



Fundación Tripartita
PARA LA FORMACIÓN EN EL EMPLEO

**GUÍA DE USO E INSTALACIÓN DE
CERTIFICADOS DIGITALES EN EL SISTEMA
DE BONIFICACIONES 2009**

Marzo 2009



ÍNDICE

Introducción	1
Objetivos	2
Glosario de términos y acrónimos	2
Instalación de certificados y software asociado	3
Instalación de certificados.	3
Instalación en entornos Windows y utilización con Internet Explorer	3
Instalación en entornos Windows y utilización con Mozilla Firefox	8
Instalación en entornos no Windows o en entornos Windows con otros navegadores	11
Instalación de software necesario para la utilización de certificados en tarjeta. . . .	11
Instalación del runtime de Java (J.R.E.)	12
Uso de los certificados en la aplicación	13
Proceso de identificación de usuarios	13
Proceso de firma	15



Introducción

Los usuarios que deseen acceder y utilizar el sistema de Bonificaciones, han de contar necesariamente con un certificado, personal o de persona jurídica, y con la clave privada del mismo, de alguna de las Autoridades de Certificación siguientes:

- Autoridad Pública de Certificación Española CERES (www.ceres.fnmt.es)
- Cámaras de Comercio (www.camerfirma.com)
- Firmaprofesional, S.A (www.firmaprofesional.com)
- Izenpe, S.A (www.izenpe.com)
- Agencia Notarial de Certificación (ANCERT (www.ancert.com))
- Autoridad de Certificación de la Dirección General de la Policía (DNIe) (www.dnie.es)
- Autoridad de Certificación ANF AC (ANF <http://www.anf.es/anf/200.0.1.html>)
- DNI electrónico.

El certificado que se emplee para acceder a la aplicación ha de estar instalado en el navegador desde el que se accede, además se tendrá instalado el software y/o hardware necesario para el uso del certificado.

Los certificados se distribuyen habitualmente en software y tarjetas criptográficas (smart cards).

En el primer caso, el proceso de instalación del certificado bajo un navegador dado, almacena el certificado y la clave privada asociada en el disco duro del ordenador, en el almacén de certificados asociado al navegador (y al usuario en su caso), y su uso no requiere ni hardware ni software adicional.

En el caso de certificados en tarjeta, se requiere para su uso un lector de tarjetas, los drivers del mismo, así como las librerías necesarias para el manejo de la tarjeta (CSP o PKCS#11) que son suministradas por el fabricante de la tarjeta y/o emisor del certificado. En este caso, no se hace una «instalación» del certificado, sino del software necesario para la utilización de la tarjeta y los certificados mantenidos en ella, en el navegador correspondiente.

Adicionalmente a los elementos básicos para la utilización de certificados enumerados anteriormente, el sistema de Bonificaciones a través de sus páginas, accede a los certificados y los utiliza mediante programas Java (applets), por lo cual, es necesario contar con el entorno de ejecución Java (J.R.E.) en el ordenador desde el que se acceda a la aplicación.



Objetivos

Los objetivos de este documento son:

- Guiar la instalación de los certificados y del software requerido por el sistema de Bonificaciones para su uso;
- describir el modo de utilización de los certificados en el sistema de Bonificaciones.

Glosario de términos y acrónimos

Término/Acrónimo	Definición
PIF	Permiso Individual de Formación
AF	Acción Formativa
CA	Certification Authority
XML	Extensible markup language
LOPD	Ley Orgánica de Protección de datos.
FNMT	Fábrica Nacional de Moneda y Timbre.
CSP	Cryptographic Service Provider
PKCS#11	Interfaz de dispositivo criptográfico



Instalación de certificados y software asociado

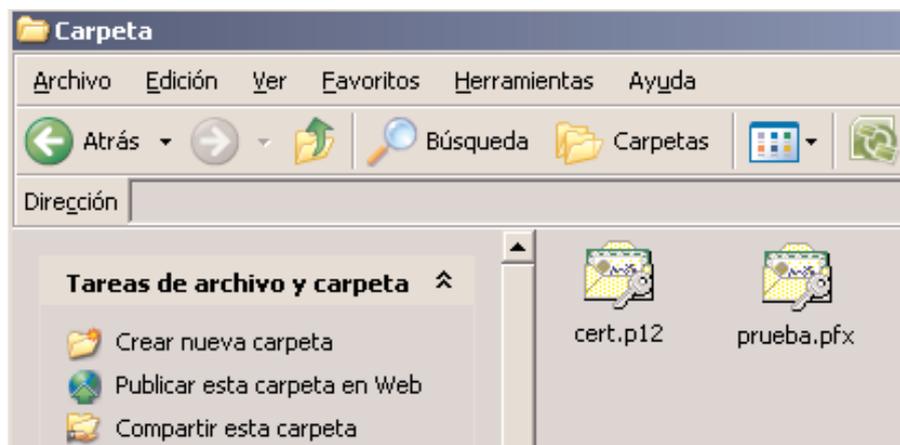
Instalación de certificados.

Sólo se instalan certificados, bajo un navegador, cuando estos se distribuyen en software. En este caso, el certificado y la clave privada correspondiente se encuentran en un fichero (habitualmente con extensión pfx ó p12) guardados en algún soporte magnético u óptico, como disquetes, memorias USB ó Cd-rom, por ejemplo. También es posible la instalación de certificados a descargándolos través de Internet, este es el modo en que algunas autoridades de certificación distribuyen los certificados que emiten. En este caso es necesario seguir las instrucciones dadas por el emisor del certificado para instalación.

