Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Instalación de
Certificados Digitales
en la iniciativa de Formación Programada por las Empresas

Guía de uso

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

ÍNDICE

1. Introducción

Los usuarios que deseen acceder y utilizar la iniciativa de Formación Programada por las Empresas, 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.cert.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 www.anf.es)
- Agencia Catalana de Certificación (CATCert www.catcert.cat)
- Autoridad de Certificación de la Comunidad Valenciana (ACCV www.accv.es)
- DNI electrónico

El certificado que se emplee para acceder a la aplicación de Formación Programada por las Empresas 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, en la iniciativa de Formación Programada por las Empresas 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.

1.1. Objetivos

Los objetivos de este documento son:

- Guiar la instalación de los certificados y del software requerido para la iniciativa de Formación Programada por las Empresas para su uso.
- Describir el modo de utilización de los certificados en la iniciativa de Formación Programada por las Empresas.

1.2. 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.

2. Instalación de certificados y software asociado

2.1. Instalación de certificados

Sólo se instalan certificados bajo un navegador, cuando estos se distribuyen en software.

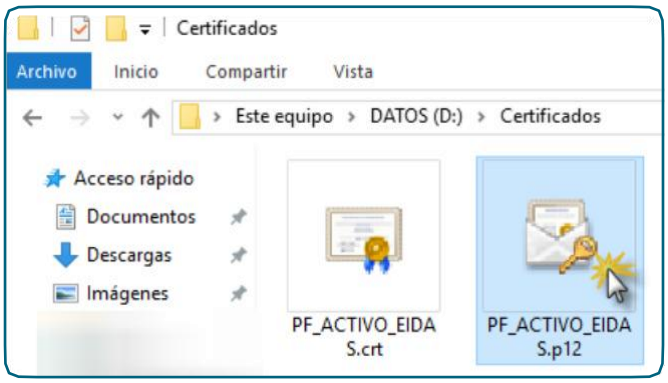
En este caso, el certificado y la clave privada correspondiente se encuentran en un fichero (habitualmente con extensión pfx o p12) guardados en algún soporte magnético u óptico, como disquetes, memorias USB o Cd-rom, por ejemplo.

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.

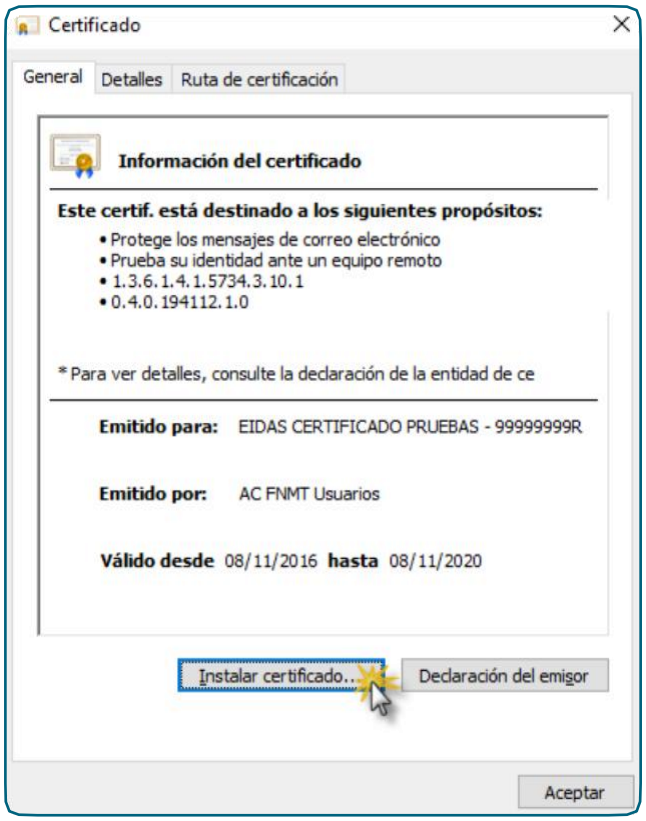
2.1.1. Instalación en entornos Windows y utilización con Internet Explorer

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 que se describe a continuación:

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

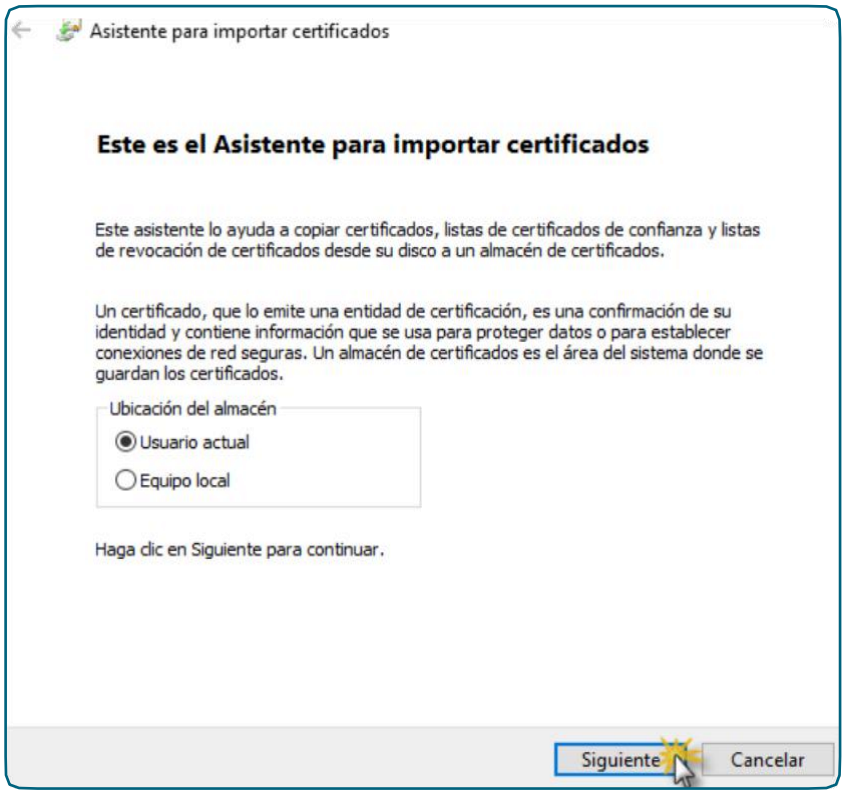


Si el certificado no está protegido con una clave privada, se abre un cuadro de diálogo en el que se muestran sus propiedades para que comprobemos la información mostrada y, si esta es correcta y pulsamos el botón **Instalar certificado**... continuando con las indicaciones del asistente.

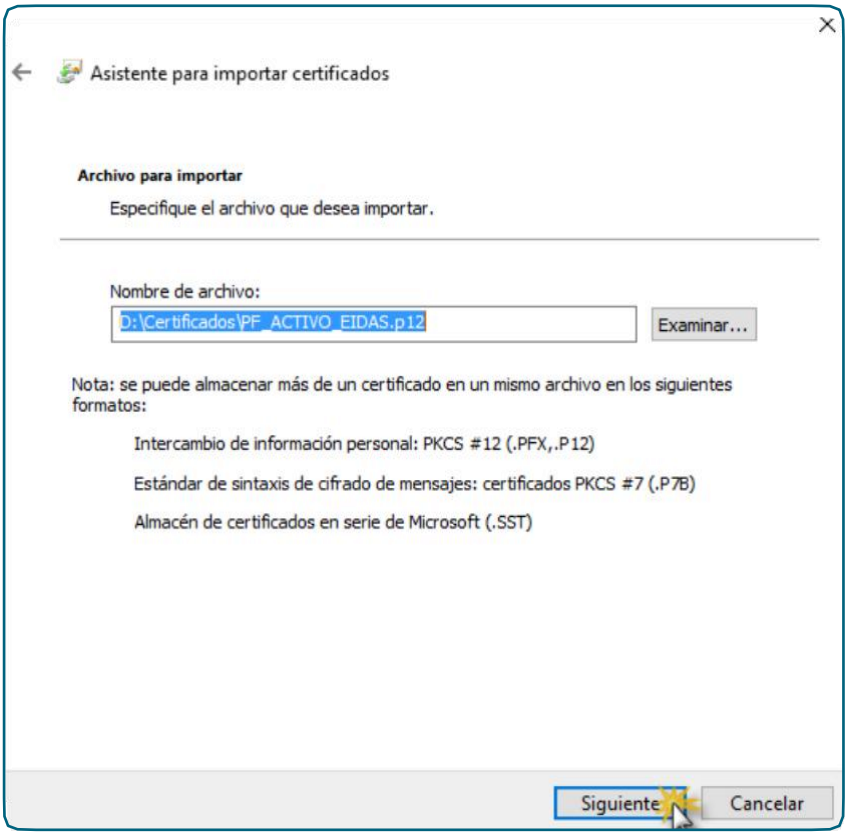


Para aquellos certificados protegidos con clave privada, la primera pantalla que nos va a mostrar el asistente nos permite seleccionar la **ubicación del almacén** en el que queremos instalar el certificado pudiendo seleccionar entre **Equipo local** o **Usuario actual**. En función de las necesidades de cada instalación, se seleccionará una u otra.

Si seleccionamos Equipo local, el certificado estará disponible para su uso, independientemente del usuario que esté logado a la máquina.

