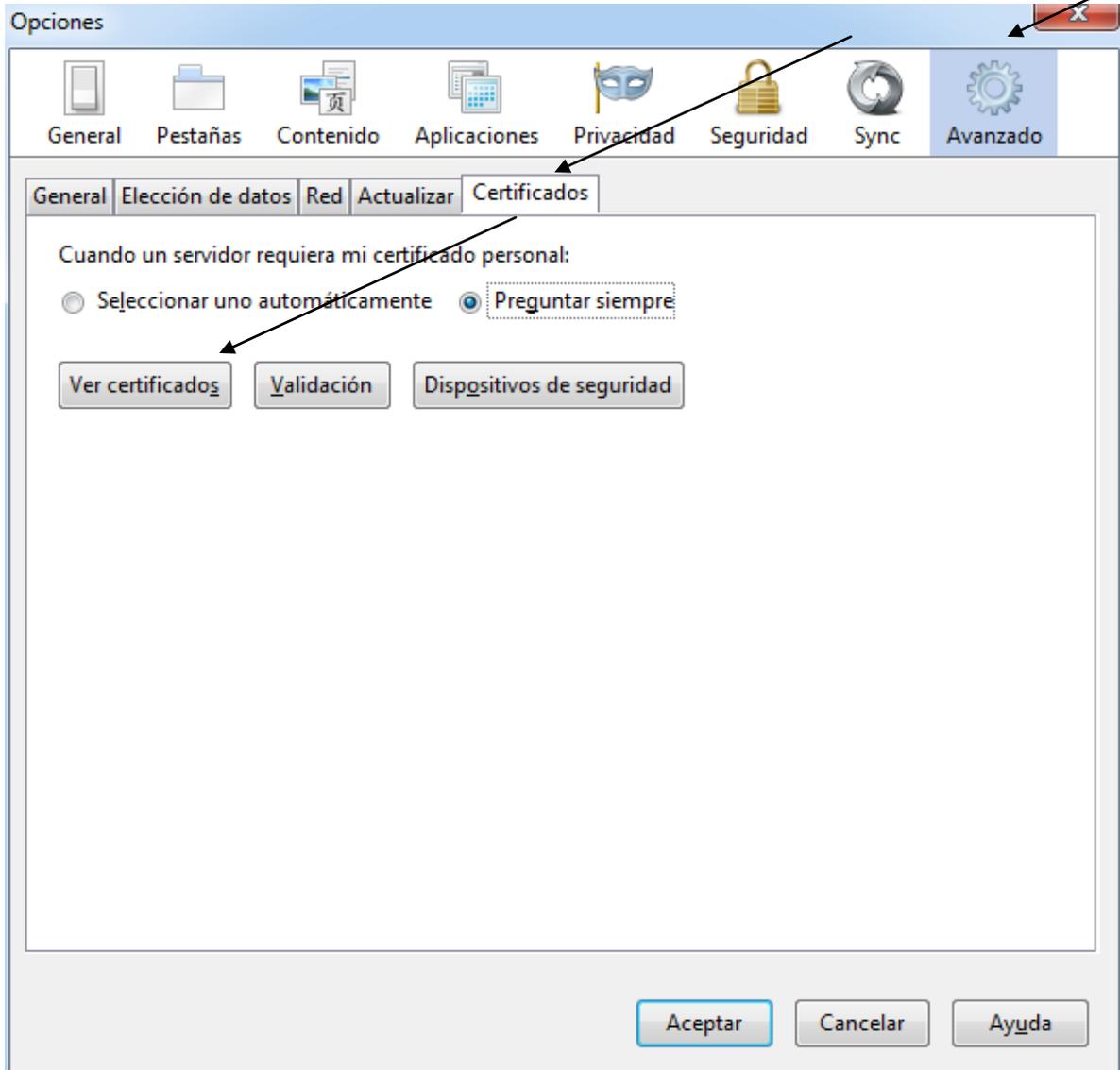


## 1.2 Importación de certificado personal en Firefox

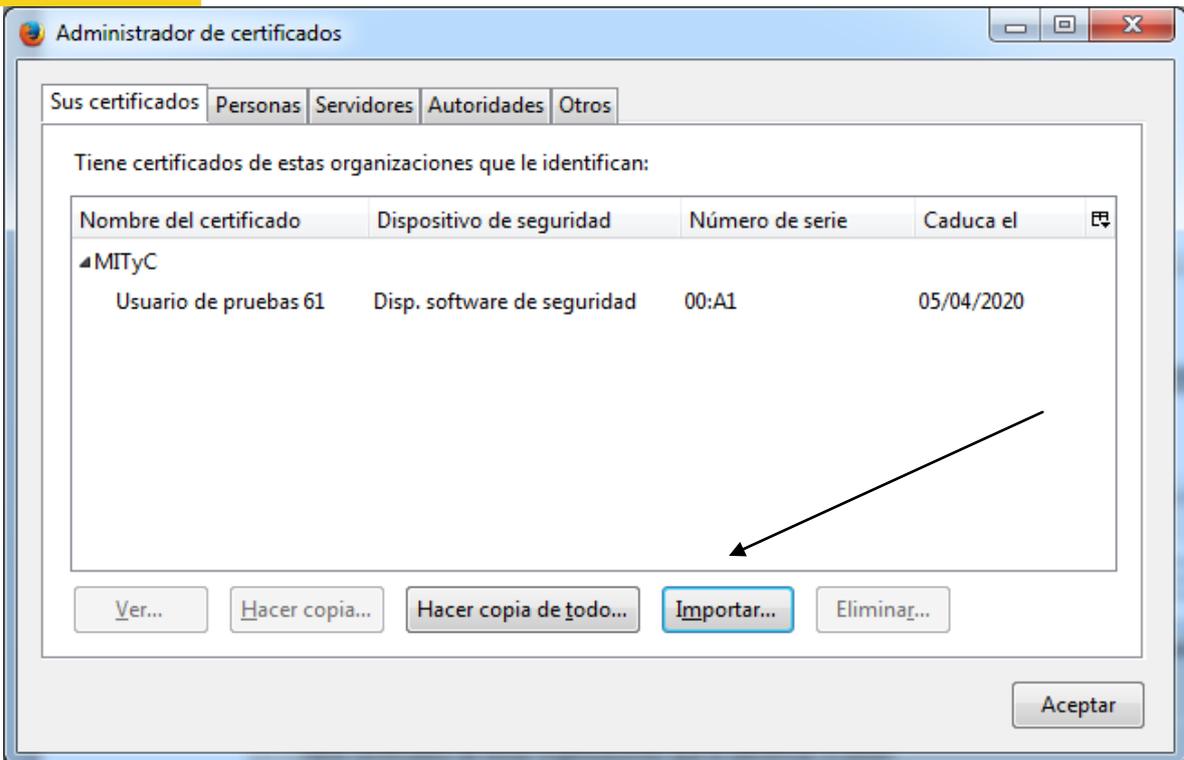
Acceder al menú *Firefox-Opciones-Opciones*.



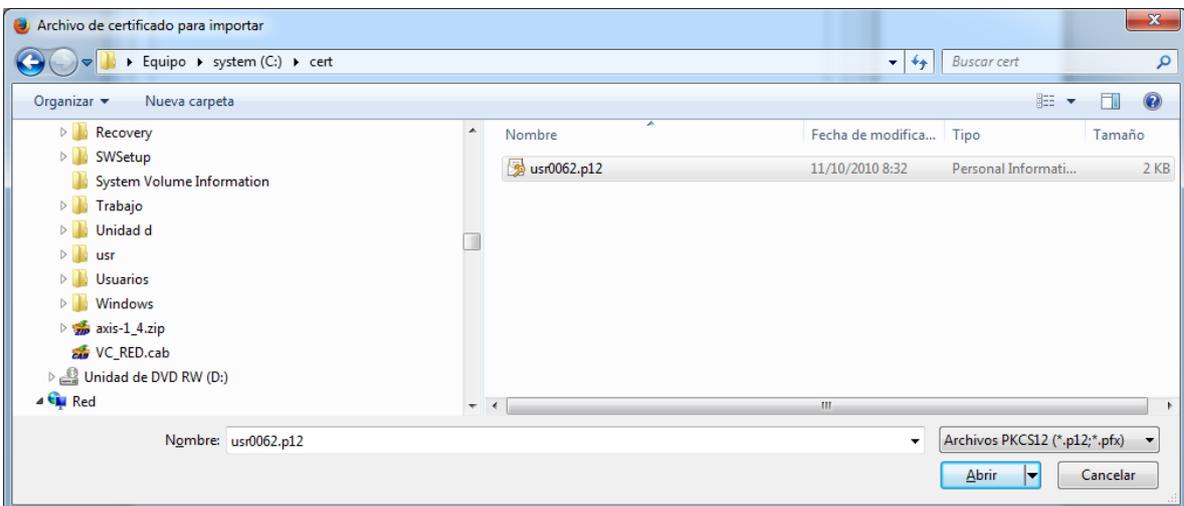
Acceder a *Avanzado* y dentro de esta opción a la pestaña *Cifrado* y pulsar el botón *Ver certificados*:



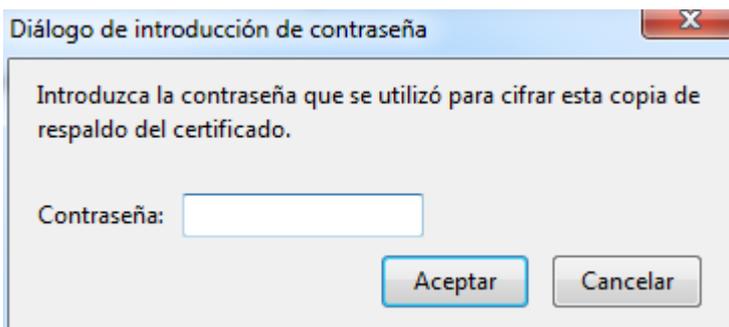
Pulsar el botón *Importar*:



Seleccionar el archivo a importar y pulse *Abrir*:



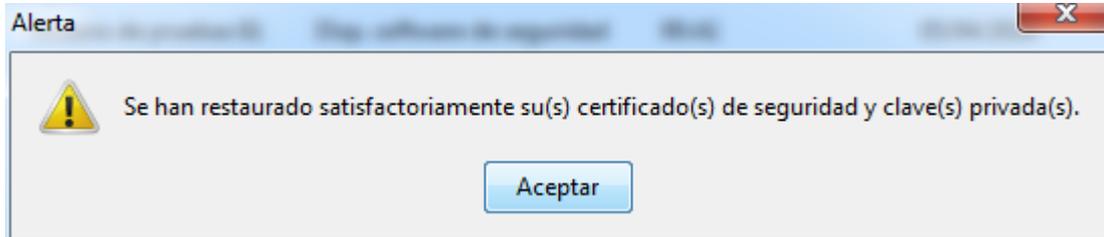
Introducir la contraseña:



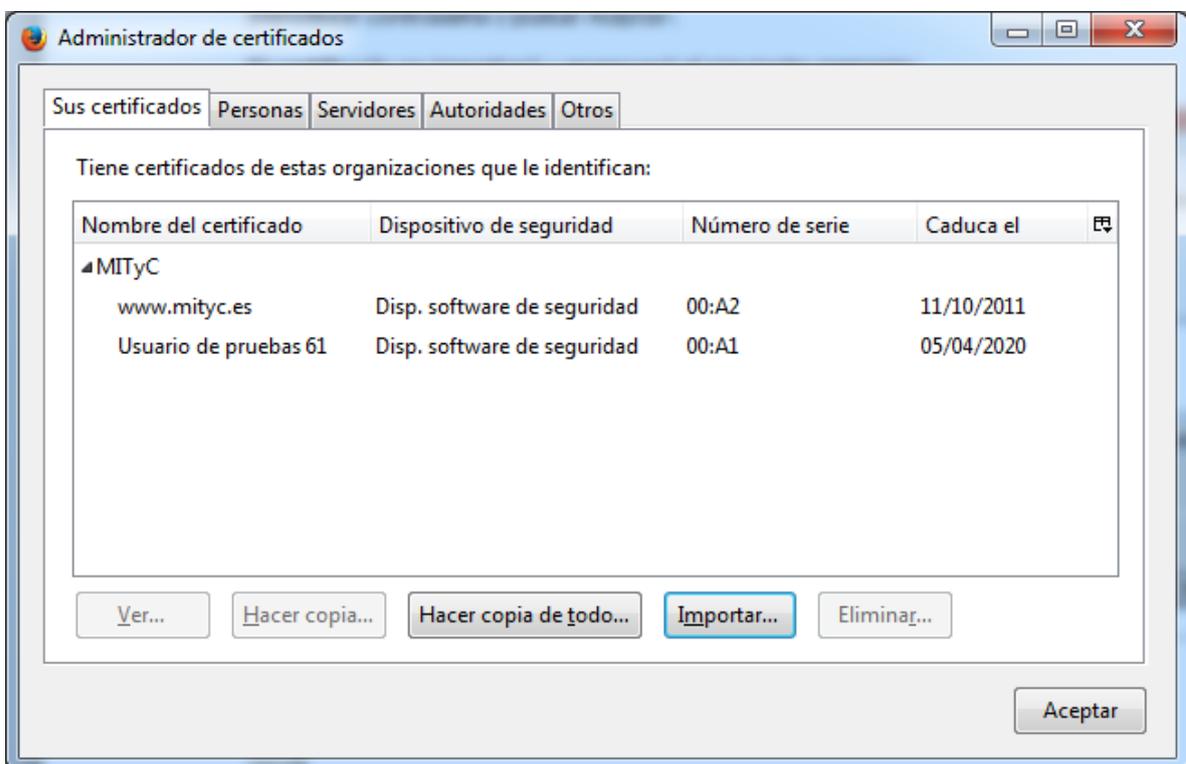


Introducir contraseña y pulsar *Aceptar*.

El certificado se importará y aparecerá el siguiente mensaje:



Pulsar *Aceptar*. A partir de ese momento se verá el certificado en el almacén:





## 2 Importación del certificado de la CA que emite el certificado de firma de código del Componente de Firma.

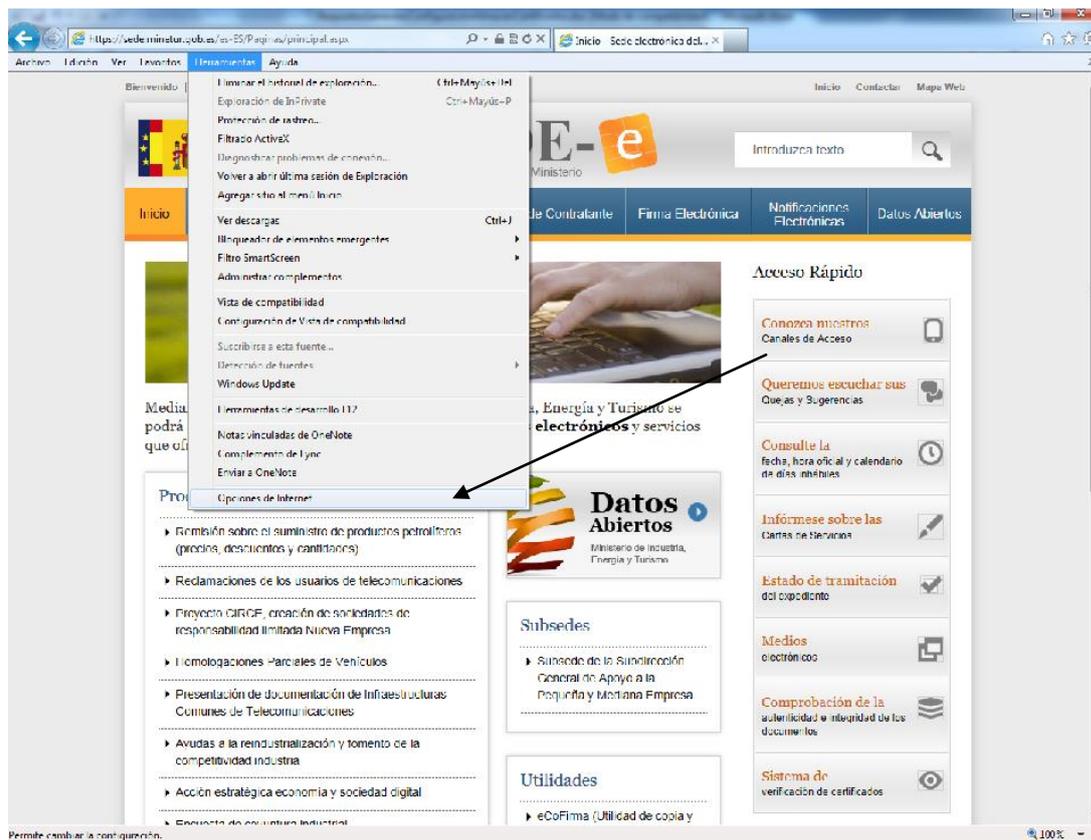
El componente está firmado con un certificado digital de firma de código del **Ministerio de Industria, Energía y Turismo** emitido por la entidad de certificación **Camerfirma**.

