



# Ayuntamiento de Logroño

Servicio de Nuevas Tecnologías

Avenida de la Paz, 11  
26071 - Logroño (La Rioja)  
Tfn: +034 941.27.70.00  
Fax: +034 941.27.70.25

**Sede Electrónica del Ayuntamiento de Logroño  
Establecimiento de canal seguro**

V1.Febrero 2015

<b>INTRODUCCIÓN.....</b>	<b>3</b>
<b>CONCEPTOS PREVIOS.....</b>	<b>3</b>
<b>COMUNICACIÓN SEGURA: PROTOCOLO SSL .....</b>	<b>4</b>
1.1. El porqué del SSL en la Sede del Ayuntamiento de Logroño .....	4
1.2. Errores SSL.....	5
1.2.1. No se pueden acordar un protocolo común. ....	5
1.2.2. Errores de Certificación.....	5
<b>ERROR DE CERTIFICADO: EXPOSICIÓN Y SOLUCIÓN .....</b>	<b>5</b>
1.3. Exposición del problema .....	6
1.4. Solución del problema.....	7
1.4.1. Instalando el Certificado Raiz FNMT .....	7
Descarga .....	8
Instalación de Certificados y edición de confianza. ....	8
1.5. Resultado.....	9
<b>ACCESO MEDIANTE CERTIFICADO DIGITAL.....</b>	<b>10</b>

## Introducción

El presente documento se confecciona con la finalidad de dar respuesta a las numerosas dudas que por parte de los usuarios de la Sede Electrónica del Ayuntamiento de Logroño, [sedeelectronica.logrono.es](http://sedeelectronica.logrono.es), se han recogido por los diferentes canales de comunicación que se brindan a los usuarios de este servicio.

El documento explica con un lenguaje sencillo y comprensible los diferentes conceptos técnicos, evitando entrar en detalles y tecnicismos que puedan impedir el objetivo del presente documento que es aportar seguridad y confianza entre la relación que se establece entre ciudadanos y Ayuntamiento de Logroño.

## Conceptos Previos

Para poder entender correctamente los siguientes apartados, vamos a introducir previamente una serie de conceptos de forma breve y comprensible.

**Navegador Web:** Es un programa informático que permite a un dispositivo electrónico, ordenador, tablet, teléfono, smarttv, etc., interactuar con otro dispositivo electrónico, servidor Web, intercambiando información en un lenguaje comprensible para ambos, paginas html.  
Ejemplos de navegadores, son Internet Explorer, google Chrome, Firefox, etc.

**Sistema Operativo:** Es el conjunto de programas informáticos que interactúan con el dispositivo electrónico y brindan sus servicios al usuario del dispositivo así como a otros programas informáticos que se ejecuten sobre el dispositivo. Ejemplos de SSOO son Windows, Linux, Android, etc.

**Encriptar:** Consiste en alterar el texto original en otro ilegible mediante una clave, el proceso inverso, descryptar, consiste en usar una clave para retornar el texto ilegible en el texto original, la clave para encriptar y descryptar no tienen por que ser la misma. En resumen, podemos entender que el proceso de encriptación y descryptación de un texto, entre un extremo origen y un extremo receptor donde ambos conocen la clave de encriptación, garantiza la confidencialidad de la información y la seguridad de que esta ha sido emitida por el extremo opuesto de la comunicación, esto es, el receptor reconoce la información descifrada como la enviada por el emisor.

**Clave Publica y Privada:** Son dos ficheros informáticos que relacionan a una misma persona, o ente, de forma que cuando un fichero informático es encriptado con la clave privada, la autoría del mismo puede verificarse mediante el uso de la clave publica. Las claves públicas pueden entregarse para ser usadas en el proceso de verificación de la autoría de un documento. Ejemplo, cuando alguien firma un documento pdf lo encripta haciendo uso de su clave privada, y cualquier persona puede usar la clave publica de quien firmo el documento para identificar al firmante. Cualquier alteración del fichero informático invalidara el proceso de verificación, por tanto, el cifrado es inviolable.