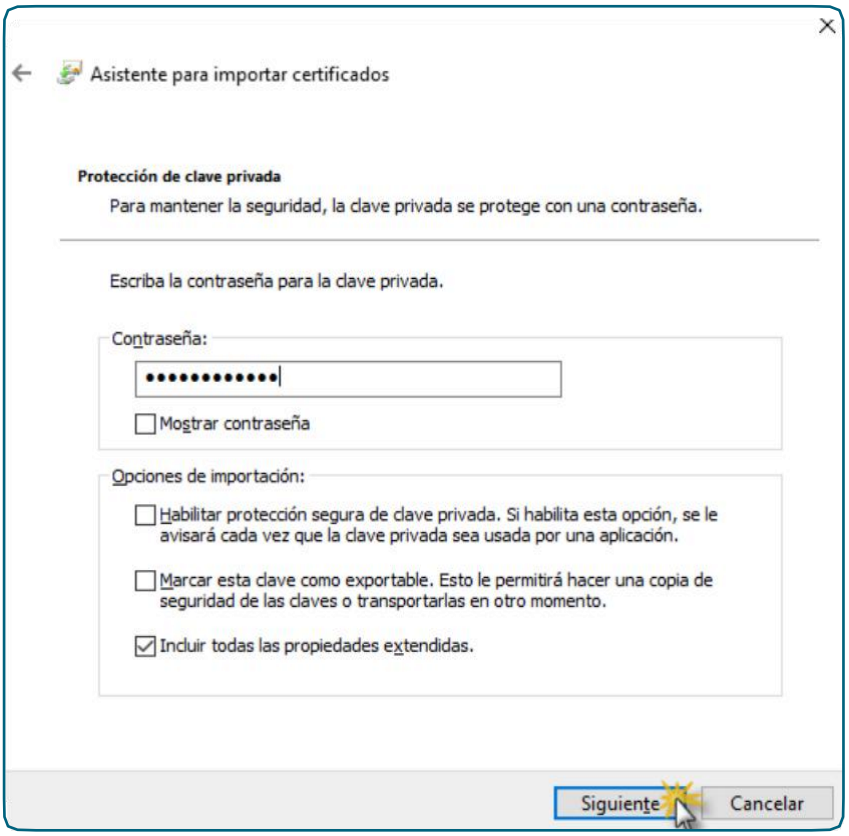


Al pulsar **Siguiente**, nos aparece una ventana en la que nos pide que especifiquemos el certificado que queremos instalar. Por defecto, nos va a aparecer seleccionado el que estamos instalando.



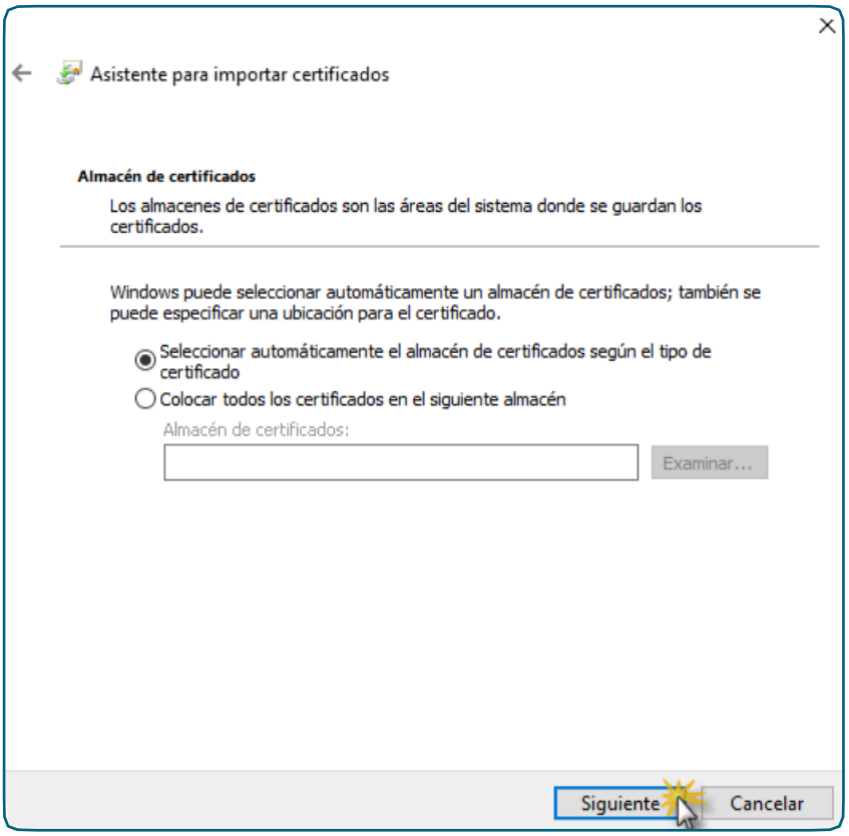
Al continuar con el asistente, nos va a pedir la contraseña del fichero contenedor del certificado.

En esta ventana se cuenta asimismo con opciones para permitir o no la exportación de la clave privada asociada al certificado y la habilitación de la protección de esta clave privada. En el dialogo posterior no se muestran las ventanas que aparecerían al seleccionar esta última opción.

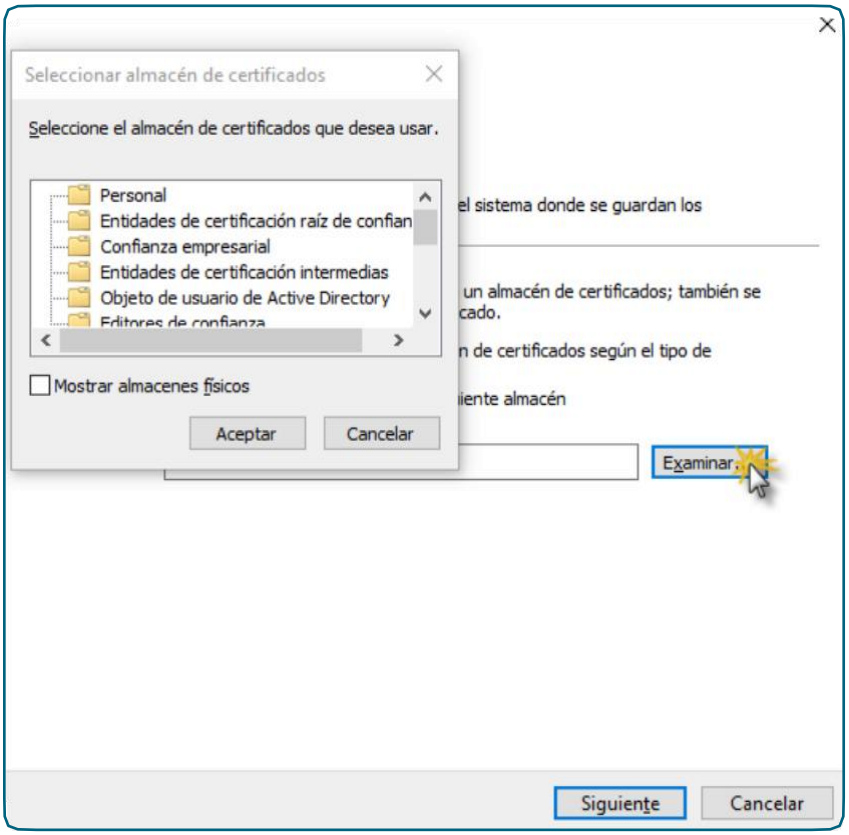


Al introducir la contraseña y pulsar el botón **Siguiente**, si la contraseña es correcta, se despliega una ventana en la que le vamos a indicar **en qué almacén** de certificados queremos que se guarde el certificado y su clave privada.

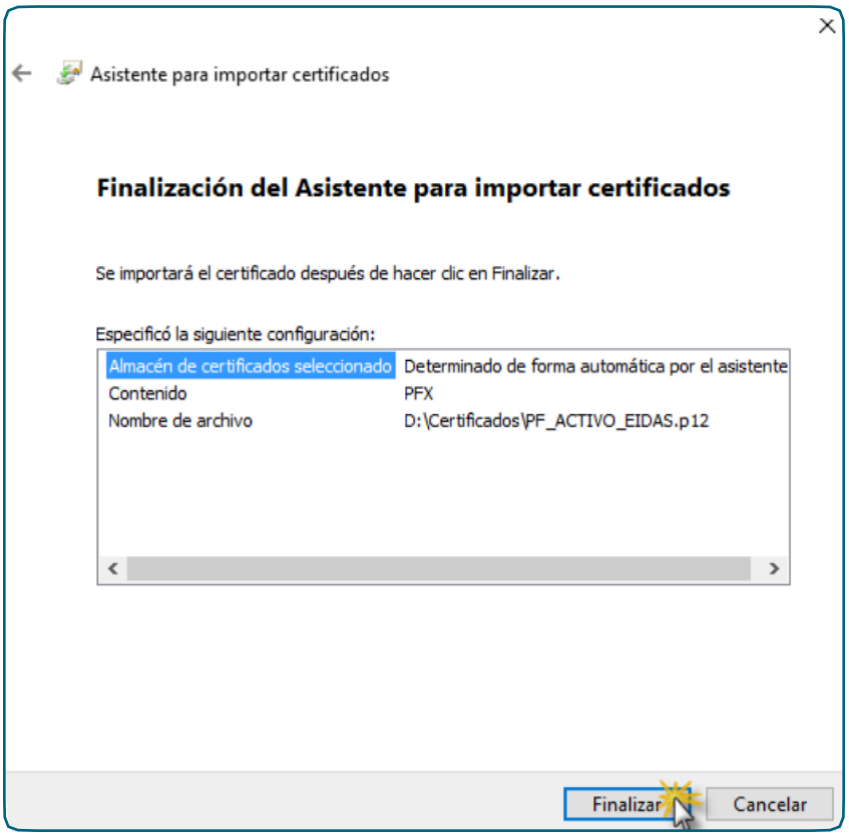
La **opción recomendada** es «Seleccionar automáticamente el almacén de certificados según el tipo de certificado».



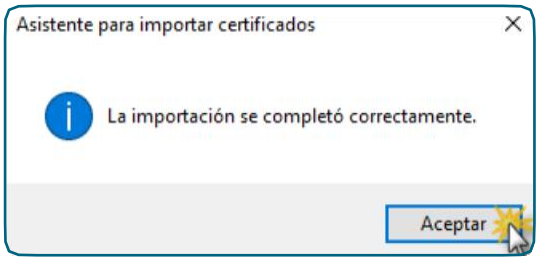
Si seleccionamos «Colocar todos los certificados en el siguiente almacén», cuando pulsamos sobre Examinar, nos aparece un cuadro de diálogo para que seleccionemos el almacén en el que lo vamos a alojar.



