Protocolo TLS/SSL
Práctica 8

1. Objetivo

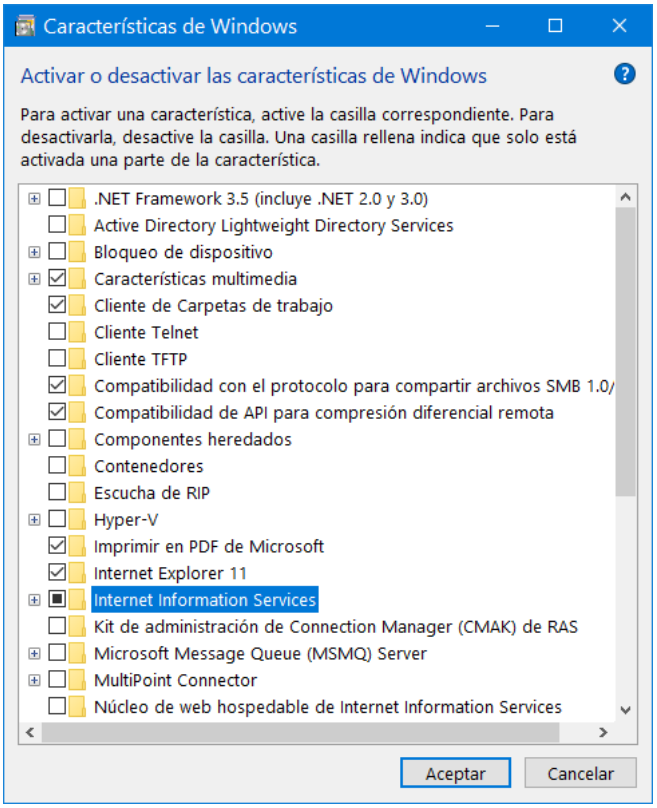
En esta práctica el alumno debe preparar un servidor web y un navegador web para que se puedan establecer comunicaciones seguras (cifradas) entre ellos usando el protocolo TLS/SSL. Habrá que crear o reutilizar los certificados necesarios que deberán ser instalados tanto en el servidor web como en los computadores en los que se ejecutan los navegadores web. Esta práctica hay que realizarla en la máquina virtual (MV) en la que el alumno tiene privilegios de administrador. El adaptador de red de la MV debe estar configurado en modo Bridge.

2. Preparación del servidor

Para utilizar un servidor web es muy cómodo activar el IIS 7.5 (Internet Information Server) que viene integrado en Windows 7.

Para activar el IIS hacer: Inicio > Panel de control > Programas y características

Seleccionar la opción que aparece en la esquina superior izquierda: "Activar o desactivar las características de Windows" y aparece esta ventana:

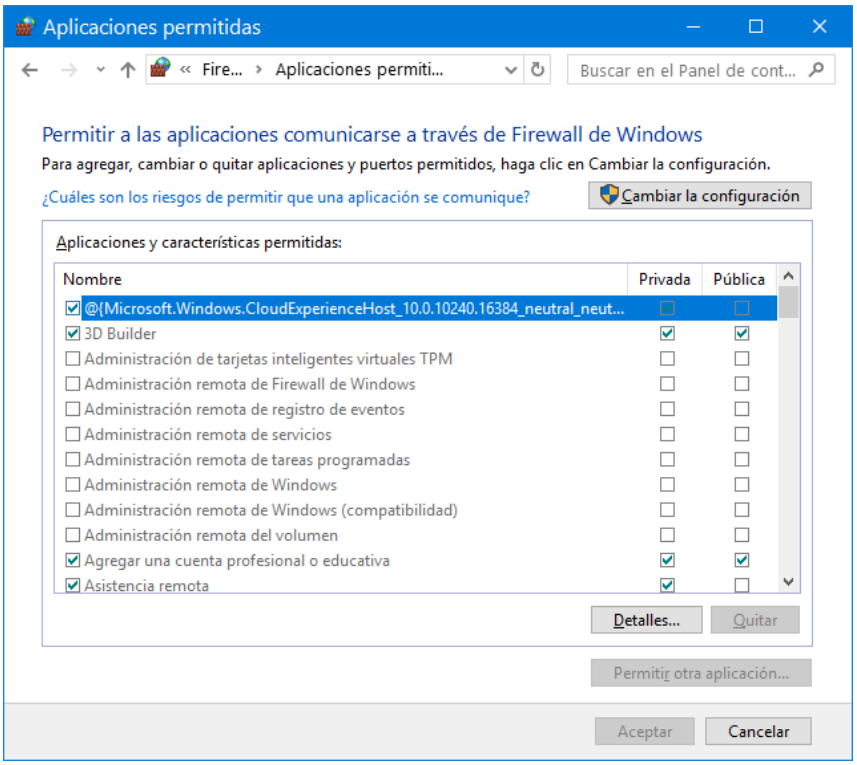


Seleccionar Internet Information Services con las opciones que vienen preseleccionadas por defecto.

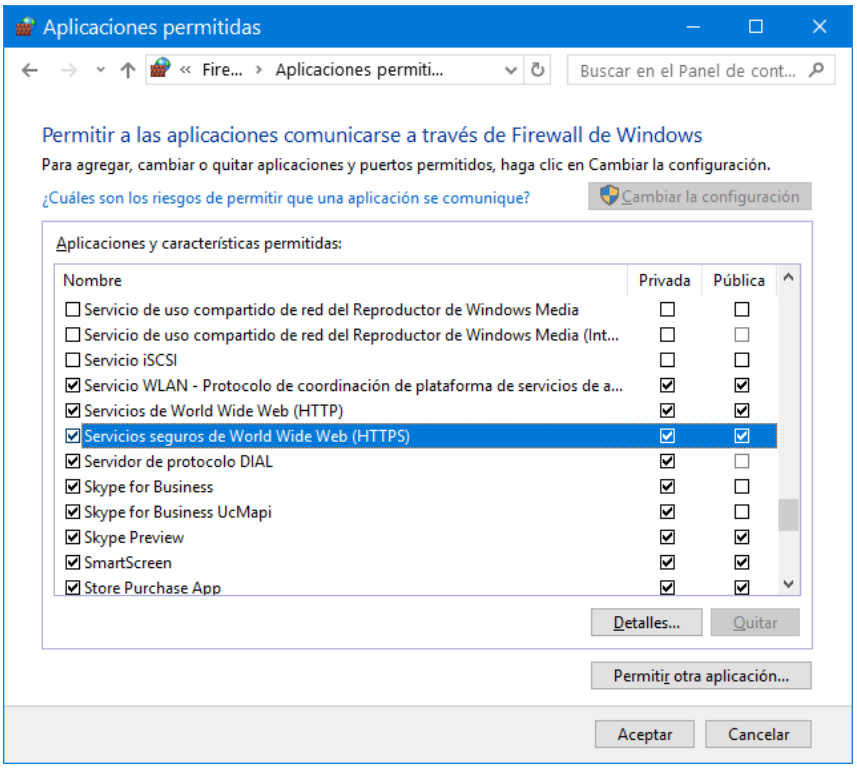
Para que el servidor sea accesible desde otros computadores es necesario abrir los protocolos y puertos adecuados en el **Firewall de Windows**. Esta operación es necesaria en Windows 7, pero Windows 10 la realiza automáticamente. Para realizar esta operación hacer:

Inicio > Panel de control > Firewall de Windows

Seleccionar la opción que aparece en la esquina superior izquierda: "Permitir un programa o una característica a través de Firewall de Windows" y aparece esta ventana:



Hay que pulsar el botón "Cambiar la configuración" y seleccionar las opciones: Servicios de World Wide Web (HTTP) y Servicios seguros de World Wide Web (HTTPS) tal como se muestra debajo:



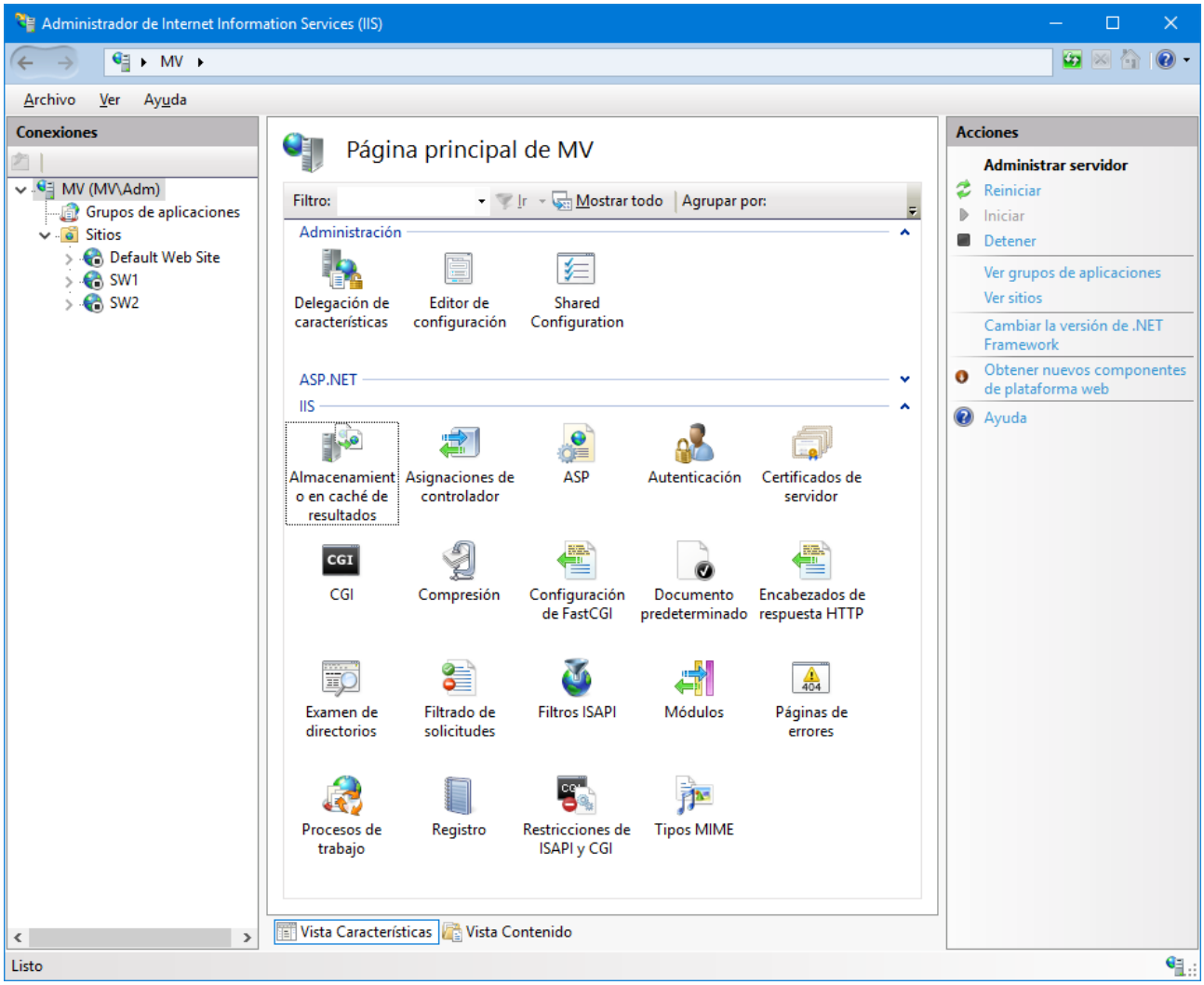
Para arrancar la herramienta de administración del IIS hacer:

Inicio > Panel de control > Herramientas administrativas > **Administrador de IIS**

También se puede teclear en Cortana **inetmgr**

O pulsa las teclas Windows+R para que aparezca la ventana Ejecutar e inserta **inetmgr**

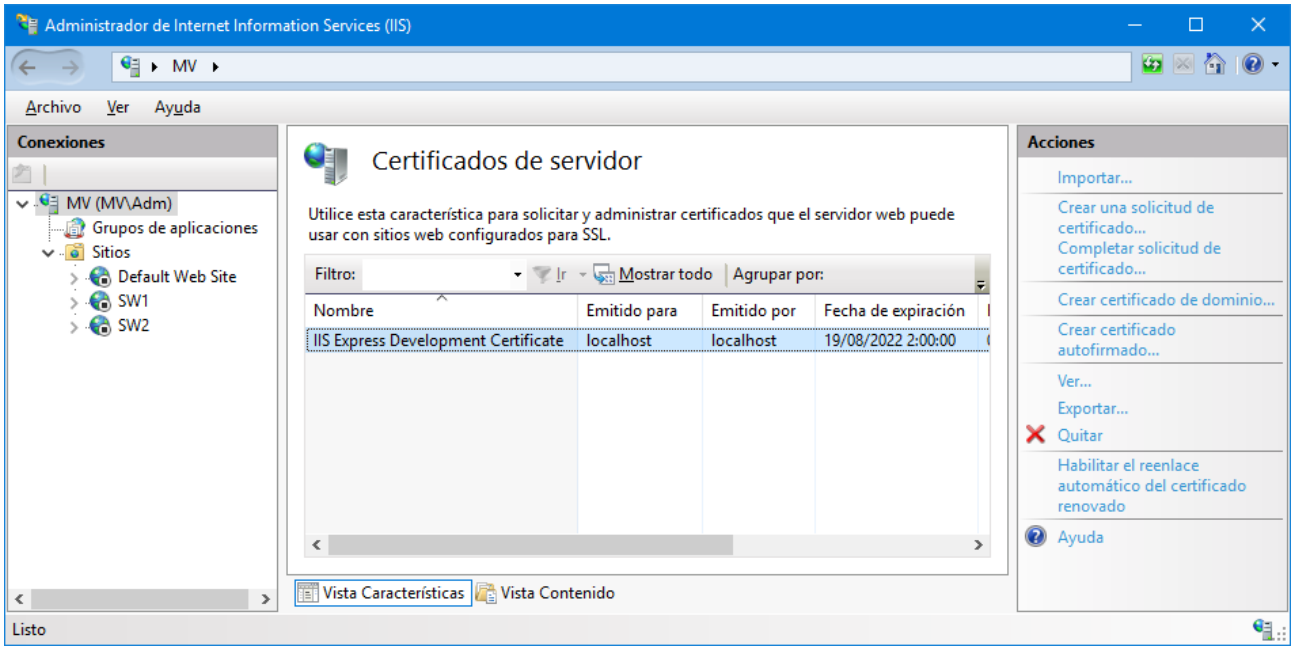
Aparece la siguiente consola de administración:



En la que se ha desplegado el árbol de conexiones en el panel izquierdo. En este panel se puede observar que hay un servidor IIS en el computador MV (nombre del equipo que se puede asignar en: Panel de control > Sistema) que aloja aplicaciones y sitios web. Un servidor IIS puede alojar varios sitios web. Por defecto aloja el sitio "Default Web Site".