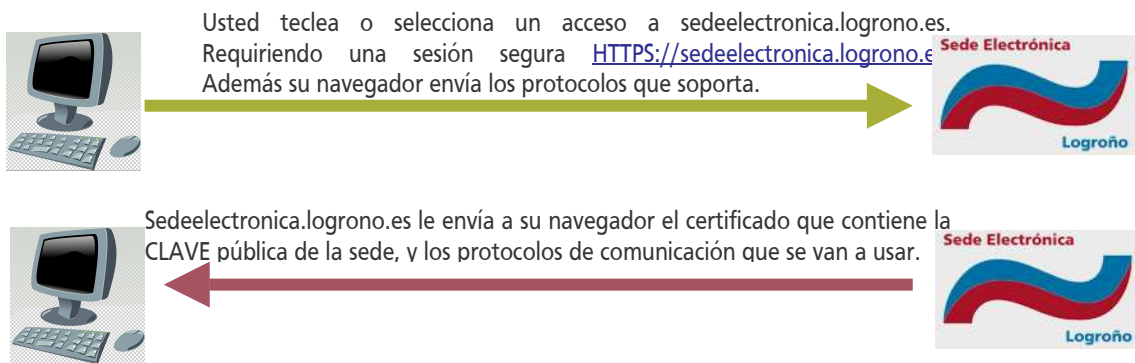
**Encriptación asimétrica o de clave pública:** Consiste en alterar la información mediante una clave (pública) y restablecer la información al original usando otra clave (privada). Para que este mecanismo funcione, las claves publicas de una persona o entidad han de ser proporcionadas. Ejemplo, si quiero enviar un fichero a PersonaA, utilizare su clave publica para encriptar el fichero y tendré la certeza de que solo la clave privada de PersonaA puede revertir el proceso, descryptar el fichero.

**Certificado Digital:** Es un fichero de ordenador que recoge datos identificativos de una persona o entidad y que esta acreditada su autenticidad e integridad por medio de una autoridad certificadora (CA). Un certificado digital contiene la firma de una entidad certificadora, esto es, al fichero original del certificado se le añade información encriptada con la clave privada de la entidad certificadora de forma que garantice:

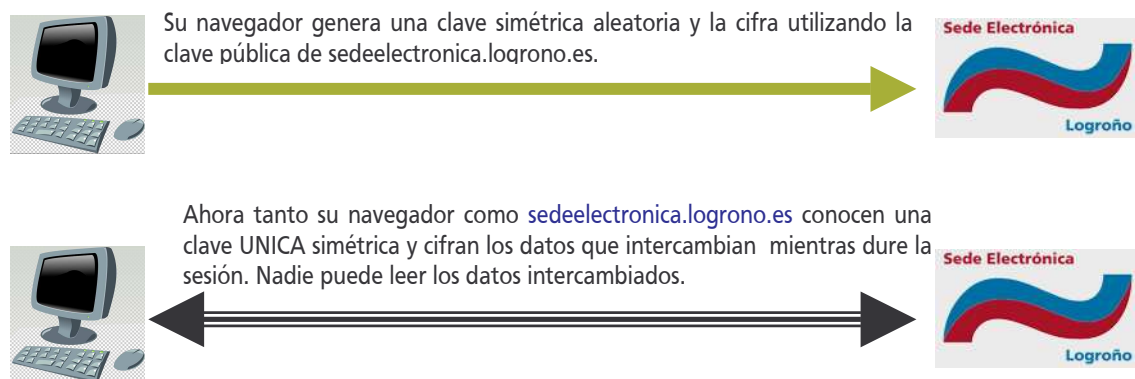
- 1) que no pueda ser alterada la información sin invalidar la firma, comprobación de autoria
- 2) se puede comprobar la autoría o quien es el autor usando la clave publica de la CA.

## Comunicación Segura: Protocolo SSL

Con los conceptos expuestos anteriormente estamos capacitados para entender como se establece el protocolo de seguridad SSL.



Su navegador AUTENTICA el certificado de [sedeelectronica.logrono.es](https://sedeelectronica.logrono.es) con la lista de Autoridades de Certificación (CA) instaladas en su navegador.  
Si el certificado [sedeelectronica.logrono.es](https://sedeelectronica.logrono.es) no es reconocido, lo será porque no tiene instaladas las CA de la FNMT y por tanto su navegador le impedirá el acceso a la sede electrónica o le solicitará su autorización para acceder. (*Depende del navegador y/o versión*)



### 1.1. El porqué del SSL en la Sede del Ayuntamiento de Logroño

Con el protocolo SSL correctamente establecido se obtienen dos características muy importantes en la comunicación ciudadano <-> SedeElectronica.logrono.es, que son:

- 1) el ciudadano tiene la certeza de que se esta comunicando con la SedeElectronica.logrono.es

- 2) la comunicación es privada e inalterable, esto es, si alguien intercepta la comunicación solo observara el texto encriptado y la comunicación no podrá ser sustituida por otra, por que para ello debiera ser encriptada por la clave acordada para la sesión establecida entre el ciudadano y la SedeElectronica.