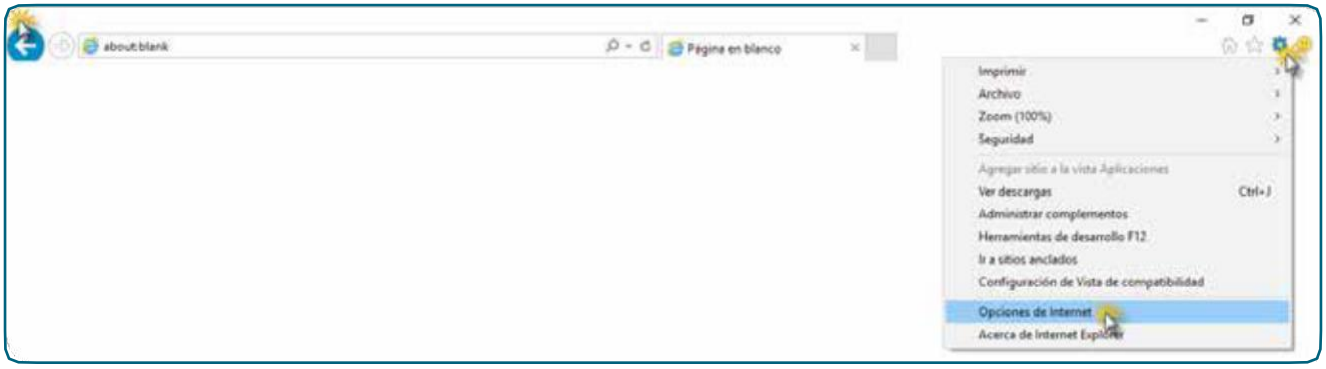
Una vez seleccionado el almacén, continuamos con la instalación y antes de finalizar, el asistente nos informa de la configuración que hemos seleccionado. Si está todo correcto y de acuerdo a la configuración que nos interesa, pulsamos **Finalizar**.



A continuación se muestra un cuadro de diálogo en el que se nos informa de que la importación se completó correctamente y pulsamos **Aceptar**.

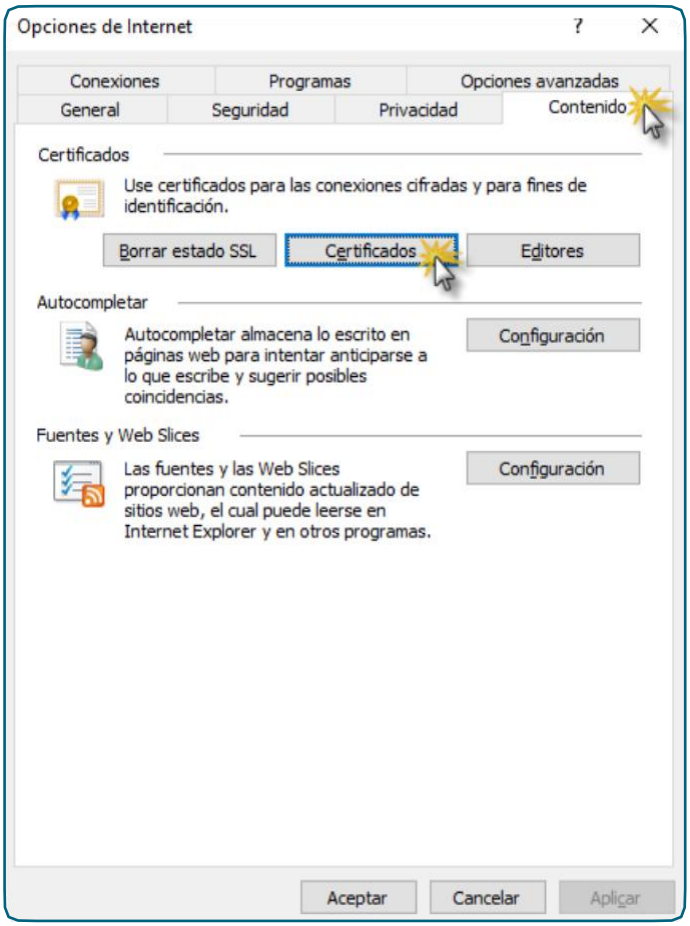


Para comprobar la correcta instalación del certificado, iniciamos el navegador Internet Explorer. Una vez iniciado, pulsamos sobre el botón **Herramientas** y elegimos **Opciones de Internet** entre las opciones desplegadas.

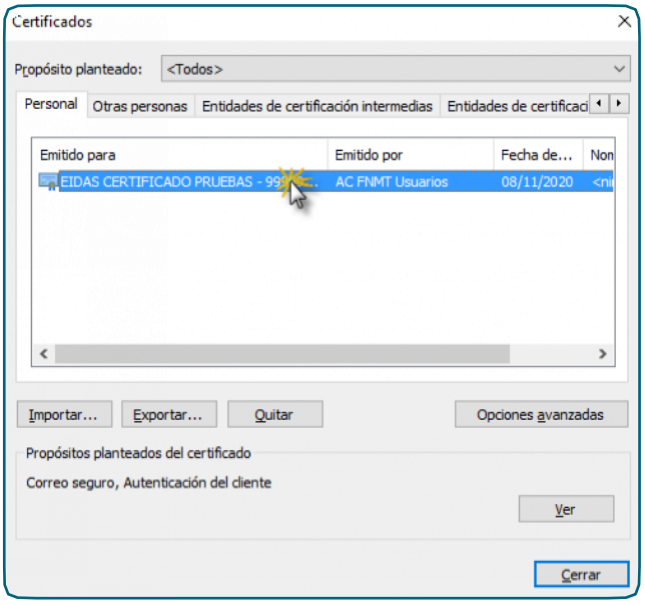


En la ventana que nos aparece a continuación, seleccionamos la pestaña Contenido.

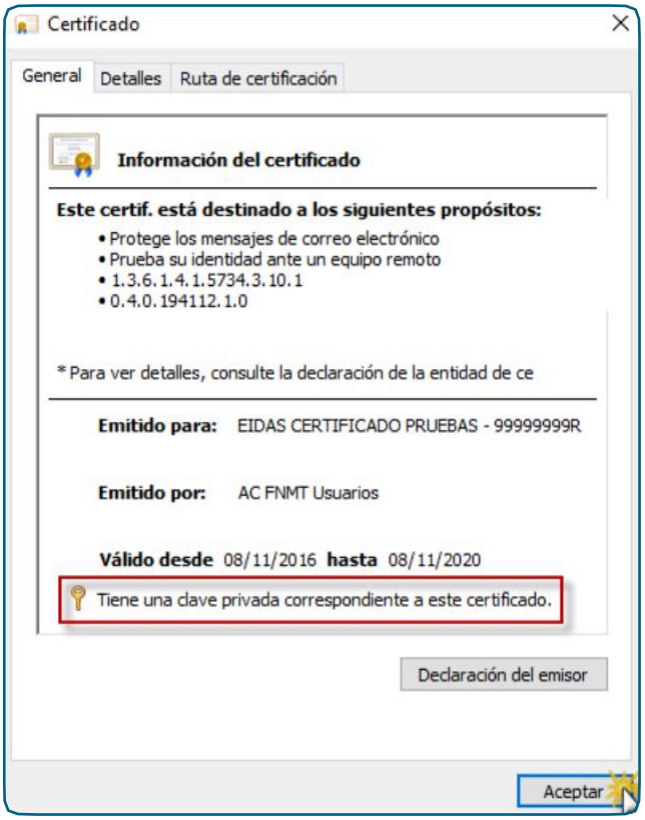
Dentro de la pestaña Contenido, pulsamos el botón **Certificados** para que se nos muestre en una nueva ventana con los certificados que tenemos instalados en el equipo.



Los certificados personales se muestran en la pestaña Personal de esta pantalla.



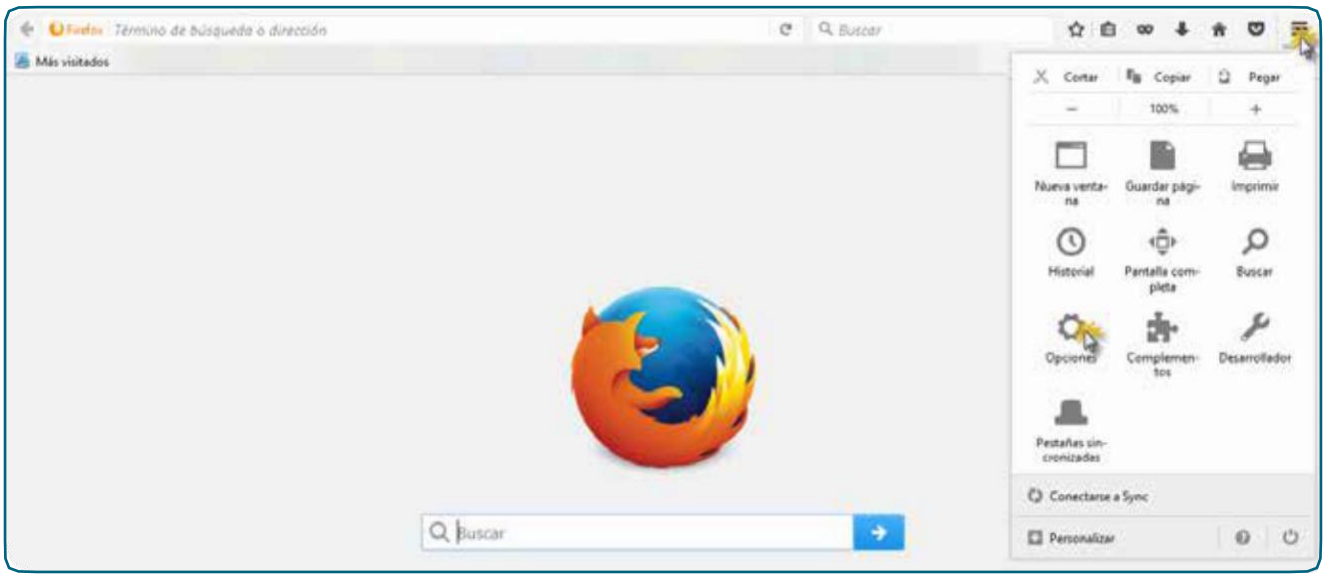
Haciendo **doble click** sobre el icono del certificado instalado deberemos ver una ventana como la mostrada a continuación en la que se pueden ver detalles del certificado y se informa de la posesión de la clave privada correspondiente del certificado (en la imagen se ha enmarcado en rojo esta información).