Para poder realizar la descarga e instalación del componente de firma, debe comprobar si en el Almacén de certificados está instalado el certificado raíz de la entidad Camerfirma. Por lo general este certificado ya estará instalado en su máquina.

### 2.1 Importación del certificado de CamerFirma con Internet Explorer.

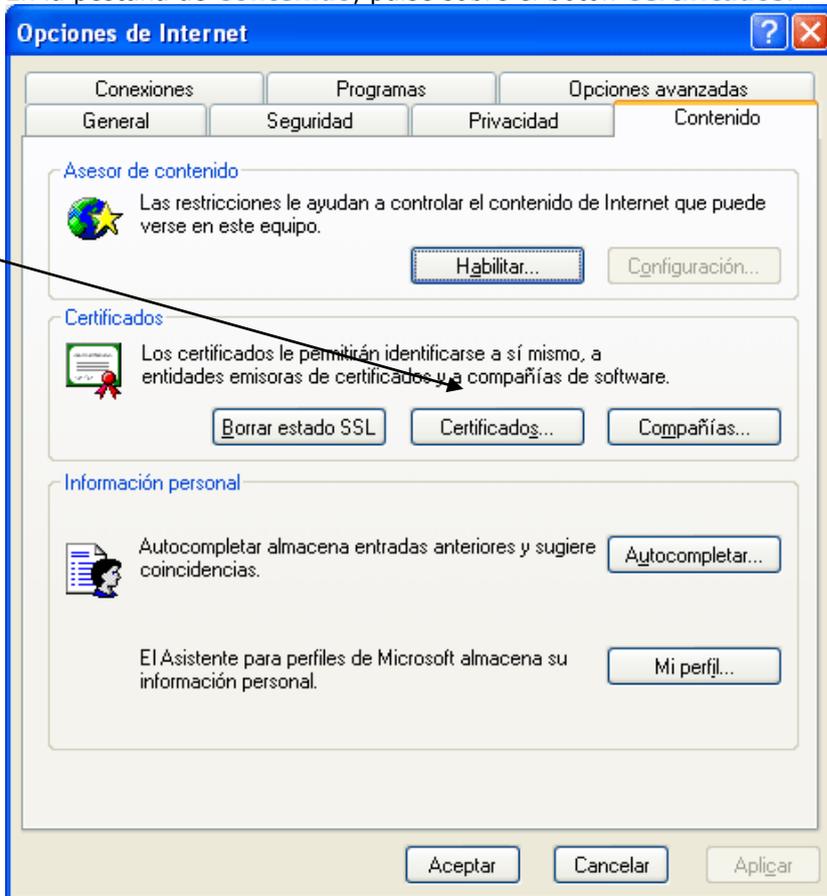
Para realizar la comprobación de si el certificado está cargado en su almacén debe seguir los siguientes pasos:

Acceda al menú de *Herramientas/Opciones de Internet* de Internet Explorer.

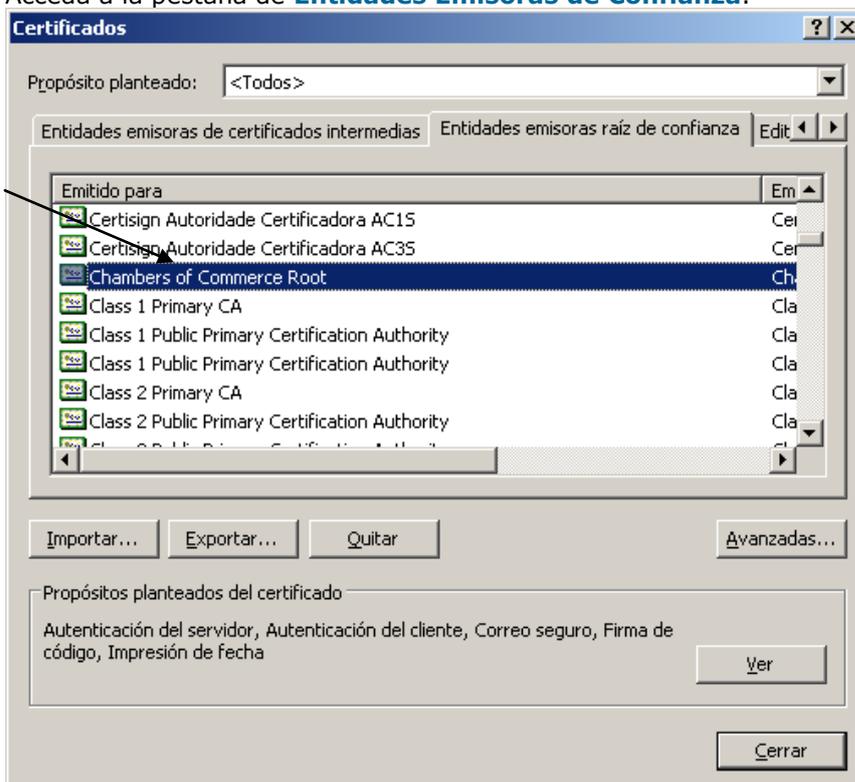




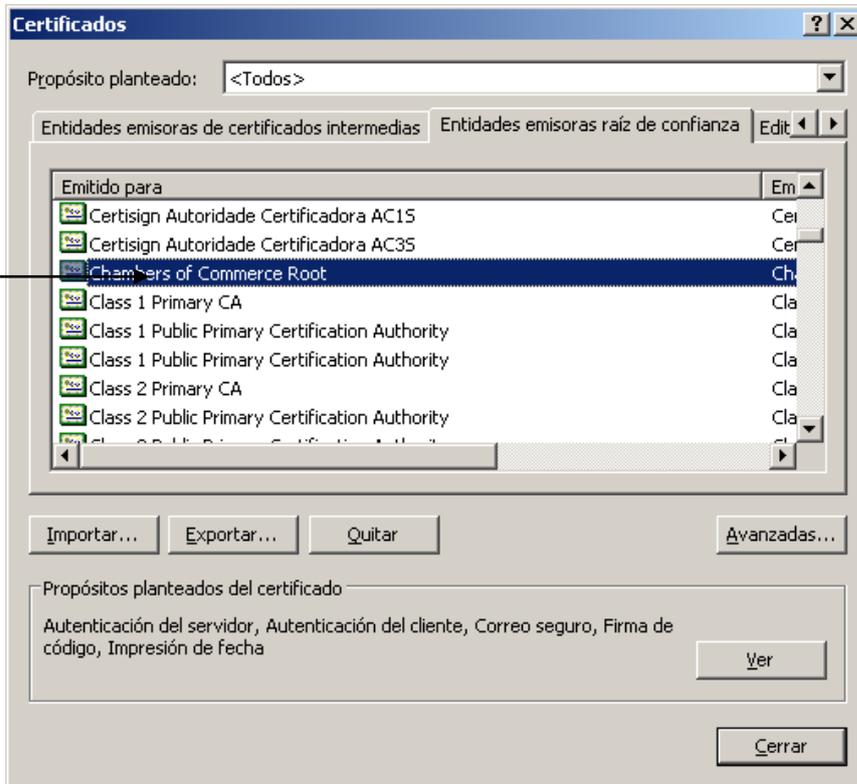
En la pestaña de **Contenido**, pulse sobre el botón **Certificados**.



Acceda a la pestaña de **Entidades Emisoras de Confianza**.



Compruebe que existe el certificado **Chambers of Comerse Root**.