Dicho esto, cuando usted introduce sus datos bancarios, consulta sus recibos, emite una queja o intercambia cualquier otro tipo de información con la Sede Electrónica del Ayuntamiento de Logroño, nadie ni nada podrá interceptar, observar o alterar esta información sin que usted se entere, por que toda alteración producirá un error en la comunicación.

No se puede evitar que alguien con algún programa informático pueda observar o “pinchar” la comunicación, pero el protocolo SSL garantiza que esa acción no pasara desapercibida para usted ni para la Sede electrónica y que además, la información “pinchada” no será legible.

## 1.2. Errores SSL

En el esquema de establecimiento del canal seguro SSL se pueden producir errores que impidan la creación del canal seguro, algunos de ellos son:

### 1.2.1. No se pueden acordar un protocolo común.

En la fase de inicial del establecimiento del canal seguro, el navegador del ciudadano y el servidor de la Sede Electrónica del Ayuntamiento de Logroño, se comunican para intercambiar la lista de protocolos, lenguajes que entienden ambas partes. Con esta información acuerdan el uso de uno de ellos, pero en ocasiones puede suceder que no exista un punto "común" y por tanto no se pueda establecer la comunicación segura.

Este error es poco frecuente y normalmente se deberá a que el navegador del ciudadano es una versión muy vieja, que no soporta ninguno de los protocolos del servidor, y su solución pasara por usar otro navegador mas reciente o actualizar el navegador por una versión actualizada.

### 1.2.2. Errores de Certificación

Este es el error mas frecuente y cuya aclaración y explicación es el objetivo de todo este documento.

Para que su navegador reconozca a <https://sedeelectronica.logrono.es> como la Sede Electrónica de Logroño, comprueba que el certificado que intercambia la Sede esta emitido por una AC (Autoridad Certificadora) reconocida, para ello busca la AC que certifica a la Sede Electrónica de Logroño entre las autoridades que reconoce, si la tiene este certificado es aceptado pero en caso contrario emite un aviso o error. Dependiendo del tipo de navegador y versión, la alerta que emite puede ser un aviso requiriendo del ciudadano la aceptación de esta eventualidad o puede impedir el acceso a la Sede Electrónica, en este segundo caso se encuentra el navegador Explorer.

El certificado de la sede electrónica esta emitido por la Fabrica Nacional de Moneda y Timbre, para su aceptación el navegador deberá tener instalado su certificado. Este certificado no viene incorporado en todos los navegadores, por lo que si no ha sido instalado con anterioridad deberá instalarse para poder comunicarse con la Sede del Ayuntamiento de Logroño.

## Error de Certificado: Exposición y solución

A continuación se va a explicar cual es el error del certificado de Sede Electrónica del Ayuntamiento de Logroño, del porque sucede y como se soluciona.

Debe considerarse que los certificados son almacenados en su sistema, pero no todos los navegadores hacen uso del mismo almacén de certificados, algunos navegadores gestionan sus certificados de forma independiente, por tanto no debiera extrañarnos que podamos acceder con normalidad con un navegador

mientras que con otro nos sea imposible, por tanto, deberemos comprobar la configuración del navegador que estemos usando y tengamos problemas.

Las capturas que se añaden a este documento están realizadas con el navegador Firefox, pero los conceptos expuestos son totalmente extrapolables al resto de navegadores, simplemente deberá identificarse en que parte de la configuración de su navegador han de realizarse las acciones especificadas.

## 1.3. Exposición del problema

Si cuando tecleamos [sedeelectronica.logrono.es](http://sedeelectronica.logrono.es) o cuando pulsamos un enlace que nos dirija a este sitio observamos la pantalla que a continuación se muestra, entonces estaremos ante el problema que vamos a resolver a continuación.



