

# **Requisitos Técnicos y de Configuración**

eLicitación







# ÍNDICE

1. LI	PASOS NECESARIOS PARA TRABAJAR CON EL SISTEMA CITACIÓN ELECTRÓNICA	DE
2.	RESUMEN REQUISITOS TÉCNICOS	4
3.	RELACIÓN DE REQUISITOS TÉCNICOS	6
З	3.1 Uso de Autofirm@	6
З	3.3 Certificados electrónicos	6
	INTERNET EXPLORER: Acceso al almacén de certificados	7
	GOOGLE CHROME: Acceso al almacén de certificados	7
	MICROSOFT EDGE: Acceso al almacén de certificados	9
З	3.4 Certificados electrónicos: Empresas Extranjeras	10
З	3.6 Asistente de configuración	10
4.	ANEXO I. Instalación del DNI Electrónico	11





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

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







# 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
Õ	la Administración General del Estado. Más
	información en la <u>Plataforma de @firma.</u>
	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.
	X 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.







# **3. RELACIÓN DE REQUISITOS TÉCNICOS**

## <u>3.1 Uso de Autofirm@</u>

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 <u>Plataforma de @firma.</u> 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.

Con	figuración	Q Buscar ajustes	
÷	Google y tú	Chrome puede protegerte frente a quiebras de seguridad de datos, extensiones dañinas y mucho más	ahora
Ô	Autocompletar	Privaridad v seguridad	
0	Comprobación de seguridad		
0	Privacidad y seguridad	Borrar datos de navegación Borra el historial, las cookies, la caché y mucho más	•
۲	Aspecto	Conkies v atros datos de sitios web	
Q	Buscador	Las cookies de terceros están bloqueadas en el modo de incógnito	,
	Navegador predeterminado	Seguridad	,
ப	Al abrir	<ul> <li>Navegación segura (protección frente a sitios web peligrosos) y otros ajustes de seguridad</li> </ul>	
Confi	guración avanzada 👻	Configuración de sitios web 32 Controla la información que pueden usar y mostrar los sitios web (ubicación, cámara, ventanas	,
		emergentes y otros)	
Exter	isiones 🖸		
Infor	nación de Chrome	Aspecto	
		Tema Abrir Chrome Web Store	Ø
		Mostrar el botón de página principal Inhabilitado	-



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.



# red.es

# 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 <u>Herramienta Configuradora del Sistema.</u>

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.

Herramienta configuradora del sistema
Se comprobará si el navegador y sistema operativo que usa está entre los homologados para usar el Sistema de Licitación Electrónica. Le recordamos que los navegadores y sistemas operativos soportados para la presentación de ofertas son: • Microsoft Internet Explorer 11 (Windows 7, Windows 8 y Windows 10) • Microsoft Edge (Windows 10) • Google Chrome / Chromium (Windows 7, Windows 8 y Windows 10) También se comprobarán las restricciones configuradas en su navegador (bloqueador elementos emergentes). Si desea mayor información sobre los requisitos necesarios y su configuración puede consultar el documento de <u>Reguisitos Técnicos</u> Sistema Operativo: Microsoft Corporation Windows Navegador: Chrome - 119 JavaScript: Habilitado Cookies: Habilitado
Sistema y navegador comprobados. Le recordamos que esta comprobación no garantiza la compatibilidad completa de su equipo, por favor continúe con la herramienta.
Contacto  Aviso Legal  Accesibilidad



# 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.



10				
Detailes	Ruta de cert	ificación		
Inform	mación del c	ertificado		
certifica	ado está des	tinado a los si	guientes propósit	05:
•Todas la	as directivas de	e emisión		
Enviado	a: AC RAIZ	DNIE		
Emitido	por AC RAIZ	DNIE		
Válido d	lesde 16/02/2	2006 hasta 09,	/02/2036	
			Declaración	del emigo
				-
	Detalles Infor •Todas l •Todas l	Detalles Ruta de cert Información del o certificado está des •Todas las directivas d •Todas las directivas d info. en dedaración de Enviado a: AC RAIZ Emitido por AC RAIZ	Detalles Ruta de certificación Información del certificado certificado está destinado a los si •Todas las directivas de emisión •Todas las directivas de la aplicación info. en declaración de entidades emise Enviado a: AC RAIZ DNIE Emitido por AC RAIZ DNIE Válido desde 16/02/2006 hasta 09	Detalles Ruta de certificación Información del certificado certificado está destinado a los siguientes propósit • Todas las directivas de emisión • Todas las directivas de la aplicación info. en declaración de entidades emisoras de certificados. Enviado a: AC RAIZ DNIE Emitido por AC RAIZ DNIE Válido desde 16/02/2006 hasta 09/02/2036