2.1.2. Instalación en entornos Windows y utilización con Mozilla Firefox

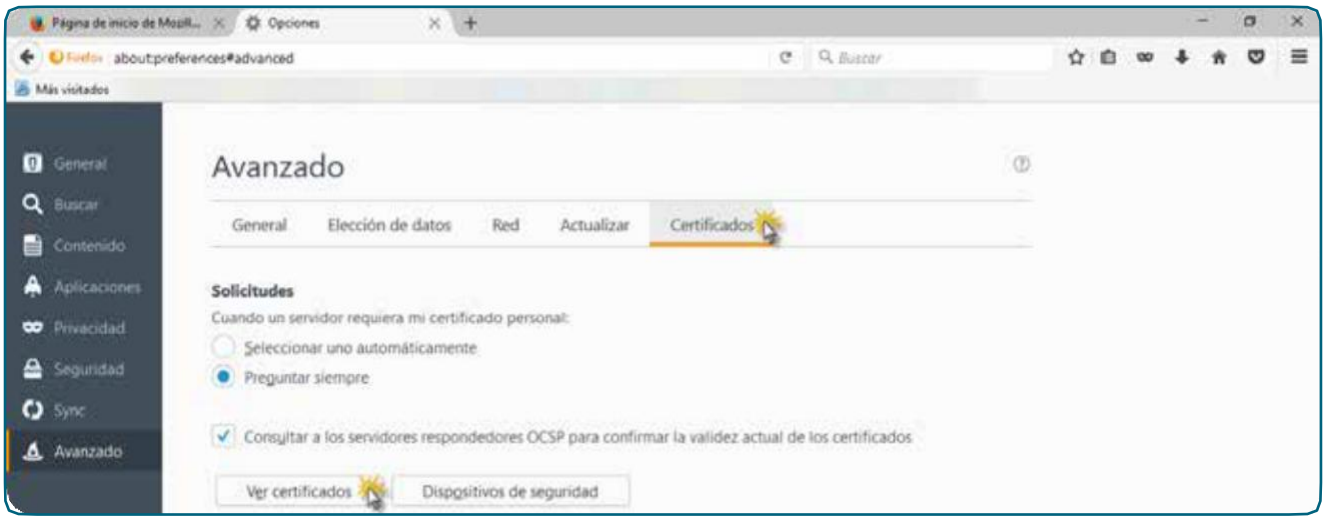
Para instalar un certificado distribuido en software en un entorno Windows y poder ser utilizado con el navegador FireFox, el proceso es el que se describe a continuación.

Iniciar el navegador Firefox y pulsar sobre el icono **Abrir menú** y pulsamos sobre el icono **Opciones**.

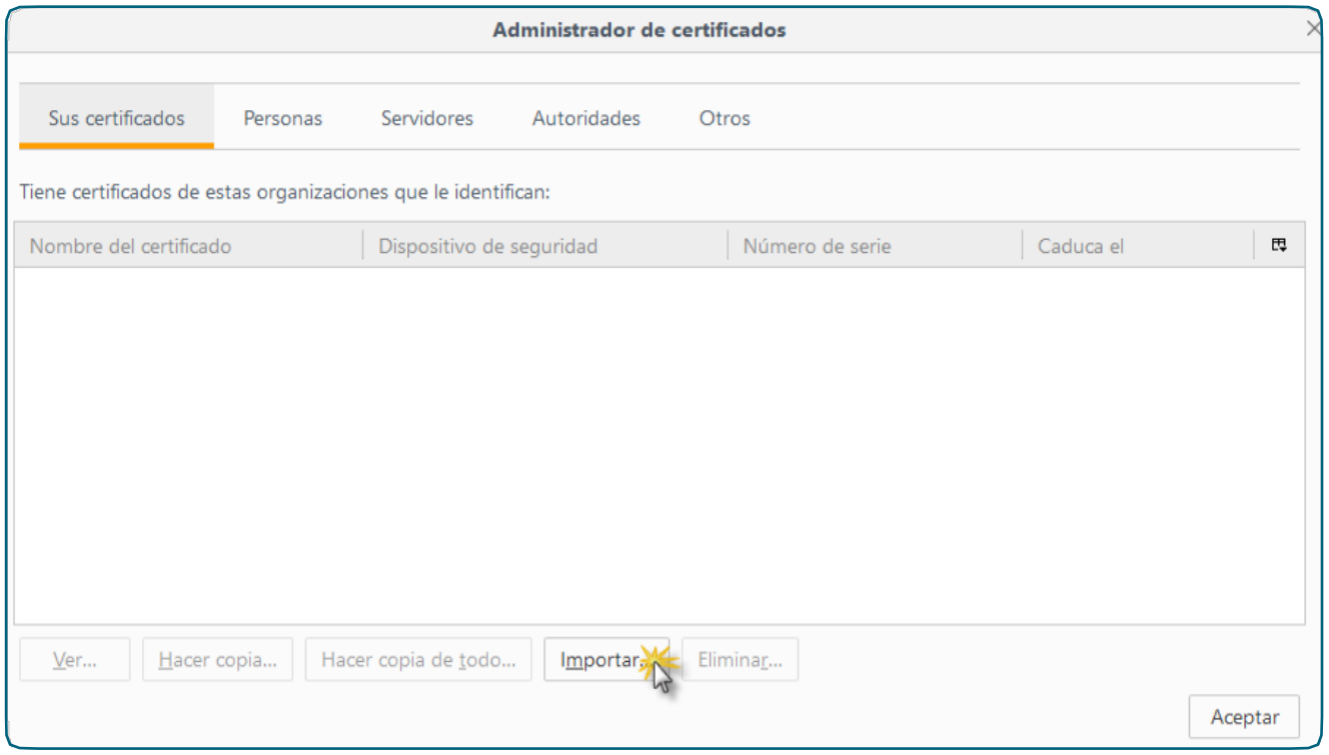


Se nos va a mostrar una nueva pestaña en la que vamos a seleccionar **Avanzado** en el menú que aparece en la parte izquierda de la pantalla.

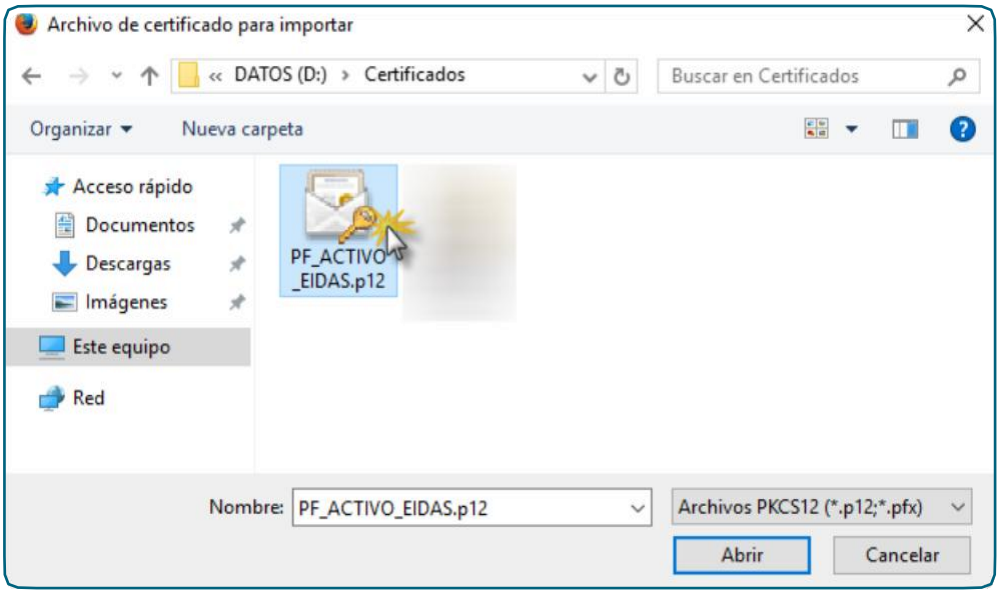
Una vez estamos en las opciones avanzadas, seleccionamos la opción **Certificados** y pulsamos el botón **Ver certificados**.



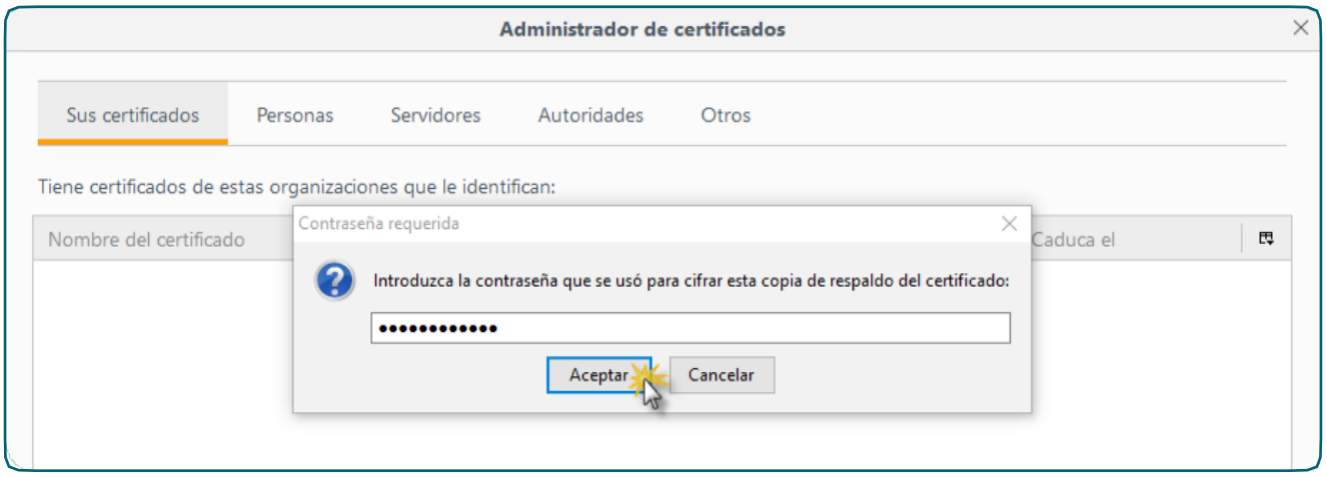
Esto nos va a mostrar una ventana en la que en la pestaña **Sus certificados**, va a mostrar los certificados que tengamos instalados, y nos va a permitir importar nuevos. Para ello pulsamos sobre el botón **Importar…**



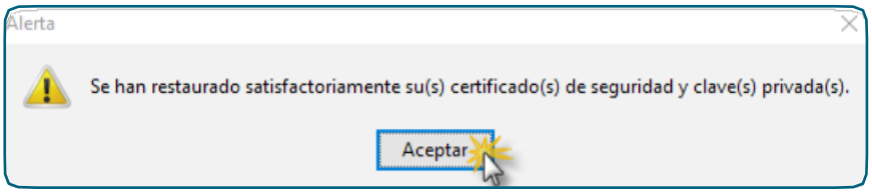
Accedemos al repositorio en el que tenemos almacenados los certificados que se pueden usar con este navegador y seleccionamos el que queramos importar.