The screenshot shows a yellow warning box with a shield icon containing a key and a lock. The text reads: "Esta conexión no está verificada". Below this, it states: "Ha pedido a Firefox que se conecte de forma segura a [sedeelectronica.logrono.es](http://sedeelectronica.logrono.es), pero no se puede confirmar que la conexión sea segura." It explains that normally, secure connections are verified, but here they are not. A section titled "¿Qué debería hacer?" suggests that if the user normally accesses the site without problems, the error might be due to someone trying to impersonate the site, and they should not continue. A button labeled "¡Sácame de aquí!" is provided. Another section titled "Detalles técnicos" states that the site uses an invalid security certificate and shows the error message: "No se confía en el certificado porque no se confía en el certificado emisor." (Error code: sec\_error\_untrusted\_issuer). A final section titled "Entiendo los riesgos" explains that the user can force Firefox to trust the site's identification, but notes that "Incluso aunque confíe en este sitio, este error puede significar que alguien esté interfiriendo en su conexión." It advises adding an exception unless the user knows a serious reason why the site should not use a trustworthy identification. A button labeled "Añadir excepción..." is also present.

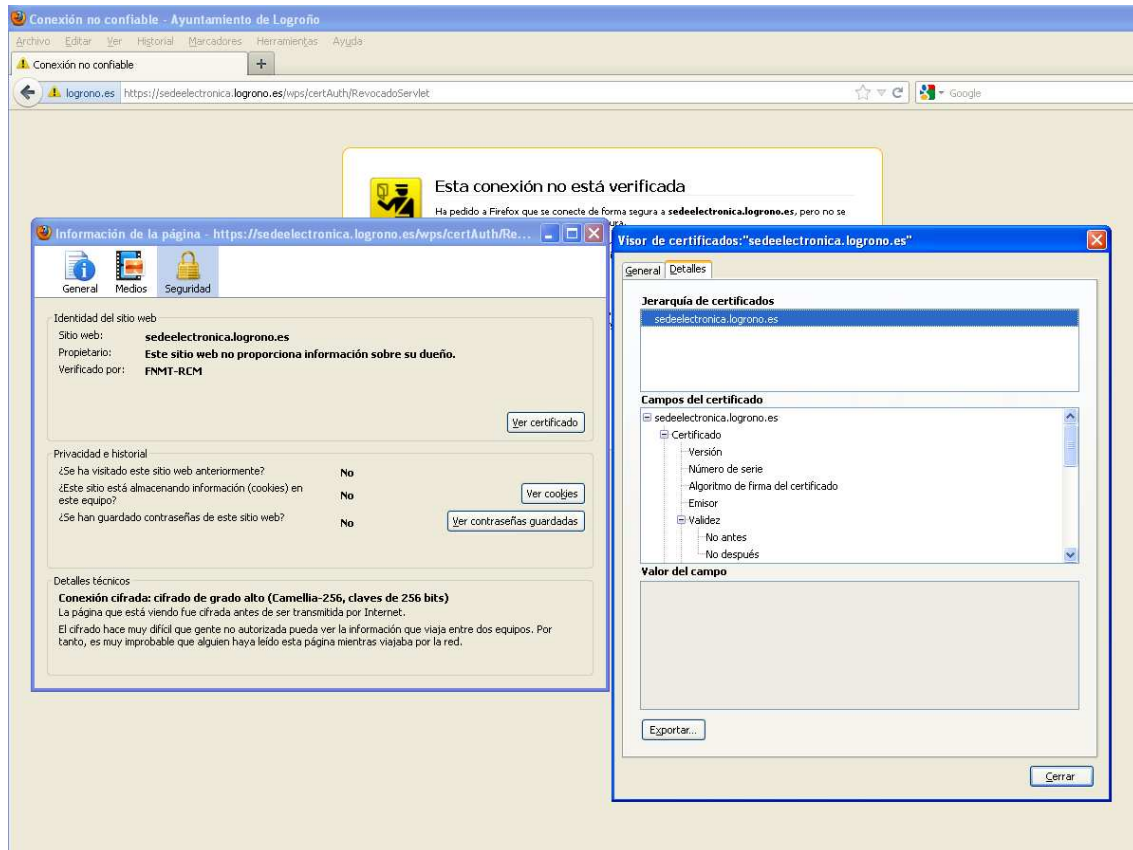
Ahora ya debíamos comprender que nuestro navegador Web nos esta informando que no reconoce como valido la acreditación obtenida al interactuar con la Sede electrónica del Ayuntamiento de Logroño.

