

Requisitos Técnicos y de Configuración

Sistema de Notificación Electrónica

Índice

1. Compatibilidades con los navegadores	3
2. Listado de certificados digitales admitidos	4
2.1 Comprobar la entidad emisora de los certificados digitales	4
3. Anexo 2: Instalar el cliente de Autofirma del MINHFP.	8
4. Anexo 3: Instalar certificados digitales	10
5.1 Internet Explorer	10
5.2 Mozilla FireFox	15
5.3 Google Chrome	19
5. Anexo 4: Instalar DNI electrónico	22

1. COMPATIBILIDADES CON LOS NAVEGADORES

La compatibilidad del miniApplet de Autofirma del MINHFP, según el navegador de internet, es la siguiente:

Navegador de Internet	AutoFirma
Internet Explorer 9	✗
Internet Explorer 10	✗
Internet Explorer 11	✓
Mozilla FireFox	✓
Google Chrome	✓
Edge	✓
Safari	✓

2. LISTADO DE CERTIFICADOS DIGITALES ADMITIDOS

El Sistema de Notificación Electrónica utiliza, para la validación de certificados, la plataforma @firma de la Administración General del Estado.

Más información en la [Plataforma de @firma](#)

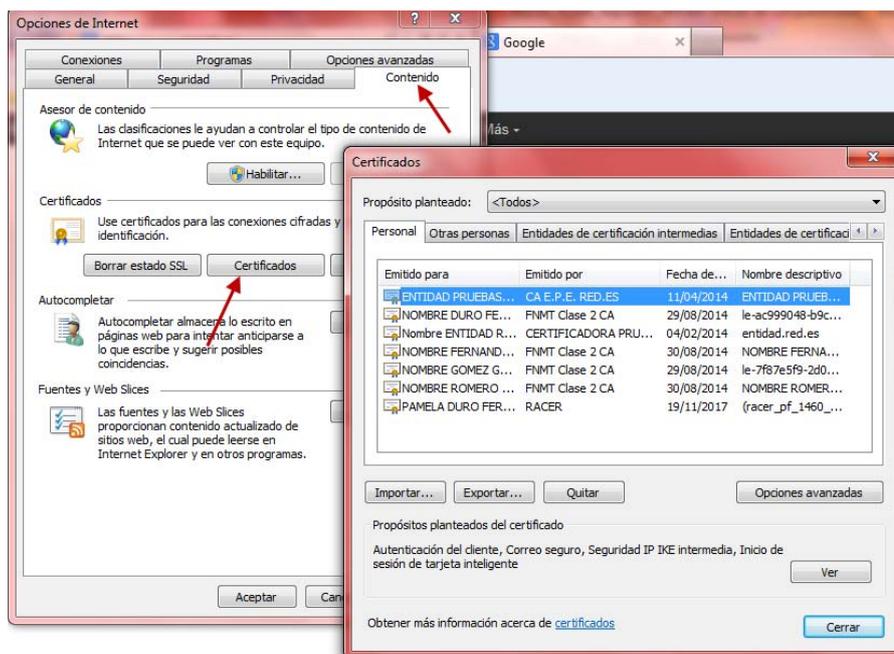
(<http://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=afirma#.VssvCI9Fyyl>).

Para obtener una lista completa de los prestadores aceptados por esta plataforma acuda a el [documento de proveedores de servicios de certificación de @firma](#) (<http://administracionelectronica.gob.es/PAe/aFirma-Anexo-PSC>).

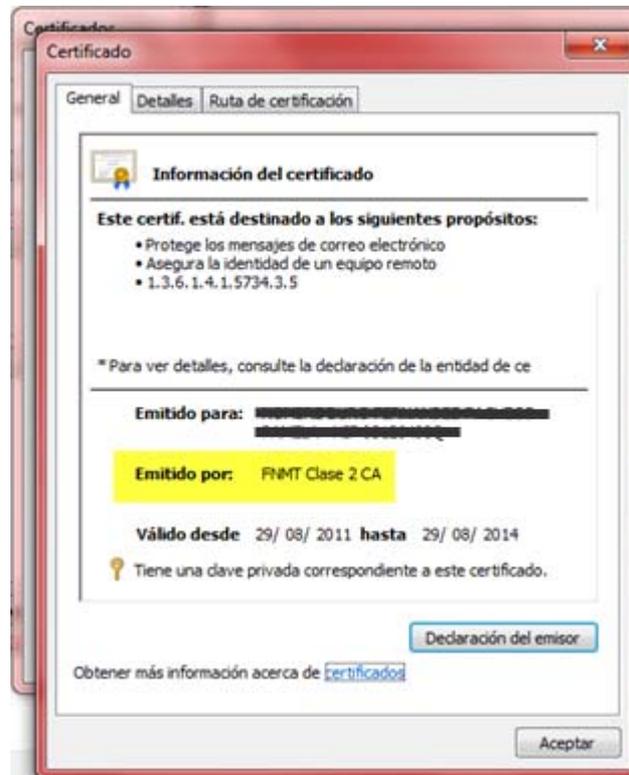
2.1 Comprobar la entidad emisora de los certificados digitales

Para comprobar en **Internet Explorer** la entidad emisora de los certificados, habrá que realizar los siguientes pasos:

- Abrir Internet Explorer
- Acceder al menú herramientas/opciones de Internet/pestaña contenido/certificados.

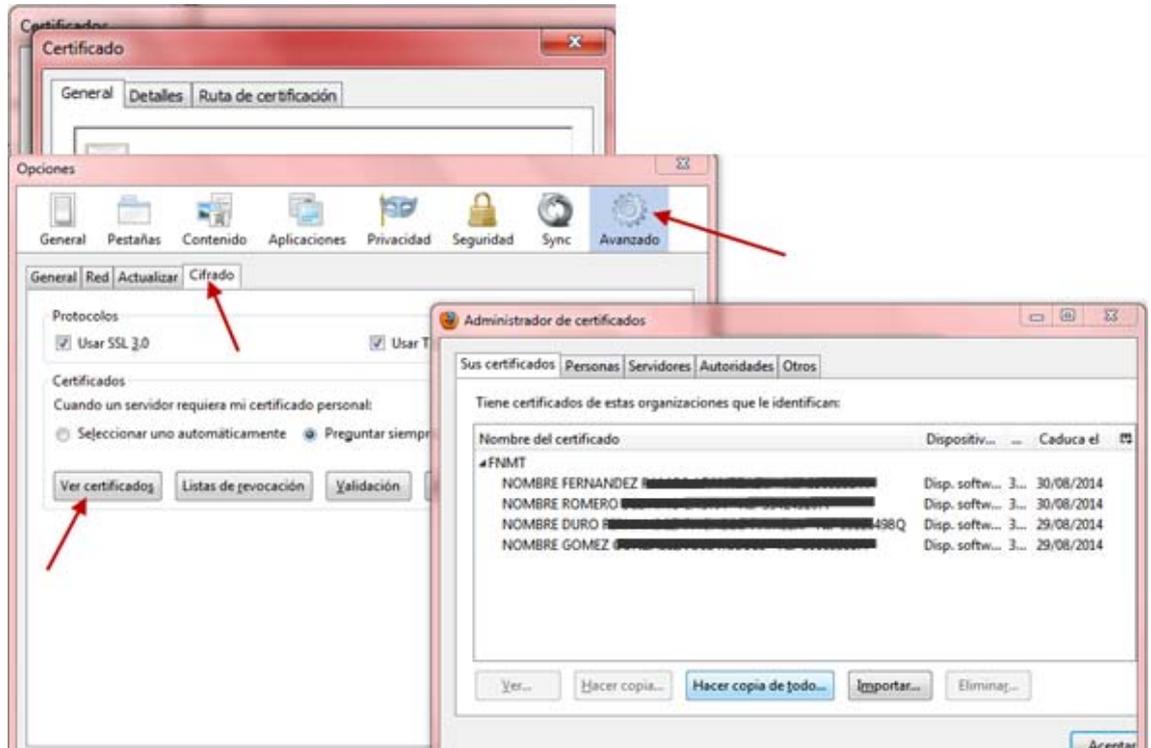


- Hacer doble click encima del certificado correspondiente y aparecerá la siguiente pantalla donde viene detallada la entidad emisora valida del certificado, en este caso, FNMT 2 AC.

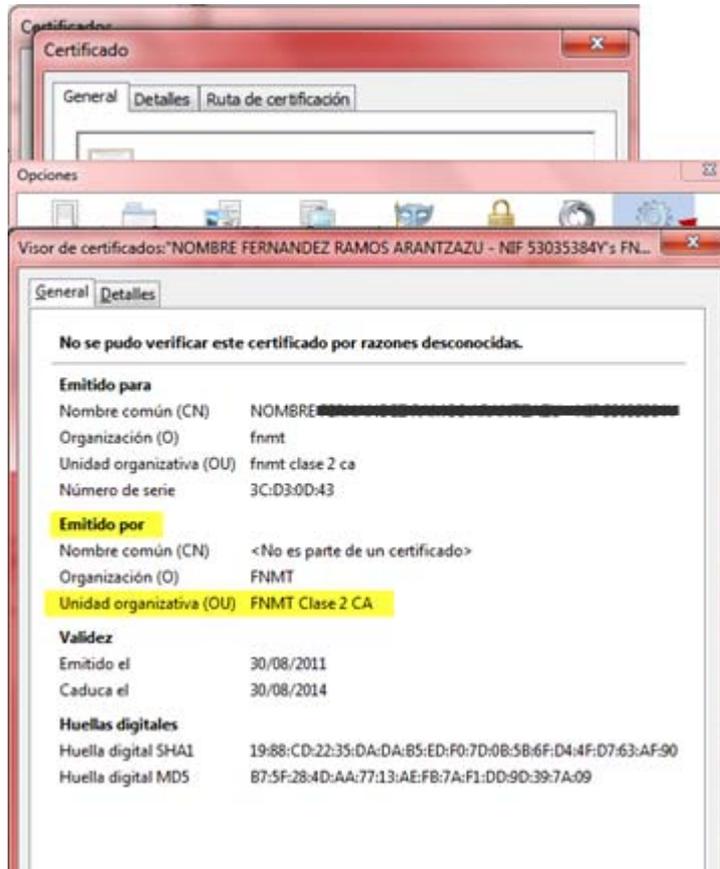


Para comprobar en **Firefox** la entidad emisora del certificado, habrá que realizar los siguientes pasos:

- Abrir el navegador desde Firefox
- Acceder al menú herramientas/opciones/avanzado/pestaña cifrado/ver certificados



- Hacer doble click encima del certificado correspondiente y aparecerá la siguiente pantalla donde viene detallada la entidad emisora valida del certificado, en este caso, FNMT 2 CA.