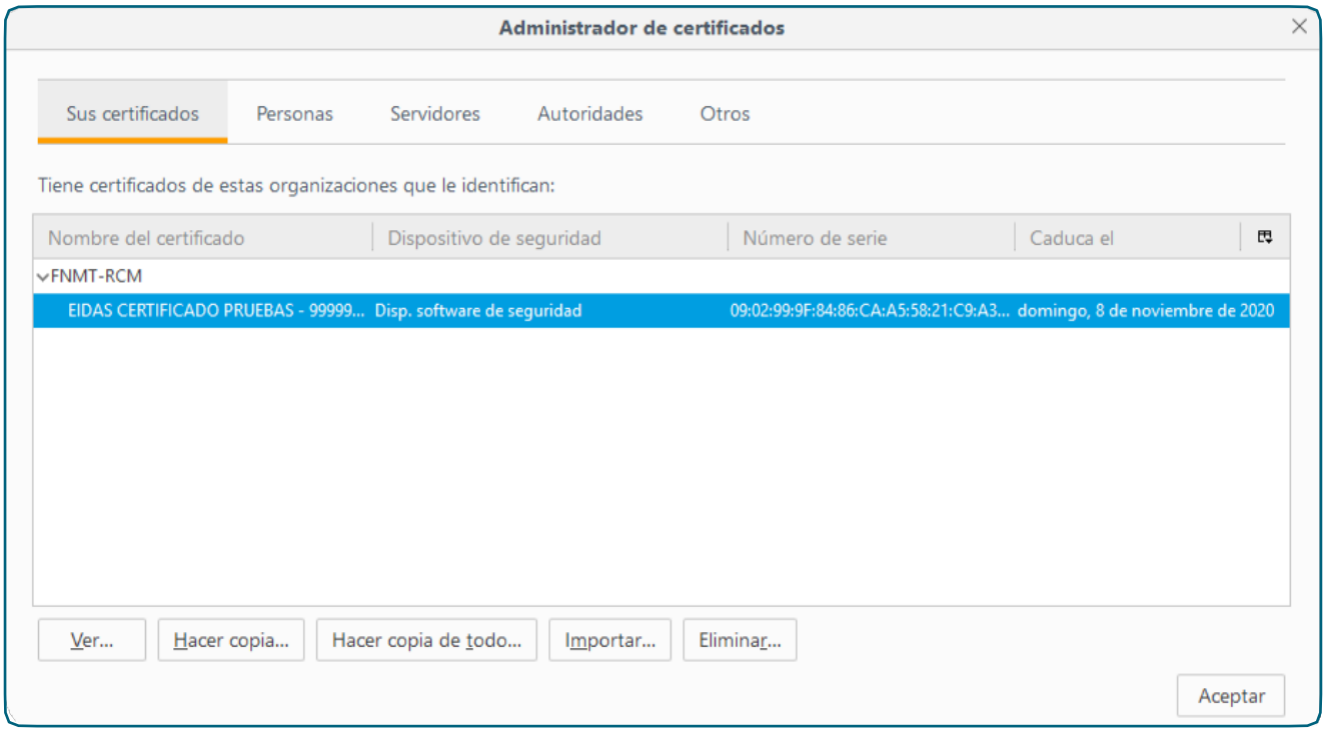
Al pulsar el botón **Abrir**, nos solicita la contraseña del certificado para poder continuar con la importación al navegador.



Si indicamos la contraseña correctamente, nos muestra un mensaje confirmando la importación del certificado en el navegador.



Al pulsar **Aceptar**, se muestra el certificado en la ventana en la que hemos realizado la importación.

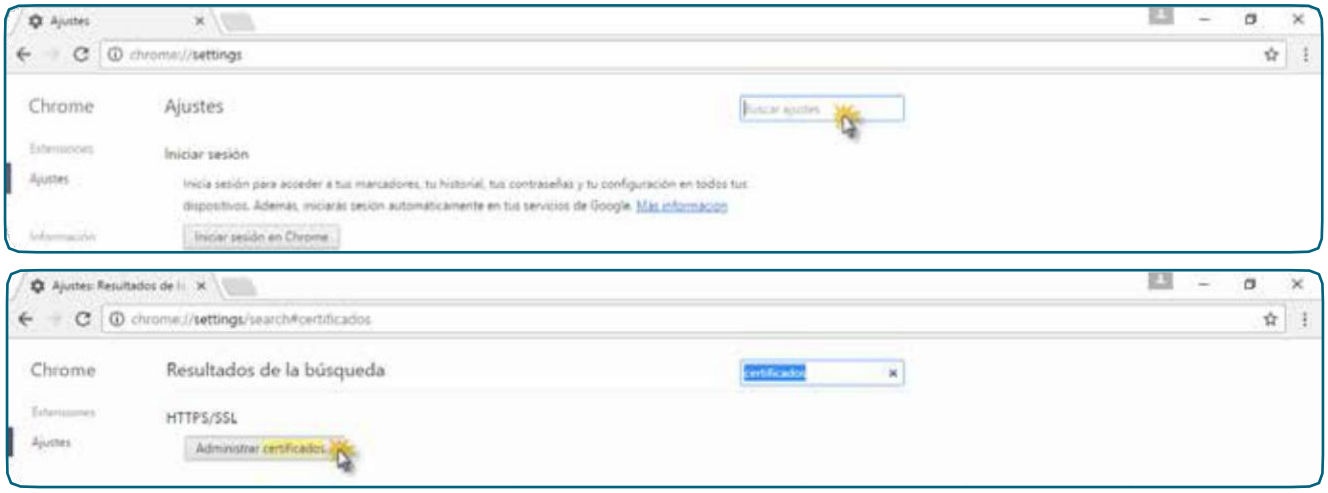


2.1.3. Instalación en entornos Windows y utilización con Google Chrome

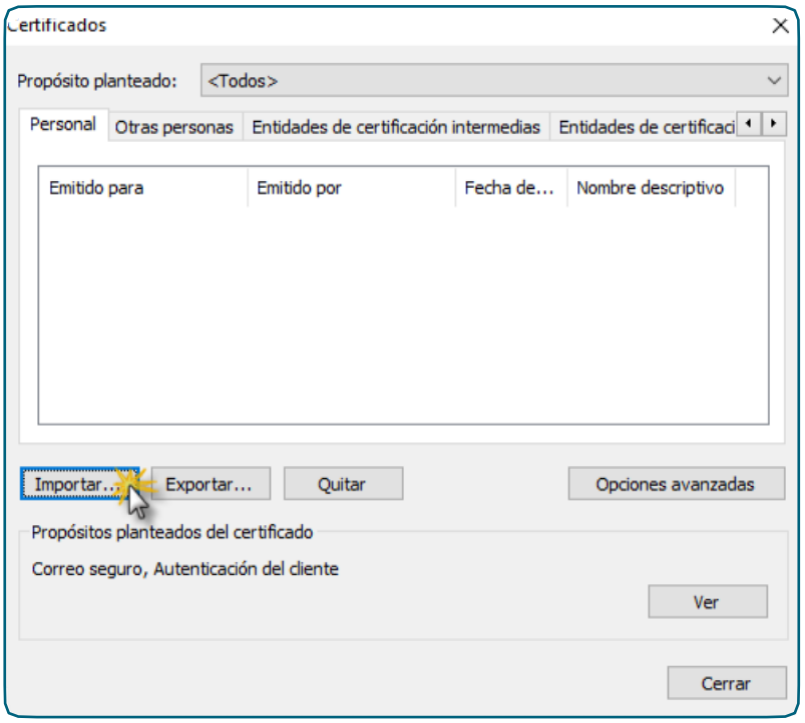
Para instalar un certificado distribuido en software en un entorno Windows y poder ser utilizado con el navegador Chrome, el proceso es el que se describe a continuación.

Iniciar el navegador Chrome y pulsar sobre el icono **Personaliza y controla Google Chrome** ⋮ y seleccionamos la opción **Configuración** en el menú desplegable que aparece.

Se nos va a mostrar una nueva pestaña desde la que gestionar la configuración de Chrome. En el **buscador de ajustes**, escribimos el texto «**certificados**» para que nos localice la entrada **HTTPS/SSL**.