Instalación en entornos Windows e utilización con Internet Explorer

Para instalar un certificado distribuido en software en un entorno Windows y para poder ser utilizado con el navegador Internet Explorer el proceso es el descrito a continuación:

- . Abrir la carpeta donde se encuentre el fichero contenedor del certificado y la clave privada y hacer doble click en él

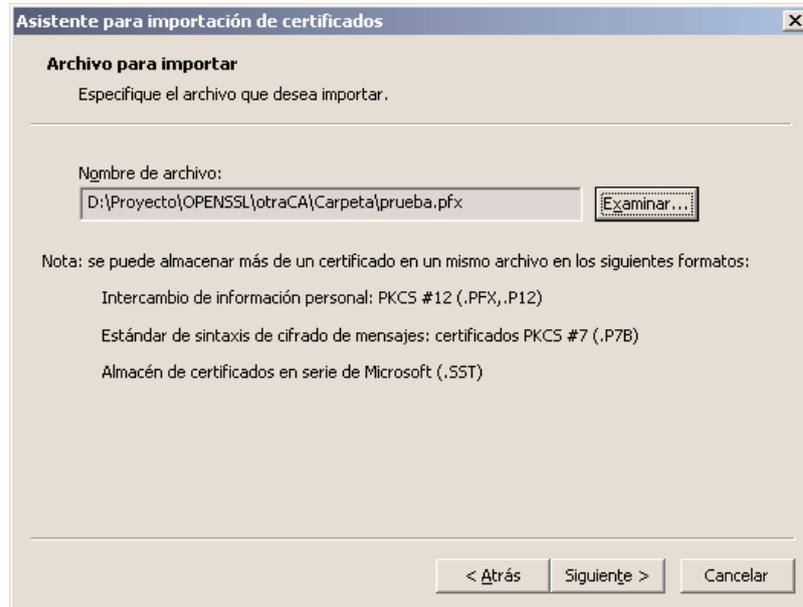


- . Tras hacer doble click se deben seguir los pasos del asistente.

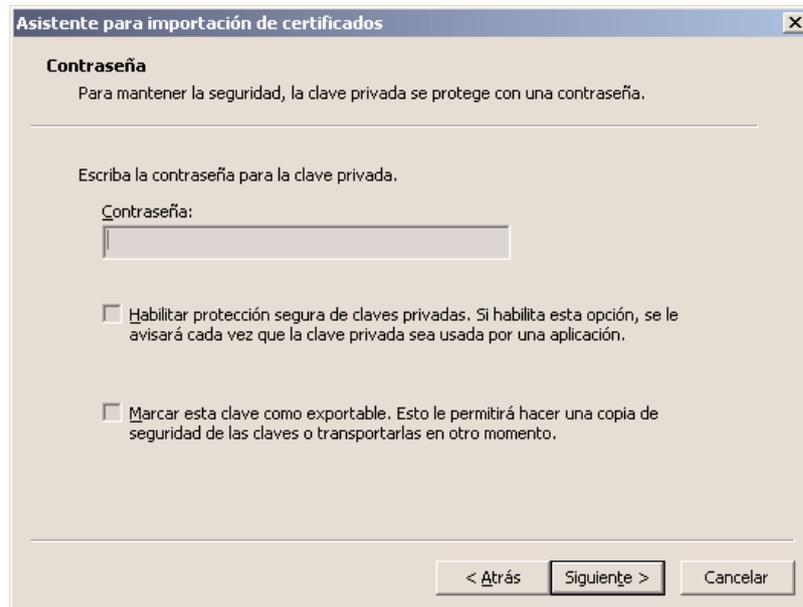




- Tras pulsar el botón «Siguiente» en la ventana de la imagen anterior, se mostrará la siguiente ventana.



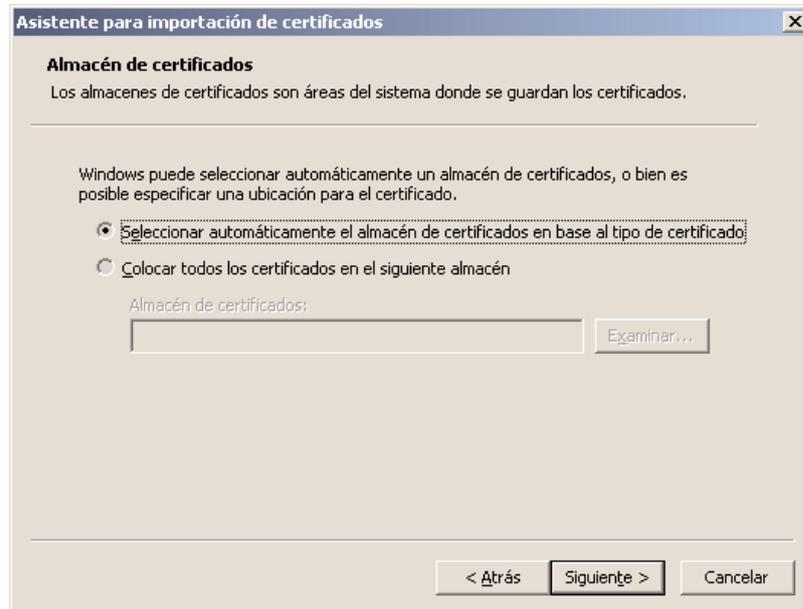
- Pulsamos de nuevo el botón «Siguiente», mostrándose la ventana siguiente en la que se ha de introducir la contraseña con la que se haya protegido el fichero.



- En la ventana mostrada se debe introducir la contraseña del fichero contenedor del certificado. En esta ventana se cuenta asimismo con opciones para posibilitar/denegar la exportación de la clave privada asociada al certificado y la habilitación de la protección de la clave privada. En el dialogo posterior no se muestran las ventanas que aparecerían al seleccionar esta última opción. Al introducir la contraseña y pulsar el botón «Siguiente», si la contraseña es correcta, se desplegará una ventana



como la de la siguiente imagen en las que se nos solicita el almacén de certificados en el que guardar el certificado y la clave privada del certificado. Se debe seleccionar la opción mostrada.