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"

Asistente para importación de certificados
Almacén de certificados Los almacenes de certificados son áreas del sistema donde se guardan los certificados.
Windows puede seleccionar automáticamente un almacén de certificados, o bien es posible especificar una ubicación para el certificado. O Seleccionar automáticamente el almacén de certificados en base al tipo de certificado O Colocar todos los certificados en el siguiente almacén
Almacén de certificados:
< <u>A</u> trás Siguien <u>t</u> e > Cancelar

5) Pulsamos sobre "Examinar"

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

Seleccionar almacén de certificados [?] 🔀
Seleccione el almacén de certificados que quiere usar.
Personal Entidades emisoras raíz de confianza Confianza empresarial Entidades emisoras de cert. intermedias Editores de confianza Certificados en los que no se confía
Mostrar almaceries (isicos Aceptar Cancelar



#### 6) Pulsamos sobre "Finalizar"

	Finalización del Asister importación de certifica Ha completado con éxito el Asistente pi certificados. Ha especificado la siguiente configuraci	ite para ados ara importación de ón:
	Almacén de certificados seleccionado Contenido	Determinado de fc Certificado
Distance of the local	< 10 M	>
	< <u>A</u> trás Finaliz	ar Cancelar

Adverte	ncia de seguridad
1	Está a punto de instalar un certificado desde una autoridad de certificados (CA) que aîrma representar a: AC RAIZ DNIE
	Windows no puede validar que el certificado procede realmente de "AC RAIZ DNIE". Póngase en contacto con "AC RAIZ DNIE" para confirmar su origen. El siguiente número le ayudará en este proceso:
	Huella digital (sha 1): B38FECEC 0B148AA6 86C3D00F 01ECC884 8E8085EB
	Advertencia: Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer dic en "Si", asume este riesgo.
	¿Desea instalar este certificado?
	Sí No

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...

Conexiones	Pro	gramas	Opcie	ones avanzadas
General	Segurdad	Priv	/acldad	Contenido
Las da Intern	asificaciones le let que se pue	ayudan a con de ver con est	ntrolar el tip te equipo.	o de contenido d
Las da Intern	asificaciones le let que se pue	ayudan a con de ver con est <u>H</u> abilitar	ntroiar el tip te equipo.	o de contenido d Configuración
Las dz Intern	asificaciones le let que se pue	ayudan a con de ver con est <u>H</u> abilitar	ntrolar el tip te equipo.	o de contenido d Configuración

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

orsonal Otras personas Fulida	ules emisoras de certific	adıs intermedias 🛛 P	intidades emi ⊀
Emitido para		Emitido por	Focha d
APELLIDOS, NOMBRE	(AUTENTICACIÓN) (FIRMA)	AC DNIE UU1 AC DNIE 001	05/03/201 05/03/201
<	100		>
mportar	Quitar		Avanzadas
ropositos planteanos ner cercio a	"		
			Ver

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



Enitido para Enitido por Fecha de caducidad Nombre descript	Este certificado está destinado a los siguientes propósitos: +Todas las deschuas de emisión
ACRAUZ DINE ACRAUZ DINE 09/02/2036 <ninguro></ninguro>	*Todas las directivas de la aplicación "Más info, en declaración de entidades enisoras de certificados.
[Importar] [Exportar] Quitar [Avenuadas]	Enviado ar ACRAIZ DVIE
Propisitos plantesetos del certificado Autenticación del servidor, Autenticación del cliente, Firma de código, Correo	Emitido por ACRAIZ DNIE
aleguro, impresson de retraj. 1.3.4. 1.5.5.7.3.9, Salena de archivos de afrado, Seguritad IP del fin del tínel, Seguridad IP delusiarin de seguridad,	Válido desde 16/02/2006 hasta 08/02/2036
	Dedaración del emigar
<u>Cerror</u>	Aceptar

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