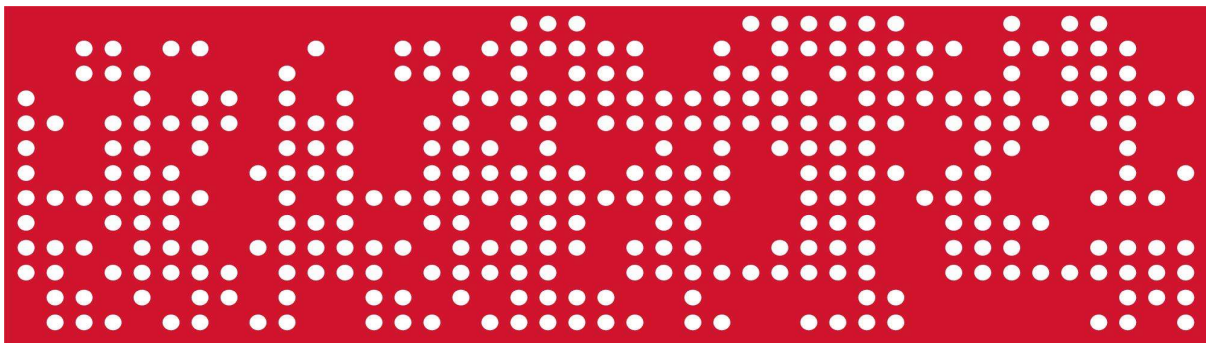
Requisitos Técnicos y de Configuración

eLicitación



ÍNDICE

1. PASOS NECESARIOS PARA TRABAJAR CON EL SISTEMA DE LICITACIÓN ELECTRÓNICA.

Pasos necesarios para que su empresa esté preparada para licitar electrónicamente:

- Identificar a las personas de su empresa que van a participar en los procesos de licitación electrónica en Red.es.

- El Sistema de Licitación Electrónica utiliza, para la validación de certificados, la plataforma @firma de la Administración General del Estado. Más información en la Plataforma de @firma

  Los certificados digitales instalados en el navegador de internet del ordenador que se va a utilizar para realizar la firma y envío de la oferta deberán tener tanto la parte pública como la parte privada.

- **Cualquier certificado admitido por esta Plataforma deberá tener asociado siempre una persona física.**

- **Red.es** actualiza sus aplicaciones, en el menor plazo posible, no más de seis meses, para utilizar la última versión de los componentes liberados por el Ministerio de Hacienda y Función Pública.

2. RESUMEN REQUISITOS TÉCNICOS

Sistemas Operativos

- Microsoft Windows 11.
- Microsoft Windows 10.
- Microsoft Windows 8.1
- Microsoft Windows 8.
- Microsoft Windows 7.
- Ubuntu 8 (32 bits).
- Ubuntu 9 (32 bits).
- Ubuntu 10 (32 bits)

Navegadores

Requisitos para trabajar con los navegadores

- Autofirma.

Certificados digitales

- El Sistema de Licitación Electrónica utiliza, para la validación de certificados, la plataforma @firma de la Administración General del Estado. Más información en la Plataforma de @firma.

  Los certificados digitales instalados en el navegador de internet del ordenador que se van a utilizar para realizar la firma y envío de la oferta deberán tener tanto la parte pública como la parte privada.

- **Cualquier certificado admitido por esta Plataforma deberá tener asociado siempre una persona física.**
- Red.es actualiza sus aplicaciones, en el menor plazo posible, no más de seis meses, para utilizar la última versión de los componentes liberados por el Ministerio de Hacienda y Función Pública.

IPs dinámicas de salida a internet.

- El ordenador que se esté utilizando para licitar debe tener una dirección IP fija de conexión a internet.

Restricciones de directivas de seguridad 	La seguridad implementada en la red donde se encuentra ubicado el ordenador no debe impedir que se transfieran ficheros a través de protocoles https a aplicaciones webs.
Número de sesiones abiertas en el Sistema de licitación 	Para trabajar correctamente con el Sistema de Licitación Electrónica de RED.es, el licitador sólo podrá tener una sesión abierta en el sistema.