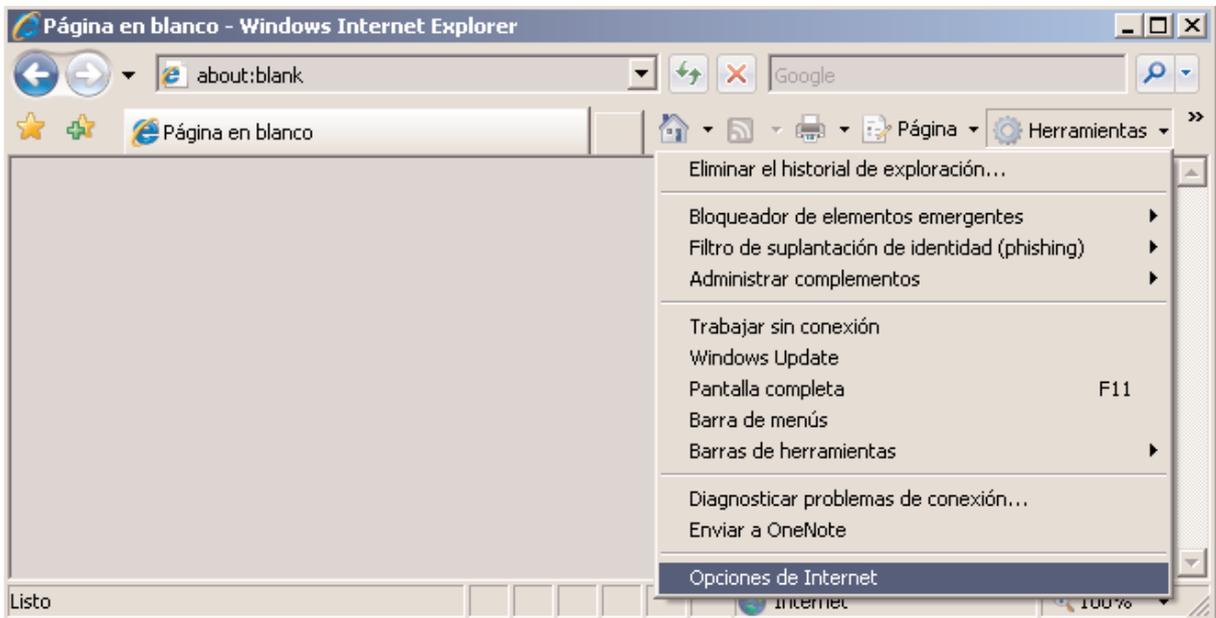


- Para finalizar, pulsar de nuevo el botón «Siguiete». El sistema informará del resultado de la instalación. En la que se pulsará el botón «Finalizar».

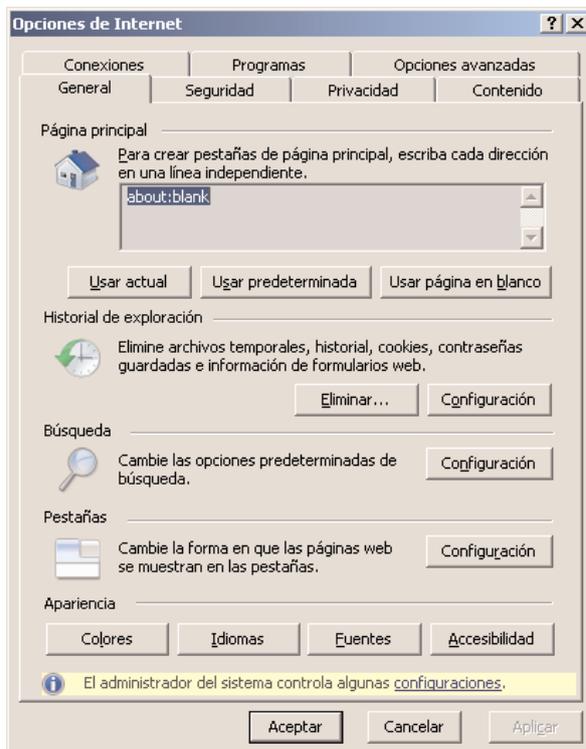




Para comprobar la correcta instalación del certificado, iniciar el navegador Internet Explorer, una vez iniciado, pulsar en el botón «Herramientas» y elegir «Opciones de Internet» entre las opciones desplegadas.



Con lo anterior se mostrará una ventana como la siguiente, en ella se selecciona la pestaña «Contenido».

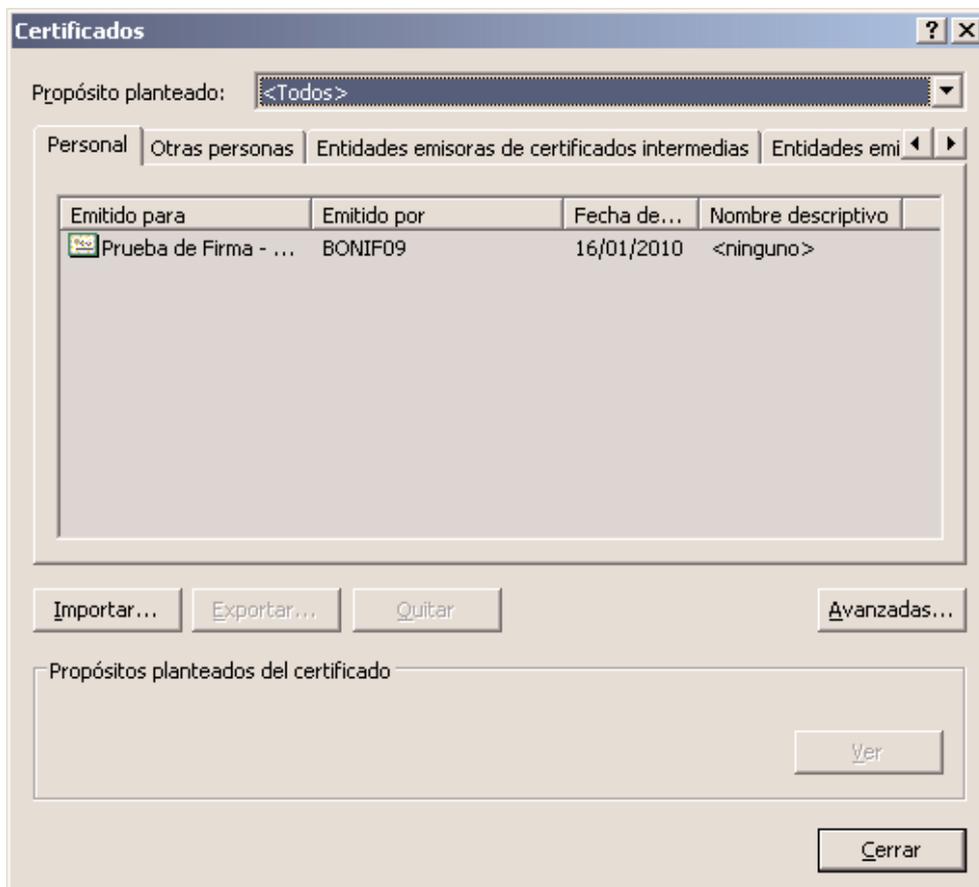




Dentro de la pestaña «Contenido» se ha de pulsar el botón «Certificados» para visualizar los certificados personales instalados.