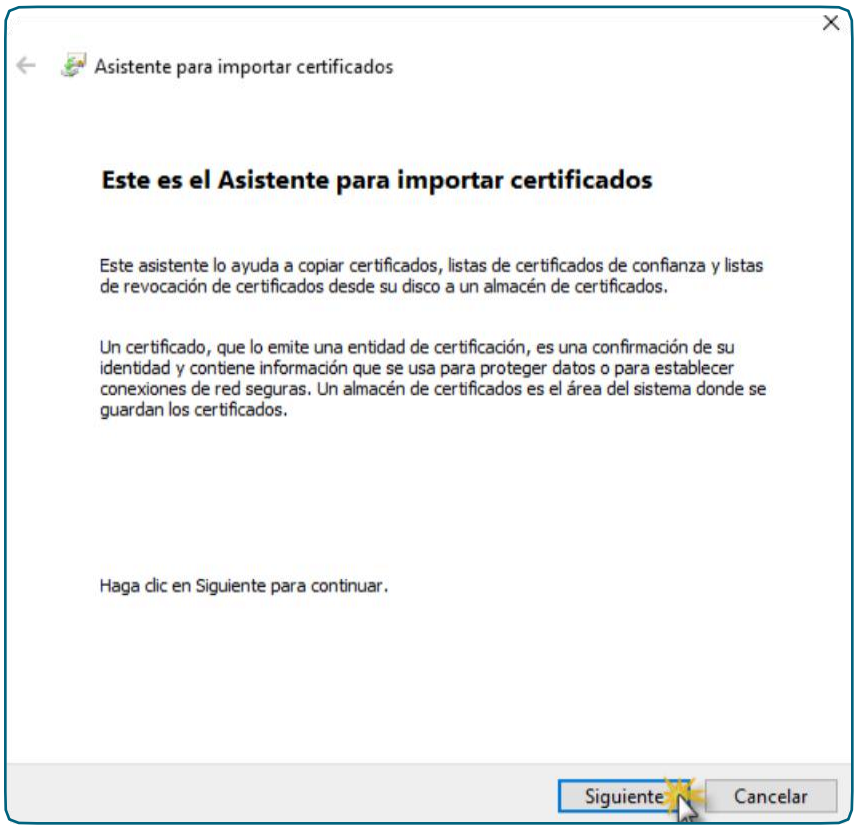


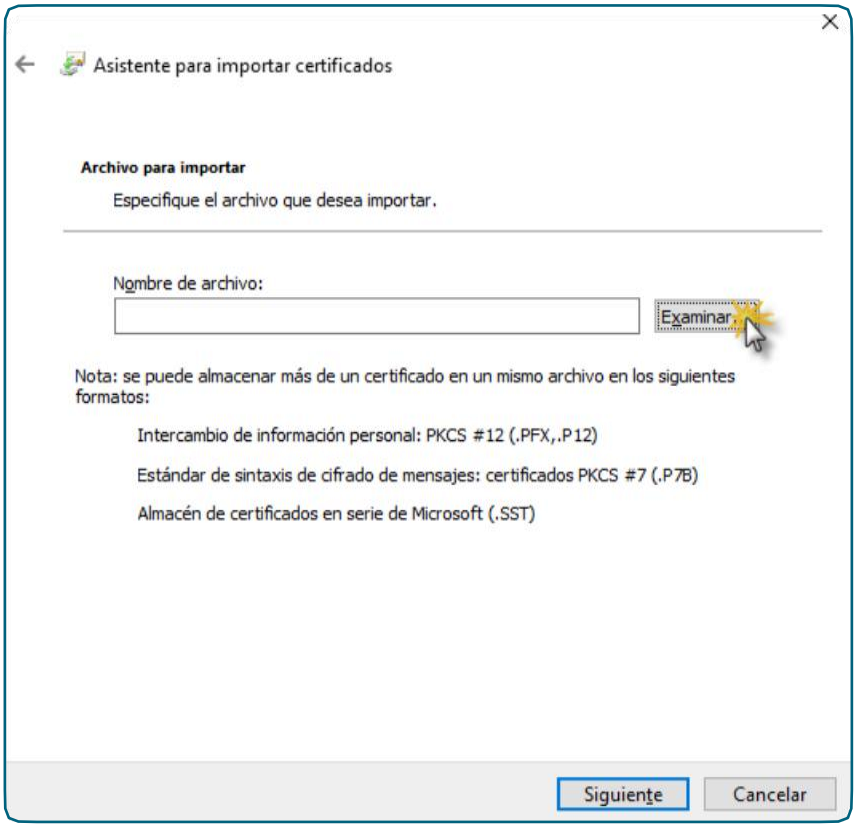
Una vez localizada la entrada, pulsamos sobre el botón **Administrar certificados**... Esto nos va a mostrar una ventana en la que nos va a mostrar los certificados que tengamos instalados y nos va a permitir importar nuevos. Para ello pulsamos sobre el botón **Importar**...

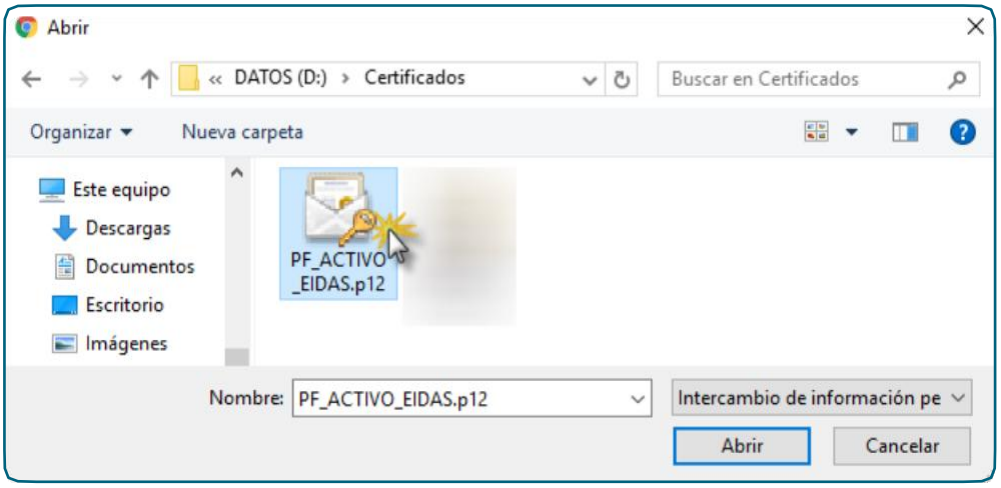


Esta acción va a lanzar el asistente de importación de nuevos certificados.

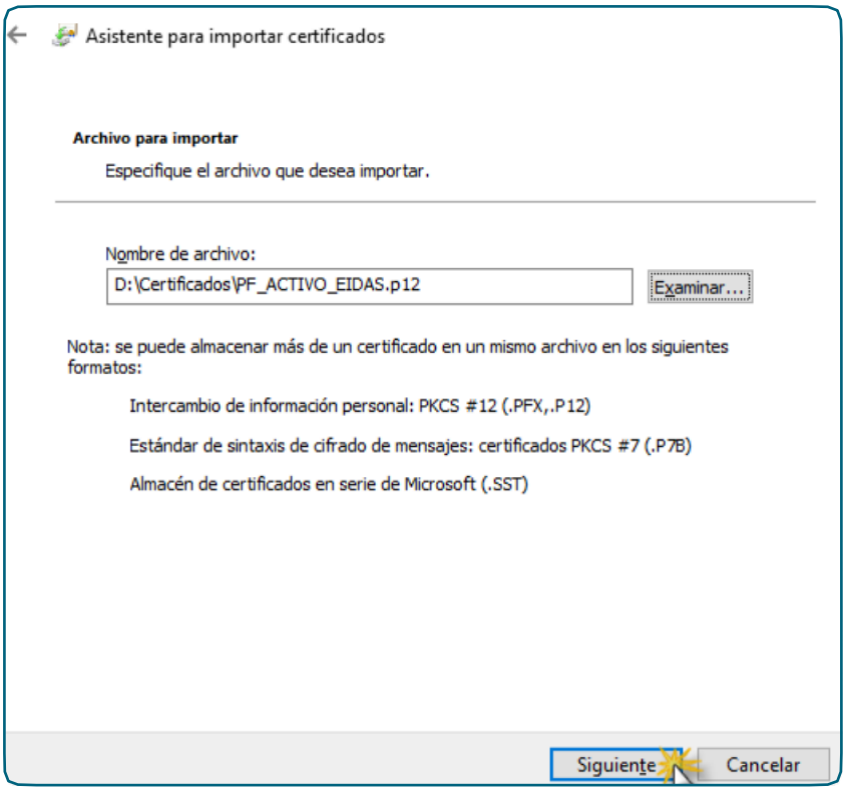
Pulsando en **Siguiente**, pasamos a una pantalla en la que vamos a seleccionar el certificado que queremos importar. Para ello, accedemos al repositorio en el que los tenemos almacenados y seleccionamos el que queramos importar.



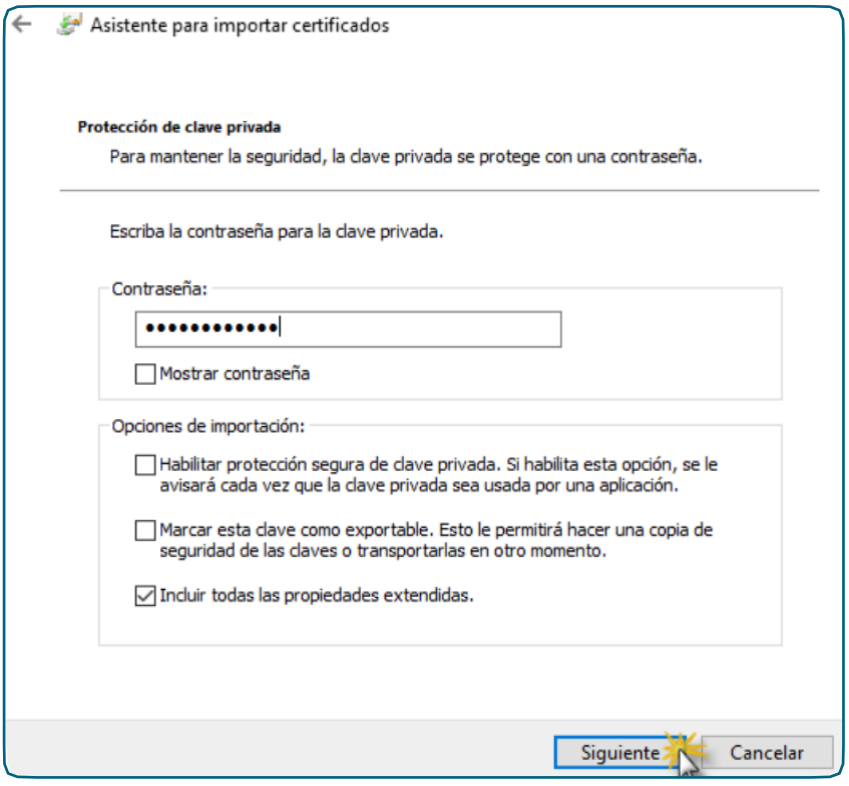

Asistente para importar certificados
Archivo para importar
Especifique el archivo que desea importar.
Nombre de archivo:
Examinar...
Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:
Intercambio de información personal: PKCS #12 (.PFX,.P12)
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
Almacén de certificados en serie de Microsoft (.SST)
Siguiente
Cancelar


Abrir
DATOS (D:) › Certificados
Buscar en Certificados
Organizar
Nueva carpeta
Este equipo
Descargas
Documentos
Escritorio
Imágenes
PF_ACTIVO_EIDAS.p12
Nombre: PF_ACTIVO_EIDAS.p12
Intercambio de información pe
Abrir
Cancelar

Con el certificado seleccionado, pulsamos **Siguiente** para continuar con el asistente de importación.