Si su almacén no dispone de ese certificado puede descargárselo según se indica en el apartado [Descarga del certificado de la entidad emisora Camerfirma](#)

Al descargar el certificado se mostrará la siguiente ventana, donde deberá pulsar el botón **Abrir**.



A continuación haga clic en el botón **Instalar certificado**.



**Certificado** [?] [X]

General | Detalles | Ruta de certificación

 **Información del certificado**

**Este certificado está destinado a los siguientes propósitos:**

- 1.3.6.1.4.1.17326.10.3.1
- Todas las directivas de la aplicación

\* Más info. en declaración de entidades emisoras de certificados.

---

**Enviado a:** Chambers of Commerce Root

**Emitido por:** Chambers of Commerce Root

**Válido desde:** 30/09/2003 **hasta:** 30/09/2037

Instalar certificado...    Declaración del emisor

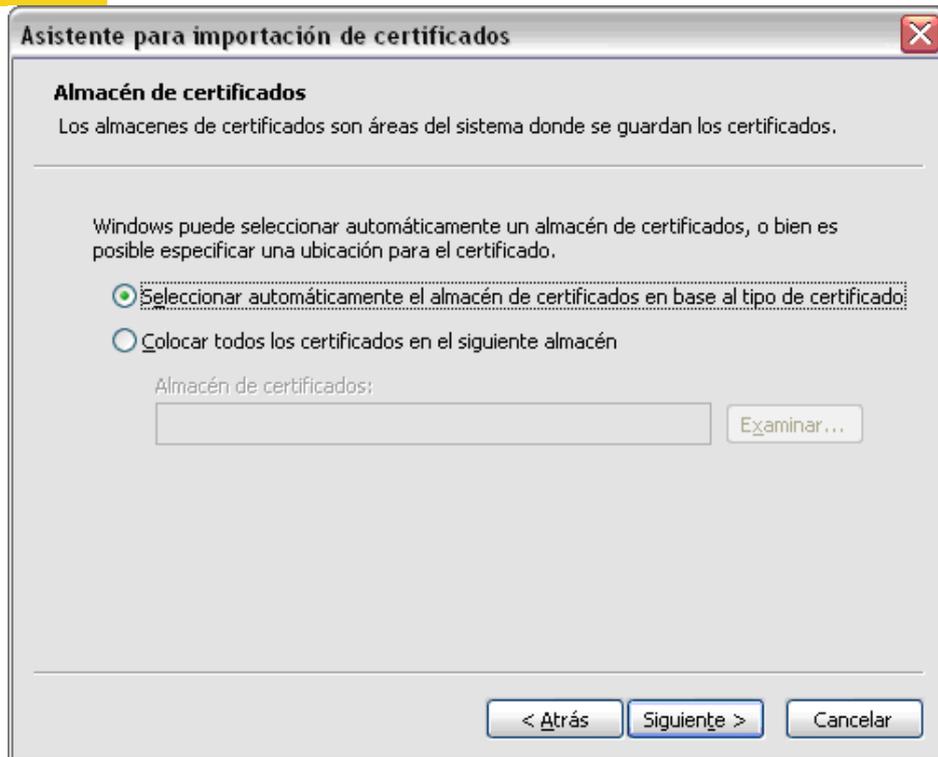
Aceptar



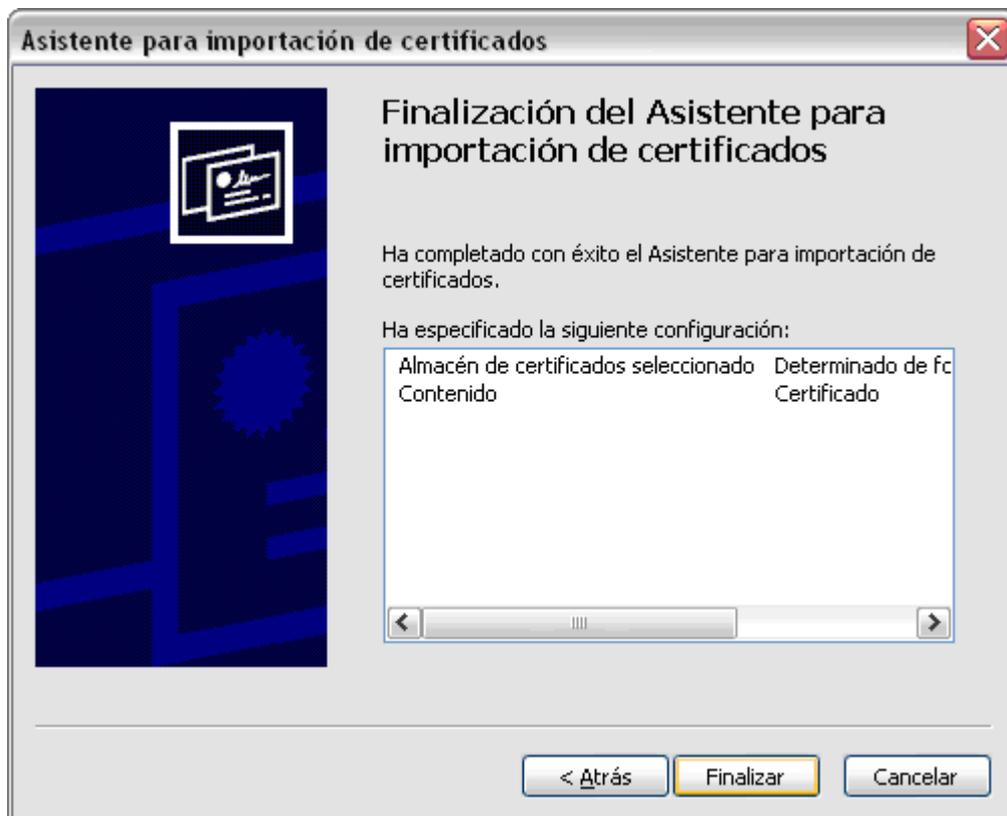
Se iniciará el asistente para la importación de certificados mostrándose la siguiente ventana en la que se deberá hacer clic en el botón **Siguiente**.



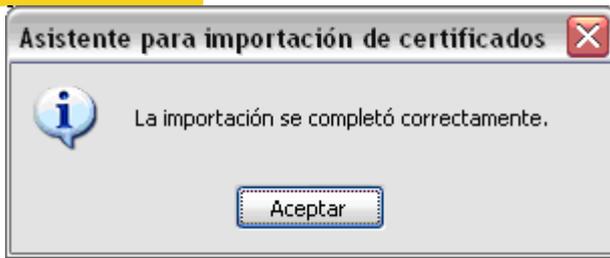
Se mostrará la siguiente ventana, donde deberá seleccionar la opción **Seleccionar automáticamente el almacén de certificados en base al tipo de certificado** y hacer clic en el botón **Siguiente**.



Para terminar con la instalación deberá hacer clic en el botón **Finalizar**.