Para utilizar el DNIe tendrá que instalar previamente el modulo criptográfico, en el **anexo II** de este documento podrá encontrar las instrucciones para la instalación.

3. ANEXO 2: INSTALAR EL CLIENTE DE AUTOFIRMA DEL MINHFP.

Para realizar la descargar del software de Autofirma, acceda la página inicial del Sistema de Notificaciones Electrónicas, y pulse en el botón “Acceder” del Área de Descarga.



GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENCIA DIGITAL

red.es

@Contacta

Sistema de Notificación Electrónica



Acceder al Sistema de Notificación Electrónica

Para poder acceder, usted necesita tener instalada la Máquina Virtual de Java o la aplicación de Autofirma del MINHFP y un certificado digital válido o DNI Electrónico.
Consultar la lista de certificados permitidos [aquí](#)

Área de Descarga

Documento de requisitos técnicos

ACCEDER

CONSULTAR

Contacto | Aviso Legal | Accesibilidad

AYUNTAMIENTO DE SAN SEBASTIÁN DE LOS REYES

OSI oficina de seguridad del internauta

UNIÓN EUROPEA

Cuando acceda al Área de Descarga, seleccione la versión de Autofirma a descargar, según el sistema operativo de su equipo.



Sistema de Notificación Electrónica - Área de Descarga



Para los navegadores de internet: Internet Explorer 9 y 10

 MÁQUINA VIRTUAL DE JAVA

Para el resto de los navegadores de internet:

 AUTOFIRMA PARA WINDOWS 32 BIT

 AUTOFIRMA PARA WINDOWS 64 BIT

 AUTOFIRMA PARA LINUX

 AUTOFIRMA PARA MAC

[VOLVER A LA PÁGINA INICIAL](#)

Contacto | Aviso Legal | Accesibilidad



El contenido del fichero comprimido que se va a descargar es el siguiente:

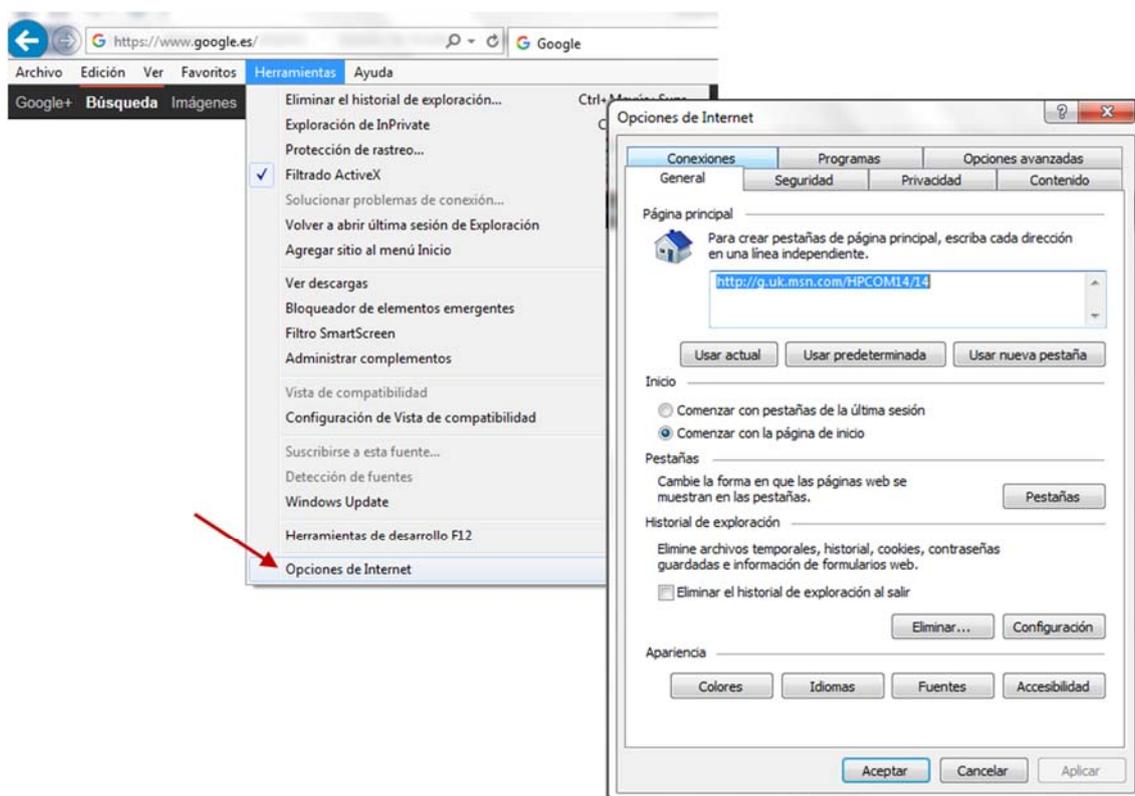
- El instalador de la aplicación Autofirma.
- El manual de instalación de la aplicación Autofirma.

4. ANEXO 3: INSTALAR CERTIFICADOS DIGITALES

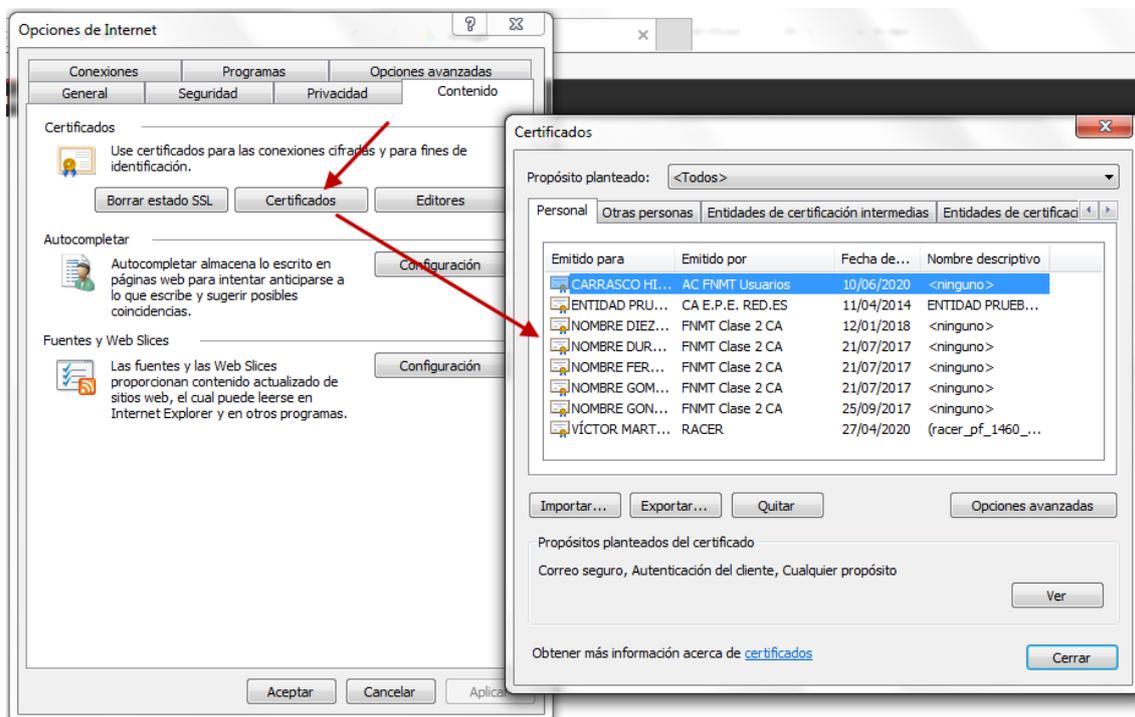
5.1 Internet Explorer

Para instalar el certificado digital en IE hay que seguir los siguientes pasos:

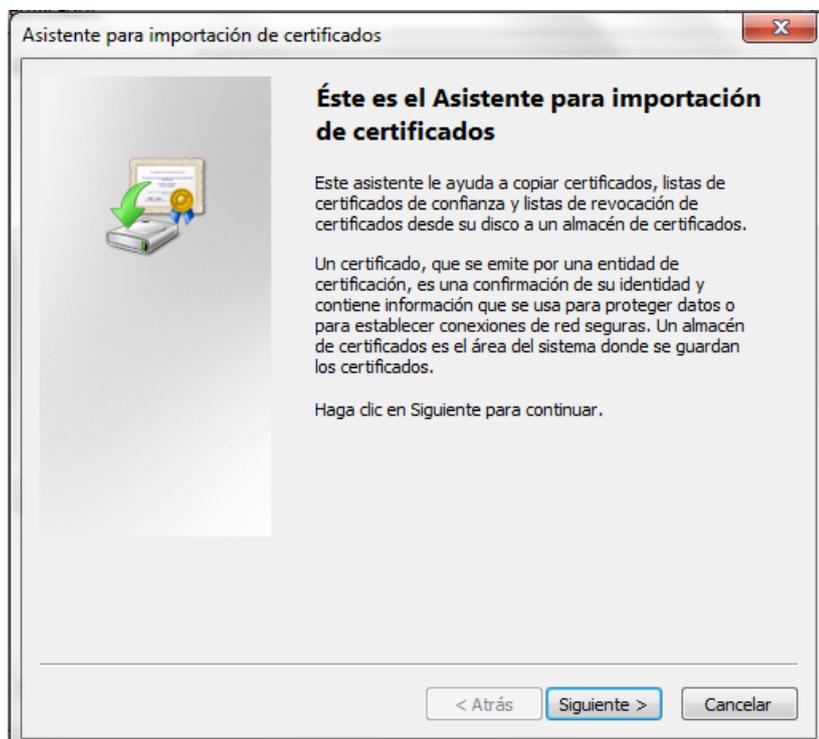
1. Abrir el navegador, y pulsar en el menú **“Herramientas / Opciones de Internet”**.