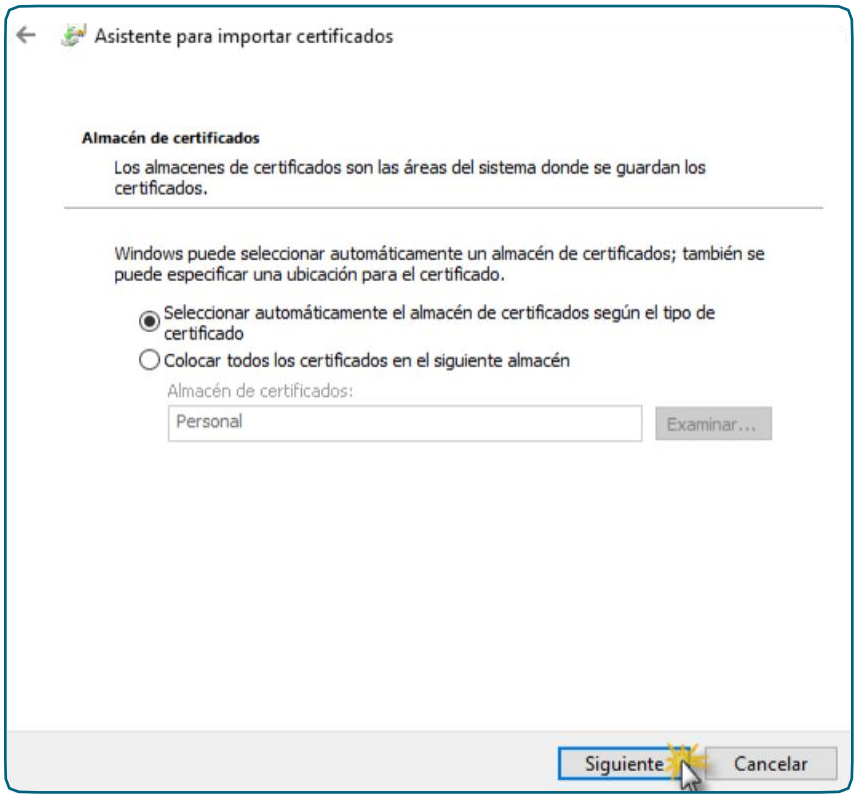


A continuación nos va a solicitar la contraseña del certificado.

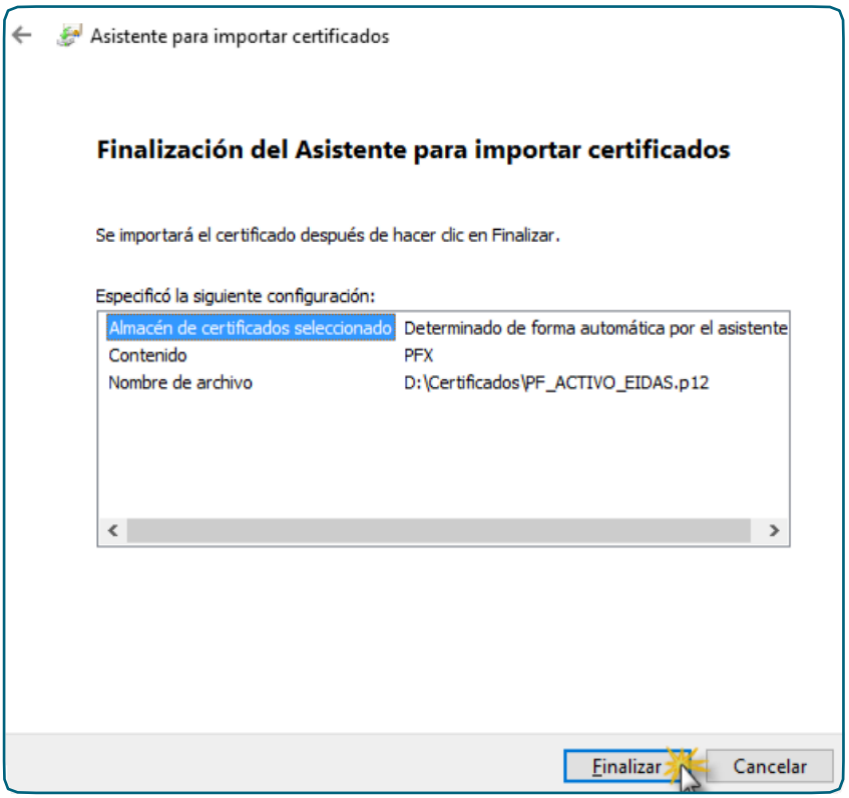


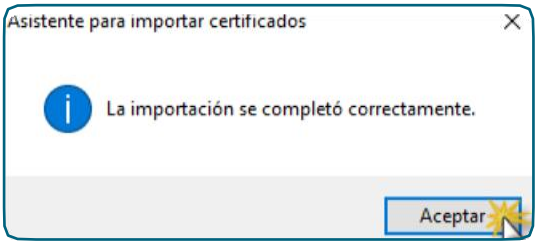
Al introducir la contraseña y pulsar el botón **Siguiente**, si la contraseña es correcta, se despliega una ventana en la que le vamos a indicar en qué almacén de certificados queremos que se guarde el certificado y su clave privada.

La **opción recomendada** es «Seleccionar automáticamente el almacén de certificados según el tipo de certificado».

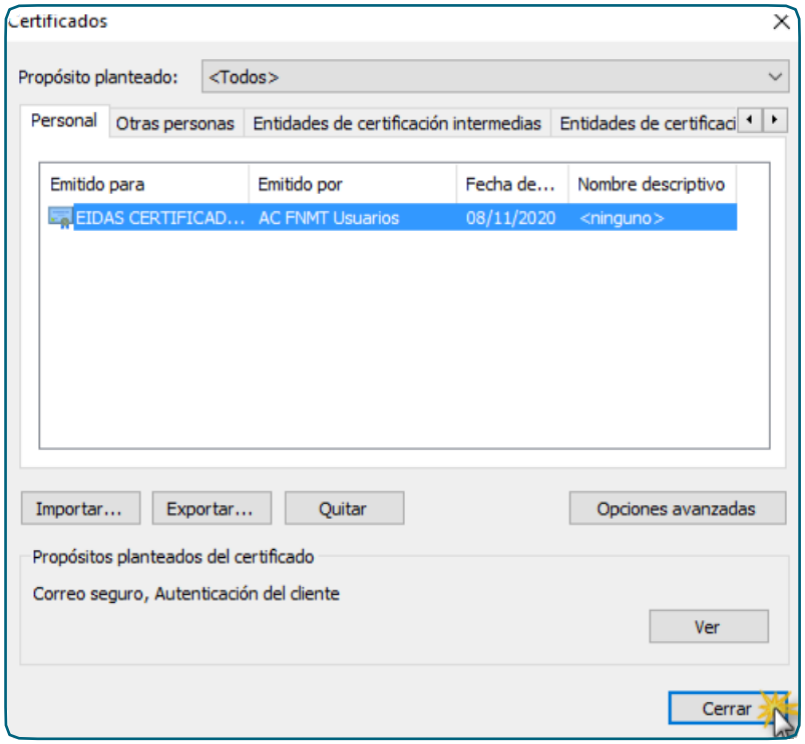


Una vez seleccionado el almacén, continuamos con la instalación y antes de finalizar, el asistente nos informa de la configuración que hemos seleccionado. Si está todo correcto y de acuerdo a la configuración que nos interesa, pulsamos **Finalizar**.





Al pulsar **Aceptar**, se muestra el certificado en la ventana en la que hemos realizado la importación.



2.1.4. Instalación en otros entornos

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

2.2. 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 su utilización 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.

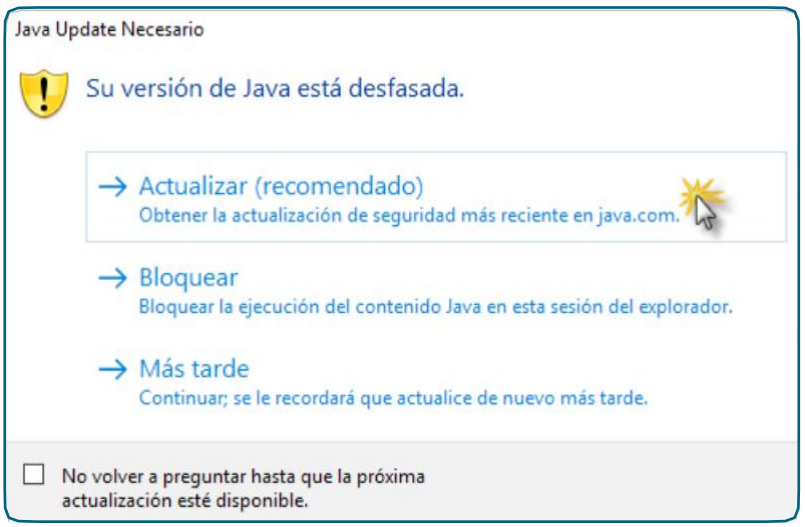
2.3. Instalación del Runtime de Java (JRE)

La versión mínima de Java requerida en la iniciativa de Formación Programada por las Empresas para manejar certificados digitales y realizar firma electrónica es la 1.8.0_121.