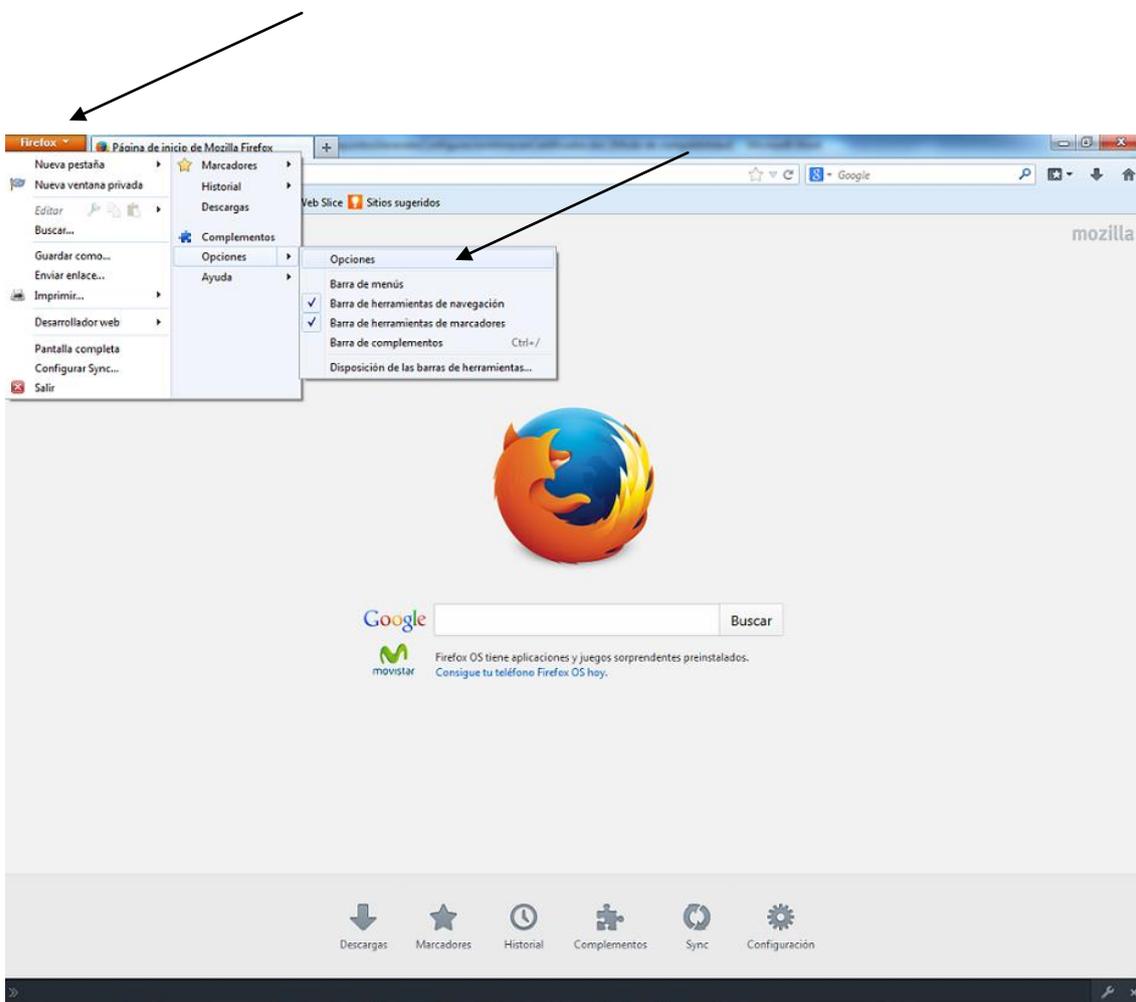
Se mostrará el siguiente mensaje informativo indicando el éxito de la importación.



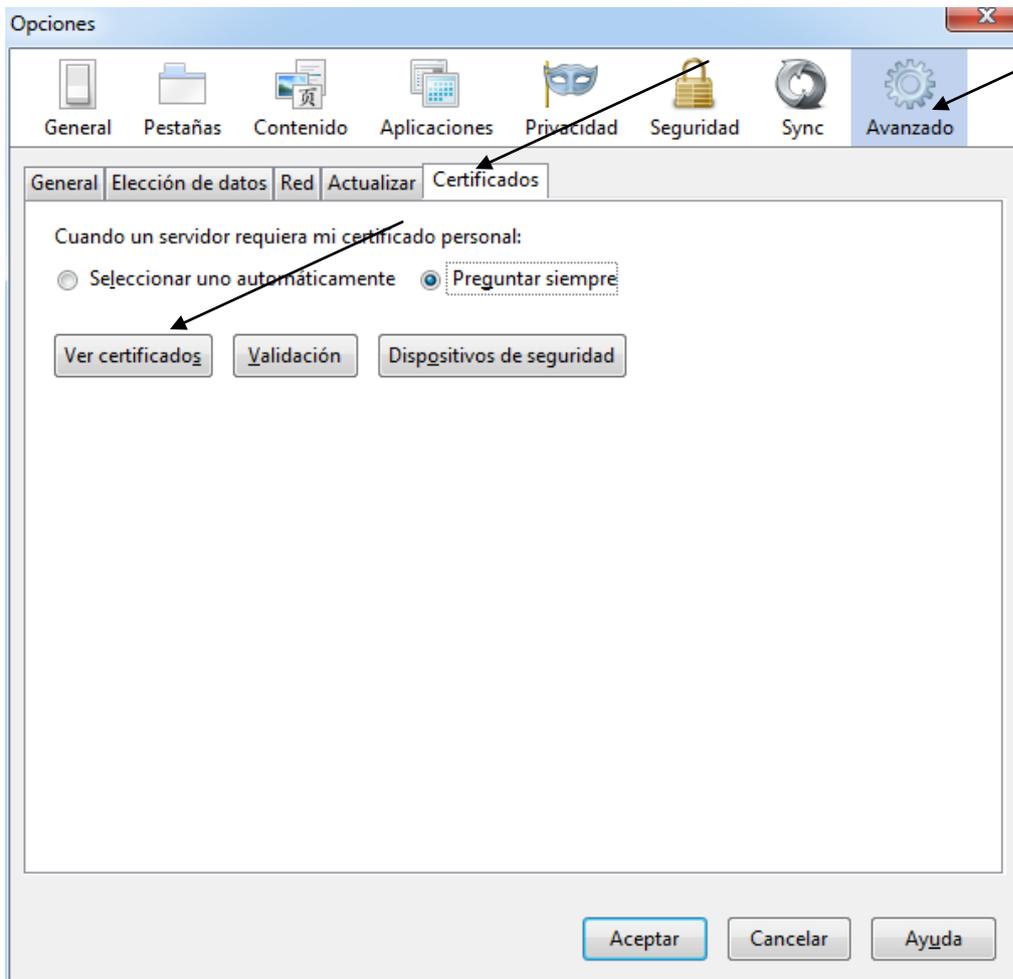
## 2.2 Importación del certificado de CamerFirma con Firefox.

Para realizar la comprobación de si el certificado está cargado en su almacén debe seguir los siguientes pasos:

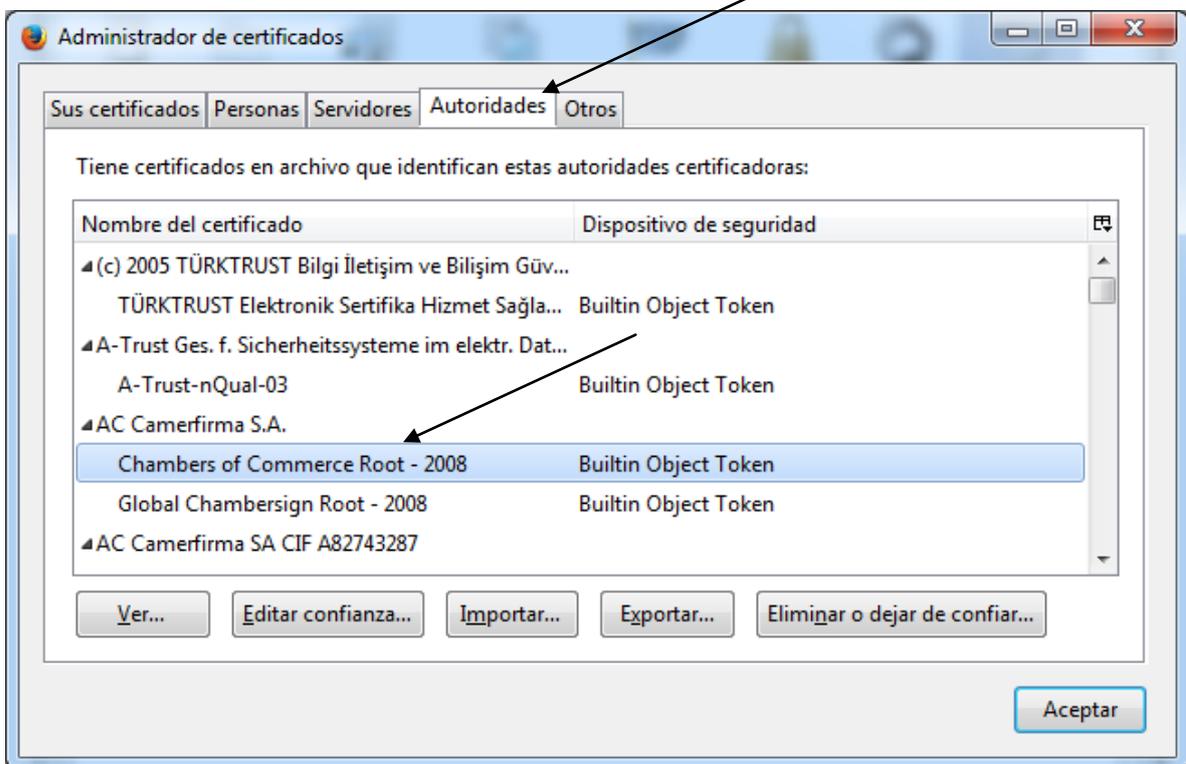
Acceder al menú *Firefox-Opciones-Opciones*.