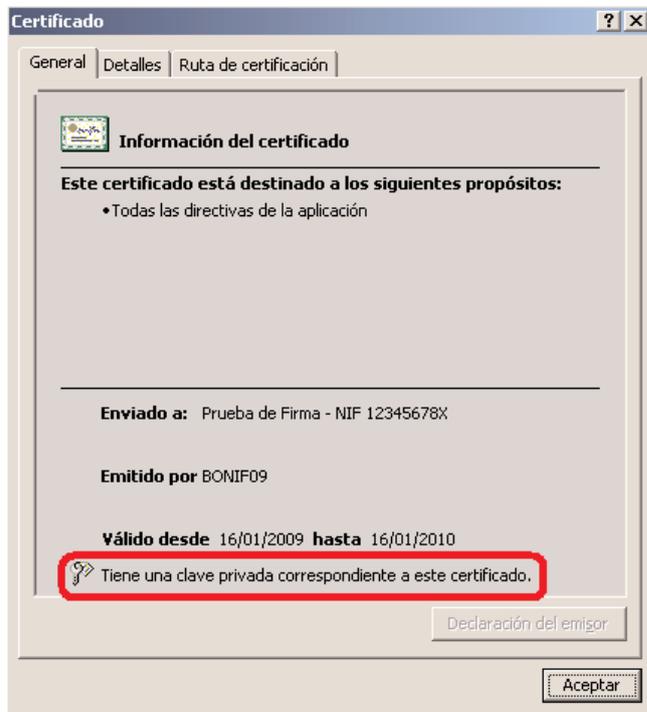


Los certificados personales se mostrarán en una ventana como la siguiente. Los certificados personales se mostrarán en la pestaña «Personal».





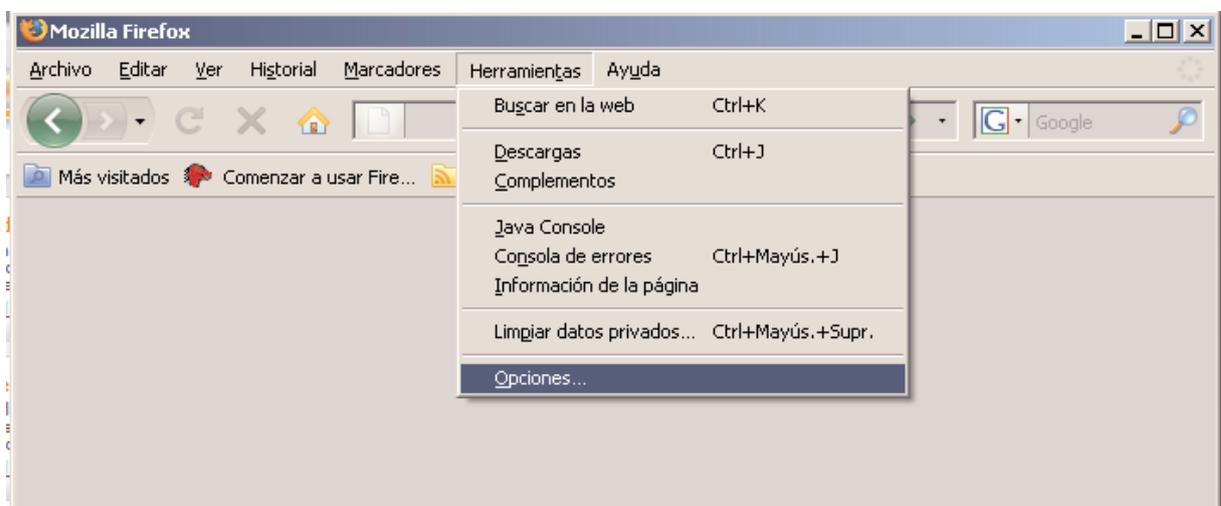
Haciendo doble click sobre el icono del certificado instalado deberemos ver una ventana como la mostrada a continuación en la que se pueden ver detalles del certificado y se informa de la posesión de la clave privada correspondiente del certificado (en la imagen se ha enmarcado en rojo esta información).



Instalación en entornos Windows e utilización con Mozilla Firefox

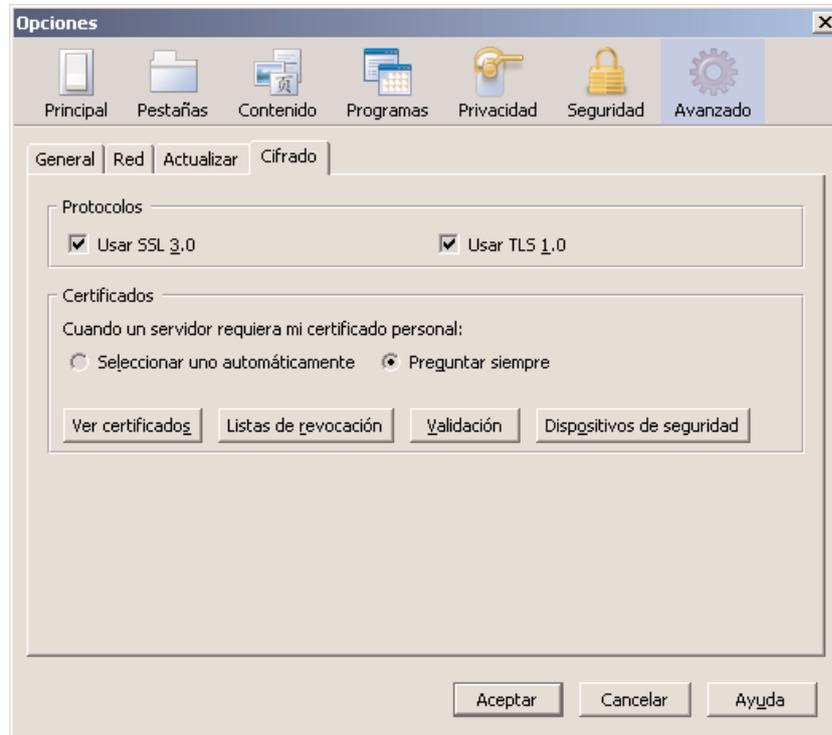
Para instalar un certificado distribuido en software en un entorno Windows y para poder ser utilizado con el navegador Fire Fox el proceso es el descrito a continuación:

- Iniciar el navegador y pulsar «Herramientas» y elegir «Opciones» entre las opciones mostradas.

