



**Govern de les Illes Balears**

Conselleria d'Economia, Hisenda i Innovació  
Direcció General de Tecnologia i Comunicacions

## **Tutorial - Certificados FNMT-Ceres**

## Uso de certificados digitales en la web de la CAIB

Para realizar trámites telemáticos, es necesario uno de los siguientes certificados digitales: DNle, ceres, tradise, camerfirma, firmaprofesional, ACA o ANCERT. (el listado completo se puede ver en

<http://www.caib.es/sacmicrofront/contenido.do?idsite=4225&cont=56025>

Para cualquier duda con el uso de certificados, puede llamar al 012.

## Obtención del certificado CERES y configuración para su uso en la web de la CAIB

Para obtener un certificado CERES (de persona física, el de persona jurídica no lo reconoce la CAIB), emitido por la Fábrica Nacional de Moneda y Timbre, debe realizar los siguientes pasos:

Para obtener el certificado si no tiene DNle:

<http://www.cert.fnmt.es/>

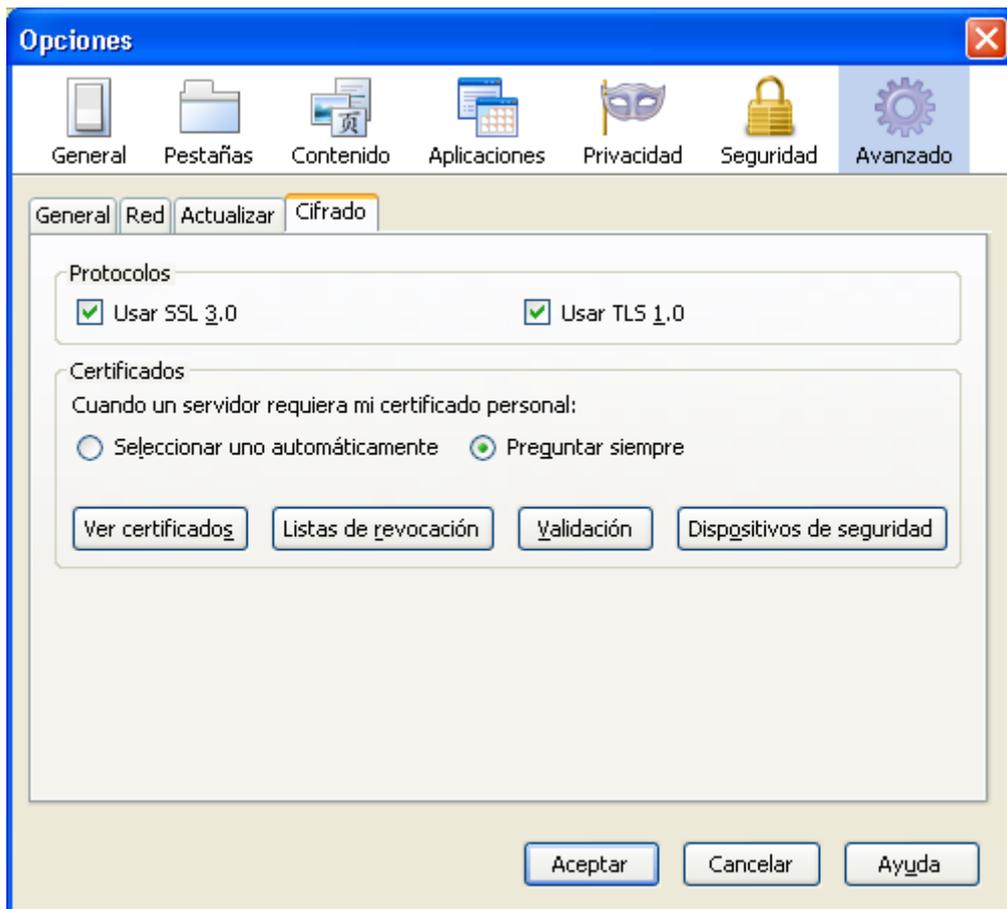
y seguir los pasos:

**Para realizar la solicitud, se recomienda usar el navegador Firefox.**

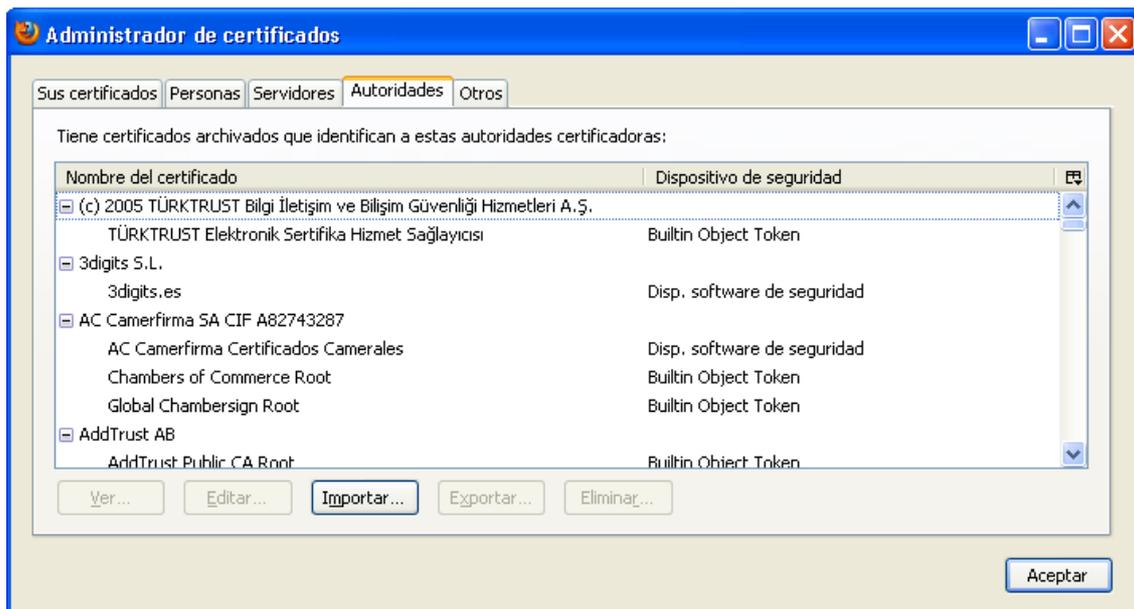
### Configurar el navegador FIREFOX:

-Debe instalar el certificado raíz de la FNMT para que el navegador admita la página de CERES como página de confianza. Para ello descargue el certificado "FNMT Clase 2 CA" de <https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt>

Guárdelo en el escritorio. Abra el firefox y vaya al menu Herramientas -> Opciones -> Avanzado



Ahora pulse el botón “Ver certificados” y vaya a la pestaña de “Autoridades”



Ahora pulse el botón “Importar” y busque el fichero que ha guardado anteriormente. Marque todas las casillas que aparecen en la pantalla siguiente:



Y finalmente pulse Aceptar.

Ahora puede volver a la página de Obtención del certificado y seguir en el paso 1.

## Solicitud del certificado

- En el paso 1 obtendrá un número de solicitud.

Si le aparece la siguiente pantalla:

 **Esta conexión no está verificada**

Ha pedido a Firefox que se conecte de forma segura a **rtir.caib.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.