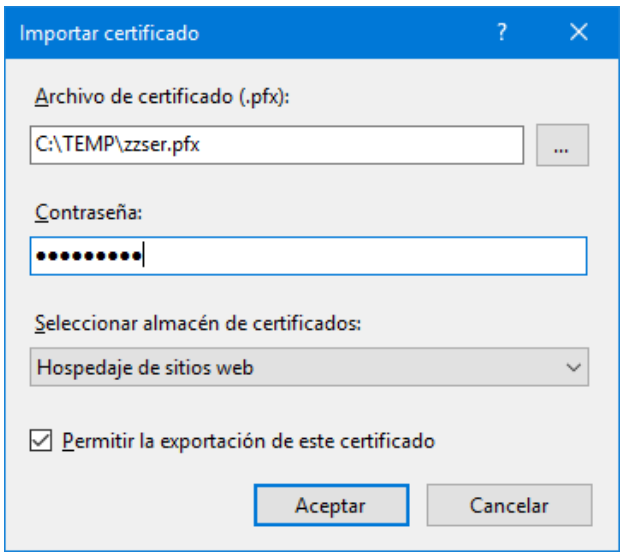
CARGAR UN CERTIFICADO PARA EL SERVIDOR

Antes de crear un sitio web seguro es necesario cargar un certificado en el servidor. Para ello seleccionar la opción "Certificados de servidor" que se puede ver en la figura previa.



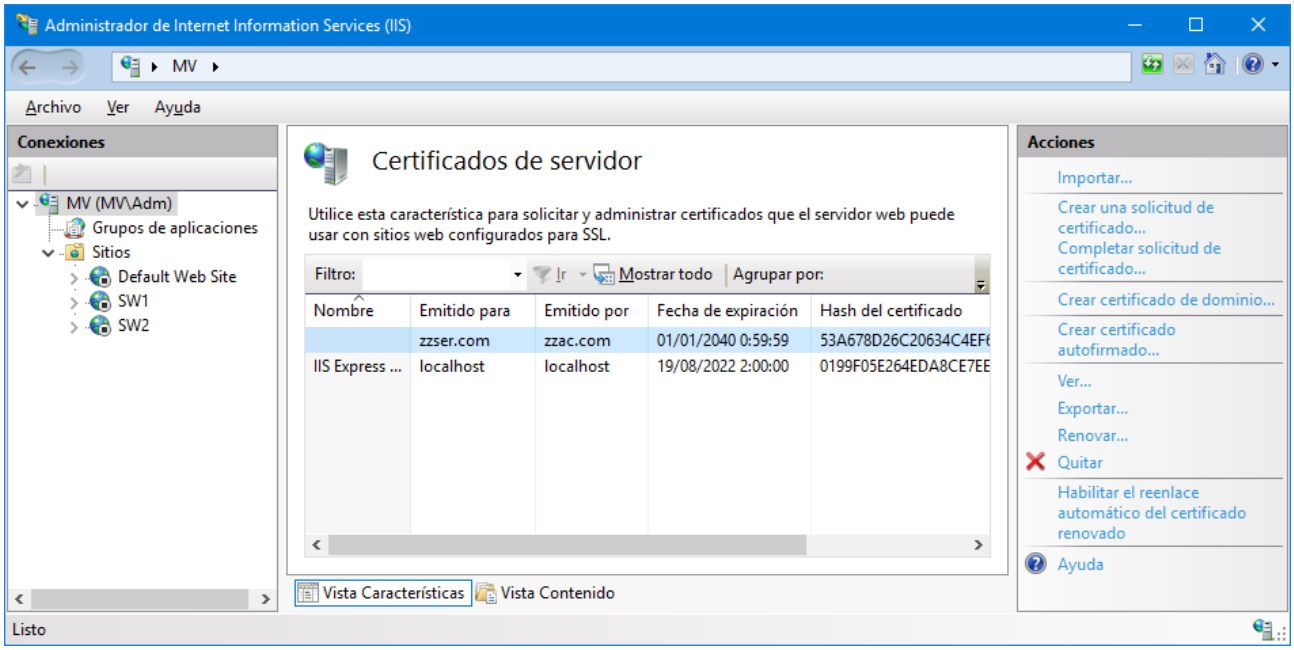
Se puede comprobar que el servidor tiene cargado un certificado para localhost.

En el panel derecho de Acciones seleccionar "Importar...". En la ventana de selección de archivos que aparece seleccionar el certificado de servidor creado previamente: zzser.pfx y proporcionar la contraseña que permite la utilización del certificado, por ejemplo conserpfx.



En Windows 7 solo se permite el almacén de certificados “Personal”. En Windows 10 se puede usar también el almacén “Hospedaje de sitios web”. Usar el almacén de Hospedaje.

Tras la importación la ventana aparece así:



Si se hace doble clic sobre el certificado se pueden ver sus propiedades. Observar que el certificado está emitido para zzser.com, que se supone que es el nombre DNS del sitio web que va a utilizar el certificado. Un formato de nombre más habitual sería www.businessname.com. Comprueba también que este certificado NO tiene una ruta de certificación válida.

Comprueba que este certificado de zzser.com está en el almacén "Hospedaje de sitios web" del "equipo local". Tendrás que usar la herramienta **certlm.msc** para gestionar los certificados del equipo local. Usando esta herramienta, carga el certificado de la autoridad certificadora, zzac.com, en el almacén "Entidades de certificación raíz de confianza" del "equipo local". Para hacer la importación debes usar en la barra de menús:

Acción > Todas las tareas > Importar ...

Puedes borrar el certificado de zzser.com en la ventana del Administrador del IIS y comprobar que desparece en la consola de administración de certificados, y luego viceversa, importarlo en la consola de administración de certificados y comprobar que aparece en la ventana del Administrador del IIS.

NOTA: Puede que los nombres de los certificados que tengas disponibles sean diferentes...

- **zzSERnombrealumno en vez de zzser.com**
- **zzACnombrealumno en vez de zzac.com**

Usa los que tengas disponibles.

CREACIÓN DE UN SERVIDOR WEB SEGURO

Antes de crear el servidor, hay que preparar un directorio para almacenar los ficheros que utilice el nuevo servidor.

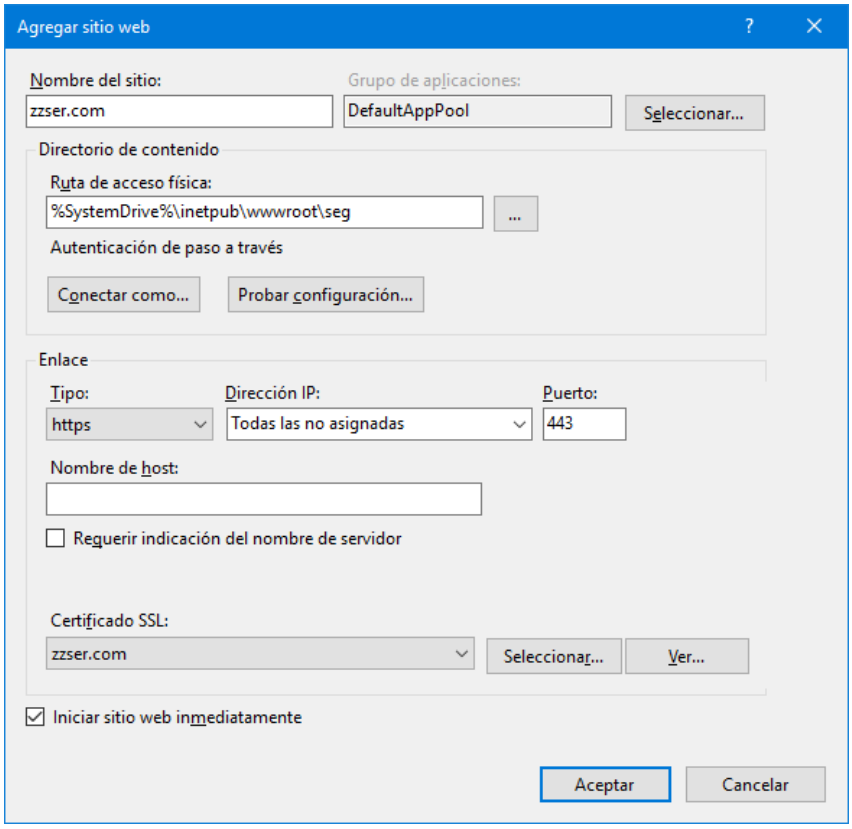
La utilización de cualquier directorio, como por ejemplo C:\Temp\ puede dar problemas de acceso con usuarios no autenticados, esto es, usuarios que acceden a la página principal del servidor seguro sin tener que autenticarse proporcionando un nombre de usuario y una contraseña.

Una buena opción es crear y usar un subdirectorio en el directorio por defecto que utiliza el sitio "Default Web Site" de IIS. Este directorio por defecto es %SystemDrive%\inetpub\wwwroot, donde la variable de entorno SystemDrive suele ser C:

Crear el directorio %SystemDrive%\inetpub\wwwroot\seg para el nuevo servidor seguro.

Para crear un nuevo sitio web seguro (que utiliza TLS/SSL en sus comunicaciones) hacer clic sobre el nombre del servidor MV en el panel izquierdo y desplegar el árbol de Conexiones.

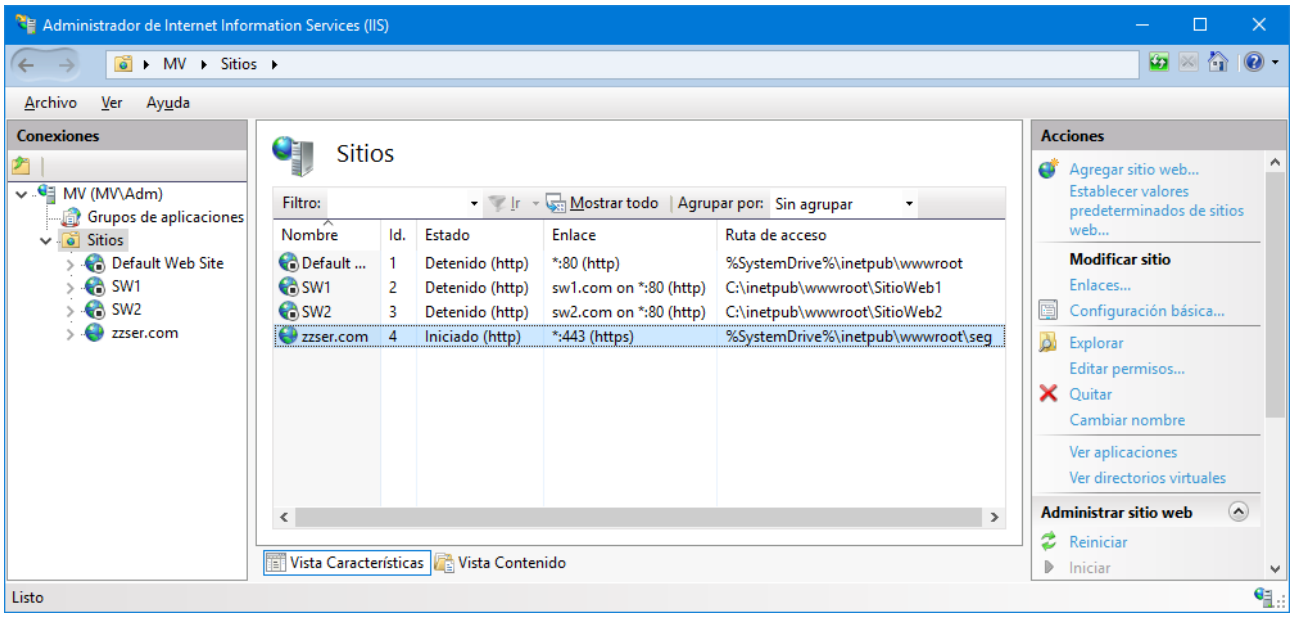
Seleccionar Sitios, hacer clic en el botón derecho del ratón y en el menú contextual seleccionar "Agregar sitio web...". En el cuadro de dialogo que aparece seleccionar las opciones que se indican a continuación:



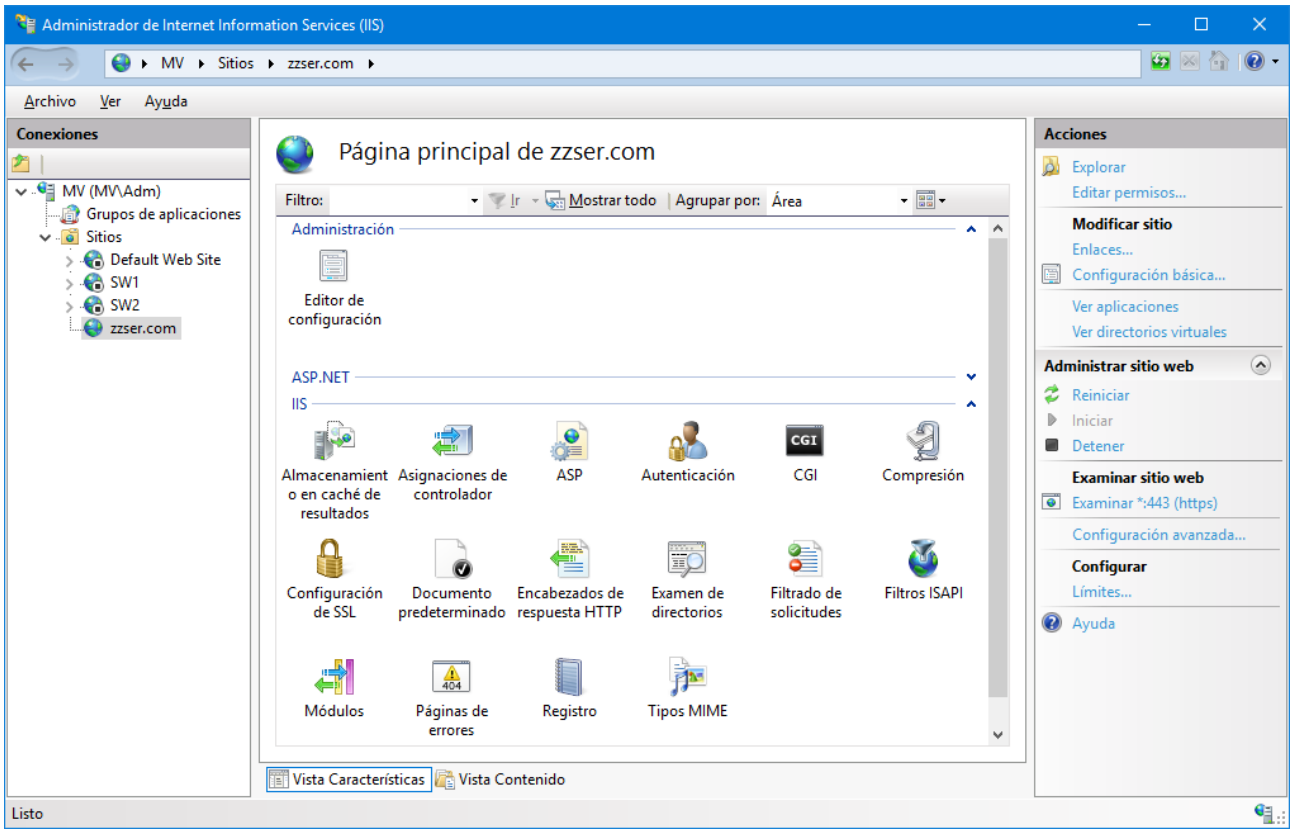
Observar cómo se elige el nombre del sitio zzser.com para que coincida con uno de los mostrados en el menú de opciones Certificado SSL. Observar que en el cuadro de diálogo previo en Certificado SSL se muestran los certificados disponibles en el almacén de certificados del IIS mostrándolos por el campo "Emitido para".

NOTA: Si el nombre del sujeto del certificado disponible es zzSERnombrealumno, el nombre del sitio debe ser también zzSERnombrealumno.

Finalmente se crea el sitio web zzser.com basado en TLS/SSL y aparece así en la página principal del Administrador de IIS.

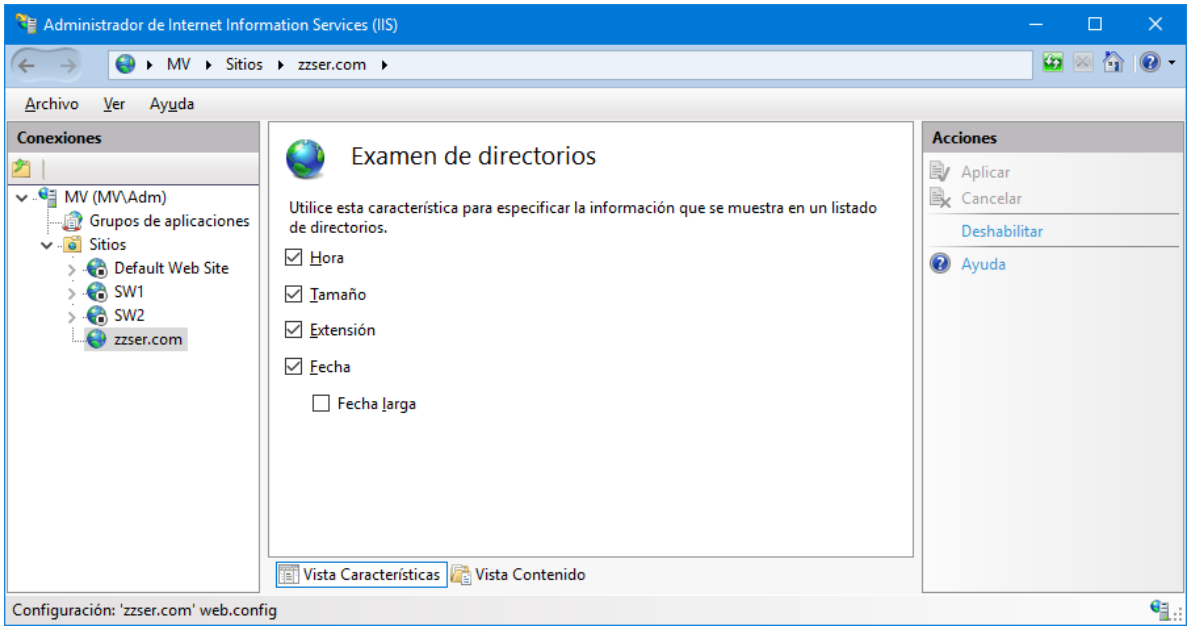


La configuración del sitio web puede incluir muchísimos aspectos y constituirían materia suficiente para una o más prácticas. A continuación se explican solo los aspectos más importantes para los objetivos de esta práctica. Si seleccionamos zzser.com en el panel izquierdo de Conexiones aparece la página principal de administración del sitio web zzser.com:



En el panel central seleccionar la opción "Examen de directorios". Normalmente esta característica aparecerá como deshabilitada para que el sitio muestre solo los documentos específicamente autorizados para mostrar. Pero para realizar esta práctica es mucho más cómodo que el sitio web permita mostrar el contenido de sus directorios.

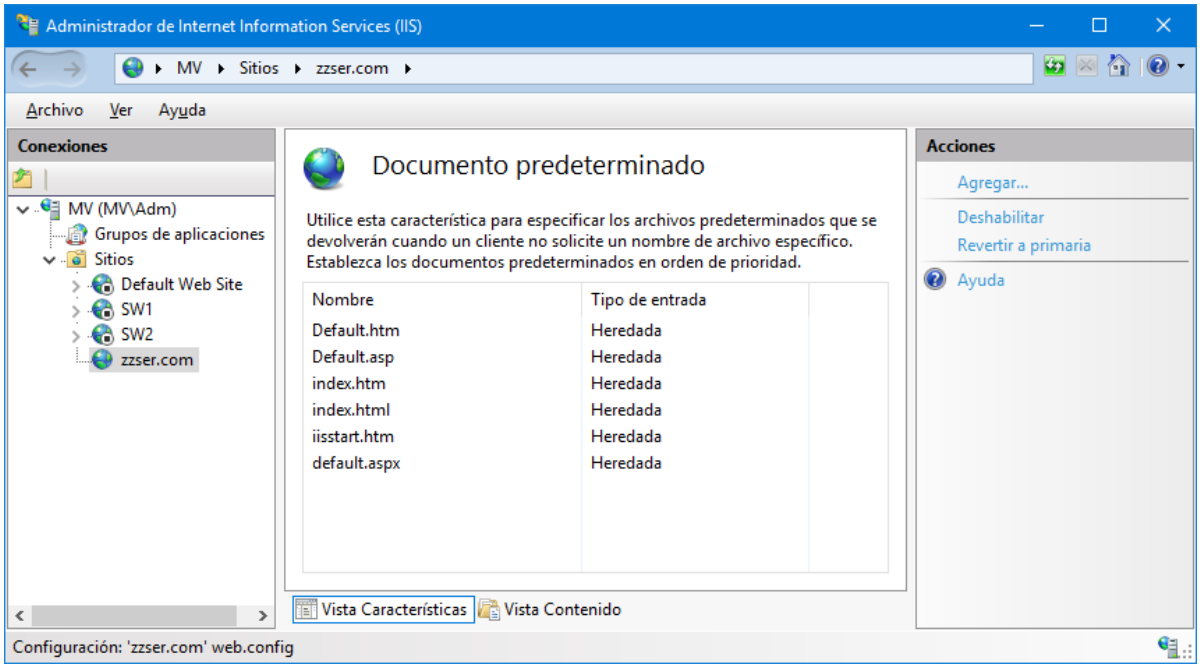
En el panel derecho hacer clic en la opción "Habilitar" y luego en el panel central seleccionar todas las opciones para que muestre la máxima información posible y finalmente en el panel derecho hacer clic en "Aplicar".



En el directorio C:\inetpub\wwwroot\seg\ se crea el archivo web.config que almacena las opciones de configuración del sitio web en formato XML.

Para probar el servidor hay que utilizar una página .html. Se puede dar cualquier nombre a la página, pero entonces el usuario del sitio tiene que conocer el nombre de página y usarlo en el URL. Es mejor dar a la página uno de los nombres que el sitio muestra por defecto cuando no se especifica el nombre del archivo que contiene la página en el URL. De esta forma cualquier usuario del sitio solo debe conocer el nombre del sitio.

En el Administrador de IIS > Página principal de zzser.com, seleccionar en el panel central la opción "Documento predeterminado" y aparece la siguiente ventana:



Como se puede comprobar el servidor mostrará primeramente una página denominada "Default.htm" si existe en el directorio C:\inetpub\wwwroot\seg\. En caso de que no exista, el servidor busca las siguientes que aparecen en la ventana previa.

Se recomienda editar el siguiente texto HTML con cualquier editor de textos, guardarlo en un archivo denominado Index.html y copiar el archivo en el directorio C:\inetpub\wwwroot\seg\.

Visual Studio es un editor de textos ideal para HTML, ya que el intellisense ayuda a completar los campos automáticamente y colorea las etiquetas y cadenas haciendo más legible el documento.

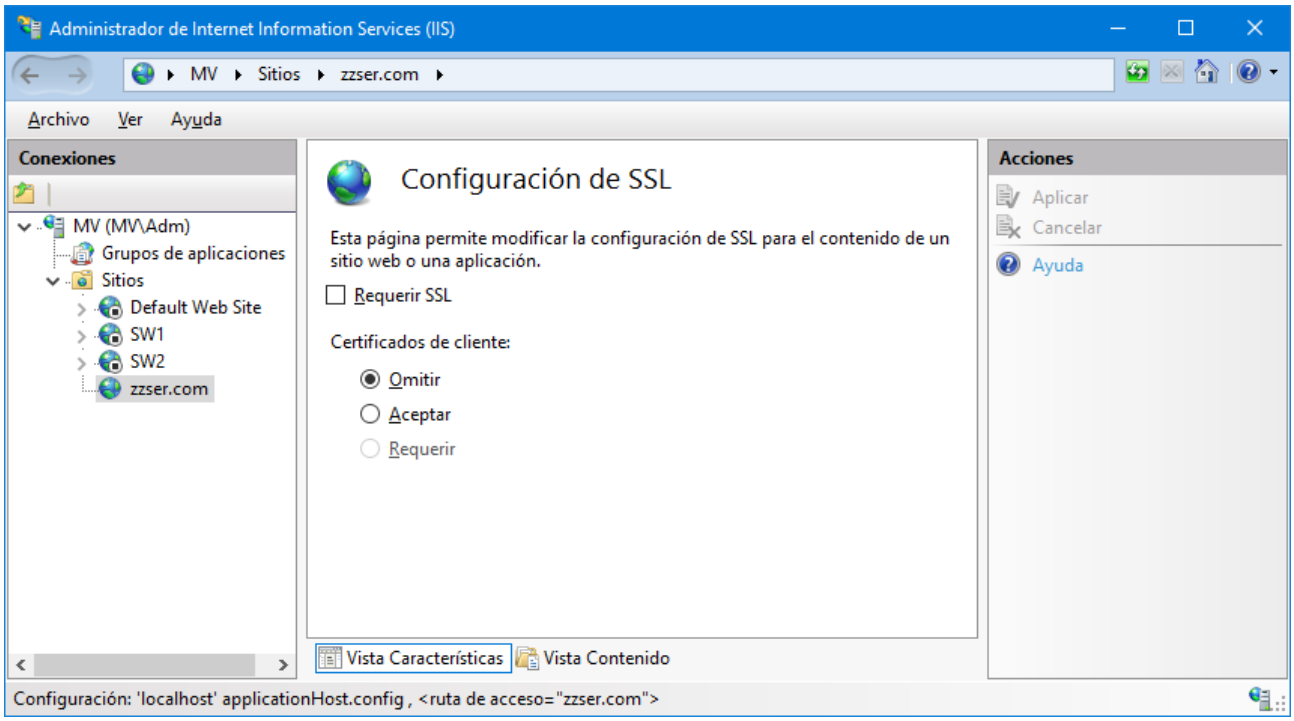
Para acelerar el desarrollo de la práctica, el fichero "Default.htm" con el código HTML se puede descargar del Campus Virtual.

```
<!DOCTYPE html>

<html lang="en" xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="utf-8" />
    <title>PAGINA DE PRUEBA TLS/SSL</title>
</head>
<body>
    <FONT FACE="Arial, Impact">
        <FONT SIZE=5>
            <FONT COLOR="#FF0000">
                <B> Estas viendo la página de prueba de TLS/SSL </B>
            </FONT>
        </FONT>
    </FONT>
    <P>
        <FONT FACE="Impact, Arial">
            <FONT SIZE=5>
                <FONT COLOR="#0000FF">
                    <I> ¡Enhorabuena! </I>
                </FONT>
            </FONT>
        </FONT>
</body>
</html>
```

El uso de esta página de inicio concreta permite comprobar claramente si estamos accediendo al servidor seguro configurado o no.