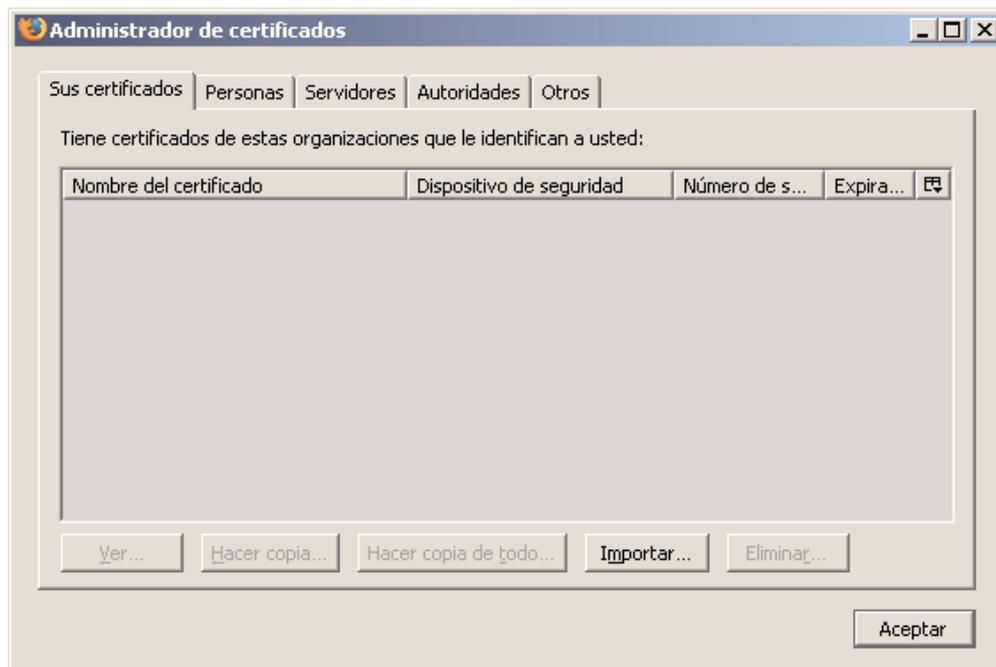




- Una vez realizado el paso anterior, se muestra la siguiente ventana en la que se seleccionará «Avanzado» (icono del engranaje) y se pulsará el botón en «Ver certificados».

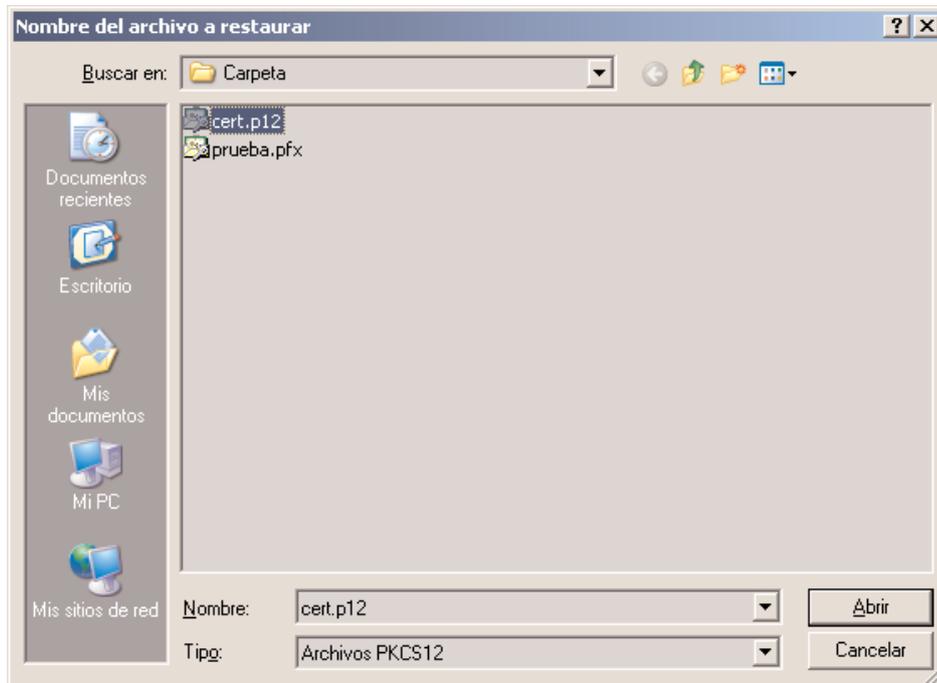


- Una vez pulsado el botón «Ver certificados» se mostrará una ventana en la que en la pestaña «Sus certificados» se mostrarán los certificados personales del usuario instalados o utilizables desde este navegador.