Ante este problema podemos:

- 1) pulsar sobre "entiendo los riesgos" en Firefox o su similar en Chrome, y aceptar como valido el certificado. En Internet Explorer, no podremos acceder.
- 2) Instalar los certificados de la FNMT que certifican la sede electrónica. Solución recomendada.

## 1.4. Solución del problema

Si pulsamos sobre la barra de direcciones, donde aparece logrono.es con la alerta amarilla y posteriormente sobre seguridad, y luego sobre ver certificado, obtendremos la captura siguiente, donde podemos ver que el certificado esta emitido por FNMT-RCM y nuestro navegador no confía en esta AC, autoridad certificadora.



### 1.4.1. Instalando el Certificado Raíz FNMT

Para poder confiar en certificados emitidos por la entidad certificadora de la Fabrica Nacional de Moneda y Timbre, deberemos instalar su certificado en nuestro navegador.

Como hemos mencionado anteriormente, los navegadores incorporan preinstalados una serie de certificados de AC, pero no contienen todos, y de ahí surge este problema.

Si accedemos a: <https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt> obtendremos el

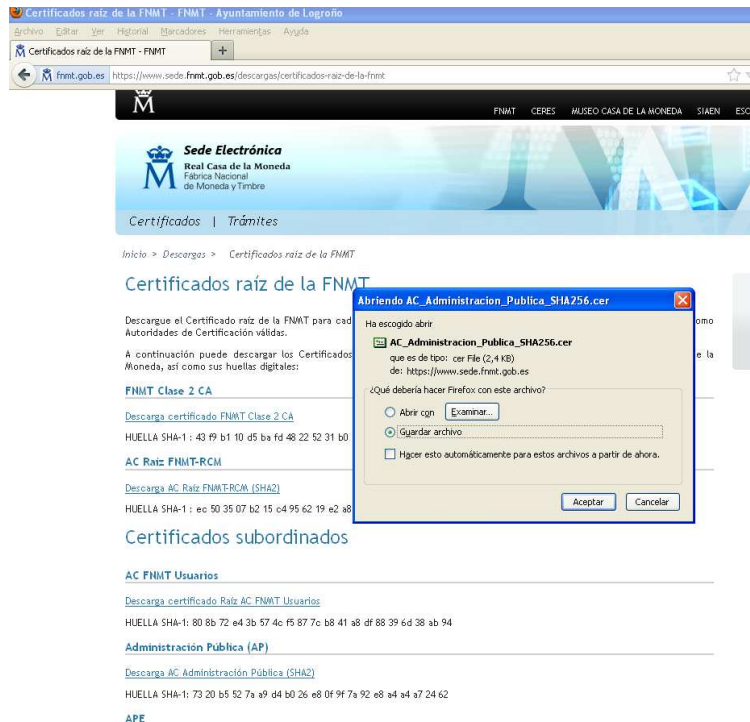


mismo problema que al visitar la [sedeelectronica.logrono.es](https://sedeelectronica.logrono.es) y es que la sede de la FNMT esta certificada por ella misma.

Solo un pequeño número de certificados pueden estar "autofirmados", o autocertificados, es lo que se denomina certificados raíz, en este caso deberemos asumir los riesgos para poder proceder a la descarga y posterior instalación, la alternativa seria

solicitarlo mediante correo electrónico a la FNMT o conseguirlo por otros medios.