A continuación acceda *Avanzado->Cifrado->Ver certificados*.



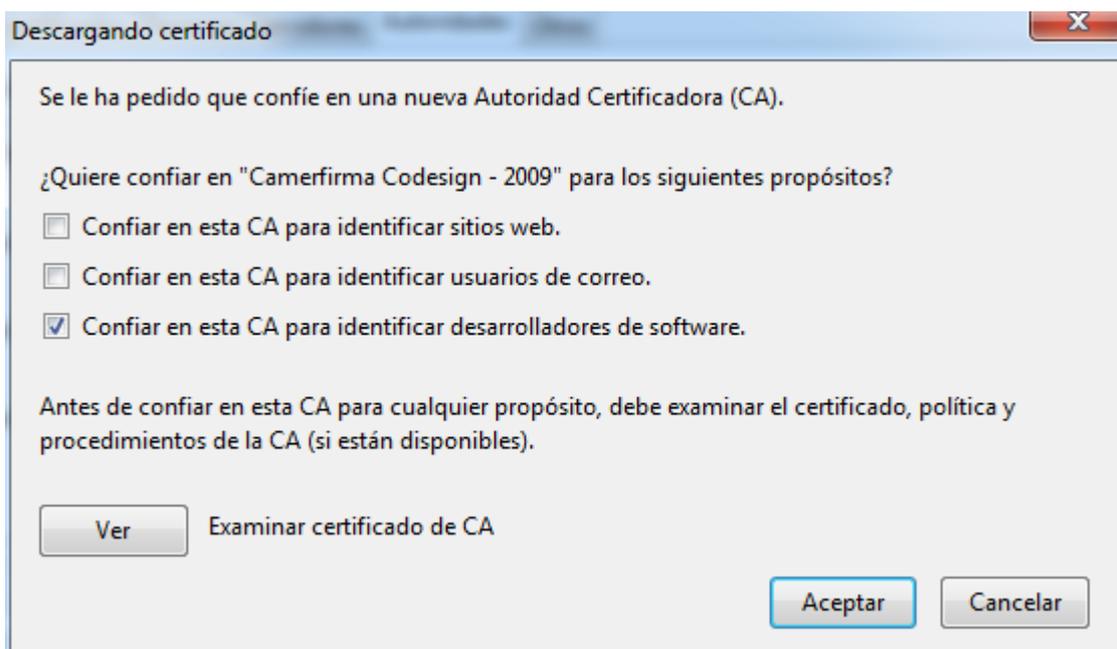
Haga clic en la pestaña *Autoridades*:



Compruebe si aparece el certificado de Camerfirma (Chambers of Commerce Root).

Si no aparece descárgelo según se indica en el apartado [Descarga del certificado de la entidad emisora Camerfirma](#).

Una vez descargados impórtelos desde la pestaña Autoridades de la imagen anterior. Para ello pulse Importar y seleccione el fichero descargado. Le aparecerá la siguiente ventana:





Seleccione la opción “*Confiar en esta CA para identificar desarrolladores de software*” y pulse *Aceptar*.

Podrá comprobar que ya aparece esa autoridad entre las Autoridades de confianza de su almacén.



## 2.3 Descarga del certificado de la entidad emisora Camerfirma

Sólo en el caso de no encontrarse en el almacén, lo debemos instalar. Para la instalación del certificado debe ir a la página web de descarga de certificado raíz de Camerfirma: <http://www.camerfirma.com/> Una vez aquí, en el menú superior pulsar sobre **ÁREA DE USUARIO** y a continuación en **DESCARGA DE CLAVES PÚBLICAS RAÍZ**.

**Claves Públicas**

Camerfirma ha realizado un trabajo importante para que sus claves sean reconocidas por el mayor número de comunidades y aplicativos: Microsoft, Mozilla, SUN, Chrome, así como por organismos e instituciones tanto públicas como privadas.

Desde esta página distribuimos la clave pública de las entidades raíz de Camerfirma "Chambers of commerce Root" y "Global Chambersign Root", de tal forma que puedan ser validados por todos aquellos que confían en los certificados digitales.

El principal activo de un prestador de servicios de certificación son sus claves criptográficas. El reconocimiento de éstas por parte de las distintas comunidades electrónicas. Enriquecen su valor y permiten tanto, a los titulares de los certificados emitidos por el prestador. Como a aquellos que reciben de las actuaciones realizadas con dichos certificados digitales, confiar en la identidad y contenido de las transacciones realizadas con los mismos.

» **Acceso seguro a las claves.**  
El código resumen o HASH nos permite comprobar si el certificado raíz es original. Comprobar con navegadores Firefox 4 (o superior) ó Microsoft Internet Explorer 7 (o superior).

**Nuevas claves 2.008**

AC Camerfirma S.A. ha creado nuevas claves raíz para sus Autoridades de certificación Root y Autoridades de Certificación delegadas de las mismas, para la actualización de algoritmos y longitudes de clave ajustadas al estado del arte de la tecnología.

La generación de nuevas claves afecta a las Autoridades de Certificación Root de AC Camerfirma, S.A, "Chambers of Commerce Root" y "Global Chambersign Root", con sus correspondientes Autoridades de Certificación Delegadas vinculadas a las anteriores.

La ceremonia de generación de las claves tuvo lugar el pasado día 22 de julio de 2008 y se celebró con todos los requerimientos de seguridad y en la presencia de la entidad Ernst & Young en calidad de Auditor Externo.

Estas claves sustituirán a las actuales una vez que todas las Administraciones y Organismos públicos y privados que actualmente reconocen los certificados Camerfirma hayan manifestado su consentimiento e incorporado las nuevas claves en sus aplicativos. La generación de las nuevas claves no implicará modificaciones adicionales respecto a los certificados digitales finales que se emiten a los suscriptores.

» **Acceso seguro a las claves.**  
El código resumen o HASH nos permite comprobar si el certificado raíz es original. Comprobar con navegadores Firefox 4 (o superior) ó Microsoft Internet Explorer 7 (o superior).

- » Descarga de Certificados
- » Renovación de Certificados
- » Consulta de Certificados
- » Anulación/Revocación de Certificados
- » Suspensión de Certificados
- » **Descarga de Claves Públicas Raíz**
- » Jerarquía Políticas y Prácticas de Certificación
- » Área de Descargas

Si tiene cualquier duda llámenos al **teléfono de atención al cliente 902 36 12 07** accede a nuestra **aplicación de soporte**

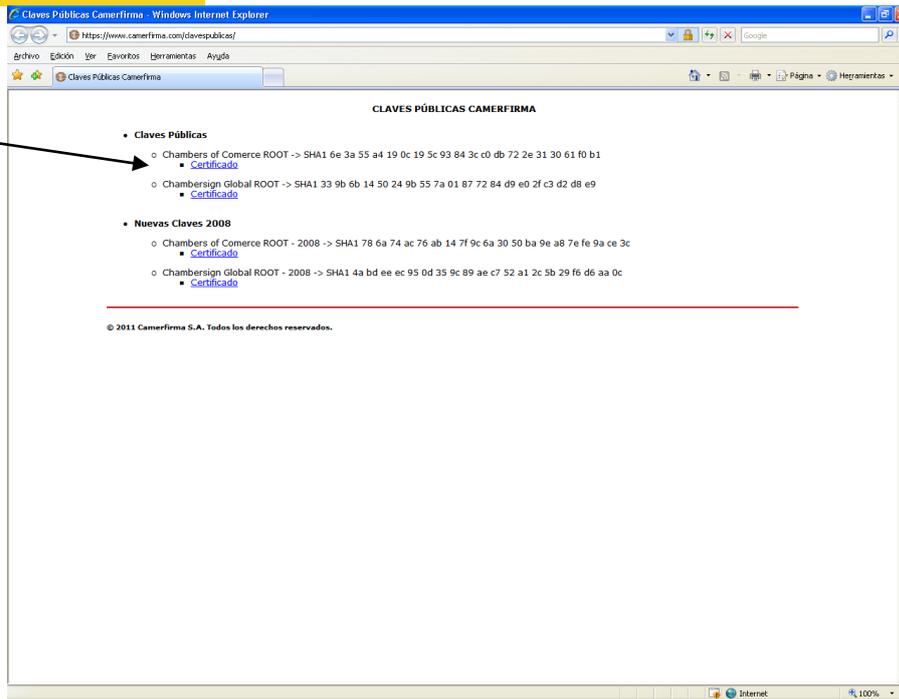
**Camerfirma**  
© 2013 Camerfirma S.A. Todos los derechos reservados.