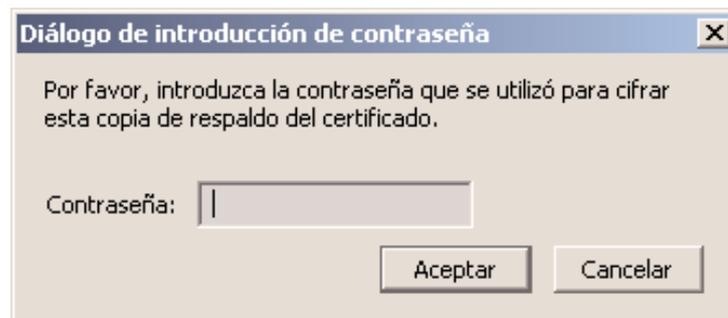




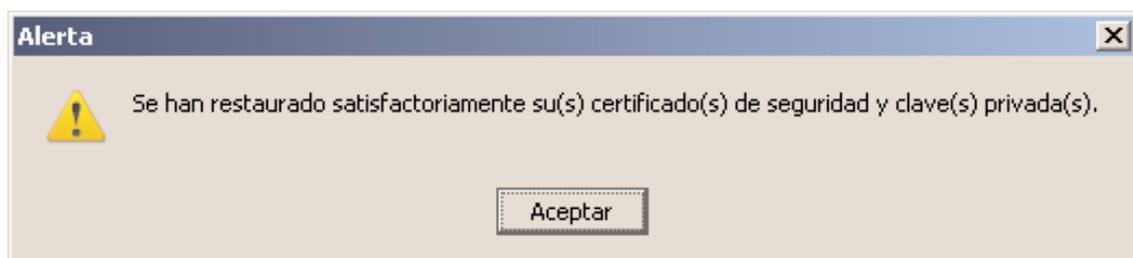
- Para instalar el certificado, pulsar el botón «Importar» y seguir los pasos del asistente. Seleccionar el fichero que contiene el certificado en la carpeta donde se halle y pulsar el botón «Abrir».



- Al pulsar el botón «Abrir», el instalador nos pedirá la contraseña del fichero contenedor del certificado y clave privada correspondiente.

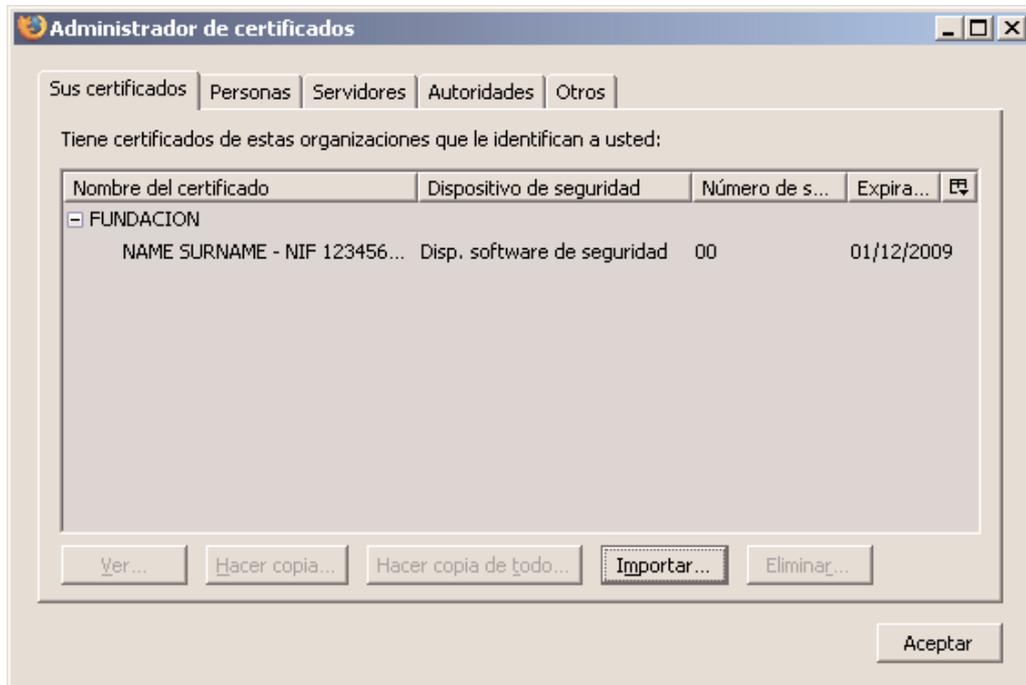


- Una vez introducida la contraseña del fichero, y tras pulsar el botón «Aceptar», si la contraseña es correcta, se mostrará una ventana informativa como la siguiente.





- Tras pulsar «Aceptar» en esta ventana, se mostrarán los certificados personales instalados en la primera ventana desplegada.



Instalación en entornos no Windows o en entornos Windows con otros navegadores

En estos casos se debe consultar la documentación al respecto del fabricante del navegador.

Instalación de software necesario para la utilización de certificados en tarjeta.

Para poder utilizar un certificado contenido en tarjeta criptográfica, primero es necesario contar con un lector de tarjetas y los drivers del mismo. Estos últimos son facilitados por el fabricante y/o emisor del certificado en tarjeta, para los sistemas operativos bajo los que el lector es utilizable.

Asimismo, el fabricante de la tarjeta y/o el emisor del certificado en tarjeta suministra los módulos necesarios para la utilización de la tarjeta en distintos sistemas operativos y navegadores. En general, se ha de disponer de un módulo CSP para la utilización de certificados en tarjeta en entornos Windows y con Internet Explorer y un módulo PKCS#11 para la utilización de los certificados en tarjeta en entornos Windows con navegadores distintos del Internet Explorer, Firefox por ejemplo, o en entornos no Windows.

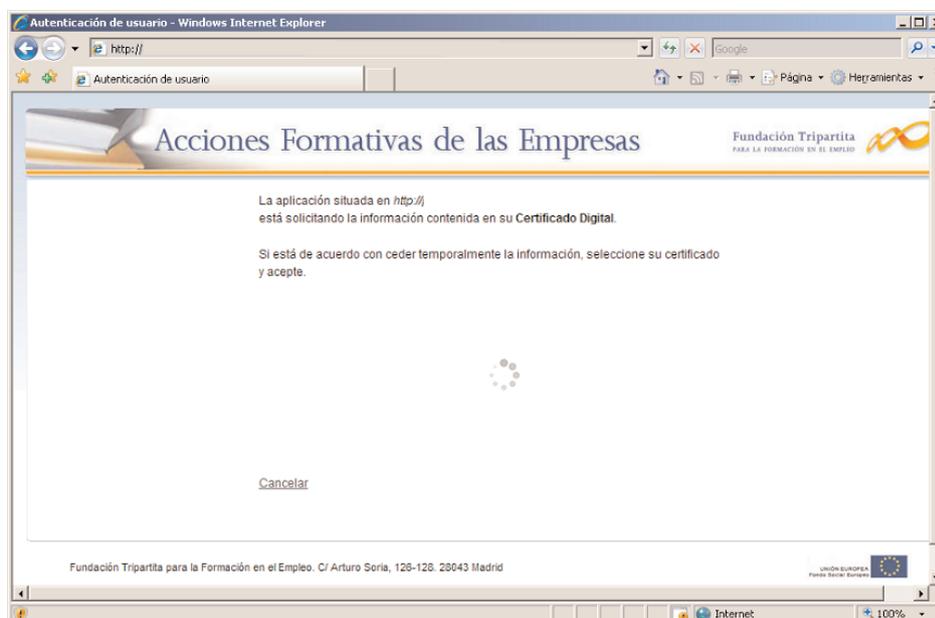


Instalación del runtime de Java (J.R.E.)