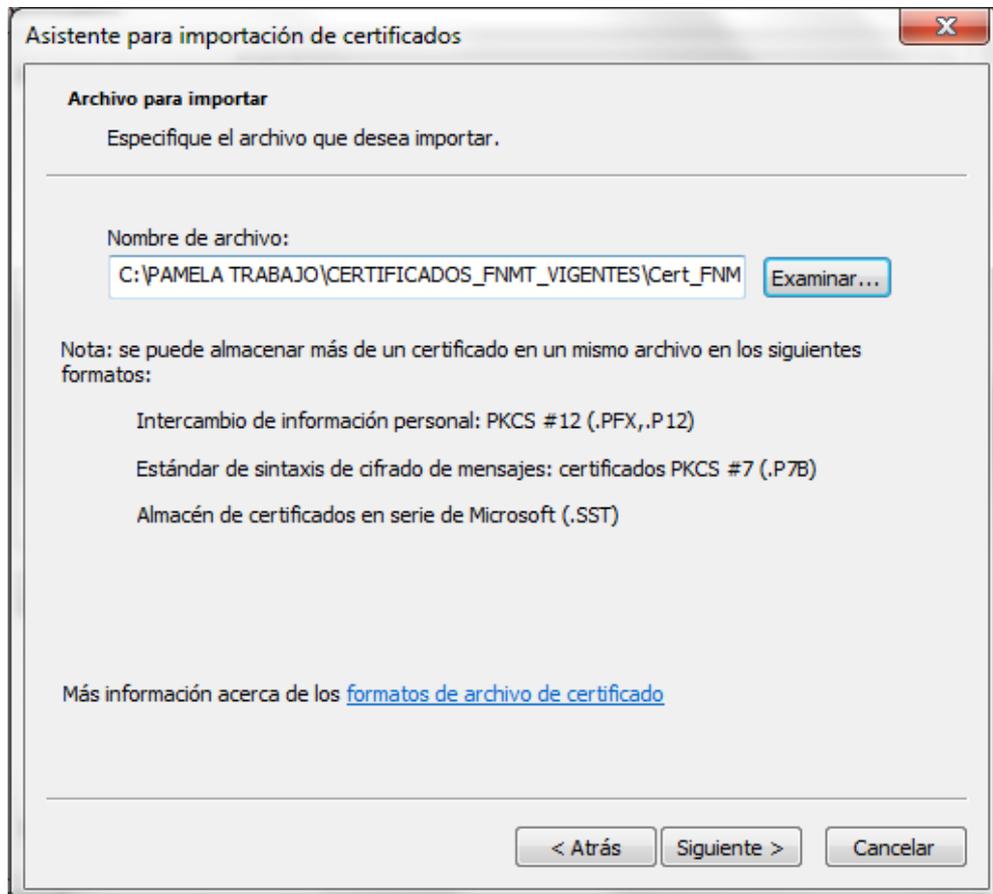
2. Pulsar sobre la **pestaña “Contenido”**. Una vez dentro de esta pestaña, pulsar sobre el **botón “Certificados”**. Se abrirá el almacén de certificados de Internet Explorer.



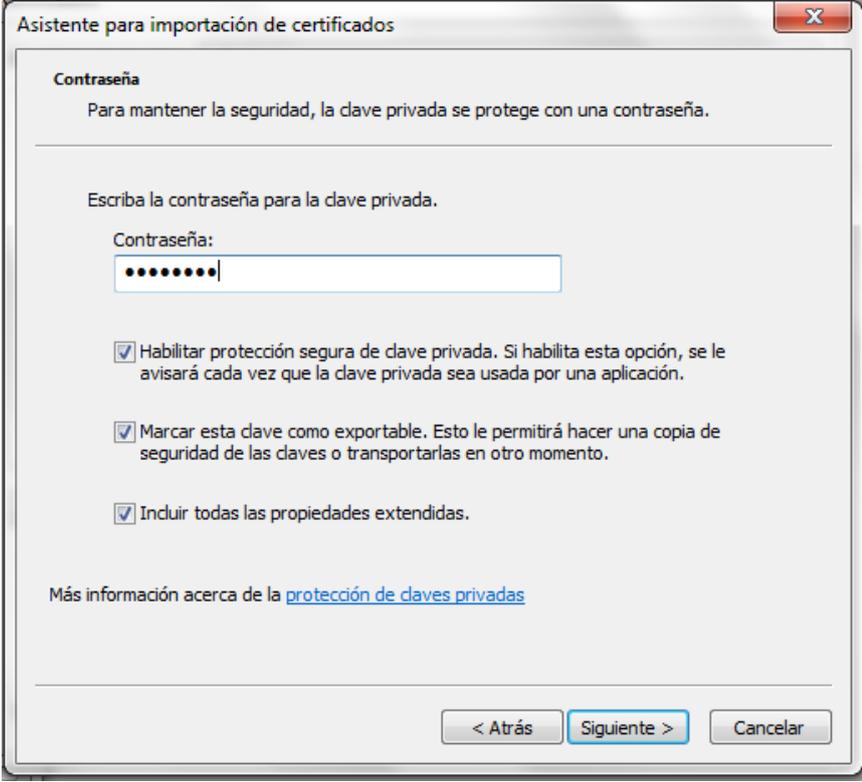
- Pulsar sobre el **botón "Importar"** para abrir el asistente de importación de certificados.



4. Pulsar en el botón "**Siguiente**". Pulsar sobre el **botón examinar** y adjuntar el certificado. Pulsar en Siguiente.



5. En la siguiente pantalla hay que cumplimentar la **contraseña** para importar el certificado. Y **marcar los 3 check** que aparecen en la pantalla. Pulsar en siguiente.



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 clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.

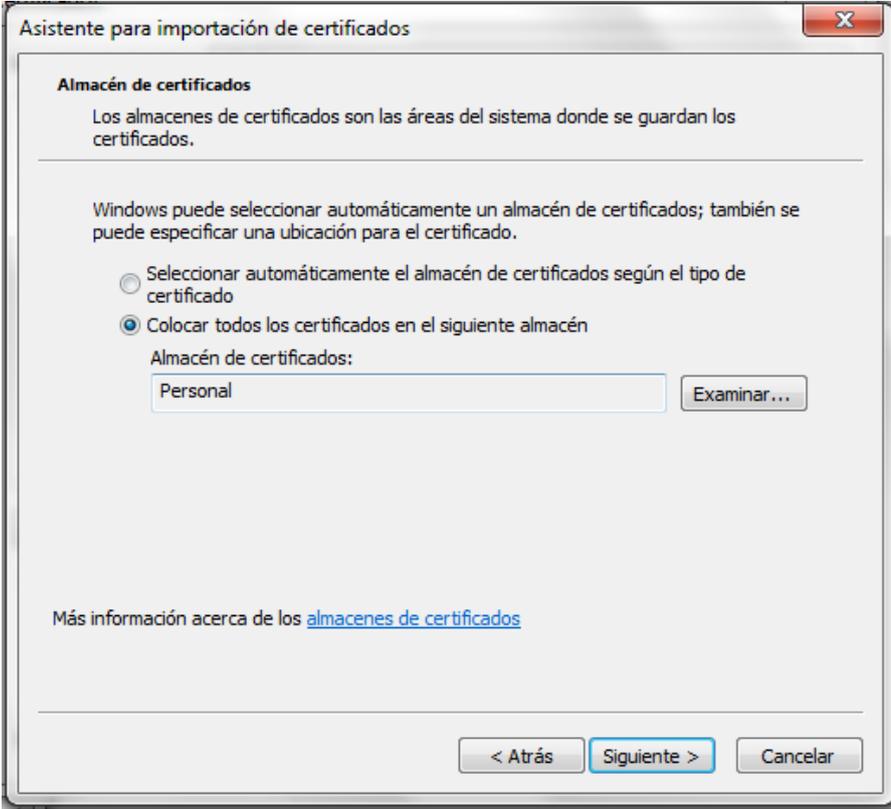
Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.

Incluir todas las propiedades extendidas.

Más información acerca de la [protección de claves privadas](#)

< Atrás **Siguiente >** Cancelar

6. En la siguiente pantalla no hay que realizar ningún cambio. Pulsar en siguiente.



Asistente para importación de certificados

Almacén de certificados

Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.

Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.