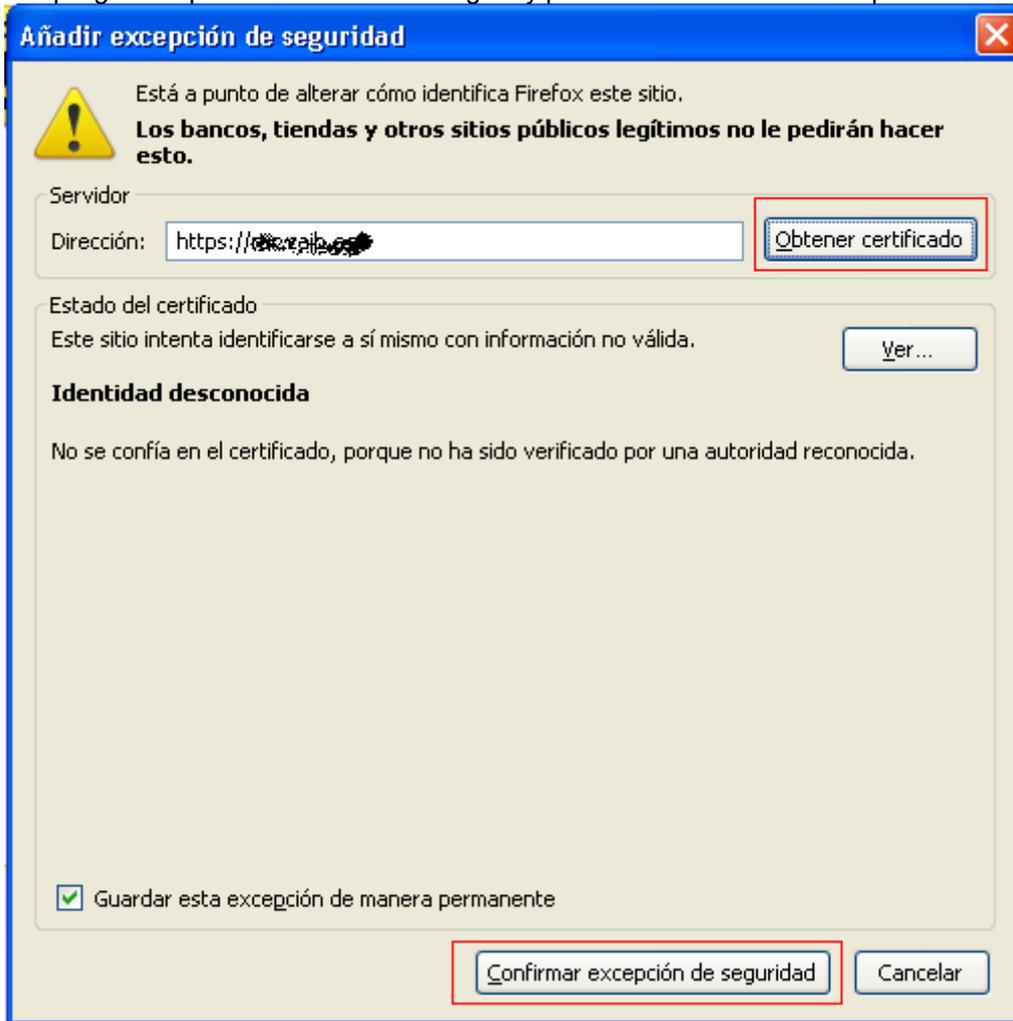
▶ **Detalles técnicos**

▼ **Entiendo los riesgos**

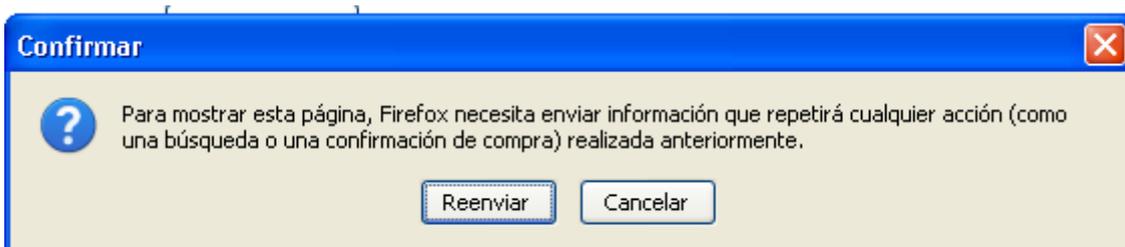
Si sabe lo que está haciendo, puede obligar a Firefox a confiar en la identificación de este sitio. **Incluso aunque confíe en este sitio, este error puede significar que alguien esté interfiriendo en su conexión.**

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

Despliegue la opción “Entiendo los riesgos” y pulse el botón “Añadir Excepción...”



Ahore pulse el botón “Obtener certificado” y después “Confirmar Excepción de seguridad” y confirme que desea reenviar la petición anterior:



## Acreditación de la identidad

En el paso 2 debe presentarse con el número de solicitud obtenido en el paso 1 y su DNI en una de las oficinas disponibles:

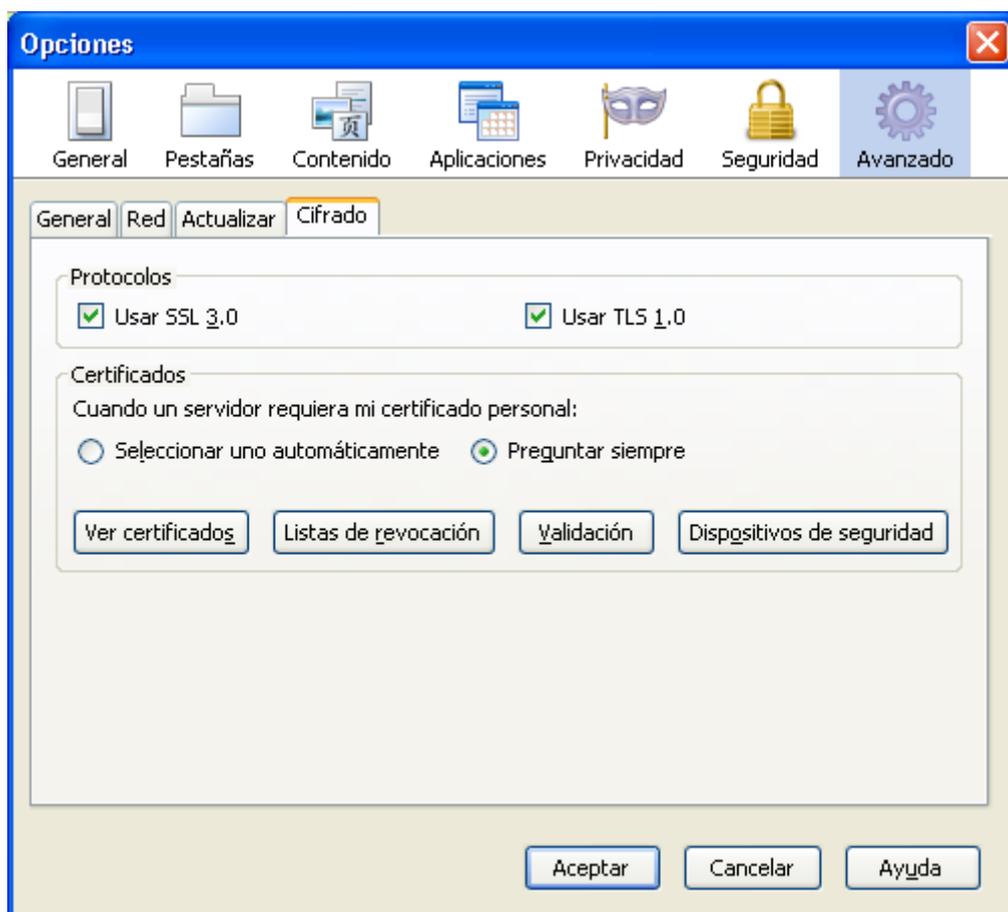
Puede buscar su oficina más cercana en:

<http://callejero.telefonica.es/PuntosCercanos/index.jsp?client=fnmt>

## Descarga y copia de seguridad del certificado

-En el paso 3 procederá a la descarga e instalación del certificado en su máquina.

-Una vez instalado el certificado, deberá acceder al menú del Internet explorer -> Herramientas -> Opciones -> Avanzado -> Cifrado



**En la pestaña de “Sus certificados” aparecerán sus certificados personales con clave privada.**

**Si no dispone de clave privada (error) aparecerán en la pestaña de “Personas”**

Una vez aquí, seleccione su certificado y pulse el botón de "Hacer Copia".

Seleccione la ruta donde desea guardar su Copia de seguridad

Introduzca la contraseña que desea que tenga la nueva copia de seguridad:

**Elegir una contraseña de respaldo para el certificado** 

La contraseña del certificado de respaldo que ponga aquí protegerá el archivo de respaldo que está a punto de crear. Debe poner esta contraseña para proceder con la copia de respaldo.

Contraseña de respaldo del certificado:

Contraseña de respaldo del certificado (confirmar):

Importante: si olvida la contraseña de respaldo de su certificado, no podrá restaurar esta copia de respaldo más tarde. Por favor, guárdela en un lugar seguro.