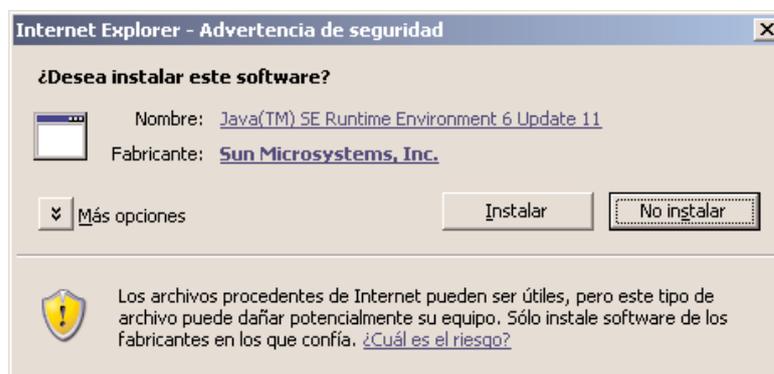
La versión mínima de Java requerida por el sistema de Bonificaciones para manejar certificados digitales y realizar firma electrónica es la 1.5.

Las páginas de la aplicación de Bonificaciones, que requieren la utilización de Java, invocan la instalación desde Internet en caso de que el entorno de ejecución de Java (JRE) no se encuentre instalado en el ordenador desde el que se accede.

Para acceder a la aplicación de Bonificaciones, lo primero que el usuario ha de hacer es solicitar desde un navegador la página inicial, donde el usuario se identifica con un certificado digital. Dicha página utiliza un programa Java (applet) para consultar los certificados personales digitales de las autoridades de certificación admitidas por la aplicación.



Por ejemplo, desde el Internet Explorer, en caso de que el sistema no tenga instalado el entorno de ejecución de Java, se mostrará una ventana como la siguiente para realizar la instalación.



Para instalar el entorno de ejecución de Java, pulsar el botón «Instalar» y seguir las instrucciones del instalador. Para poder realizar la instalación se han de aceptar las condiciones de la licencia que se muestran en el proceso de instalación.

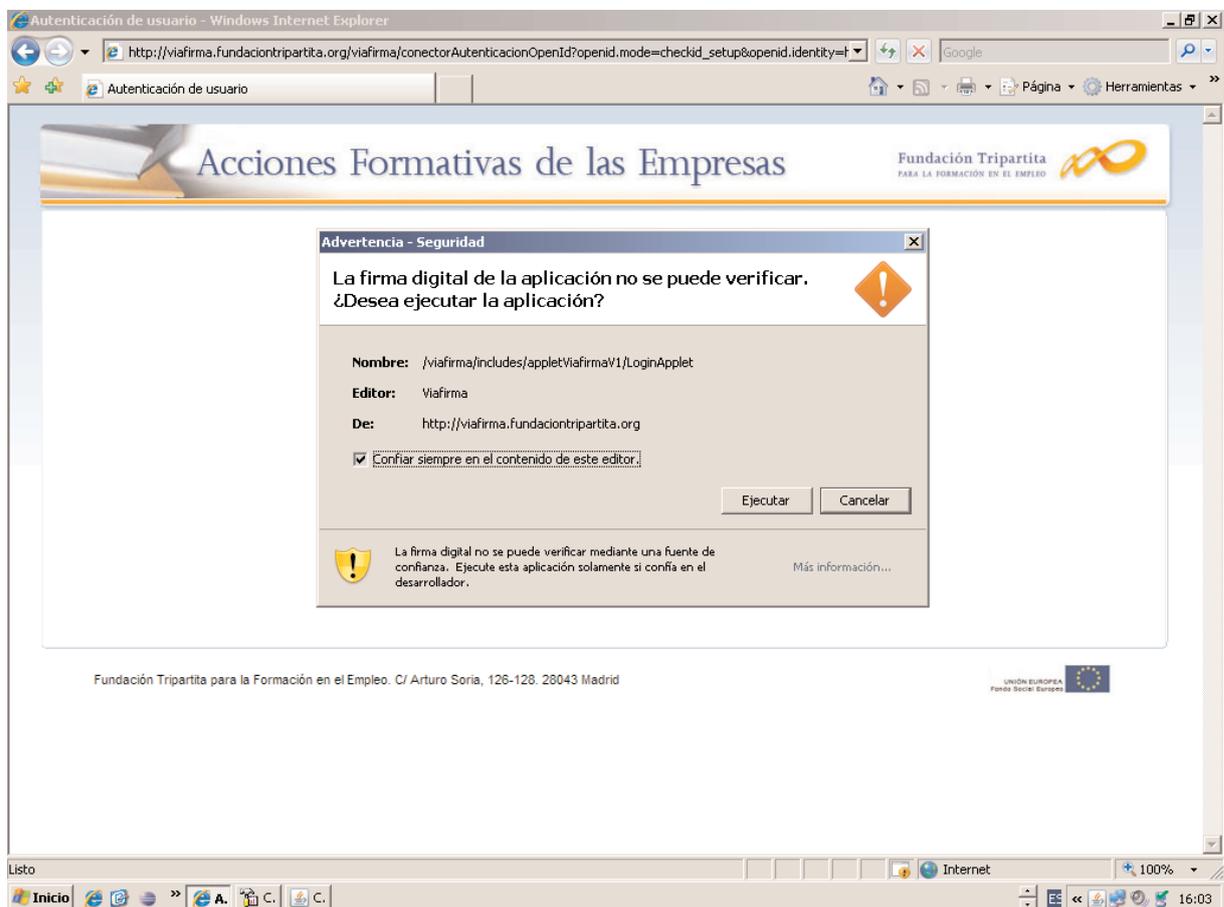


Uso de los certificados en la aplicación

La aplicación de Bonificaciones requiere el uso de certificados digitales, personales o de persona jurídica, en el proceso de identificación de usuarios, en el acceso, y en la firma de datos necesaria para realizar algunos trámites.