Seleccionar automáticamente el almacén de certificados según el tipo de certificado

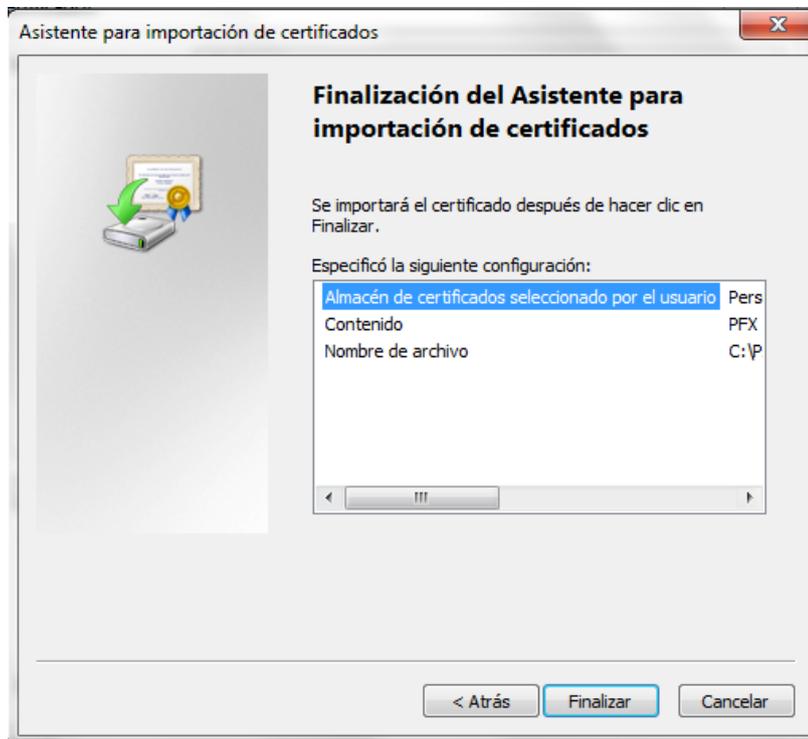
Colocar todos los certificados en el siguiente almacén

Almacén de certificados:
Personal Examinar...

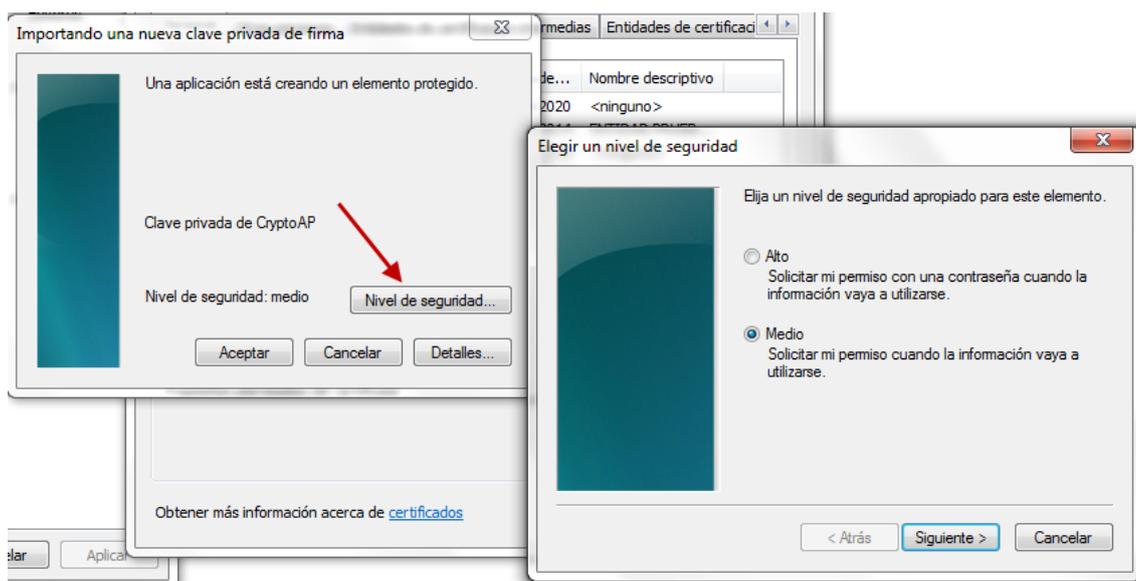
Más información acerca de los [almacenes de certificados](#)

< Atrás **Siguiente >** Cancelar

7. Pulsar en el **botón “Finalizar”** para terminar la importación correctamente.



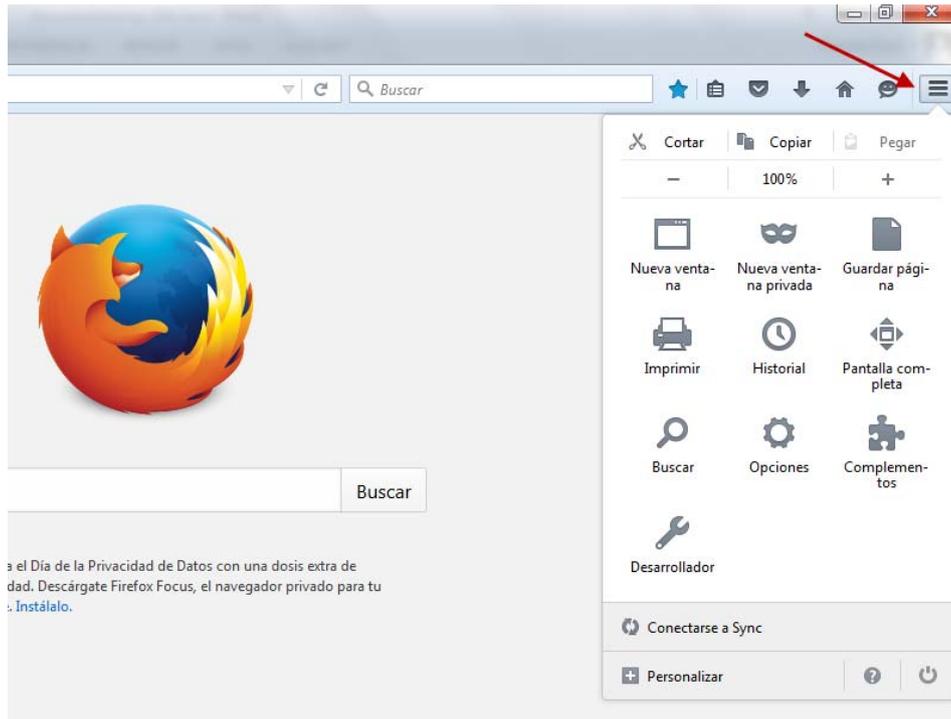
Si queremos **modificar el nivel de seguridad**, pulsar sobre el botón “Nivel de seguridad”, si marcamos nivel Alto, nos pedirá una contraseña, que posteriormente habrá que añadir siempre que se use el certificado.



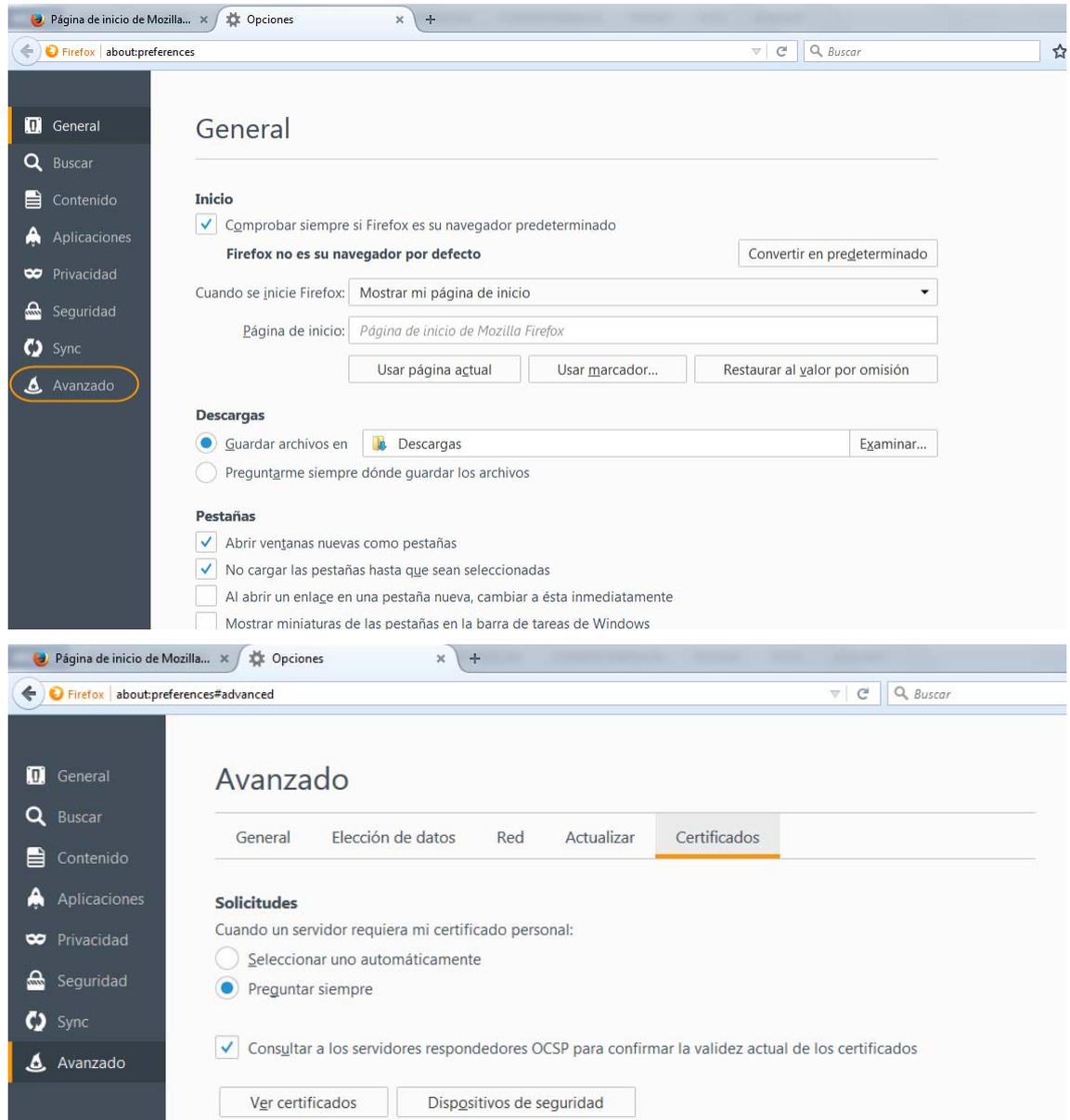
5.2 Mozilla FireFox

Para importar el certificador en este navegador, hay que seguir los siguientes pasos:

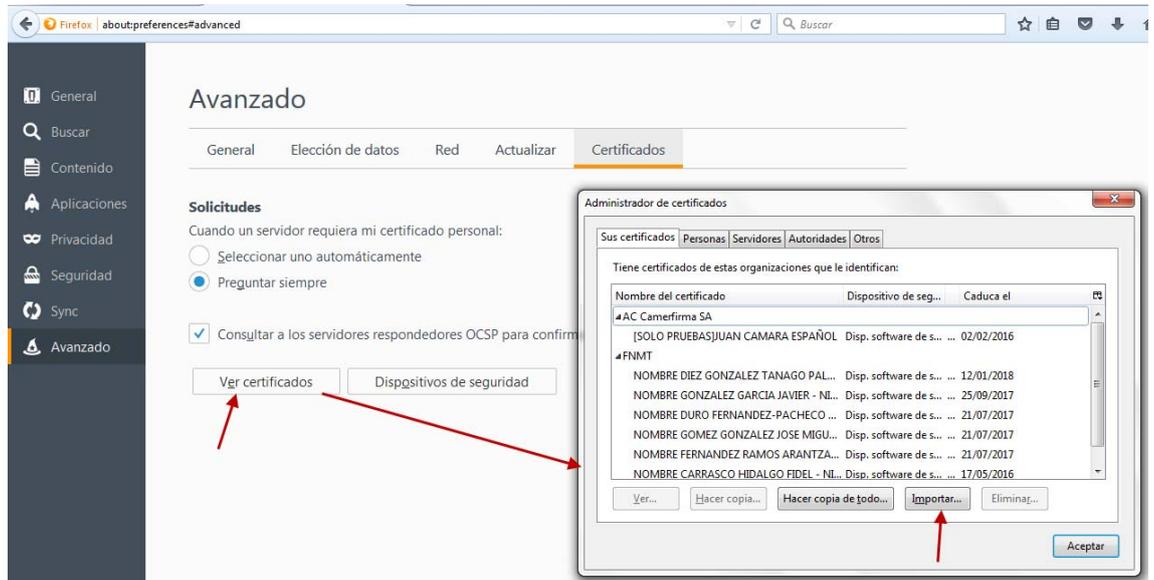
1. Abrir Firefox, y pulsar el icono que aparece en la parte superior derecha.



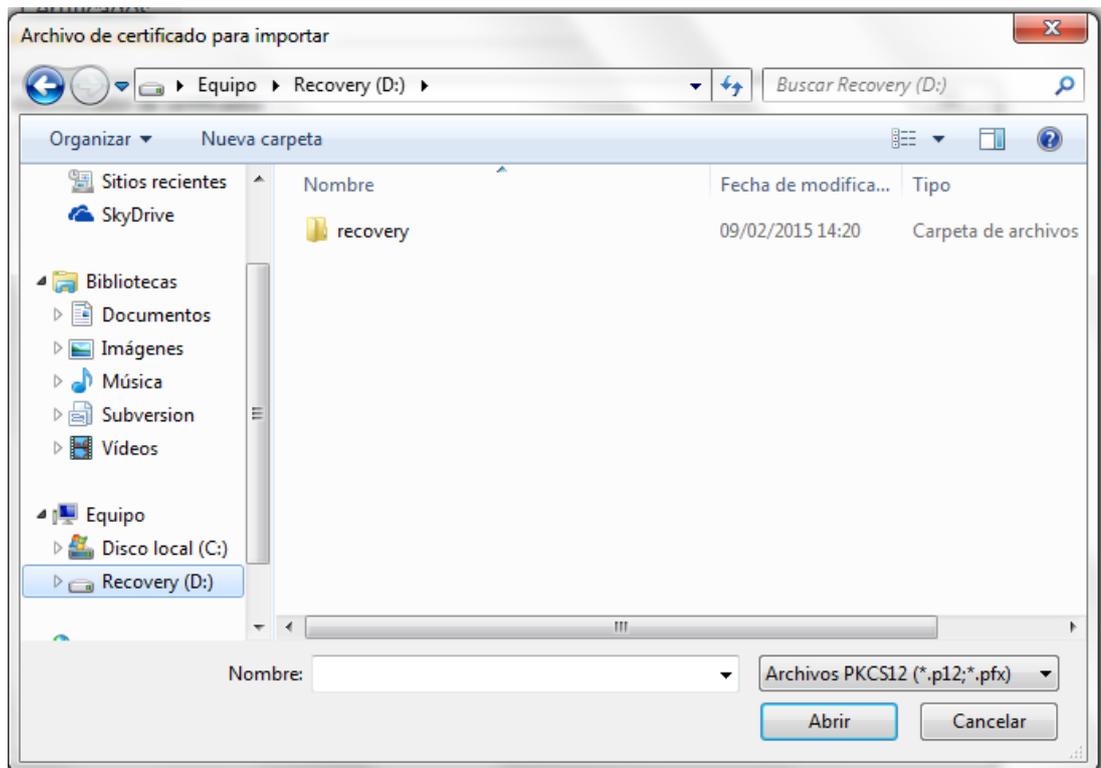
2. Pulsar en el **icono "Opciones"**  **Opciones**, aparecerá la siguiente pantalla, en la cual tenemos que pulsar sobre la opción de menú "Avanzado"



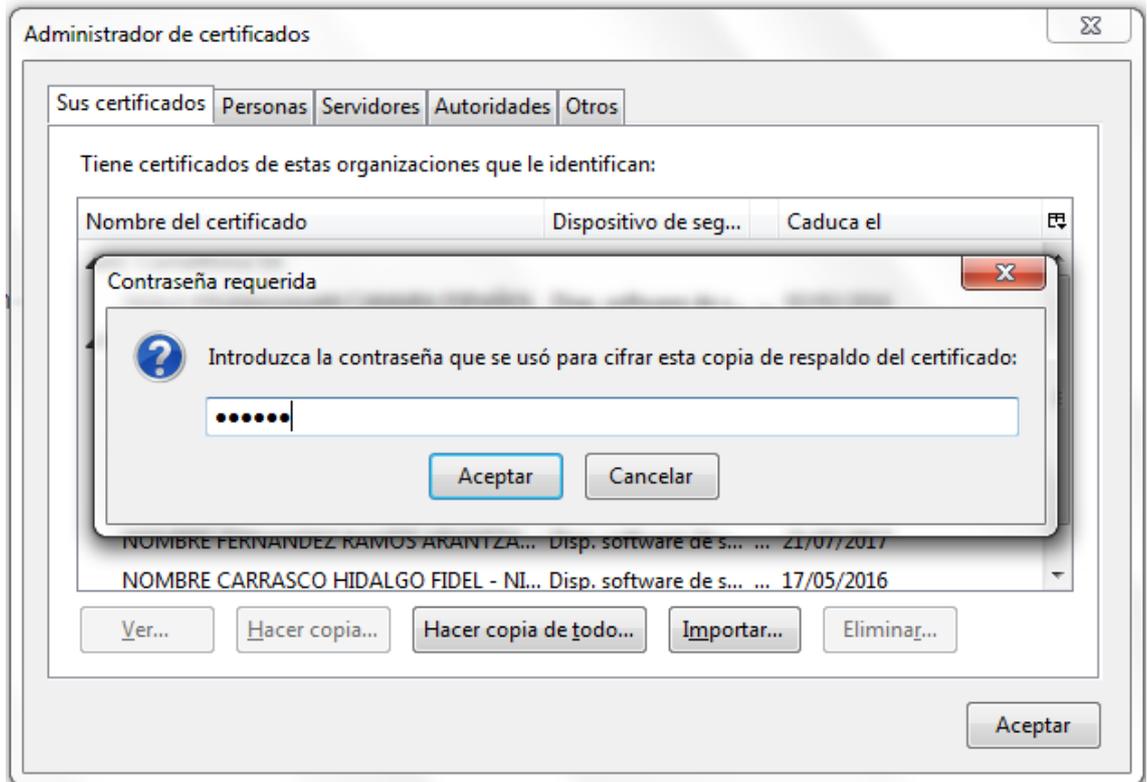
3. Pulsando sobre el botón **“Ver certificados”**, se abrirá la pantalla del almacén de certificados de Firefox. Desde la cual tendremos que pulsar sobre el botón **“Importar”**.