3. RELACIÓN DE REQUISITOS TÉCNICOS

3.1 Uso de Autofirm@

El licitador deberá permitir la ejecución de Autofirm@ para que **cualquier navegador** invoque sus servicios tanto para la autenticación como para la firma de ofertas.

3.3 Certificados electrónicos

Este Sistema de Licitación Electrónica utiliza, para la validación de certificados, la plataforma @firma de la Administración General del Estado. Más información en la Plataforma de @firma. Red.es actualiza sus aplicaciones, en el menor plazo posible, no más de seis meses, para utilizar la última versión de los componentes liberados por el Ministerio de Hacienda y Función Pública.

Cualquier certificado admitido por esta Plataforma deberá tener asociado siempre una persona física.

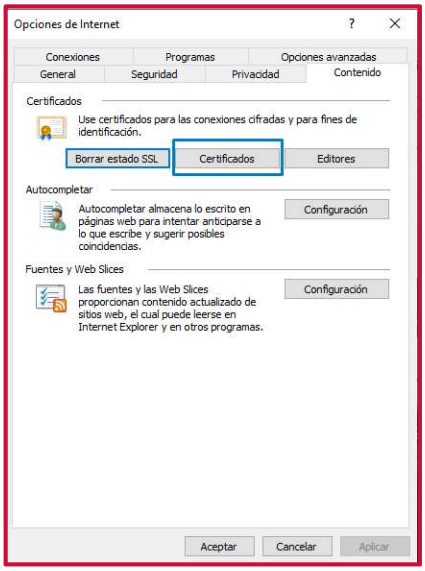
El certificado electrónico instalado en el navegador deberá tener activada la propiedad de firma. Para tal objetivo verifique que la extensión del certificado instalado en el equipo es **.pfx.** Si el certificado instalado tiene la extensión **.cer** no tendrá activada la propiedad de firma.

Se deberá tener presente que los navegadores INTERNET EXPLORER y GOOGLE CHROME comparten el mismo almacén de certificados. Sin embargo, el navegador FIREFOX utiliza su propio almacén de certificados.

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

INTERNET EXPLORER: Acceso al almacén de certificados

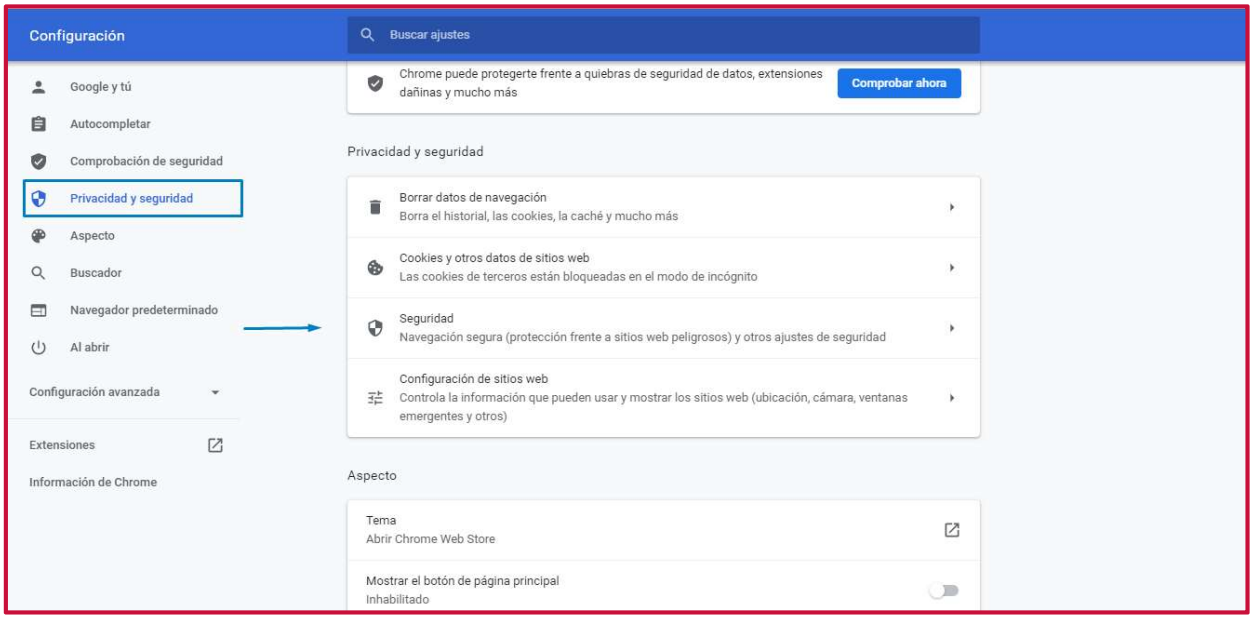
Ruta de Acceso: Opciones de Internet > Contenido.