Proceso de identificación de usuarios

El proceso de identificación de usuarios por la aplicación se realiza en la página inicial, la invocación de esta página, solicitará al usuario el consentimiento para ejecutar un programa Java para detectar los certificados digitales. Con objeto de no tener que dar el consentimiento cada vez que se acceda a la aplicación, es aconsejable hacer check sobre la opción «Confiar siempre en el contenido de este editor» y pulsar el botón «Ejecutar».





Tras la operación anterior, el programa descargado buscará los certificados digitales del usuario y los mostrará para que el usuario elija aquel que utilizará para acceder a la aplicación. En las siguientes imágenes se muestra la secuencia descrita.

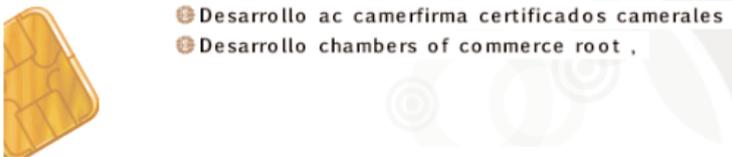
Espera mientras se recuperan los certificados almacenados en su sistema.



[Cancelar](#)

Certificados personales hallados.

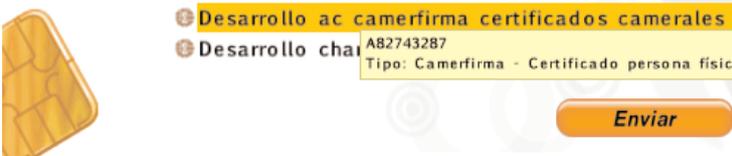
Seleccione el certificado que desea utilizar:



[Cancelar](#)

Selección del certificado a presentar para acceder a la aplicación.

Seleccione el certificado que desea utilizar:



[Cancelar](#)

Al pulsar el botón «Enviar», se remite al servidor el certificado para validar su autenticidad, vigencia, no revocación y haber sido emitido por alguna de las Autoridades de Certificación aceptadas por el sistema. En caso de no ser auténtico, o estar caducado, o no estar aún vigente, o haber sido revocado o no poder verificar su no revocación, o no haber sido emitido por una Autoridades de Certificación aceptada, se impide el acceso al sistema y se informa al usuario del problema detectado.

En caso de superar las validaciones expuestas, se obtiene el NIF (y el CIF en el caso de certificado de persona jurídica) y se contrasta la autorización de acceso del usuario a la aplicación.



Proceso de firma

Como se ha indicado anteriormente, la aplicación, actualmente, requiere la firma digital de datos para realizar los siguientes trámites:

- Alta de usuario
- Borrado de usuario
- Inicio de grupo
- Inicio de PIF
- Fin de grupo
- Fin de PIF
- Fin de acción formativa
- Desfinalización de grupo
- Desfinalización de acción formativa
- Anular grupo
- Anular PIF notificado
- Alta empresa participante

Para realizar cualquiera de estos trámites, se muestra un formulario con los datos del trámite a realizar y un botón para realizar la firma o cancelar la acción.

Bonificación mensual:	
Mes	Bonificación
Febrero	1,01 €
Marzo	2,02 €
Junio	10,22 €

Estado tras la notificación

Si procede a realizar la notificación con los datos arriba indicados:
a) El estado del PIF será **Notificado**

Al pulsar el botón «Firmar» se invoca al proceso de firma de la aplicación, que recibirá los datos a firmar, y buscará el certificado con el que se ha de realizar la firma (que debe ser el utilizado para acceder a la aplicación, salvo en el caso del DNIe, que se habrá de utilizar el certificado de firma del DNIe).

Firma de ficheros por el usuario - Windows Internet Explorer

http://viafirma.fundaciontripartita.org/viafirma/connectorFirmaOpenId

Acciones Formativas de las Empresas

Fundación Tripartita
PARA LA FORMACIÓN EN EL EMPLEO

Para completar el proceso de firma, compruebe la información que aparece en el documento a firmar, seleccione un certificado digital válido y pulse en Firmar.

Seleccione el certificado que desea utilizar:

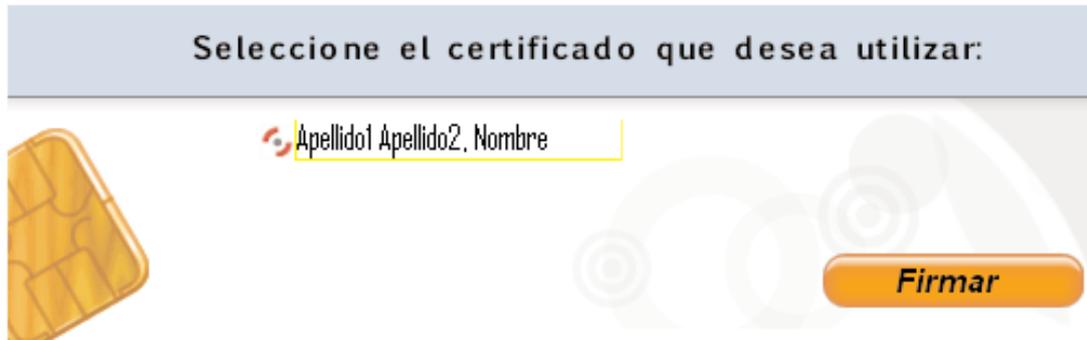
Apellido1 Apellido2, Nombre

[Si lo desea puede descargar el documento a firmar.](#)

Cancelar



A continuación, se ha de seleccionar el certificado y pulsar el botón Firmar.



[Si lo desea puede descargar el documento a firmar.](#)

[Cancelar](#)

El sistema realizará la firma de los datos pasados a la firma y realizará las actualizaciones correspondientes en la aplicación para realizar el trámite «solicitado.»