Finalmente en el panel central de la página principal de zzser.com seleccionar la opción "Configuración de SSL".



Seleccionar "Requerir SSL" para habilitar un mecanismo de cifrado de datos con clave de 40 bits para proteger las comunicaciones entre el servidor y los clientes.

En la tecnología TLS/SSL, el servidor determina si necesita autenticar al cliente o no. El cliente no puede decidir libremente si se autentica o no. El comportamiento del servidor se determina seleccionando una de las tres opciones de "Certificados de cliente":

- Omitir: El servidor NO acepta certificados de cliente (opción predeterminada). Los clientes no tienen que probar su identidad al servidor antes de acceder a los contenidos.
- Aceptar: El servidor acepta certificados de cliente (si se proporcionan) y comprueba la identidad del cliente antes de permitirle el acceso a los contenidos.
- Requerir: El servidor requiere certificados de cliente para comprobar la identidad del cliente antes de permitirle el acceso a los contenidos.

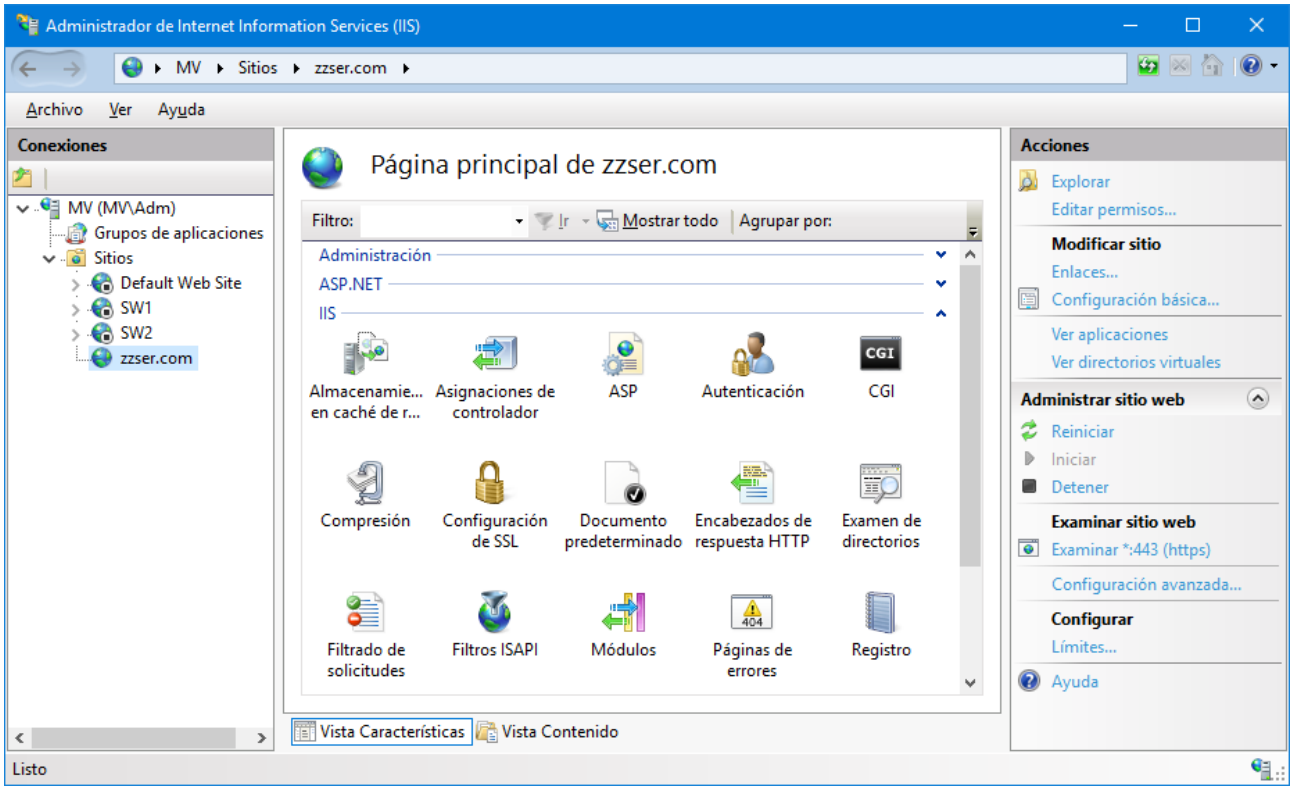
Inicialmente utiliza la opción predeterminada de Omitir. Posteriormente podrás experimentar con las otras opciones.

Para terminar, en el panel derecho de acciones hay que pulsar Aplicar o Cancelar para guardar o descartar los cambios realizados en la página de configuración.

PROBAR SI FUNCIONA EL SERVIDOR

Hay varias formas probar el funcionamiento del servidor.

Observa el panel derecho de **Acciones** de la página principal del sitio web zzser.com:



En la sección Examinar sitio web, hay la opción “Examinar *:443 (https)”. Al pulsarla se solicita el acceso a la página https://localhost/ por el navegador predeterminado. Si el navegador predeterminado es Microsoft EDGE, indicará que hay problemas, pero no importa, continúa el acceso.

Realiza la misma prueba desde el mismo computador usando dos navegadores: Microsoft EDGE y Google Chrome. Abre los navegadores y después accede a la página https://localhost/.

Finalmente haz que tu compañero de prácticas acceda a tu servidor desde su máquina física o virtual con los dos navegadores indicados, accediendo a la página https://A.B.C.D/, donde A.B.C.D es la IPv4 del computador en el que se está ejecutando el servidor web seguro.

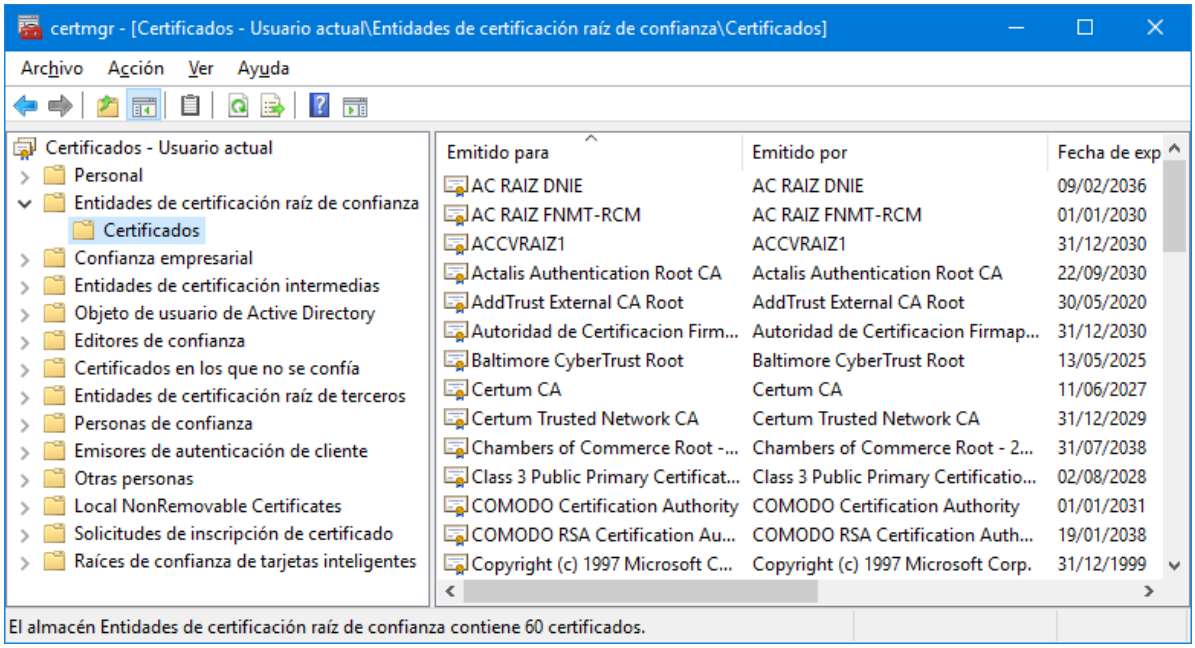
Aunque los navegadores indiquen que hay problemas, continuar el acceso hasta visualizar la página de bienvenida. Es lógico que haya problemas, pues aún no se han configurado los navegadores. Después de configurarlos, se harán pruebas de funcionamiento más detalladas.

PARAR LOS SERVIDORES WEB

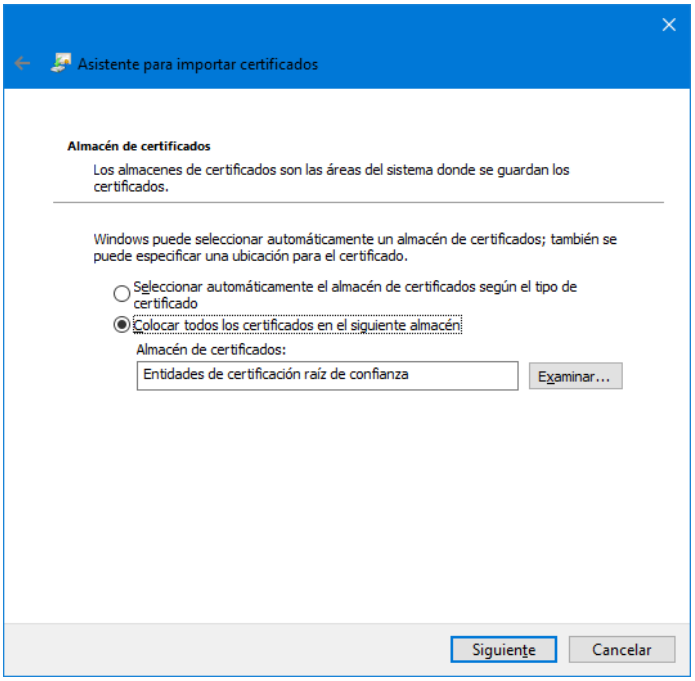
Observa que tras la instalación realizada hay dos servidores IIS en funcionamiento. Aunque no consumen muchos recursos, conviene detenerlos cuando no se vayan a utilizar e iniciarlos para realizar las pruebas. Las opciones Reiniciar/Iniciar/Detener están en el panel derecho de Acciones.

3. Preparación del navegador

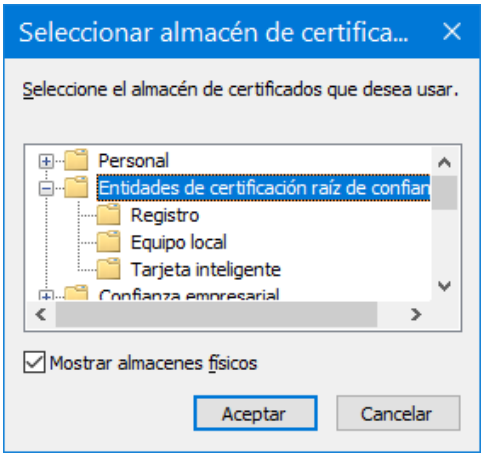
Para que el navegador pueda conectarse con éxito al sitio web debe tener instalado el certificado de la autoridad certificadora raíz de confianza que también ha emitido (firmado) el certificado del sitio web. Abrir la consola de administración de certificados tecleando en Inicio > Buscar programas y archivos el texto siguiente: **certmgr.msc**. En el panel izquierdo ir a "Entidades de certificación raíz de confianza > Certificados". Observar en la barra de estado, el número de certificados que contiene este almacén.



Usar el menú Acción > Todas las tareas > Importar o clic derecho sobre Certificados > Todas las tareas > Importar, para abrir el "Asistente de importación de certificados". Cuando se abre la ventana examinar hay que elegir a la derecha-abajo el tipo de certificado (.cer, .pfx, ...). Utilizar el certificado zzAC.cer. Después elegir el almacén de certificados en el que se desea importar el certificado.

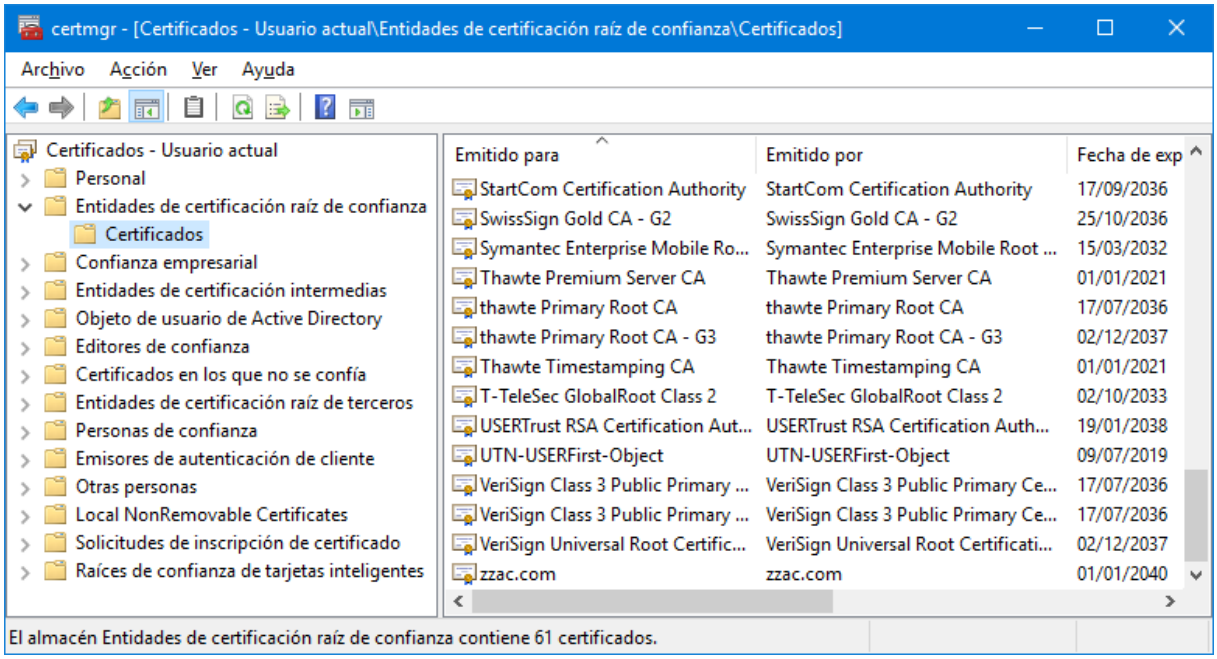


Si se desea tener un control mayor del almacén en el que se importa el certificado conviene pulsar el botón Examinar... y se despliega el cuadro de dialogo "Seleccionar almacén de certificados" en que se puede marcar la opción "Mostrar almacenes físicos".