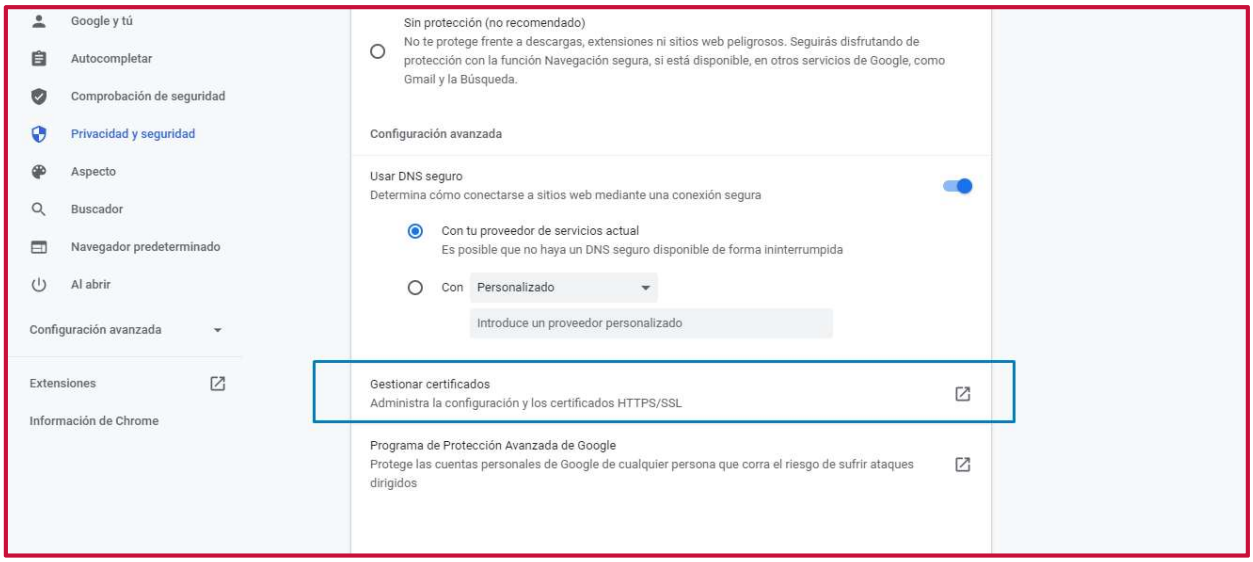
GOOGLE CHROME: Acceso al almacén de certificados

Ruta de Acceso: Configuración > Privacidad y Seguridad.

Se deberá seleccionar la **opción de Seguridad**, tal como se muestra en la siguiente imagen.