Síguenos en:

[Intranet](#) | [Mapa del sitio](#) | [LOPD/LSSI](#) | [English](#)

Ha de pulsar en el apartado Claves Públicas sobre el enlace "Acceso seguro a las claves".

Una vez cargada la página descárguese los certificados de la misma pulsando en los enlaces "Certificado".



Importe los certificados según se indica en los apartados anteriores.

Descárguese también el certificado de la CA de Camerfirma que emite certificados de firma de código accediendo desde el menú *USUARIOS->JERARQUÍA POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN*.

Para ello pulse sobre el candado que aparece en la fila correspondiente a *AC Firma de Código*.

Para confiar en algunos de los servidores del MINETUR también necesitará el certificado de *AC Camerfirma Express Corporate Server v3*, para lo que tendrá que pulsar sobre el enlace v3 según se indica en la imagen siguiente.

## Jerarquía Políticas y Prácticas de Certificació

Inicio / Usuarios / Jerarquía Políticas y Prácticas de Certificación

### Declaración de Practicas de Certificación (CPS/DPC)

Es el conjunto de prácticas adoptadas por un prestador de servicios de certificación para la emisión de certificados. Contiene información detallada sobre el sistema de seguridad, soporte, administración y emisión de los certificados,... y en general, una descripción de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

- » Acceso a la Declaración de Practicas de Certificación de AC Camerfirma (811KB).
- » 27/ABRIL/2011 NUEVA VERSION DPC v 3.2.3 (785KB).
- » AGOSTO/2012 NUEVA VERSION DPC v 3.2.5 (1.2MB).
- » MAYO/2013 NUEVA VERSION DPC v 3.2.6 (1.3MB).

**Jerarquías de Certificación** Estructura bajo la cual se emiten los distintos certificados digitales de Camerfirma. El objeto fundamental de la misma es construir una red de confianza para la emisión y gestión de los certificados digitales. Camerfirma dispone de dos Jerarquías, Chambersign Global Root y Chambers of Commerce Root, que emiten certificados en distintos ámbitos.

### Jerarquía Chambers of Commerce Root 1.3.6.1.4.1.17326.10.3.1

Esta Jerarquía está diseñada para construir una red de confianza que tiene por objeto fundamental la emisión de certificados digitales de identidad empresarial y donde las Autoridades de Registro (en adelante AR o AR's) suelen encontrarse gestionadas por las Cámaras de Comercio, Industria y Navegación.. Esta jerarquía incorpora Autoridades de Certificación intermedias que emiten certificados digitales empresariales en diferentes entornos. A continuación indicamos una relación de los certificados emitidos bajo esta Jerarquía y sus Autoridades de Certificación intermedias e incorporamos los datos del OID (Identificador de la Política de certificación del certificado), la correspondiente Política de Certificación, y en su caso un certificado de prueba:

Políticas de Certificación.				
	O.I.D.	Política	Actuales	ClavesNuevas
<b>CHAMBERS OF COMMERCE ROOT</b>	1.3.6.1.4.1.17326.10.3.1	▶ 781KB	▶	▶
<b>AC Camerfirma Express Corporate Server.</b>	1.3.6.1.4.1.17326.10.11.1		▶ v1 ▶ v3	Continuada en AC Camerfirma Corporate Server-2009
Certificados para servidor Seguro OV	1.3.6.1.4.1.17326.10.11.2	▶ 183KB		Se emite bajo AC Camerfirma Corporate Server-2009
Certificado de sello electrónico de empresa.	1.3.6.1.4.1.17326.10.11.3	▶ 189KB		Se emite bajo AC Camerfirma Corporate Server-2009
<b>AC Firma de Código.</b>	1.3.6.1.4.1.17326.10.12.1		▶	▶
Certificado de firma de código.	1.3.6.1.4.1.17326.10.12.2	▶ 188KB		

Importe estos certificados en el almacén correspondiente según se indica en el punto [Importación del certificado de la CA que emite el certificado de firma de código del Componente de Firma.](#)



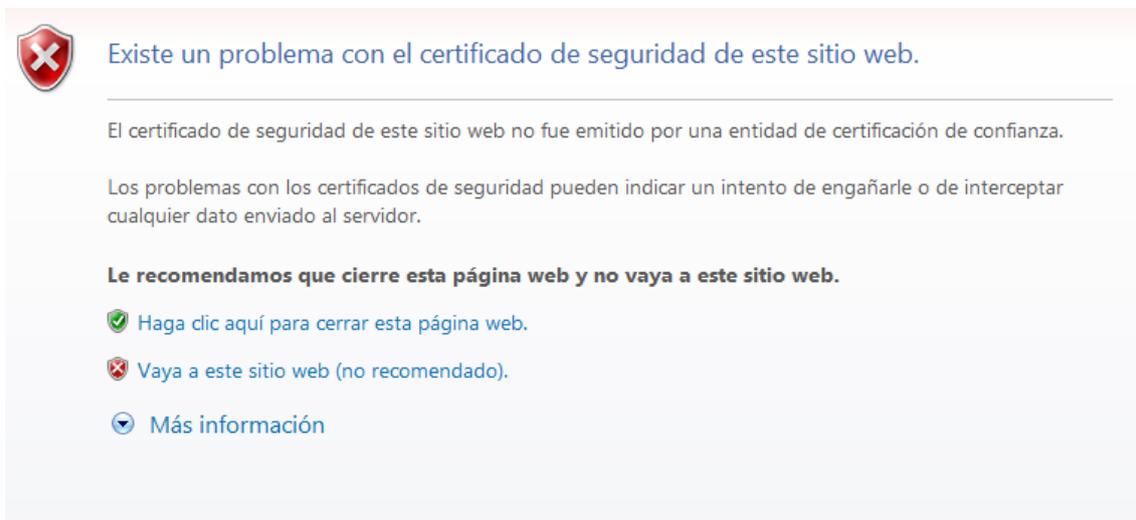
### 3 Acceso a servidores seguros

Algunas páginas de Oficina Virtual utilizan una conexión segura para el envío de información (https).

El certificado instalado en el servidor ha sido emitido por la CA "AC Camerfirma Express Corporate Server v3" de Camerfirma.