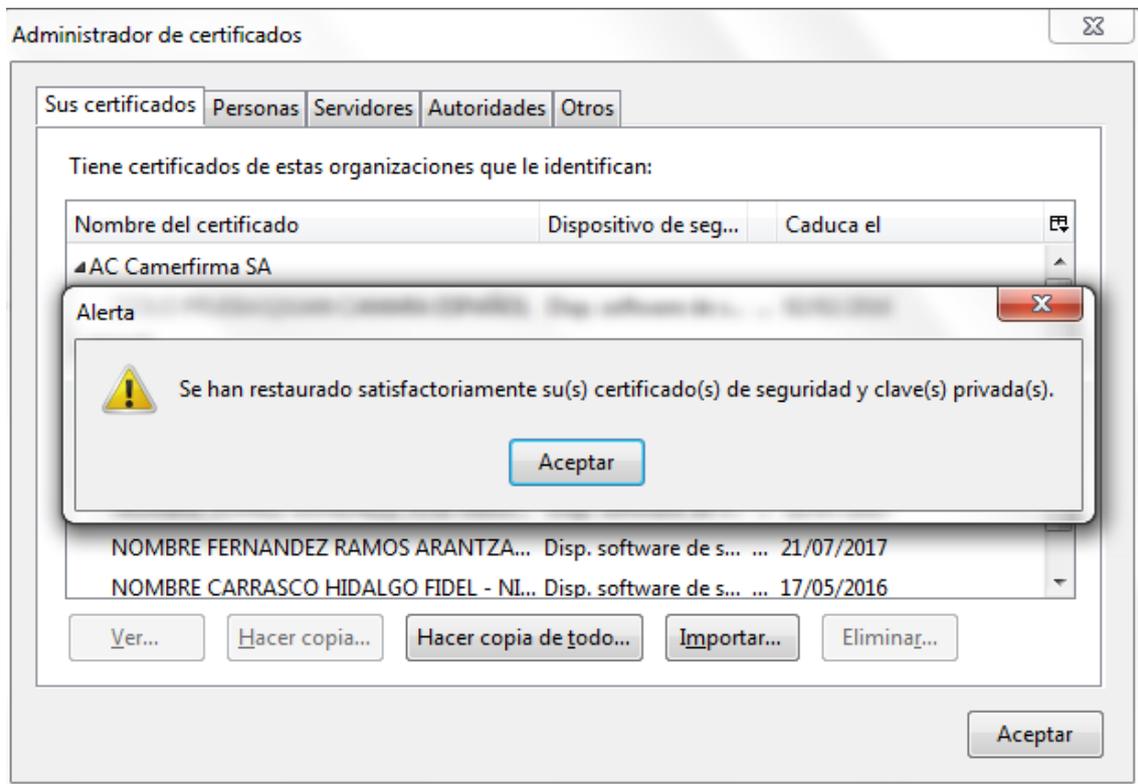
Al pulsar sobre este botón, se abrirá la siguiente pantalla para buscar el certificado.



4. Al seleccionar el certificado, se habilitará la pantalla para **introducir la contraseña** de importación del certificado. Introducirla y pulsar en Aceptar.



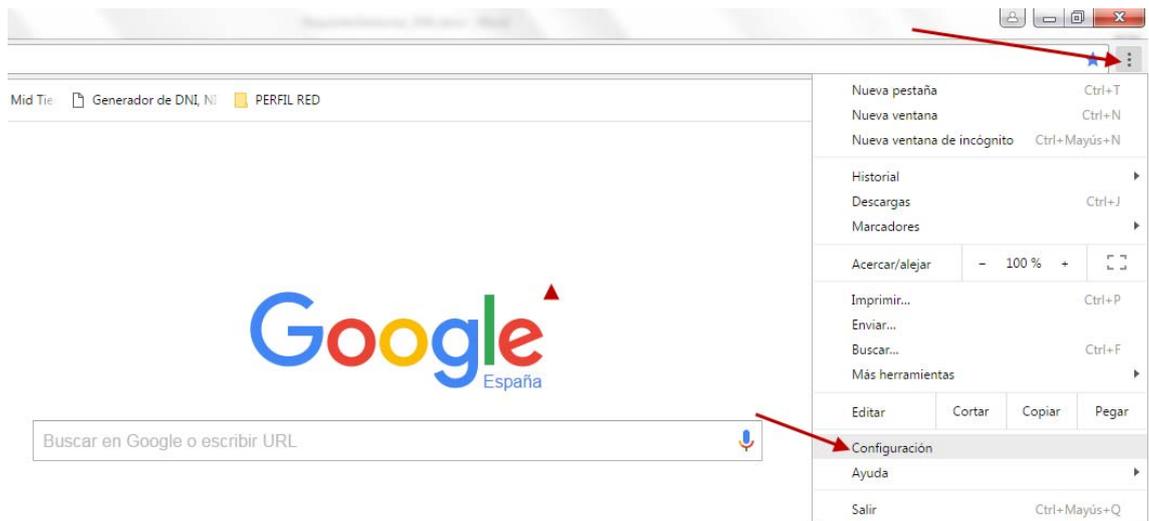
5. La importación ha finalizado con éxito.



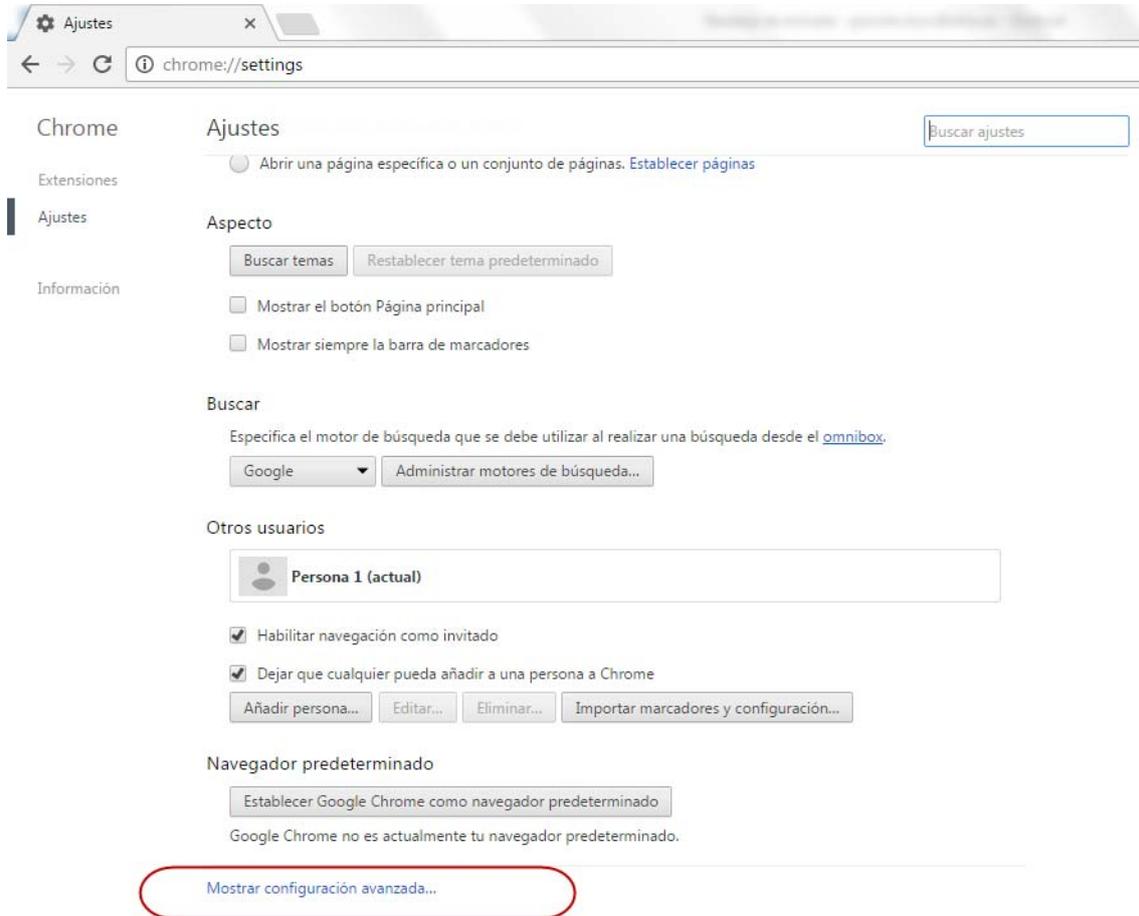
5.3 Google Chrome

Para instalar el certificado digital en el navegador Chrome hay que seguir los siguientes pasos.

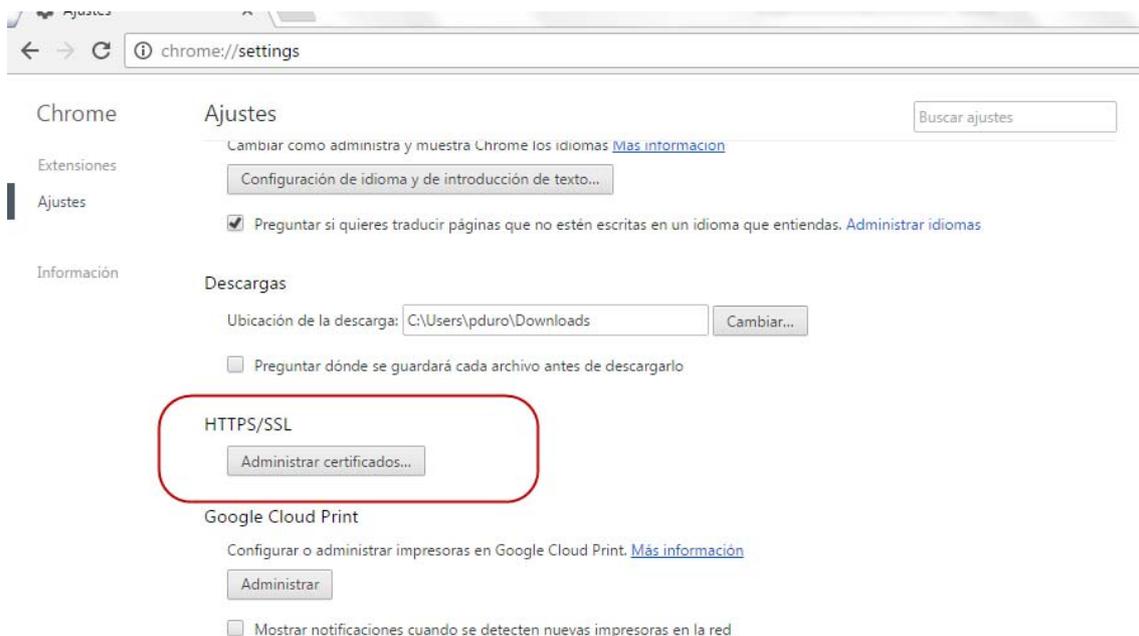
1. Abrir el navegador Google Chrome, pulsar sobre el icono que se encuentra en la parte superior derecha y pulsar sobre "Configuración". Se abrirá la pantalla de "Ajustes" de Chrome.