Por ejemplo, elegir Equipo local.

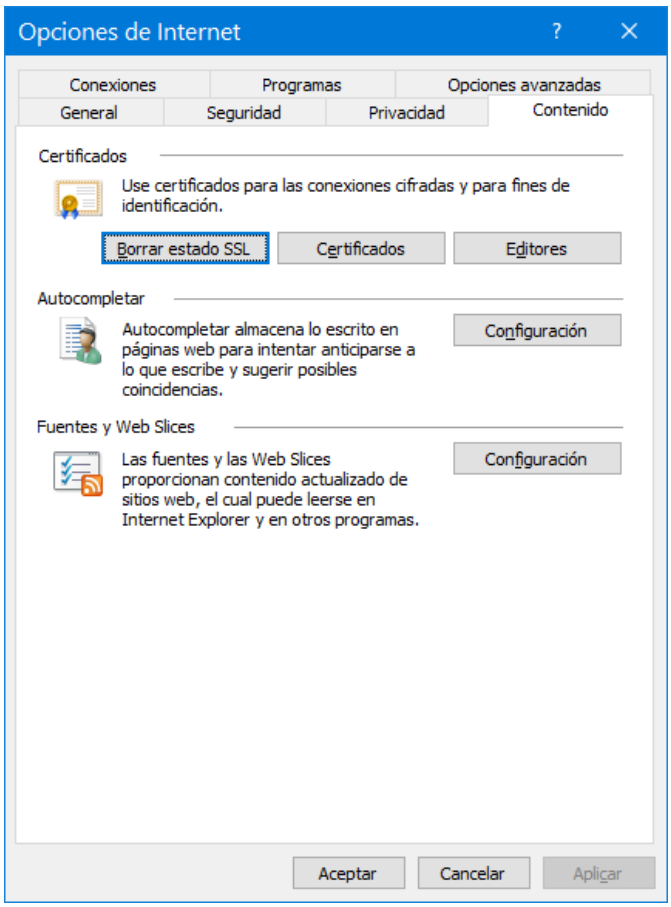
Para que la consola de administración de certificados muestre el nuevo certificado es preciso pulsar el botón Actualizar (sexto empezando por la izquierda, es una flecha circular verde).



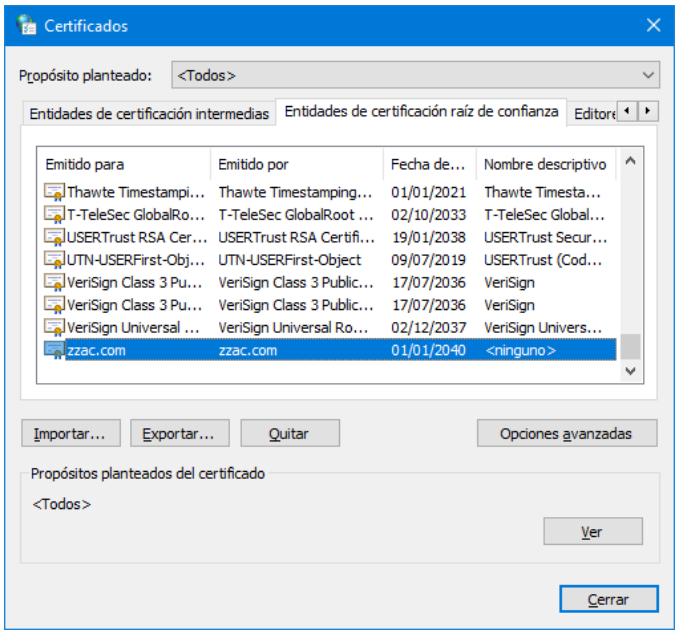
Observar que ahora aparece al final de la lista el certificado zzac.com y que en la barra de estado se contabiliza un certificado más que antes en el almacén.

Para comprobar que el navegador dispone del nuevo certificado, en el caso del Internet Explorer, una vez arrancado ir al menú Herramientas > Opciones de Internet. En el cuadro de dialogo "Opciones de Internet" seleccionar la ficha "Contenido". Observar que en la ficha hay una sección dedicada a Certificados.

Con Microsoft Edge, seleccionar la opción ··· que aparece en la esquina superior derecha y el menú que se despliega elegir “Abrir con Internet Explorer”.



Pulsar el botón Certificados. Aparece el cuadro de diálogo "Certificados". Seleccionar la ficha "Entidades de certificación raíz de confianza" y comprobar que está el certificado zzac.com.



Desde este cuadro de diálogo podemos Importar, Exportar y Ver los certificados, así como modificar sus propósitos, pulsando el botón "Opciones avanzadas".

NOTA: La ventana “Opciones de Internet” también está disponible en el “Panel de control”.

ACTUALIZACIÓN DE LOS NAVEGADORES

Conviene tener los navegadores actualizados entes de realizar las pruebas.

Los navegadores de Microsoft, EDGE e Internet Explorer, se actualizan mediante las actualizaciones de Windows. Para comprobar la versiones hacer:

En **EDGE** pulsar el botón "Configuración y más" (Alt+X), representado por ···, en la esquina superior derecha de la ventana de navegación. En el panel que aparece seleccionar la última opción "Configuración". En el nuevo panel que aparece sustituyendo al anterior, observar en la parte inferior la sección "Acerca de esta aplicación". En Noviembre-2019 la versión disponible deber ser la 44.18362.387.0.

En **Internet Explorer 11** pulsar el botón "Herramientas" (Alt+X), representado por una rueda dentada, en la esquina superior derecha de la ventana de navegación. En el menú vertical que aparece seleccionar la última opción "Acerca de Internet Explorer". En Noviembre-2019 aparece la ventana siguiente:

Seleccionando el enlace (KB4519974) para ver la información de la última actualización: "Cumulative security update for Internet Explorer: October 8, 2019"

En **Chrome** pulsar el botón "Personaliza y controla Google Chrome", representado por tres puntos verticales, en la esquina superior derecha de la ventana de navegación. En el menú vertical que aparece selecciona "Ayuda > Información de Google Chrome". El navegador abre una nueva pestaña en la que muestra la versión actual y la actualiza automáticamente. En Noviembre-2019 la versión disponible debe ser la 78.0.3904.97.

En **Firefox** pulsar el botón "Abrir menú", representado por tres guiones horizontales, en la esquina superior derecha de la ventana de navegación. En el menú vertical que aparece selecciona la penúltima opción "Ayuda" y en el nuevo panes que aparece seleccionar "Acerca de Firefox". Entonces se muestra la ventana siguiente:

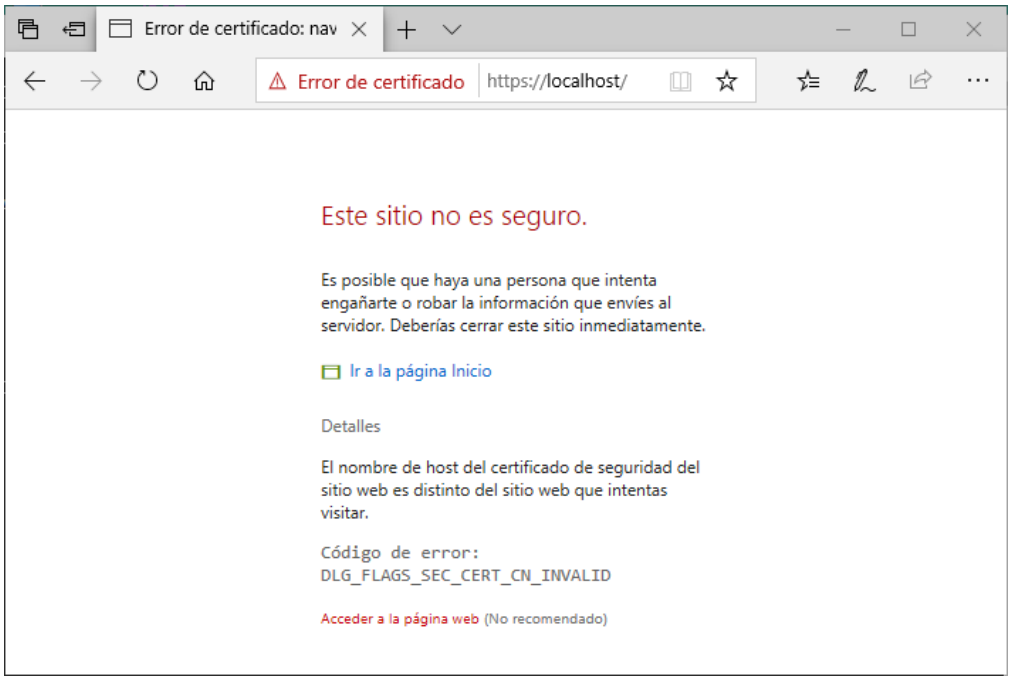
Si Firefox no está actualizado, en la ventana se muestra la actualización automática. En Noviembre-2019 la versión disponible debe ser la 70.0.1.

4. Pruebas de funcionamiento

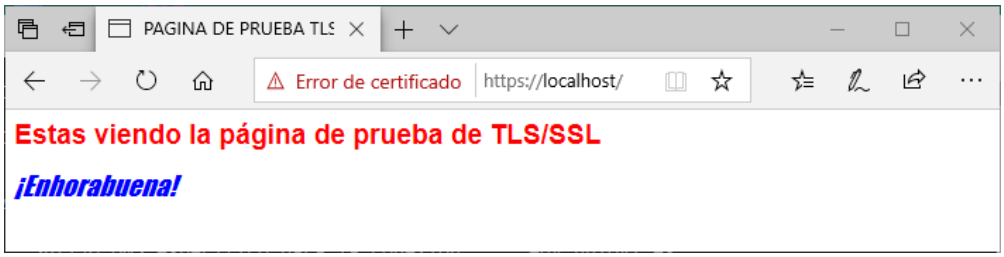
En el computador que funciona como servidor se puede abrir un navegador para usarlo también como cliente local. Utiliza el navegador EDGE.

Al usar la URL http://localhost/ se muestra la página de bienvenida de IIS.

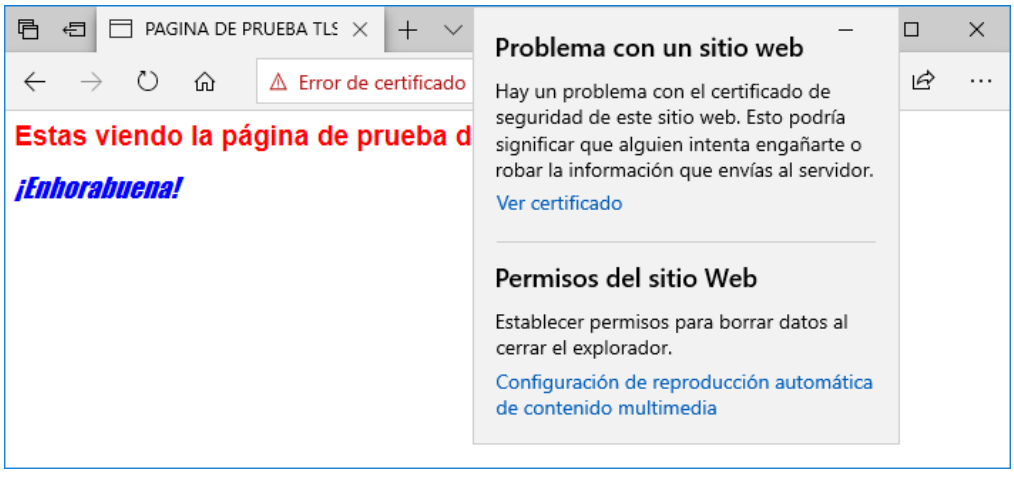
Al usar la URL https://localhost/ aparece la siguiente ventana, en la que ha seleccionado la opción "Detalles" para que aparezca la información detallada:



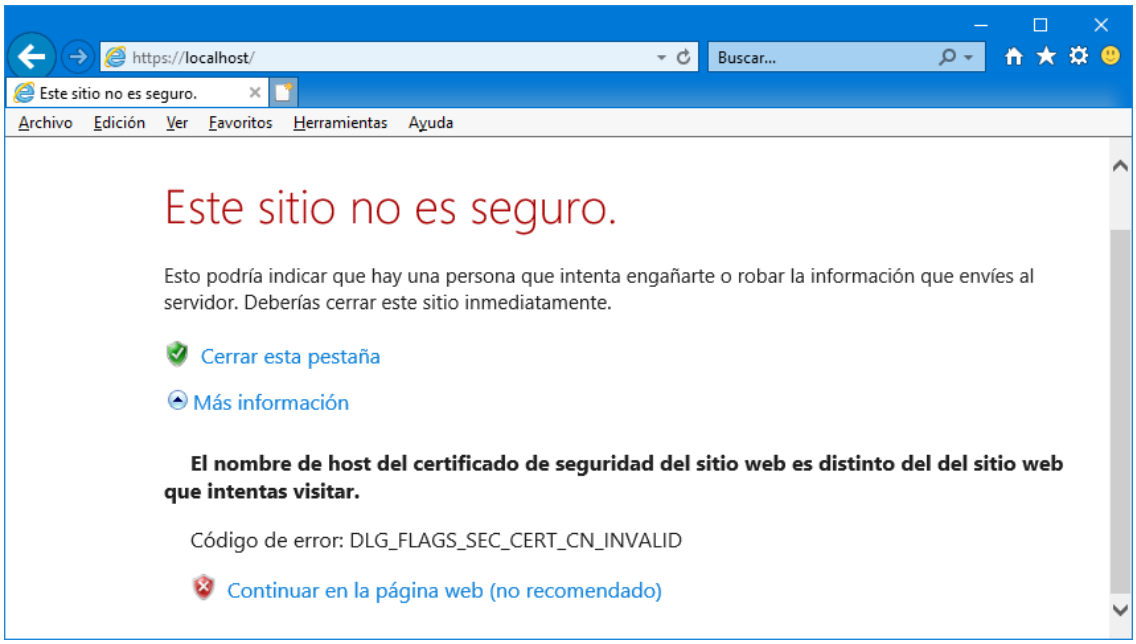
Seleccionado la opcion "Acceder a la página web (Not recommended) se obtiene:



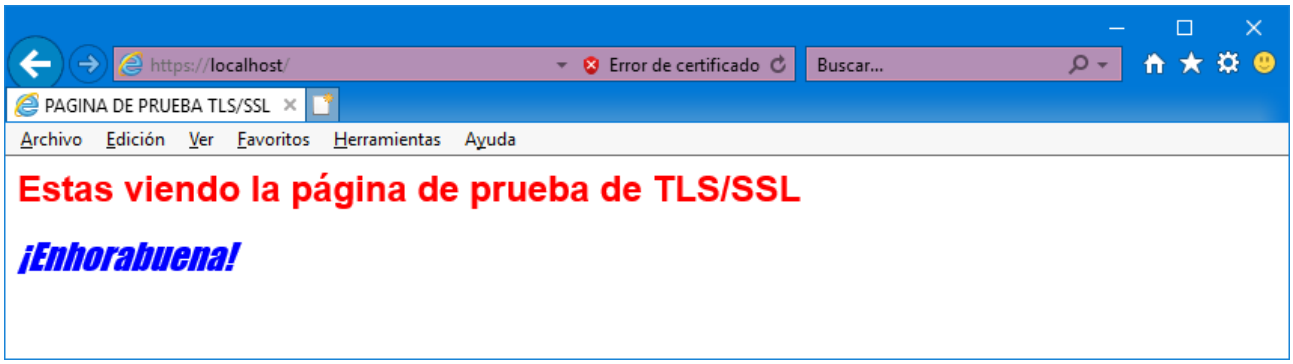
Se visualiza la página web de bienvenida del sitio seguro pero aparece un triángulo rojo indicando que hay un error. Al hacer clic sobre el triángulo se abre una ventana explicativa:



Ahora abre el navegador Internet Explorer y accede nuevamente a la página https://localhost/. Aparece la ventana siguiente:

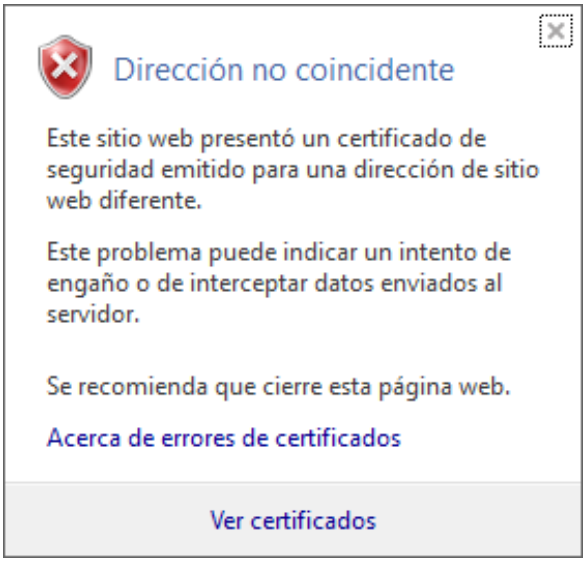


Seleccionando la opción "Continuar en la página web (no recomendado)" se obtiene:



Se visualiza la página web de bienvenida del sitio seguro pero el fondo de la URL está en rojo (rosa) indicando que la conexión establecida no es segura (no se está cifrando la información).

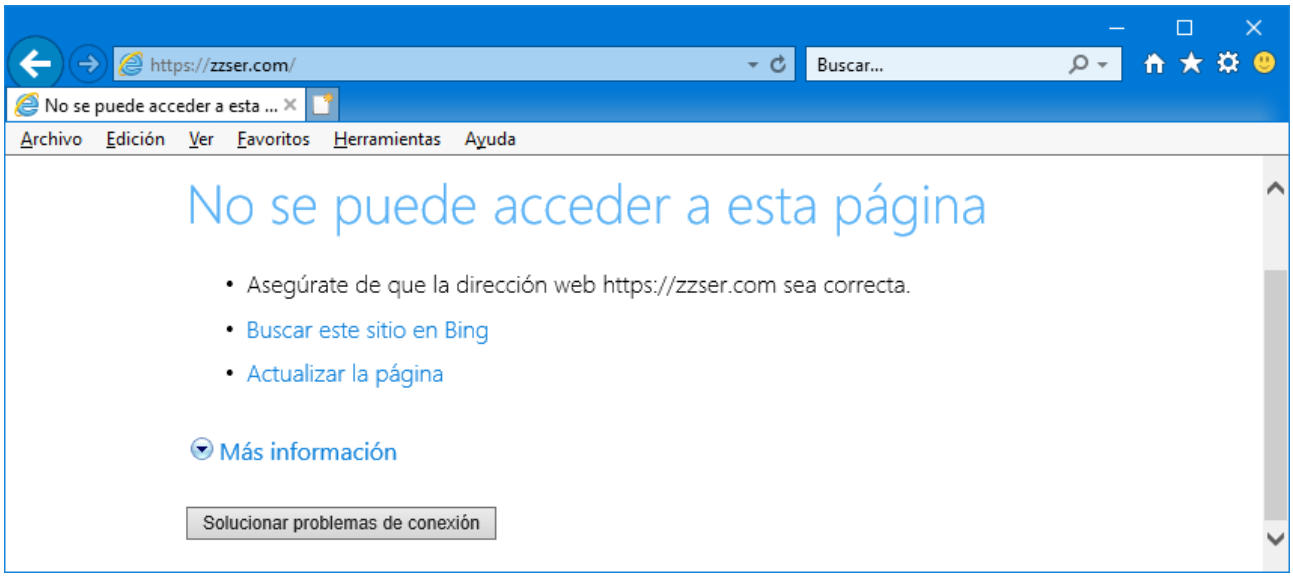
Al pinchar en "Error de certificado" se despliega una ventana en la que se explica la causa del error.



¿Qué quiere decir que el certificado se ha emitido para una dirección de sitio web diferente?

El certificado ha sido emitido para un sitio web denominado "zzser.com", pero se está accediendo al servidor con el nombre localhost.

Al utilizar el nombre del sitio web seguro en el navegador obtenemos:



Esto se debe a que el DNS no es capaz de resolver el URL "https://zzser.com". Un método sencillo para resolver el nombre es incluirlo en los nombres que se resuelven localmente. Para ello hay que editar el archivo:

C:\Windows\system32\drivers\etc\hosts

Y añadir la línea siguiente:

A.B.C.D zzser.com

Donde A.B.C.D es la dirección IPv4 del computador en el que se ejecuta el servidor web.

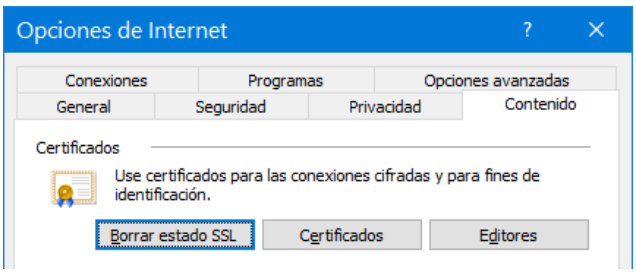
Para modificar el archivo hosts hay que ejecutar el editor como Administrador.

En Windows 7 teclear cmd en Inicio y en Windos 10 teclear cmd en Cortana. Cuando aparece …

Poner el puntero del ratón sobre "Símbolo del sistema" y hacer clic en el botón derecho. En el menú que aparece seleccionar "Ejecutar como administrador". Para editar el archivo hosts, simplemente teclear en la consola notepad hosts.

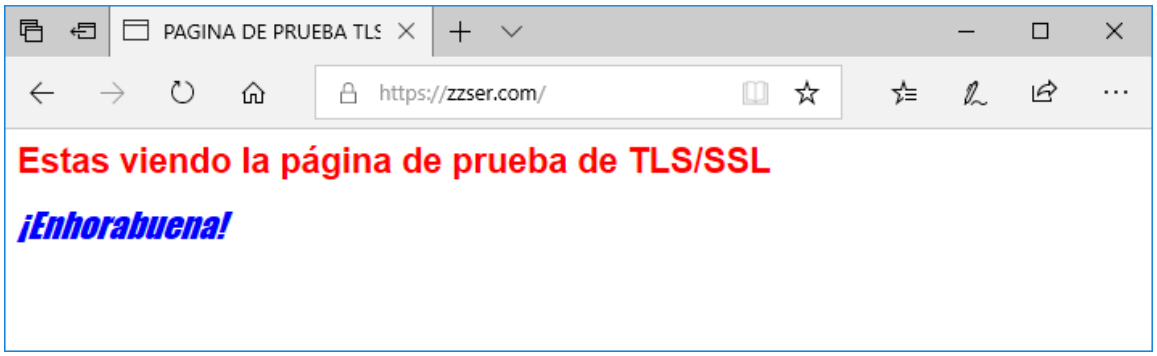
Tras incluir la línea en el archivo hosts, vuelve a acceder al sitio web seguro.

Antes de cada acceso, conviene borrar el estado SSL, para realizar los accesos siempre en las mismas condiciones. El borrado se hace pulsando un botón en la ventana Opciones de Internet.



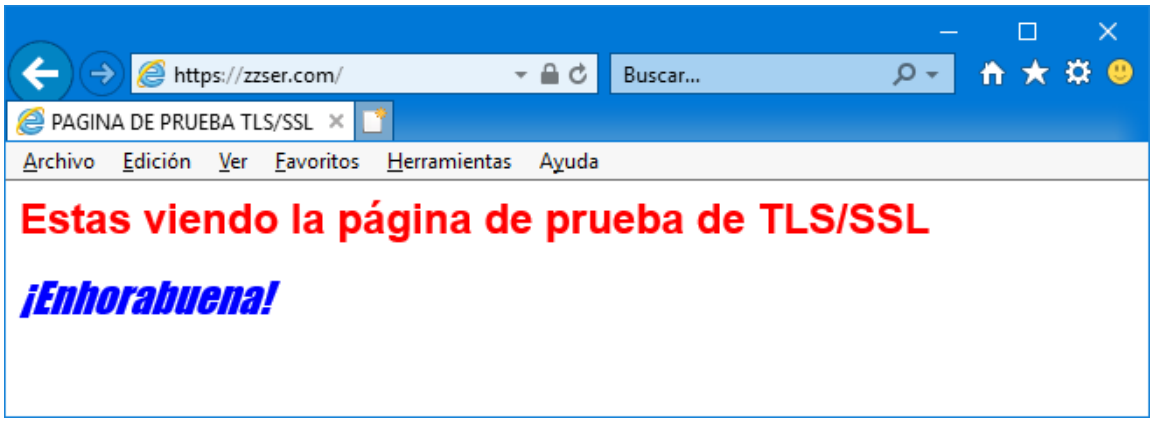
Acceder con EDGE a https://zzser.com

Se obtiene este resultado:

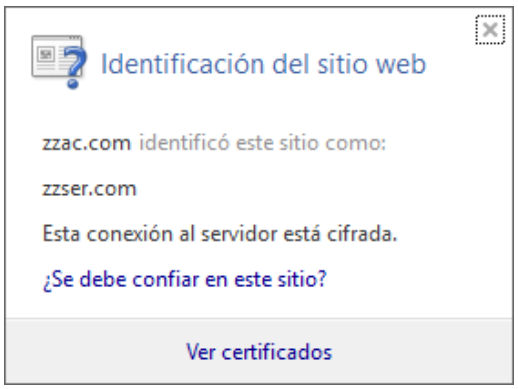


Acceder con Internet Explorer 11 a https://zzser.com

Se obtiene este resultado:



Comprobar cómo el acceso es correcto. Si pinchamos en el candado amarillo obtenemos un informe de la seguridad que se está utilizando entre el navegador y el servidor.



Comprobar cómo la conexión con el servidor está cifrada.

El navegador Internet Explorer 11 utiliza colores en los candados para suministrar información adicional:

Rojo: El certificado está caducado, no es válido o tiene un error.

Amarillo: No se pudo comprobar la autenticidad de un certificado o de la entidad de certificación que lo emitió. Esto podría indicar un problema con el sitio web de la entidad emisora. No obstante la comunicación con el sitio web está cifrada.