#### 3.1 Acceso a servidores seguros desde Internet Explorer

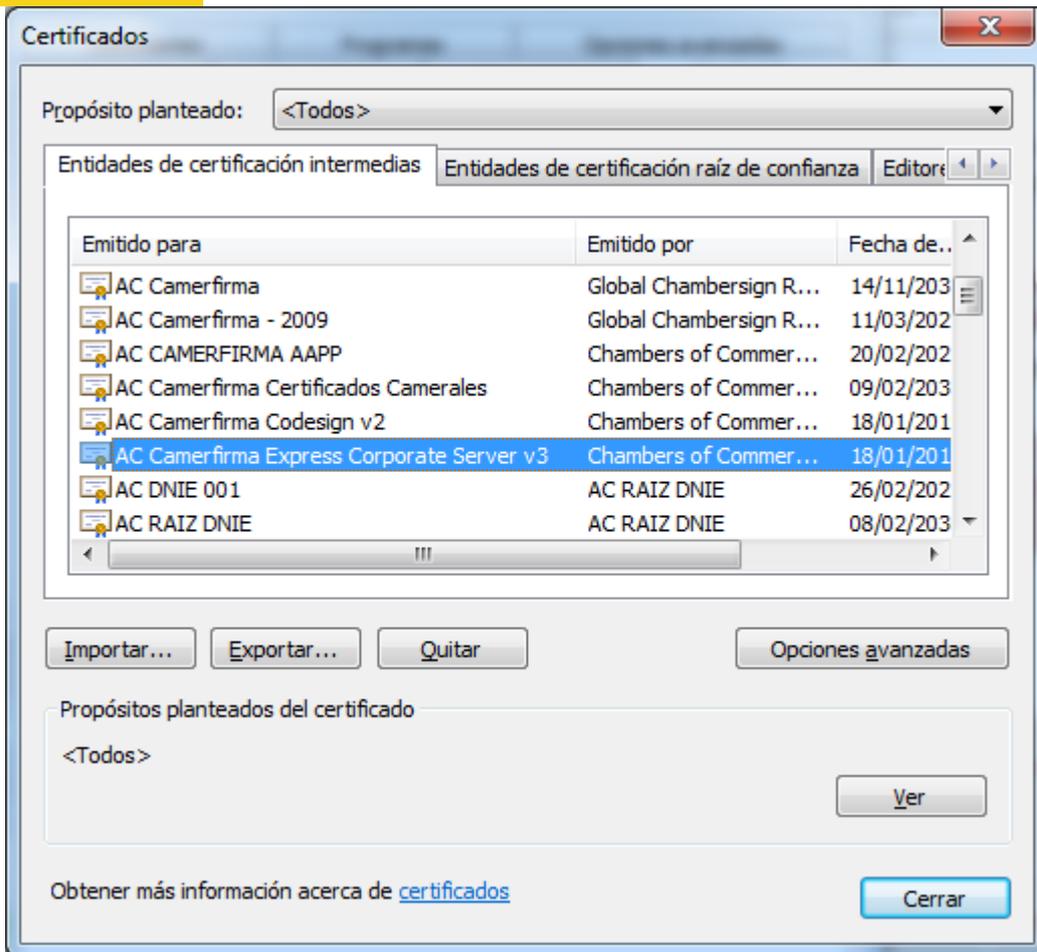
Si no tuviera cargado el certificado de la CA que ha emitido el certificado del servidor al que accede aparecerá la siguiente pantalla:



Para que este mensaje no aparezca en lo sucesivo debería cargar el certificado de la CA que ha emitido el certificado del servidor, siempre que confíe en él, aunque si no desea realizar esta operación puede pulsar "Vaya a este sitio web (no recomendado)", con lo que el mensaje continuará apareciendo en sucesivos accesos.

Para comprobar si dispone de este certificado puede hacerlo accediendo al menú *Herramientas->Opciones de Internet*, en la pestaña *Contenido* pulsando sobre el botón *Certificados* y accediendo a la pestaña *Entidades Emisoras raíz de confianza*.

Aparecerá una ventana con las entidades emisoras de confianza según aparece en la siguiente imagen:



Si no tiene instalado ese certificado en su navegador podrá descargarlo desde la página web de Camerfirma: <http://www.camerfirma.com/area-de-usuario/politicas-y-practicas-de-certificacion/> pulsando sobre el enlace v3 de la fila *AC Camerfirma Express Corporate Server*.

## Jerarquía Políticas y Prácticas de Certificació

Inicio / Usuarios / Jerarquía Políticas y Prácticas de Certificación

### Declaración de Practicas de Certificación (CPS/DPC)

Es el conjunto de prácticas adoptadas por un prestador de servicios de certificación para la emisión de certificados. Contiene información detallada sobre el sistema de seguridad, soporte, administración y emisión de los certificados,... y en general, una descripción de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

- » Acceso a la Declaración de Practicas de Certificación de AC Camerfirma (811KB).
- » 27/ABRIL/2011 NUEVA VERSION DPC v 3.2.3 (785KB).
- » AGOSTO/2012 NUEVA VERSION DPC v 3.2.5 (1.2MB).
- » MAYO/2013 NUEVA VERSION DPC v 3.2.6 (1.3MB).

**Jerarquías de Certificación** Estructura bajo la cual se emiten los distintos certificados digitales de Camerfirma. El objeto fundamental de la misma es construir una red de confianza para la emisión y gestión de los certificados digitales. Camerfirma dispone de dos Jerarquías, Chambersign Global Root y Chambers of Commerce Root, que emiten certificados en distintos ámbitos.

### Jerarquía Chambers of Commerce Root 1.3.6.1.4.1.17326.10.3.1

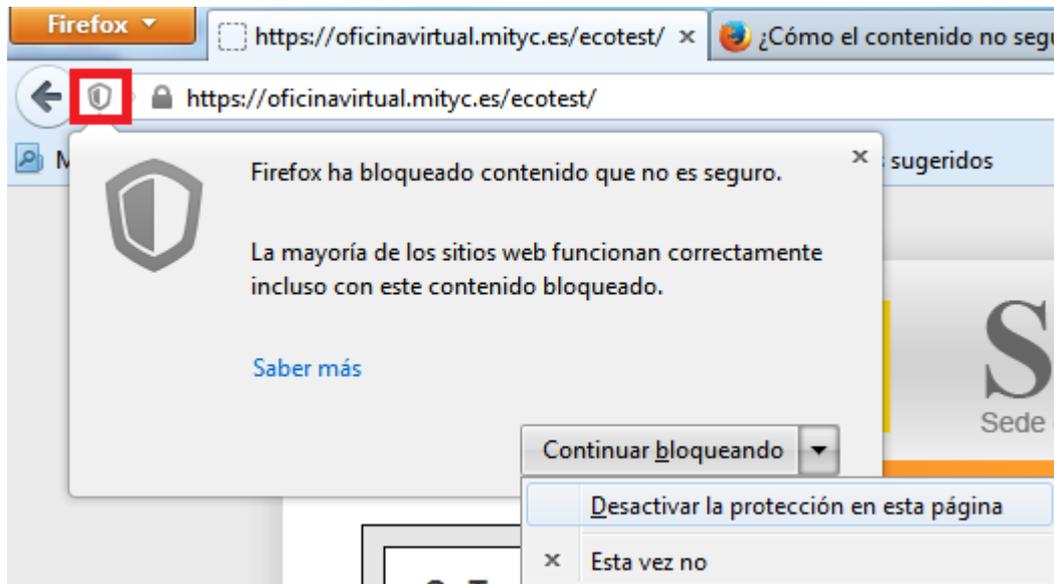
Esta Jerarquía está diseñada para construir una red de confianza que tiene por objeto fundamental la emisión de certificados digitales de identidad empresarial y donde las Autoridades de Registro (en adelante AR o AR's) suelen encontrarse gestionadas por las Cámaras de Comercio, Industria y Navegación.. Esta jerarquía incorpora Autoridades de Certificación intermedias que emiten certificados digitales empresariales en diferentes entornos. A continuación indicamos una relación de los certificados emitidos bajo esta Jerarquía y sus Autoridades de Certificación intermedias e incorporamos los datos del OID (Identificador de la Política de certificación del certificado), la correspondiente Política de Certificación, y en su caso un certificado de prueba:

Políticas de Certificación.				
	O.I.D.	Política	Actuales	ClavesNuevas
<b>CHAMBERS OF COMMERCE ROOT</b>	1.3.6.1.4.1.17326.10.3.1	 781KB		
<b>AC Camerfirma Express Corporate Server.</b>	1.3.6.1.4.1.17326.10.11.1		 v1  v3	Continuado en AC Camerfirma Corporate Server-2009
Certificados para servidor Seguro OV	1.3.6.1.4.1.17326.10.11.2	 183KB		Se emite bajo AC Camerfirma Corporate Server-2009
Certificado de sello electrónico de empresa.	1.3.6.1.4.1.17326.10.11.3	 189KB		Se emite bajo AC Camerfirma Corporate Server-2009
<b>AC Firma de Código.</b>	1.3.6.1.4.1.17326.10.12.1			
Certificado de firma de código.	1.3.6.1.4.1.17326.10.12.2	 188KB		

Una vez descargado podrá importarlo en su almacén del mismo modo que se indica en el apartado [Importación del certificado de la CA que emite el certificado de firma de código del Componentes de Firma.](#)

### 3.2 Acceso a servidores seguros desde Firefox

Si el certificado de la *AC Camerfirma Express Corporate Server v3* no se encuentra en su almacén de certificados aparecerá la imagen incluida dentro de un recuadro rojo en la siguiente imagen.



Pulse sobre la imagen, despliegue la lista de opciones y elija "*Desactivar la protección en esta página*".

Hecho esto podrá acceder al contenido de la página.