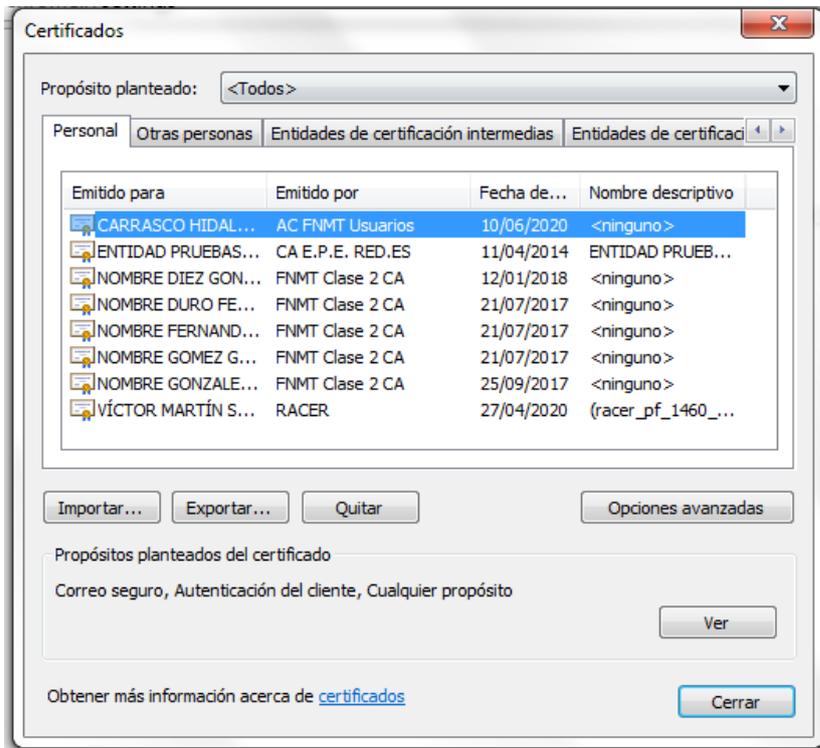


2. En la pantalla "Ajustes", pulsar sobre el link "Mostrar configuración avanzada..."



3. En la opción HTTPS/SSL, pulsar sobre el botón "Administrar certificados". Se abrirá el almacén de certificados, que es el mismo que para Internet Explorer, como muestra la pantalla.





4. Para importar el certificado, hay que seguir los mismos pasos que se han explicado en el punto 5.1 de este manual (Importar certificado en Internet Explorer)

5. ANEXO 4: INSTALAR DNI ELECTRÓNICO

Deberá entrar en la siguiente página Web para descargar el módulo criptográfico del DNI Electrónico para sistema Windows.

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1100

Una vez dentro de la página deberá seleccionar el sistema operativo adecuado para su PC.



The screenshot shows the 'Área de Descargas' (Downloads Area) of the DNIe website. The page header includes the 'Cuerpo Nacional de Policía' logo and navigation tabs for 'Ciudadanos', 'Empresas', 'Administraciones', and 'Oficina Técnica'. A breadcrumb trail reads 'Inicio / Área de Descargas'. The main content area is titled 'Área de Descargas' and lists several download categories with expandable icons: 'Sistema Windows', 'Sistemas GNU/Linux y Sistemas MacOS', 'Certificados x509, Autoridades de Certificación y Autoridades de Validación', 'Código fuente pkcs11', and 'Código fuente completo de aplicaciones Android, y documentación para desarrolladores, para uso de DNIe 3.0 en dispositivos móviles con tecnología NFC'. A footer note provides contact information for the 'Oficina Técnica' at oficinatecnica@dnielectronico.es. Logos for 'POLICÍA NACIONAL' and 'sede electrónica' are visible at the bottom.



The screenshot shows the 'Software para Windows' page on the DNIe website. The breadcrumb trail is 'Inicio / Área de Descargas / Software para Windows'. The main content area is titled 'Software para Windows' and lists several download categories with expandable icons: 'Documentos con recomendaciones de instalación', 'Sistemas Windows de 32 bits. Compatible con sistemas W7, W8, W8.1 y Windows 10', 'Sistemas Windows de 64 bits. Compatible con sistemas W7, W8, W8.1 y Windows 10', 'Instalación Desatendida', and 'Histórico de Versiones de Software del DNIe compatibles con XP y Vista. (No compatible con DNI 3.0)'. A note states: 'Nota: Microsoft ha dejado de dar soporte al Sistema Operativo Windows XP SP3 en fecha El 8 de abril de 2014, por motivos de seguridad al carecer de este soporte no se da continuidad al nuevo DNI 3.0 sobre este sistema operativo.' A red warning text at the bottom reads: 'Las nuevas versiones de drivers publicadas son compatibles con los sistemas XP y con el DNIe en su versión anterior, pero **no podrá utilizarse el nuevo DNI 3.0 con el sistema operativo Windows Vista, XP o anteriores.**' Logos for 'POLICÍA NACIONAL' and 'sede electrónica' are visible at the bottom.

Una vez seleccionado, aparecerá la siguiente pantalla, en la cual se deberá pulsar sobre el ejecutable.



The screenshot shows the website for the 'Cuerpo Nacional de Policía' (National Police Corps) under the 'DNI y Pasaporte' (ID and Passport) section. The page is titled 'Sistemas Windows de 64 bits. Compatible con sistemas W7, W8, W8.1 y Windows 10'. A red box highlights the download link: 'MD5: ae80c7e10da33c3acb38dded344eaa12 DNIe v13_0_2 (64 bits).exe'. Below this, there is a section for 'Smart Card Mini-Driver' with instructions on how to install it on Windows 7, 8, 8.1, and 10. The instructions mention that the driver is available through Microsoft Windows Update and that it allows the DNIe to work as a plug&play device. It also notes that the driver is based on the 'Smart Card Mini-Driver' architecture and that it requires the installation of the cryptographic module and the Firefox browser.

Al ejecutarlo, aparece la pantalla para seleccionar el idioma en el cual nos lo queremos descargar.



The screenshot shows a dialog box titled 'Instalable DNIe - InstallShield Wizard'. The dialog box contains the text 'Seleccione uno de los idiomas siguientes para la instalación.' (Select one of the following languages for installation). Below this text is a dropdown menu with 'Español' (Spanish) selected. There are two buttons at the bottom: 'Aceptar' (Accept) and 'Cancelar' (Cancel).

Al pulsar en aceptar, aparecerá la siguiente pantalla, que nos llevará al asistente de instalación.

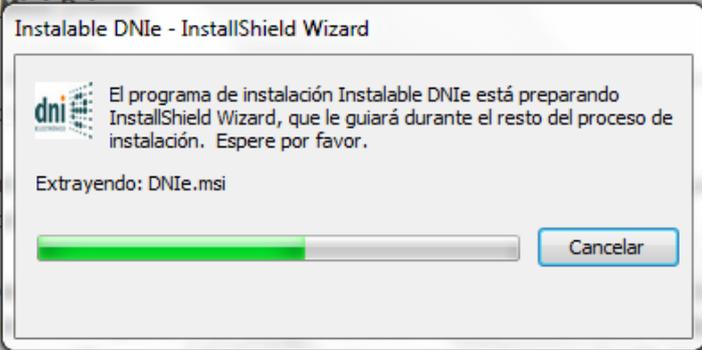
[Inicio](#) / [Área de Descargas](#) / [Sistema para windows](#) /
Sistemas Windows de 64 bits. Compatible con sistemas W7, W8, W8.1 y Windows 10

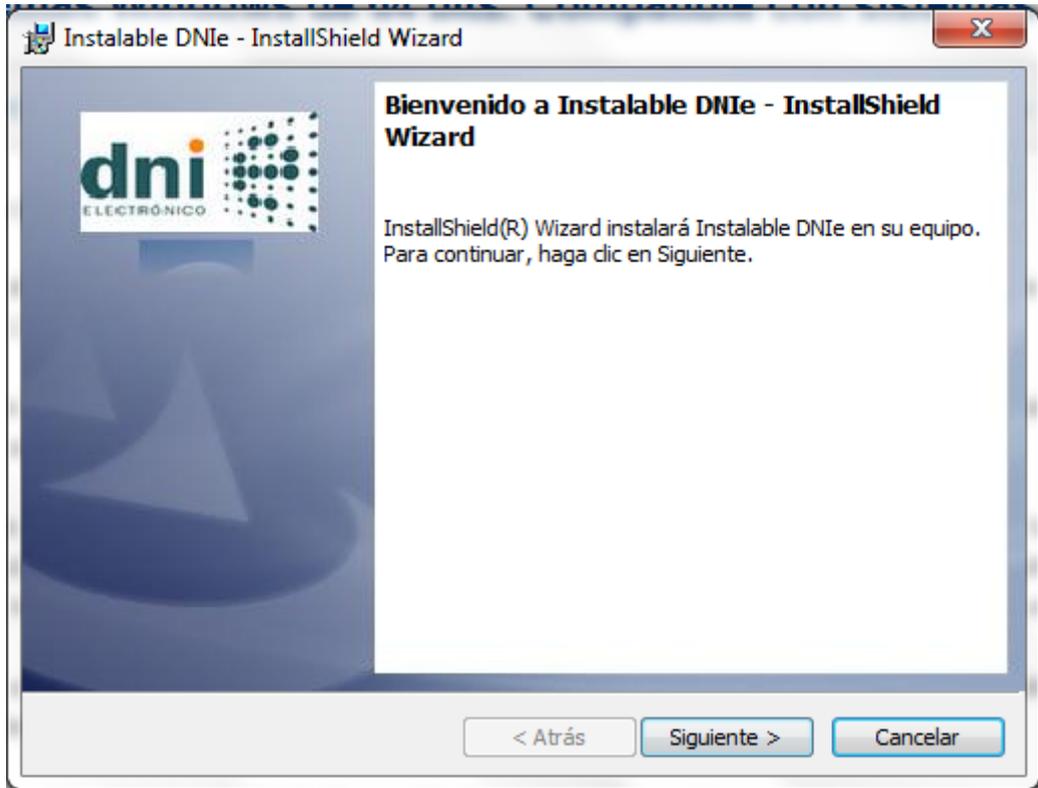
Sistemas Windows de 64 bits. Compatible con sistemas W7, W8, W8.1 y Windows 10