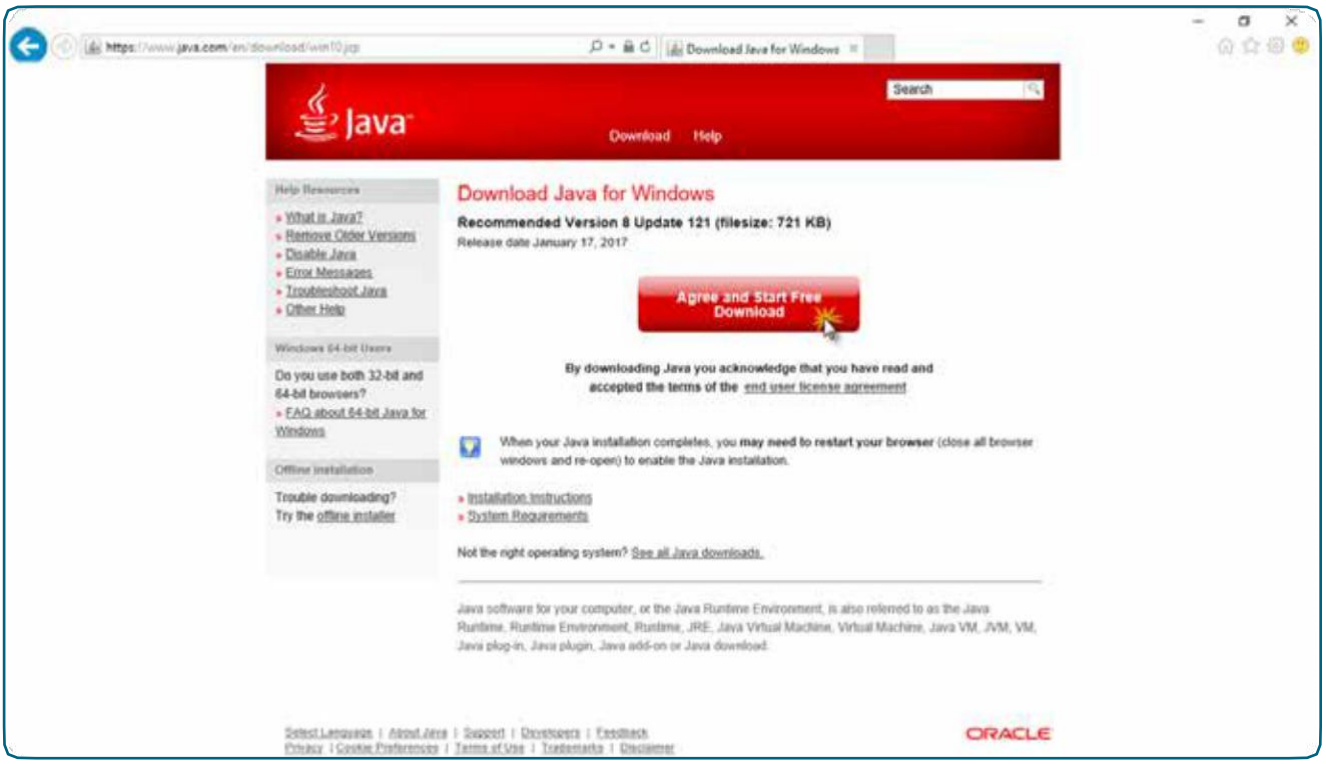
Las páginas de la aplicación de Formación Programada por las Empresas, que requieren la utilización de Java, invocan la instalación desde Internet en caso de que el entorno de ejecución de Java (JRE) no se encuentre instalado en el ordenador desde el que se accede.

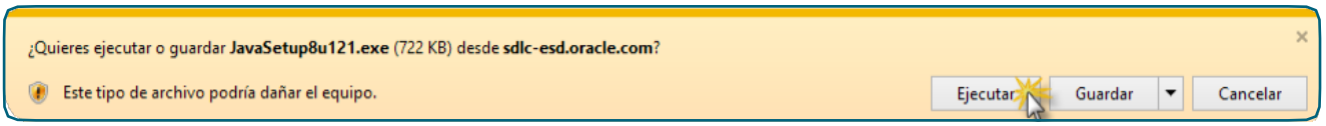
Para acceder a la aplicación de Formación Programada por las Empresas, lo primero que el usuario ha de hacer es solicitar desde un navegador la página inicial, donde el usuario se identifica con un certificado digital. Dicha página utiliza un programa Java (applet) para consultar los certificados personales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

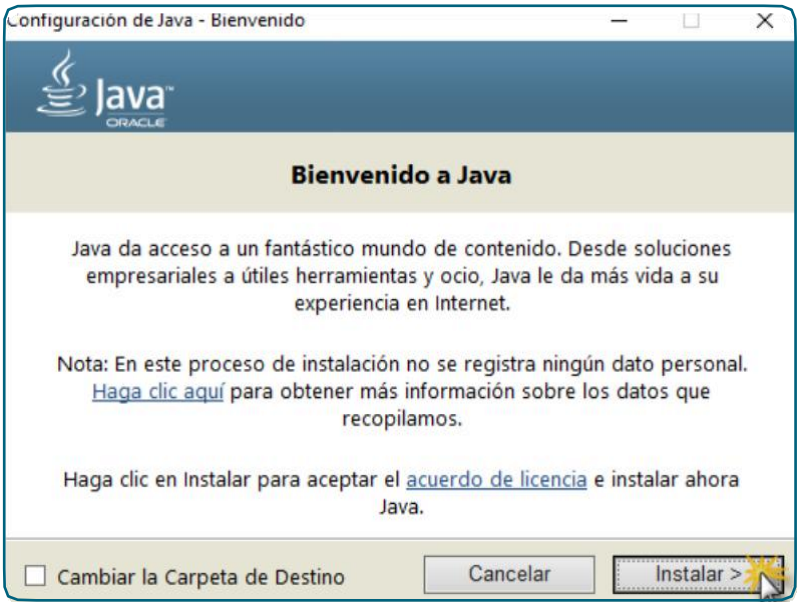
Desde el Internet Explorer, en caso de que el sistema no tenga instalado el entorno de ejecución de Java o de no estar correctamente actualizado, se mostrará una ventana como la siguiente para realizar la instalación.



Para instalar el entorno de ejecución de Java, pulsamos el botón **Actualizar (recomendado)** y seguimos las instrucciones del instalador. Para poder realizar la instalación se han de aceptar las condiciones de la licencia que se muestran en el asistente pulsando en el botón **Agree and Start Free Download**.

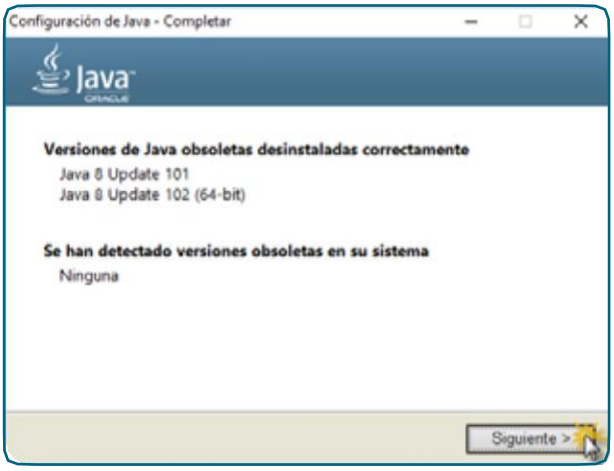



¿Quieres ejecutar o guardar JavaSetup8u121.exe (722 KB) desde sdlc-esd.oracle.com?
Este tipo de archivo podría dañar el equipo.
Ejecutar
Guardar
Cancelar


Configuración de Java - Bienvenido
Java
ORACLE
Bienvenido a Java
Java da acceso a un fantástico mundo de contenido. Desde soluciones empresariales a útiles herramientas y ocio, Java le da más vida a su experiencia en Internet.
Nota: En este proceso de instalación no se registra ningún dato personal. Haga clic aquí para obtener más información sobre los datos que recopilamos.
Haga clic en Instalar para aceptar el acuerdo de licencia e instalar ahora Java.
Cambiar la Carpeta de Destino
Cancelar
Instalar >


Configuración de Java - Progreso
Java
ORACLE
Estado: Instalación de Java
3 Billion
Devices Run Java
Java
#1 Development Platform
ORACLE

En el caso de que el instalador de Java detecte versiones obsoletas en nuestro equipo, nos va a advertir de que conservarlas puede conllevar riesgos de seguridad, por lo que se recomienda su desinstalación desde el asistente.



3. Uso de los certificados en la aplicación

La aplicación de Formación Programada por las Empresas 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 determinados trámites.

3.1. Proceso de identificación de usuarios

El proceso de identificación de usuarios por la aplicación de Formación Programada por las Empresas se realiza en la página inicial. La invocación de esta página solicita 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 marcar la opción «**No volver a mostrar esto otra vez para aplicaciones del publicador y ubicaciones anteriores»** y pulsar el botón **Ejecutar**.

Tras la operación anterior, el programa descargado busca los certificados digitales del usuario y los muestra para que el usuario elija el que va a utilizar para acceder a la aplicación. Seleccionamos el certificado y pulsamos el botón **Aceptar**.

Al pulsar el botón Aceptar, se remite al servidor el certificado para validar su autenticidad, vigencia, estado de revocación y si ha 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 (persona física o Jurídica) y se contrasta la autorización de acceso del usuario a la aplicación.

3.2. Proceso de firma

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

- Activar Usuario.
- Alta de cuenta de cotización.
- Alta empresa participante.
- Alta de usuario.
- Anular grupo.
- Anular PIF notificado.
- Aula Virtual
- Aula Virtual (PIF)
- Baja de cuenta de cotización.
- Datos de Empresa.
- Desactivar Usuario.
- Desfinalizar grupo.
- Fin de grupo.
- Fin de PIF.
- Incidencia de grupo.
- Incidencia de PIF.
- Inicio de grupo.
- Inicio de PIF.
- Incidencia de grupo.
- Incidencia de PIF.
- Modificaciones de Tutores y Centros.
- Observaciones de empresa.

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.

Al pulsar el botón de firma se invoca al proceso de firma de la aplicación que recibe los datos a firmar y busca el certificado con el que se ha de realizar la firma. Este debe ser el utilizado para acceder a la aplicación, salvo en el caso del DNIe, para el que hay que utilizar el propio certificado de firma del DNIe.

El sistema realiza el firmado de los datos pasados a firma y realiza las actualizaciones correspondientes en la aplicación para completar el trámite solicitado.