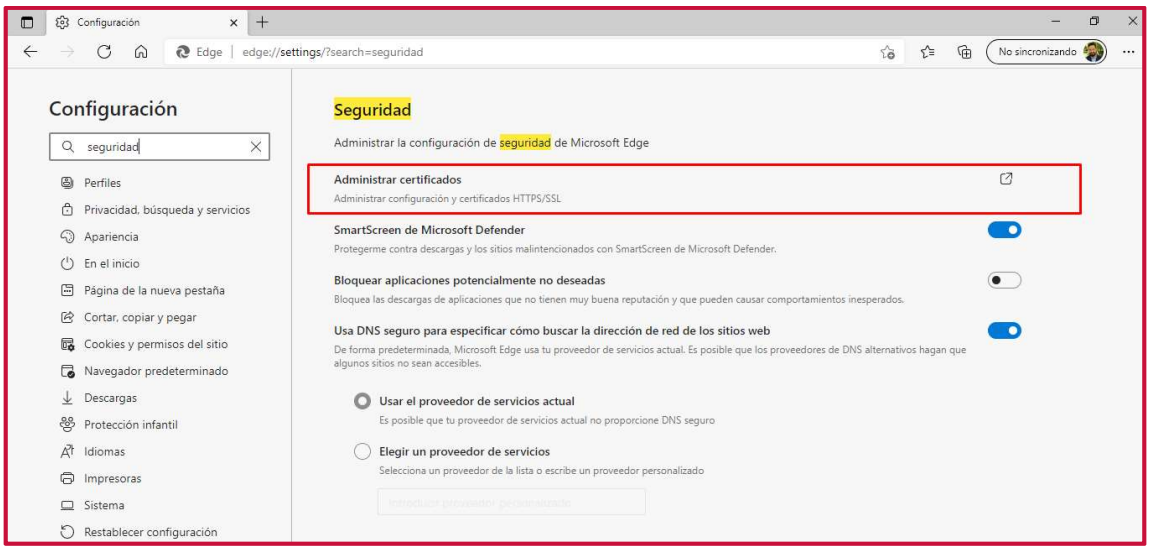
En las Opciones de Seguridad, se deberá seleccionar **Gestionar Certificados.**



MICROSOFT EDGE: Acceso al almacén de certificados

Ruta de Acceso: edge://settings/profiles

En el buscador disponible en la parte superior izquierda de la pantalla, introduciremos la palabra **Seguridad** y pulsaremos la tecla ENTER para que el sistema realice la búsqueda. Si hemos introducido los parámetros correctos, el navegador mostrará el siguiente resultado:



El usuario pulsará sobre la opción de **Administrar Certificados** para acceder a la gestión de los certificados electrónicos instalados en su equipo.

3.4 Certificados electrónicos: Empresas Extranjeras

Si el certificado electrónico expedido para la empresa extranjera no es reconocido por la Plataforma de Licitación Electrónica de Red.es, deberá ponerse en contacto con el servicio de soporte a través de los canales establecidos.

Se solicitará al licitador la clave pública del certificado electrónico para que puedan realizarse las respectivas configuraciones técnicas necesarias para la autenticación y firma electrónica de la oferta con el certificado electrónico expedido por una autoridad certificadora extranjera.

3.6 Asistente de configuración

Para ejecutar la herramienta configuradora habrá que seguir los siguientes pasos;

1) Acceder a la Plataforma de Licitación Electrónica.
2) Pulsar el enlace Herramienta Configuradora del Sistema.

El sistema habilitará la herramienta de configuración para comprobar que el equipo local del usuario está preparado para trabajar con la Plataforma a través de un único paso.

4. ANEXO I. INSTALACIÓN DEL DNI ELECTRÓNICO

Instalación del Módulo Criptográfico para el DNIe

En la página Web encontrará el software con el ejecutable para la instalación del citado modulo criptográfico para sistemas Windows en el siguiente enlace http:

http://www.dnielectronico.es/descargas/index.html

Con solo ejecutar el fichero descargado se instalará el módulo CSP para el entorno Microsoft Windows y el módulo PKCS#11 para navegadores Firefox Mozilla y Netscape sobre Windows.

Deberá reiniciar el PC para finalizar la instalación. En el reinicio se instalará el Certificado AC RAIZ DNIE en los navegadores que estén instalados previamente en el equipo. También se configuran los dispositivos de seguridad de los navegadores Firefox Mozilla y Netscape instalados.

1) En el directorio C:\DNIe se ubicará un archivo de log y los dos archivos siguientes para futuras configuraciones por parte del usuario:

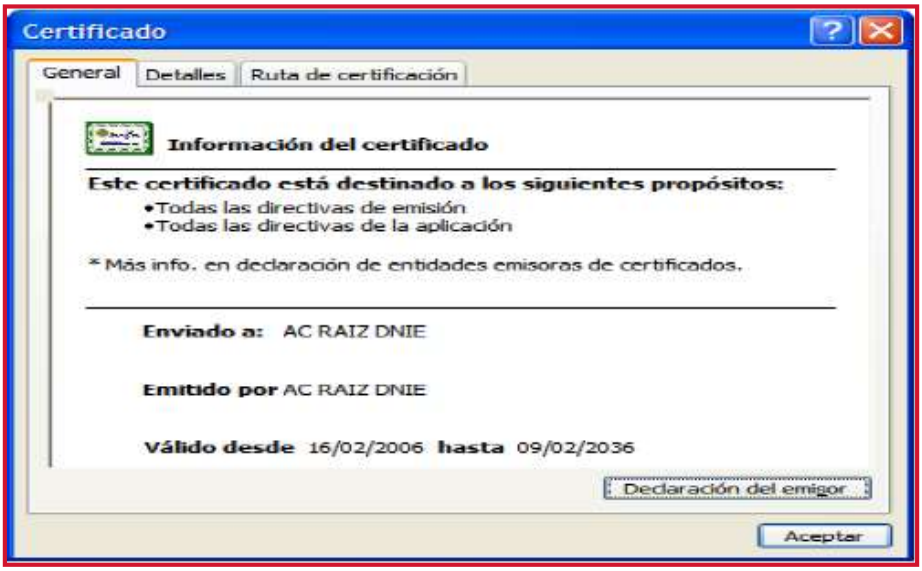
Certificado raíz de la DGP:

ACRAIZ_CERTIFICATE_AND_CRL_SIGNING_SHA1.crt

Módulo PKCS#11 para la instalación:

instalac.htm

2) Si se trata de la primera vez que instala el CSP del DNIe, al reiniciar el equipo le aparecerá la pantalla siguiente que indica que se va a proceder a instalar el certificado AC RAIZ DNIE.



3) Si ya había sido instalado anteriormente, esta ventana no será mostrada. Igualmente puede no aparecer esta ventana si el navegador Internet Explorer está suficientemente actualizado, ya que este certificado se instala automáticamente con un parche de actualización de Microsoft.

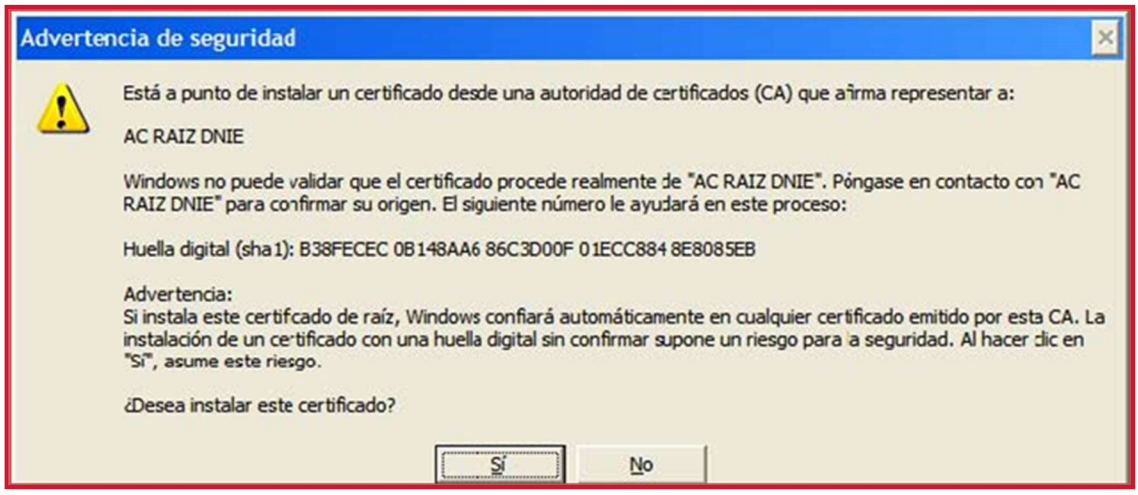
   Le solicitará que confíe/instale el certificado raíz del DNIe, deberá aceptar/instalar. Este paso es necesario para el correcto funcionamiento del DNIe.

4) Pulsamos sobre "**Siguiente**"

5) Pulsamos sobre "**Examinar**"

Seleccionamos el Almacén de certificados: "**Entidades Emisoras Raíz de Confianza**"

6) Pulsamos sobre "**Finalizar**"



7) En este punto pulsar sobre el botón "**Sí**" para permitir que la autoridad raíz del DNIe, **AC RAIZ DNIE**, se instale en el navegador y de esta forma se pueda establecer adecuadamente la cadena de confianza de certificación. (La desinstalación del CSP del DNIe **no borra el certificado raíz del navegador**, por lo que si realiza una segunda instalación, o actualiza la versión no volverá a mostrarse este mensaje)

Verificación de Instalación Correcta del DNIe

Para verificar que la instalación se ha realizado correctamente se puede hacer uso de cualquiera de los servicios disponibles como se indica en:

http://www.dnielectronico.es/servicios_disponibles/.