MD5: [ae80c7e10da33c3acb38dded344eaa12](#) [DNIE v13_0_2 \(64 bits\).exe](#)

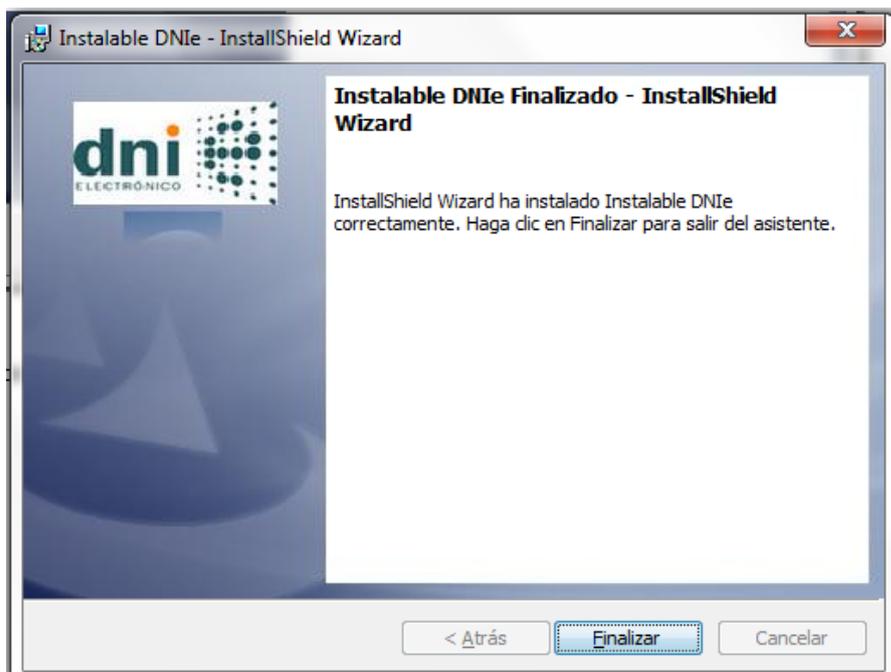
Smart Card

En el servicio de Smart Card de Windows 7, Windows 8.1 y Windows 10, el sistema operativo instala automáticamente el driver del módulo criptográfico del módulo criptográfico y se debe instalar primeramente el navegador Firefox y luego el módulo criptográfico. Este nuevo driver se instala de forma automática en un lector de tarjetas inteligentes. Este driver también es conocida también como la arquitectura PKCS#11. No será posible instalarlo de forma directa en aquellos equipos que ya cuenten con algún tipo de driver instalado.





Habrá que ir pulsando en siguiente, hasta finalizar la instalación



Al pulsar en Finalizar el sistema nos pedirá que reiniciemos el PC.

Verificación de Instalación Correcta del DNIE

1. Internet Explorer

A través del menú **Herramientas / Opciones de Internet / Contenido / Certificados...**



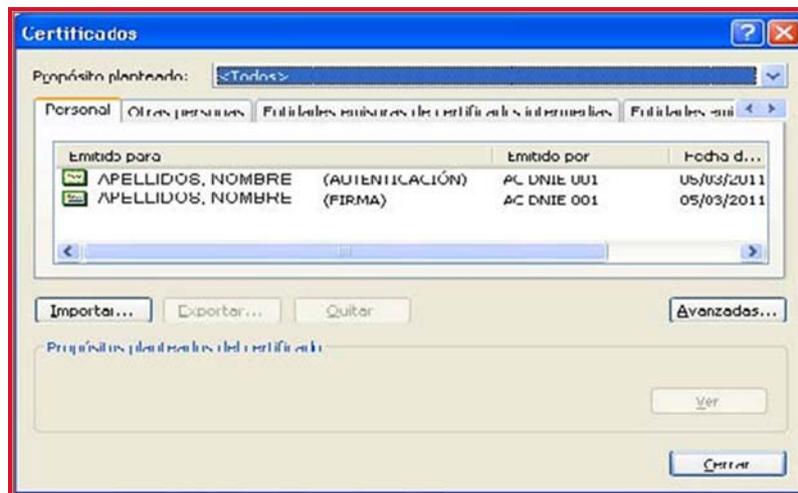
Si está instalado correctamente el módulo CSP del DNIE y tiene correctamente instalados los drivers del lector de tarjetas criptográficas e introducido éste en el citado lector, le pedirá el PIN del DNIE.



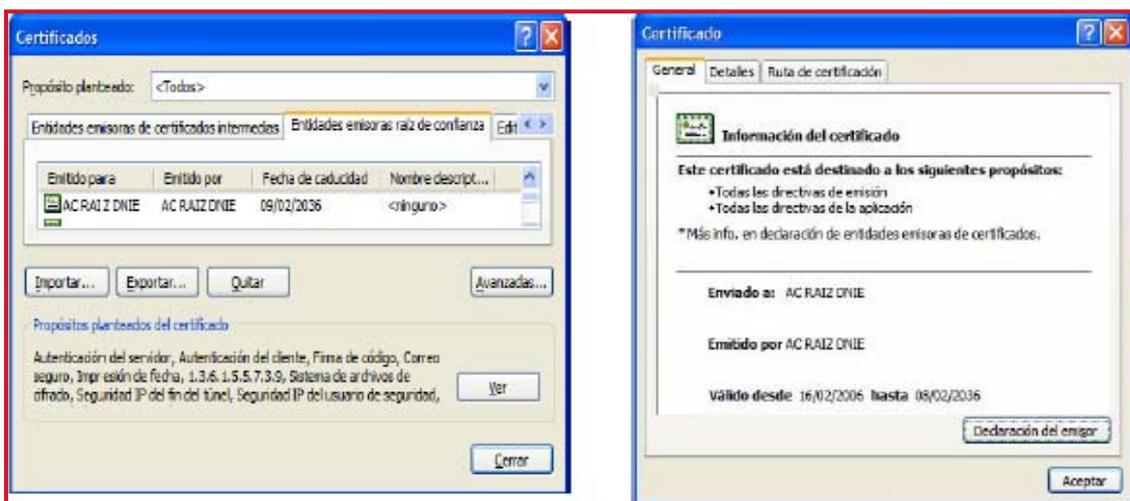
Una vez lo introduzca podrá ver los siguientes certificados:

1. Los certificados del DNIE en la pestaña **Personal**:

- un certificado con propósito de **Autenticación**.
- y otro certificado con propósito de **Firma**.



2. En la pestaña **Entidades emisoras raíz de confianza** podrá visualizar el certificado raíz **AC RAIZ DNIE**.



Si ha podido seguir los pasos anteriores y ver los certificados esto indica que está

correctamente instalado el módulo CSP y el certificado raíz para Microsoft.

2. Mozilla Firefox

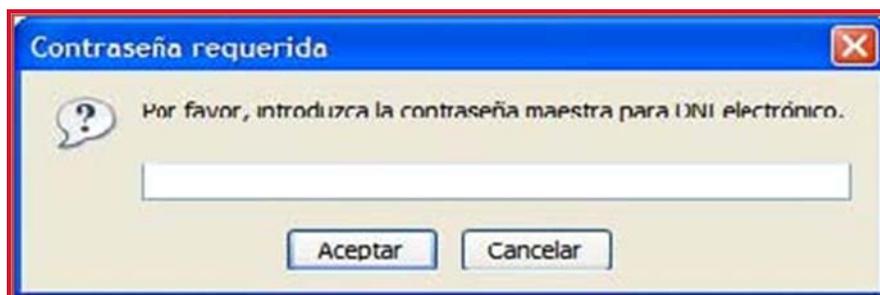
Siguiendo el menú **Herramientas / Opciones / Avanzado**, pestaña Seguridad botón "**Dispositivos de Seguridad**"



Si está correctamente instalado el módulo PKCS#11 aparecerán en la lista de Módulos de seguridad y dispositivos instalados el módulo ***DNIe Modulo PKCS#11***.



Con el módulo ***DNIe Modulo PKCS#11*** instalado, para ver los certificados del *DNI electrónico* hay que abrir el navegador Firefox, y seguir el menú **Herramientas / Opciones / Avanzado / Ver certificados**, esto le pedirá el PIN del DNIe:



Después de introducir correctamente el PIN y a través de la ventana Opciones, pulse el botón **“Ver Certificados”**

En la pestaña Sus Certificados podrá ver sus dos certificados:

- un certificado con propósito de Autenticación
- y otro certificado con propósito de Firma.

En la pestaña **“Autoridades”** podrá visualizar el certificado intermedio **AC DNIE**

00X (el valor de X será 1, 2 ó 3) y el certificado raíz **AC RAIZ DNIE**.



Si ha podido seguir los pasos anteriores y ver los certificados, esto indica que está correctamente instalado el módulo PKCS#11 y el certificado raíz para Firefox.