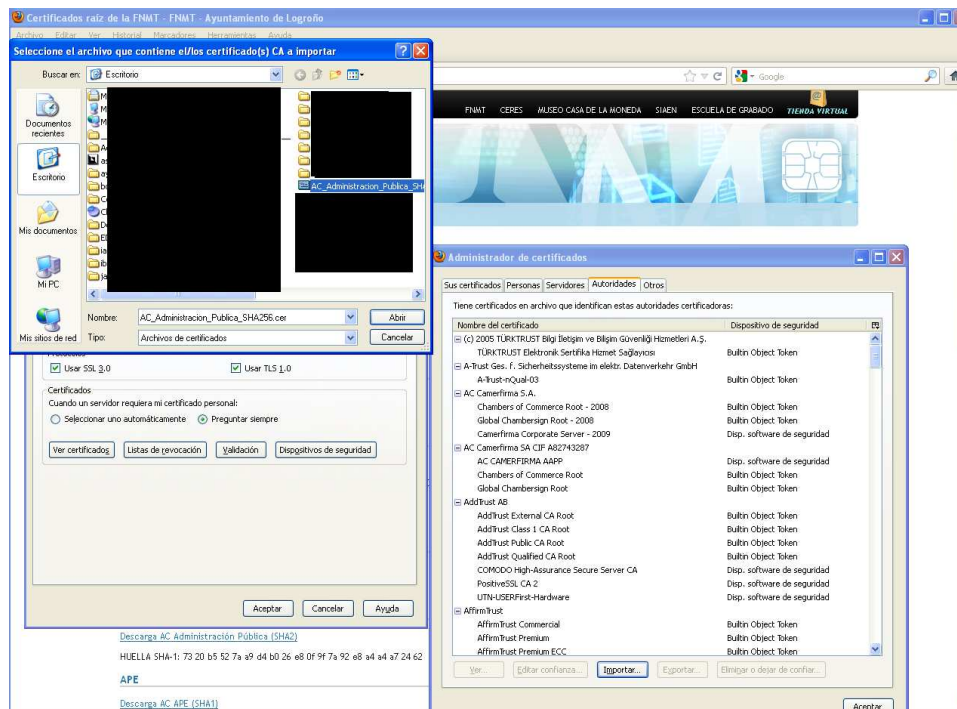
## Descarga



The screenshot shows the website 'Certificados raíz de la FNMT - FNMT - Ayuntamiento de Logroño'. The page lists various certificates for download, including 'FNMT Clase 2 CA', 'AC Raíz FNMT-RCM', and 'AC FNMT Usuarios'. A dialog box titled 'Abriendo AC\_Administracion\_Publica\_SHA256.cer' is overlaid on the page, asking the user to save the file.

Deberemos descargar los certificados FNMT Raíz y AC Administración Pública. Las descargas no conllevan mayor complejidad de la de cualquier otro fichero, simplemente deberemos recordar donde los ubicamos en nuestro sistema de ficheros, para posteriormente instalarlos.

## Instalación de Certificados y edición de confianza.



The screenshot shows the Windows 'Administrador de certificados' (Certificate Manager) window. The 'Importar' (Import) button is highlighted, and the 'Importar' dialog box is open, showing the file 'AC\_Administracion\_Publica\_SHA256.cer' being imported. The main window shows a list of certificates with columns for 'Nombre del certificado' and 'Dispositivo de seguridad'.

Se debe recalcar de que adicionalmente a la incorporación de los certificados en nuestro navegador, deberemos editar la confianza de estos, para indicarle a **nuestro navegador** que confiamos en estos certificados para realizar ciertas comprobaciones, como la de servir de AC, autoridad certificadora.

Para incorporarlo a nuestro navegador, deberemos acceder a :