Medidor de calidad de la contraseña

Y pulse Aceptar

**Alerta** 

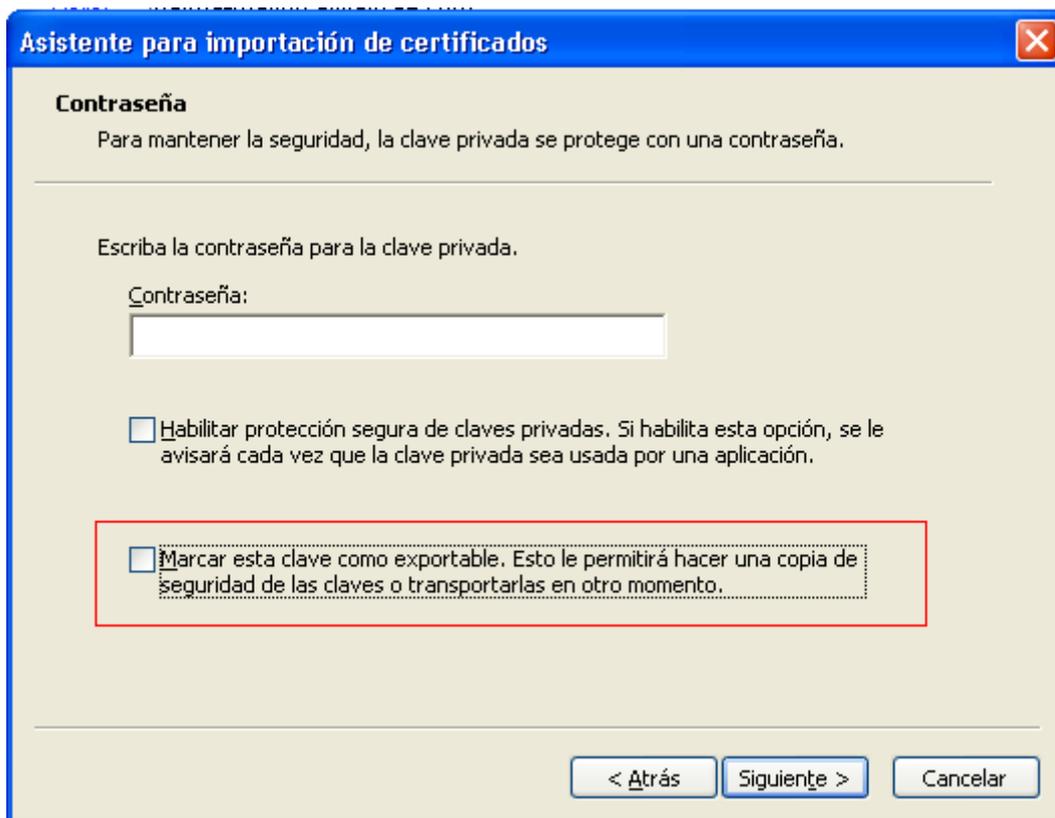
 La copia de seguridad de su(s) certificado(s) de seguridad y clave(s) privada(s) se ha realizado con éxito.

## Instalación del certificado para firma electrónica

**Para poder realizar firma electrónica del certificado, es imprescindible instalar su copia de seguridad del certificado en el navegador "Internet Explorer"**

Haga doble click sobre el fichero al que se ha exportado su certificado, y le aparecerá un asistente de importación de certificados. Introduzca la contraseña y asegúrese que la casilla que se indica en rojo no está marcada.

Si desea tener un nivel más alto de seguridad ( que para poder usar el certificado deba introducir una contraseña, deberá seleccionar la casilla "habilitar protección segura de claves privadas" y seleccionar el nivel alto.)



Una vez terminada la importación, ya se podrá usar el certificado CERES para realizar trámites telemáticos de la CAIB.

Advertencia: Si ha marcado la casilla de "habilitar protección segura de claves privadas", cuando acabe de importar el certificado, le aparecerá la siguiente ventana:



Pulse al botón marcado en rojo, y escoja una de las siguientes opciones:

- Nivel Alto: Le pedirá un PIN cada vez que quiera usar el certificado
- Nivel Bajo: Le mostrará una alerta cada vez que se vaya a usar el certificado

## Uso de los certificados CERES en la web de la CAIB:

Cuando acceda a una pantalla que requiera el uso de un certificado digital como el mostrado en la siguiente figura:

Formulario de carga de certificado digital. Incluye un botón "Cargar certificado", un menú desplegable "Certificados disponibles:" con la opción "EMPLEADO EMPLEADO DEMO" seleccionada, un campo de texto "PIN Certificado" y un botón "Inicia".

- Si no ha marcado la casilla de "habilitar protección segura de claves privadas", no deberá introducir ningún PIN cuando se le requiera para usar el certificado.
- Si ha marcado la casilla de "habilitar protección segura de claves privadas", "nivel bajo", tampoco deberá introducir ningún PIN cuando se le requiera para usar el certificado.
- Si ha marcado la casilla de "habilitar protección segura de claves privadas", "nivel alto", tampoco deberá introducir ningún PIN cuando se le requiera para usar el certificado, pero le aparecerá una ventana donde sí que deberá introducirlo.

Ventana de seguridad de firma que aparece al intentar usar un certificado. El título es "Se están firmando datos con su clave privada de firma". El mensaje principal dice: "Una aplicación está solicitando acceso a un elemento protegido." Hay un campo de texto "Clave privada de CryptoA" con caracteres ocultos por puntos y una casilla "Recordar contraseña" desmarcada. En la parte inferior hay botones "Aceptar", "Cancelar" y "Detalles...".