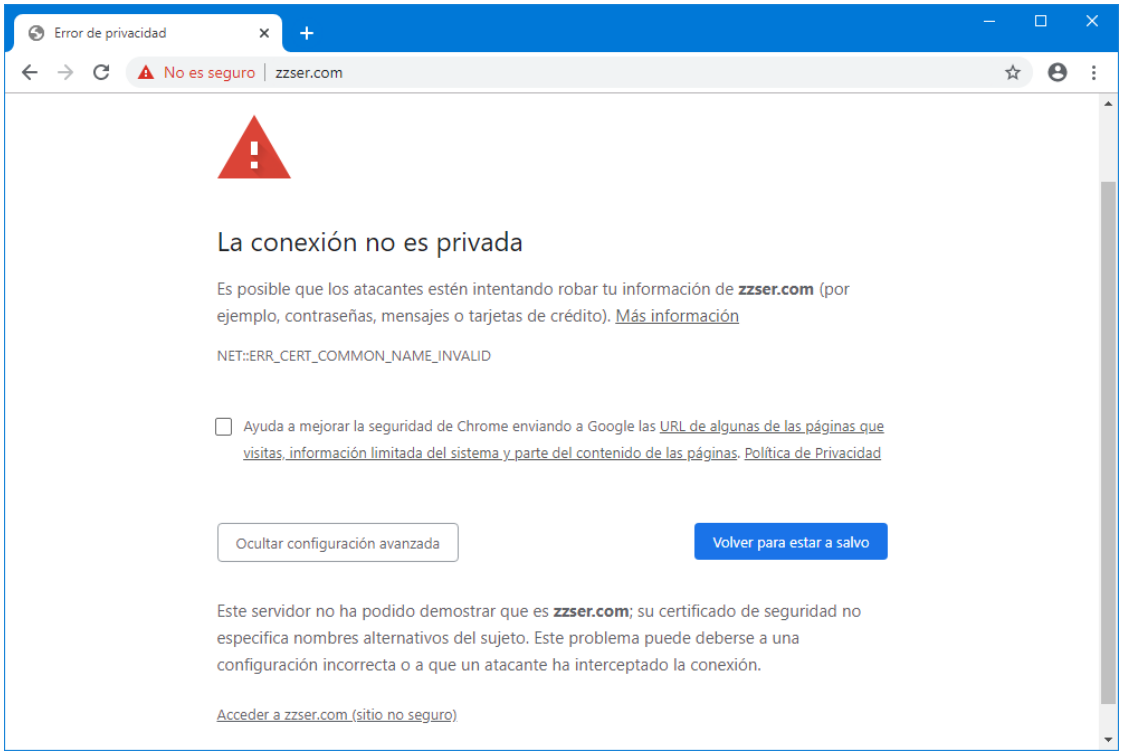
Blanco: El certificado tiene una validación normal. Esto significa que la comunicación con el sitio web está cifrada.

Verde: El certificado usa una validación extendida. Es decir, la comunicación entre el explorador y el sitio web está cifrada y la entidad emisora del certificado confirma que el propietario o administrador del sitio web es una empresa constituida legalmente conforme a la jurisdicción mostrada en el certificado y en la barra de estado de seguridad.

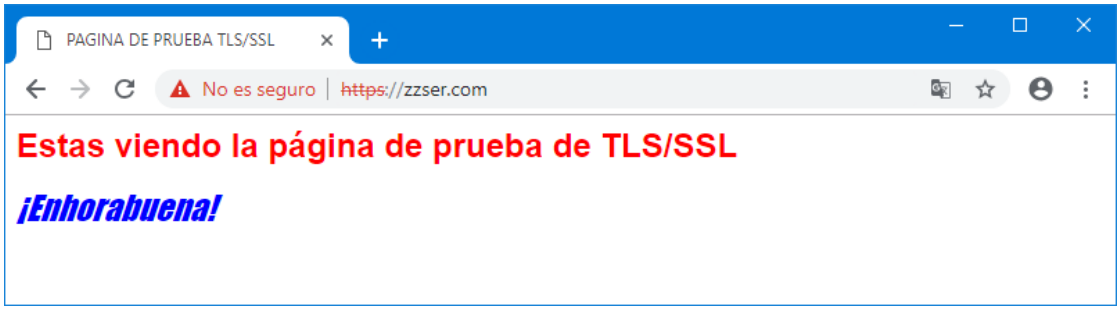
Es interesante leer información sobre "***Extended Validation Certificate***".

Accede con Google Chrome a https://zzser.com

Se obtiene este resultado:



Al pulsar en "Acceder a zzser.com (sitio no seguro)" se obtiene:



En este caso el navegador Chrome termina accediendo a la página **pero sin cifrar la conexión**.

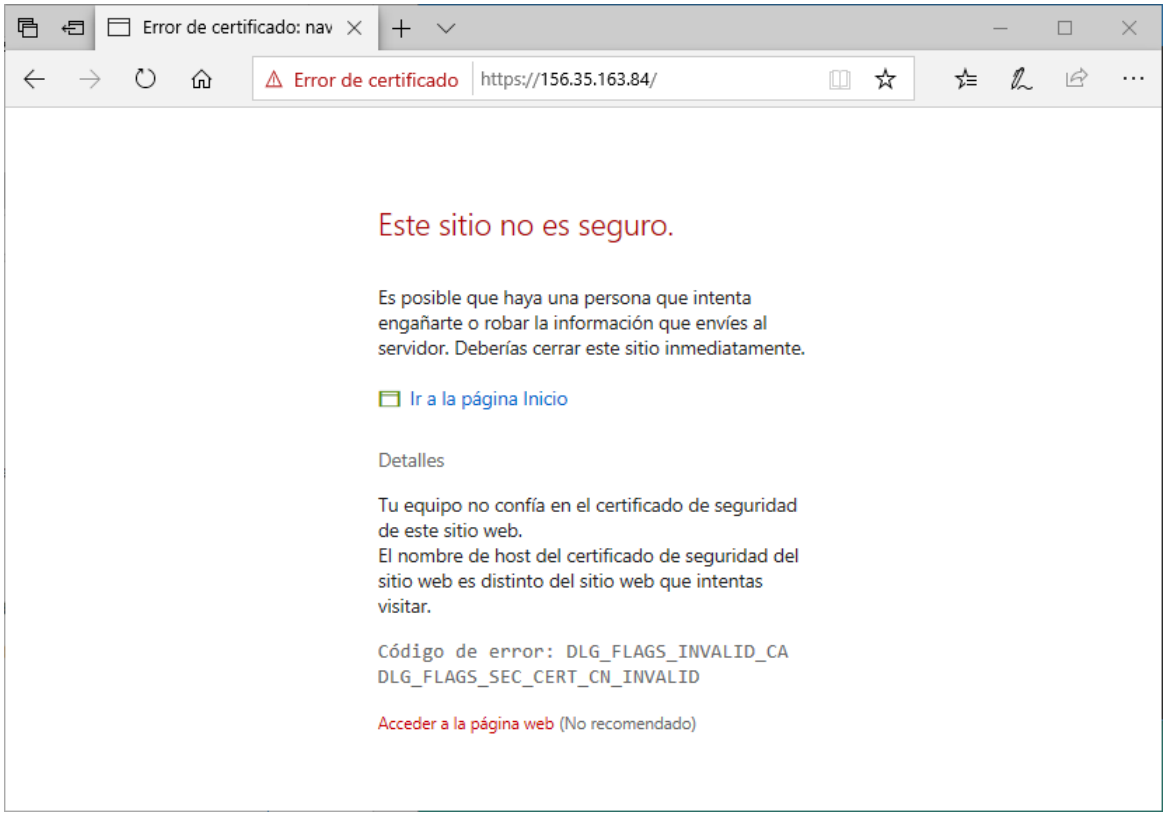
Realizar las mismas pruebas pero desde otro computador.

El servidor https debe ejecutarse en una máquina virtual y el cliente https en otra máquina virtual (o en una máquina física en la que se tengan privilegios de administración). En ambas máquinas virtuales, el adaptador de red debe estar configurado en modo puente.

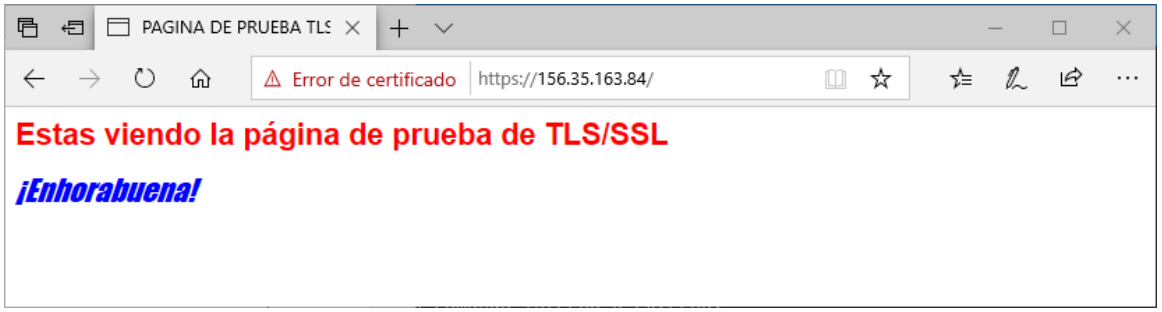
Recuerda que antes de realizar cada prueba conviene borrar el historial de navegación de los navegadores y el estado SSL.

En la máquina cliente accede al servidor seguro usando un URL con el formato https://A.B.C.D/

Por ejemplo al usar el navegador EDGE se obtiene:



Tras seleccionar "Acceder a la página web" se obtiene:



Observa que se indica la presencia de DOS errores: no se confía… y el nombre es distinto…

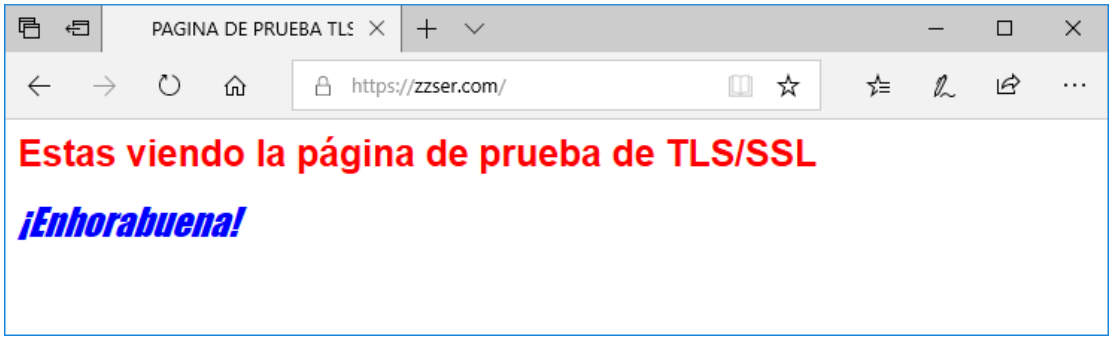
Para solucionar el primer problema es necesario instalar en la máquina cliente el certificado de la autoridad certificadora que ha emitido el certificado del servidor.

Para solucionar el segundo problema es necesario acceder al servidor mediante su nombre permitiendo que el DNS resuelva el nombre en la dirección IP adecuada. Se puede hacer integrando la dirección IP y el nombre del servidor en el fichero hosts.

Una vez realizadas las DOS acciones, se puede acceder directamente al sitio sin errores.

Accede con EDGE a https://zzser.com

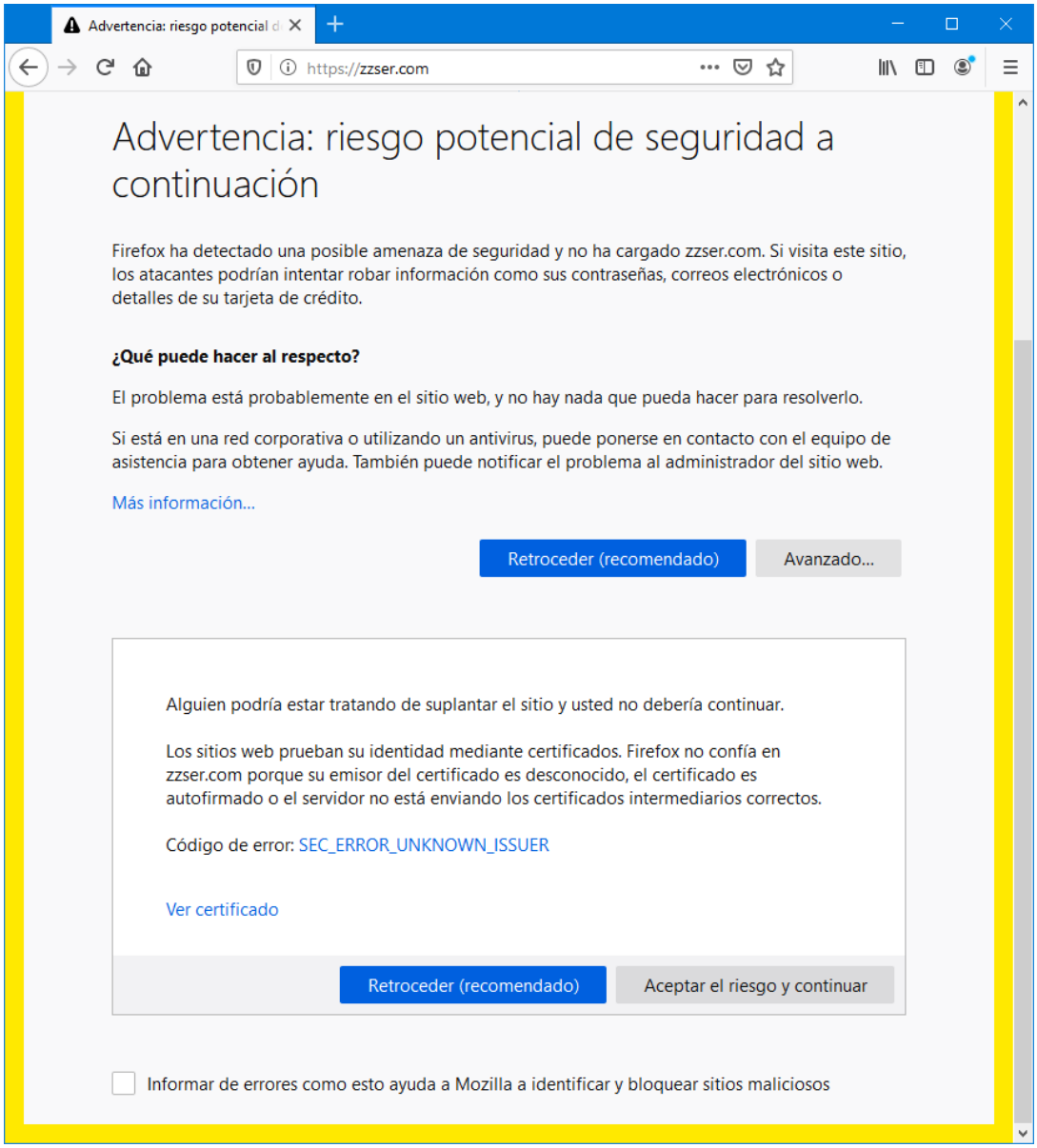
Este el resultado al acceder:



El mismo resultado se obtiene accediendo con Internet Explorer 11.