También se puede verificar de modo manual como se indica a continuación. Dependiendo de los navegadores instalados en su PC:

1. Internet Explorer

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

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

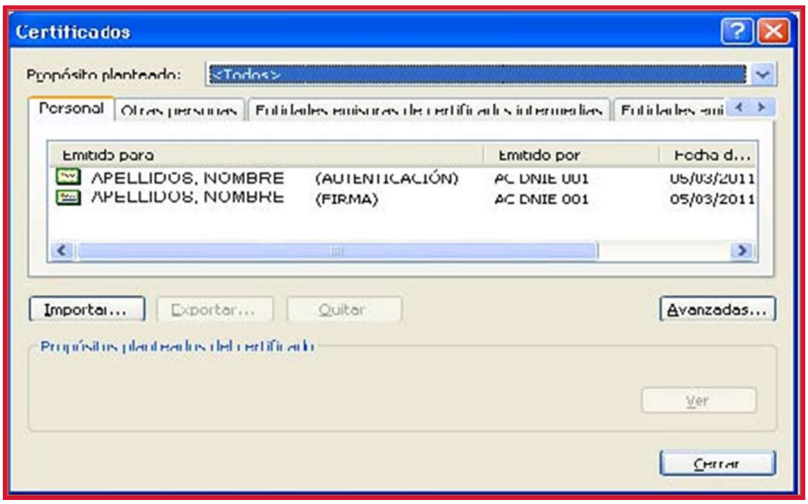
Una vez lo introduzca podrá ver los siguientes certificados:

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

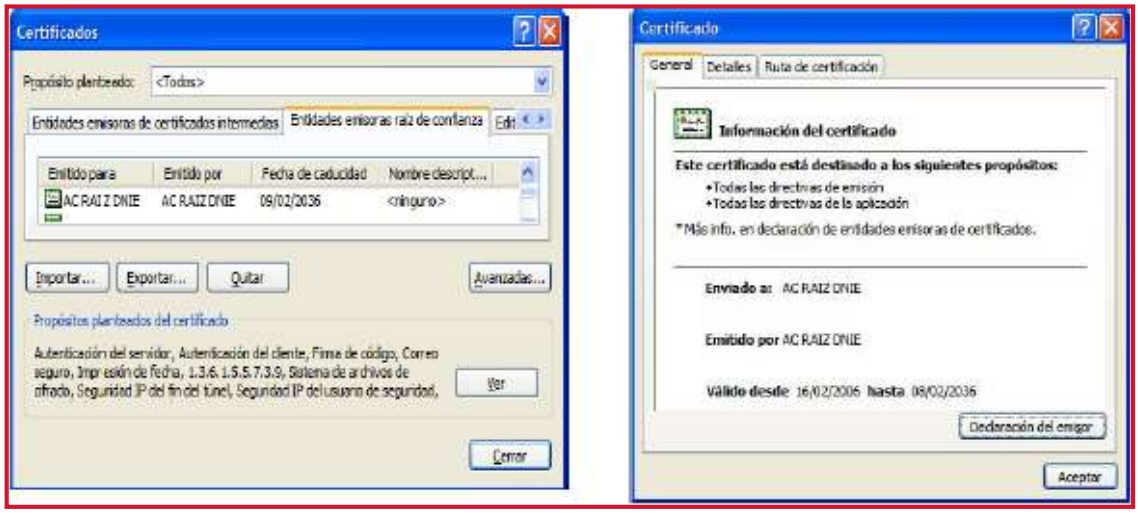
- un certificado con propósito de **Autenticación**.
- y otro certificado con propósito de **Firma**.

Nota: si introducido el PIN no puede ver su certificado siga los pasos descritos en:

http://www.dnielectronico.es/como_utilizar_el_dnie/ComprobacionBloqueoPIN.pdf



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.