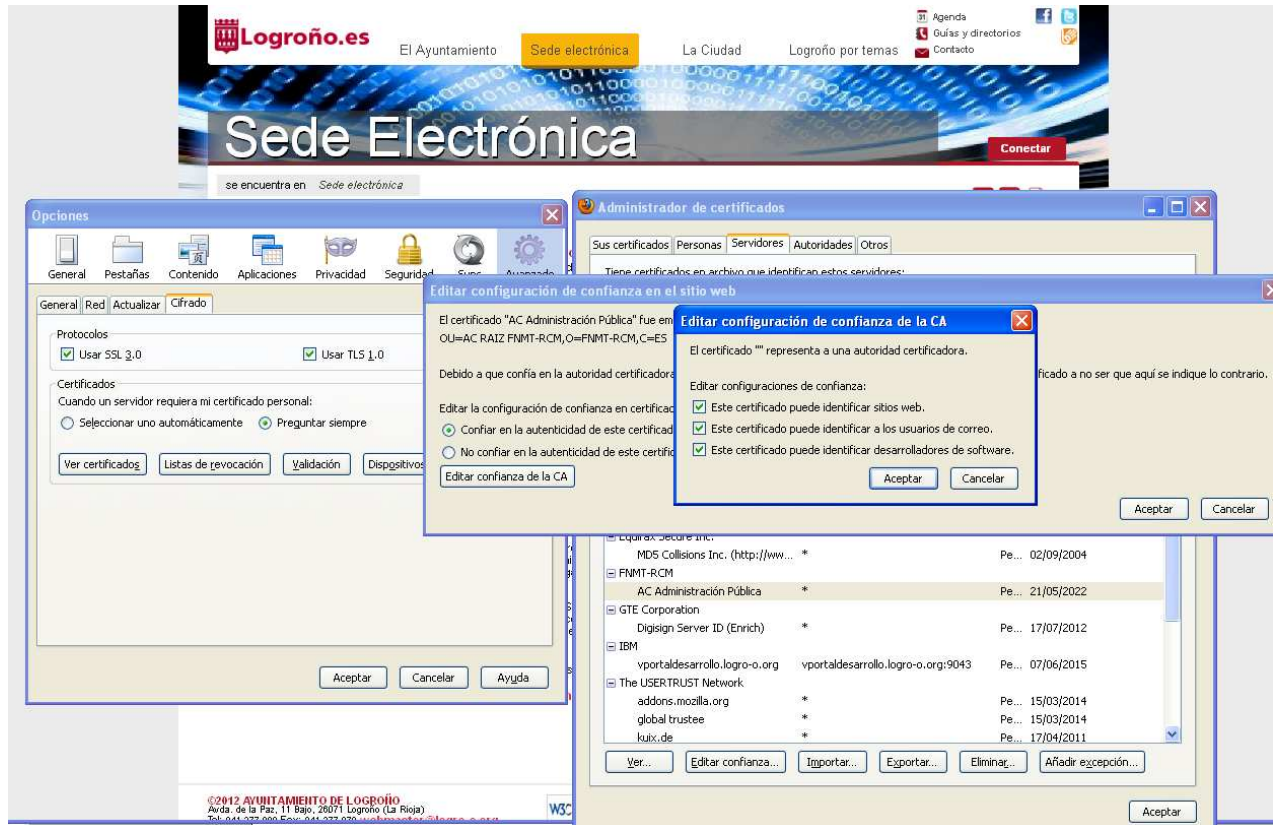
**Firefox:** Herramientas > Opciones > Ver Certificados > Autoridades > Importar.

**Chrome:** Configuración > Mostrar Opciones Avanzadas > Administrar certificados > importar



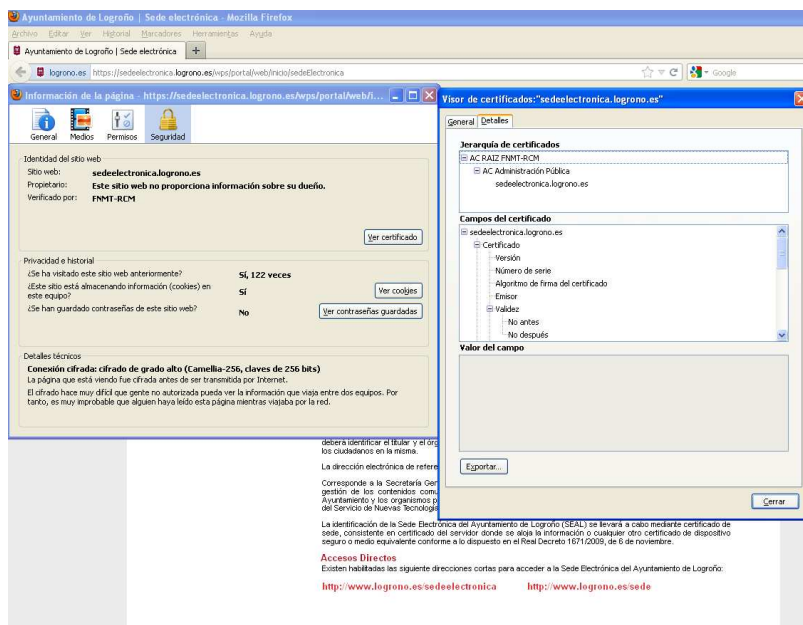
Explorer: Herramientas>Opciones de Internet>Contenido>Certificados>Importar

Una vez incorporado al sistema y desde la misma pantalla deberemos editar la confianza del mismo



Para ello seleccionaremos los certificados recién instalados, AC Raíz FNMT RCM y AC administración Pública, y pulsamos editar confianza, seleccionamos Confiar en la autenticidad de este certificado y pulsamos editar confianza de la CA y posteriormente seleccionamos todas las opciones siguientes.

## 1.5. Resultado



Tras incorporar a nuestro navegador los certificados de la AC de la FNMT, nuestro navegador reconocerá el certificado de la sedeelectronica.logrono.es, emitido por la FNMT como un certificado válido para el establecimiento de un canal seguro SSL.

En la captura podemos observar la cadena o jerarquía de certificación, donde sedeelectronica.logrono.es esta certificado por AC administración Pública y esta por la raíz de la FNMT.

## Acceso mediante certificado Digital

No es objeto de este documento explicar el registro y acceso mediante certificado digital personal, de ciudadano o persona jurídica a la Sede Electrónica, pero queremos aprovechar para hacer una introducción somera al mismo.

Con la instalación del certificado de AC, se consigue un protocolo seguro, SSL para las comunicaciones.

La SedeElectronica del ayuntamiento de Logroño cuenta con dos zonas:

- 1) **Zona Publica**, donde no se necesita identificación de usuario, estamos en una zona publica, pero segura y confiable, es la zona publica de la SedeElectronica del Ayuntamiento de Logroño. Esta zona es identificable por el color **gránate** y por que la url contendrá la palabra **portal**.
- 2) **Zona Privada**, donde cada ciudadano tras mostrar sus credenciales de usuario y tras su autenticación o comprobación de que puede hacer uso de ellas, contraseña de usuario o de uso de certificado, accede a contenidos propios o privados. Esta zona es identificable por el color **azul** y por que la url contendrá la palabra **myportal**.

La instalación de un certificado personal, es similar a la incorporación de cualquier otro certificado



The screenshot shows the website interface for the Ayuntamiento de Logroño. The browser address bar displays the URL: [https://sedelectronica.logrono.es/wps/portal/web/inicio/sedeElectronica/teAyudamos/buscadorTramites/tut/p/c5/04\\_SB8K8xLLM9M55aPy8xBe9CP0os3hD1wNI](https://sedelectronica.logrono.es/wps/portal/web/inicio/sedeElectronica/teAyudamos/buscadorTramites/tut/p/c5/04_SB8K8xLLM9M55aPy8xBe9CP0os3hD1wNI). The page features a navigation menu with options like 'El Ayuntamiento', 'Sede electrónica', 'La Ciudad', and 'Logroño por temas'. The main heading is 'Sede Electrónica' with a 'Conectar' button. A sidebar on the left lists categories such as 'Información General', 'Normativa Sede Electrónica', 'Seguridad y Privacidad', 'Te Ayudamos', and 'Servicios'. The 'Te Ayudamos' section is expanded to show 'Buscador de trámites'. The main content area, titled 'Buscador de Trámites', explains that users can search for services in either physical or electronic mode. It notes that information is structured homogeneously and can be searched by text, area, or theme. Below this, there is a search interface with tabs for 'Por texto', 'Por área', 'Por tema', and 'Presentación'. The 'Por texto' tab is selected, showing a text input field and a 'Buscar' button.



The screenshot shows a web browser window with the following elements:

- Browser Tab:** Ayuntamiento de Logroño | ¿Qué puedo hacer? - Ayuntamiento de Logroño
- Browser Menu:** Archivo, Editar, Ver, Historial, Marcadores, Herramientas, Ayuda
- Address Bar:** logrono.es https://sedeelectronica.logrono.es/wps/myportal/web/inicio/miSedeElectronica/quePuedoHacer
- Page Header:** Logroño.es, Con certificado, Última conexión: 11/02/2015 10:27:36, Fecha Hora oficial, Contacto
- Main Title:** Mi Sede Electrónica
- Navigation:** Desconectar
- Breadcrumbs:** se encuentra en Mi sede electrónica > ¿Qué puedo hacer?
- Left Menu:**
  - Mis gestiones
  - Mi calendario
  - Fecha y Hora Oficial
  - ¿Qué puedo hacer?
  - Información General
  - Datos Personales
- Search Section:**
  - Buscador de trámites**
  - Por texto | Por área | Por tema | Presentación
  - Texto libre
  - Input field
  - Buscar