Accede con Firefox a https://zzser.com

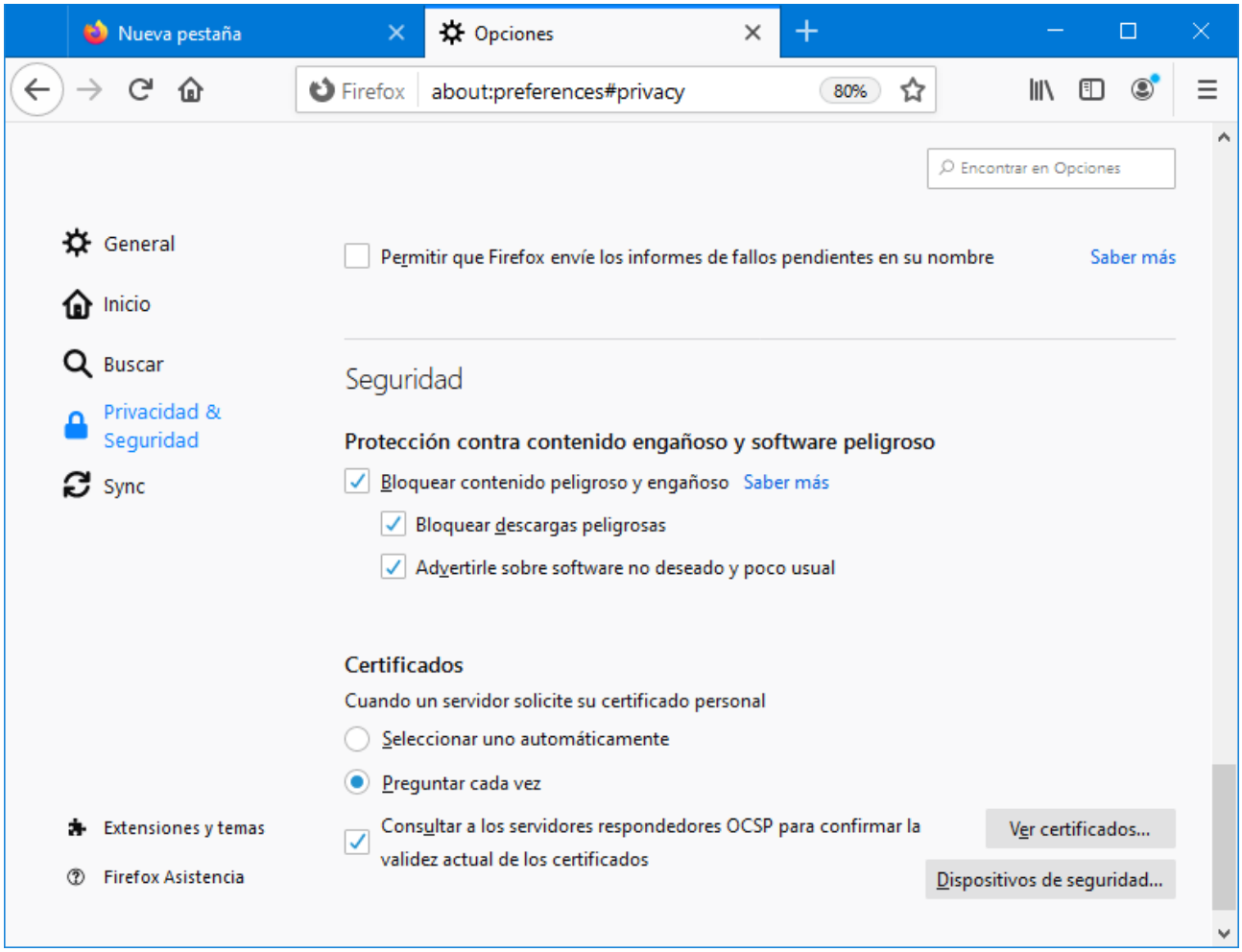
Al intentar acceder con Firefox al sitio web se obtiene un error:



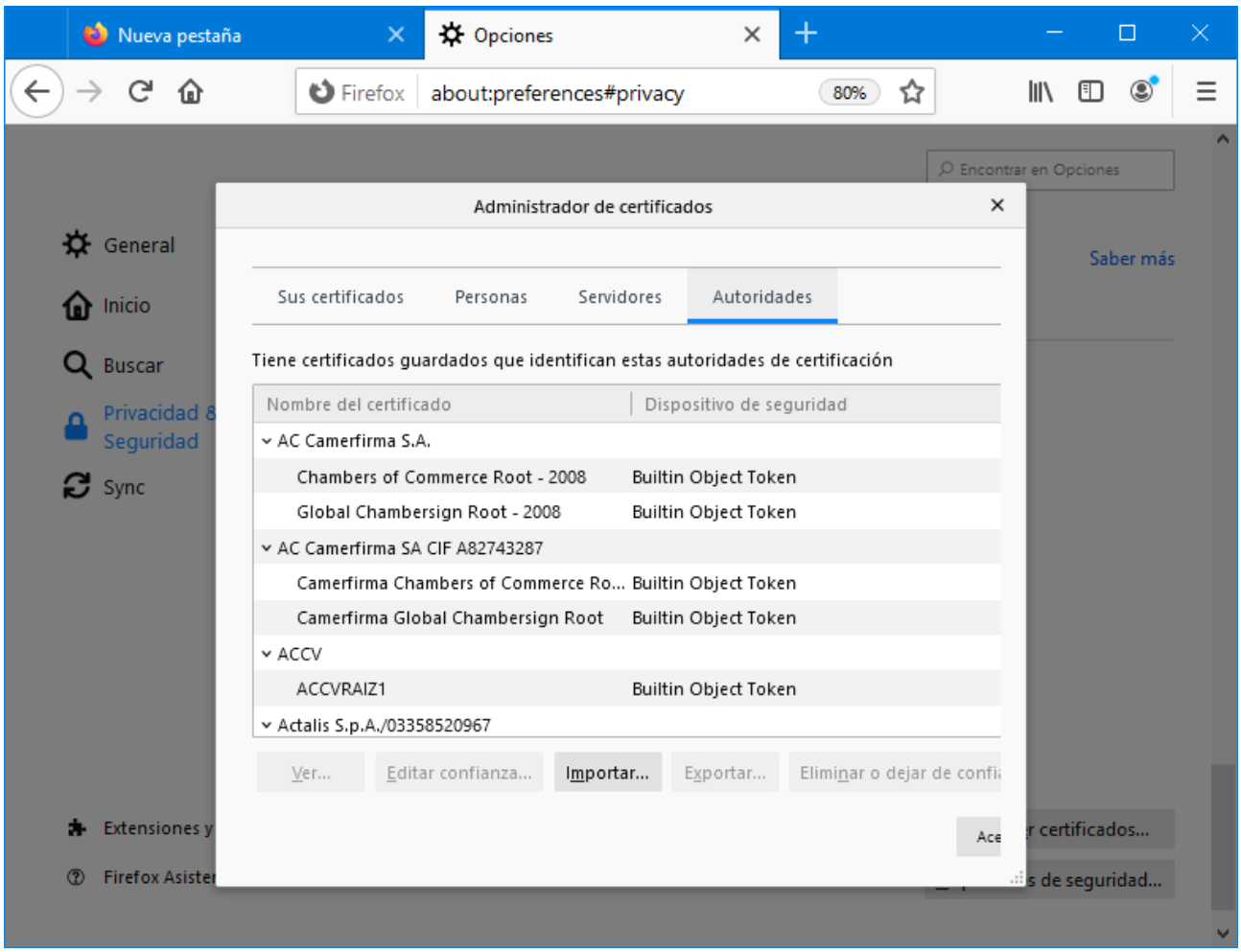
Firefox NO CONOCE el certificado emisor del certificado que ha recibido del servidor. Este problema surge porque Firefox NO utiliza el almacén de certificados de Windows ya que dispone de su propio almacén.

Para solucionar este problema tienes que importar el certificado de la autoridad certificadora en el almacén de certificados de autoridades de Firefox. Procede del modo siguiente:

En cualquier página del navegador haz clic en el botón menú (tres barras horizontales) en la esquina superior-derecha. En la ventana que se abre selecciona "Opciones". Entonces se abre la página Opciones en una nueva pestaña. En la página Opciones selecciona "Privacidad & Seguridad" en el panel izquierdo y después vete al final de la página en la que aparece la sección "Certificados". El resultado se puede observar en la figura siguiente:



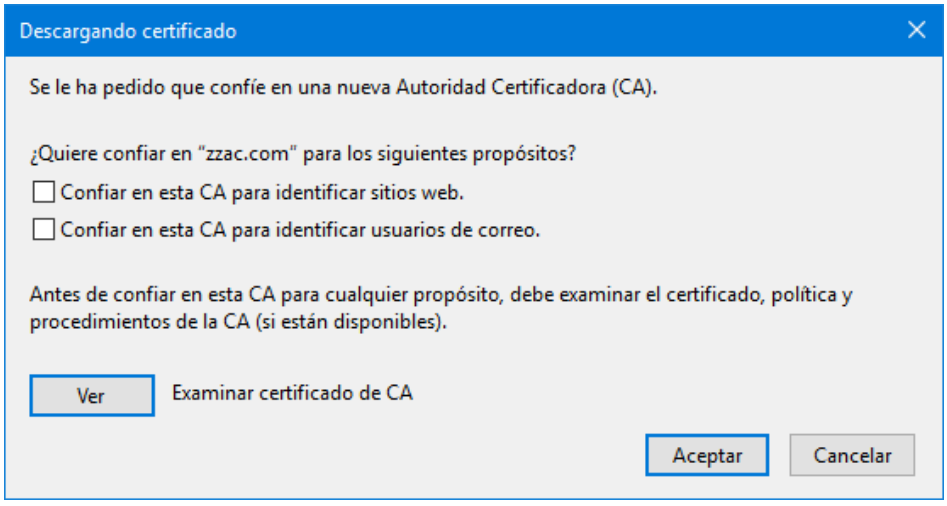
Haz clic en el botón "Ver certificados" y aparece el "Administrador de certificados". Selecciona "Autoridades" para ver los certificados Raíz de Confianza. La figura siguiente muestra la ventana a la que hay que acceder.



En esta ventana desplázate al final para comprobar que no aparece el certificado de zzac.com ya cargado en el almacén de certificados de Windows.

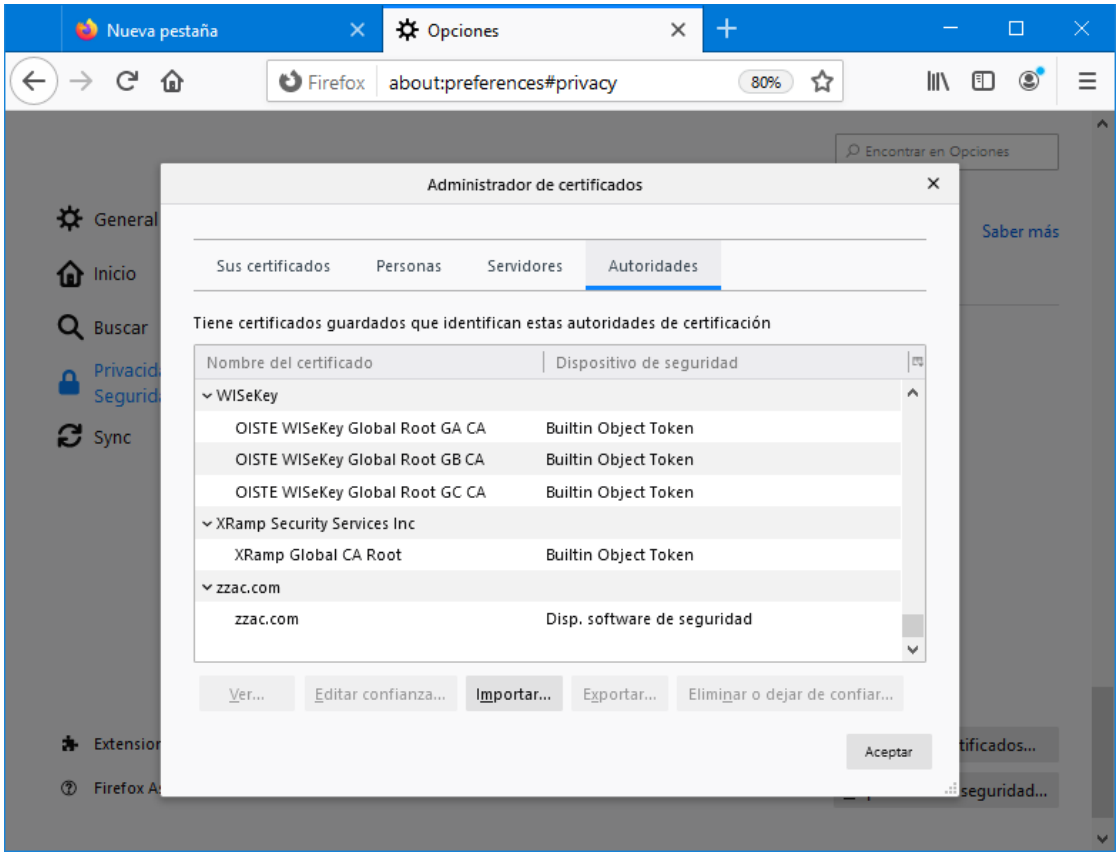
Pulsa el botón “Importar…” y se solicita un fichero con el certificado.

Tras indicar el fichero zzac.cer aparece la ventana siguiente:

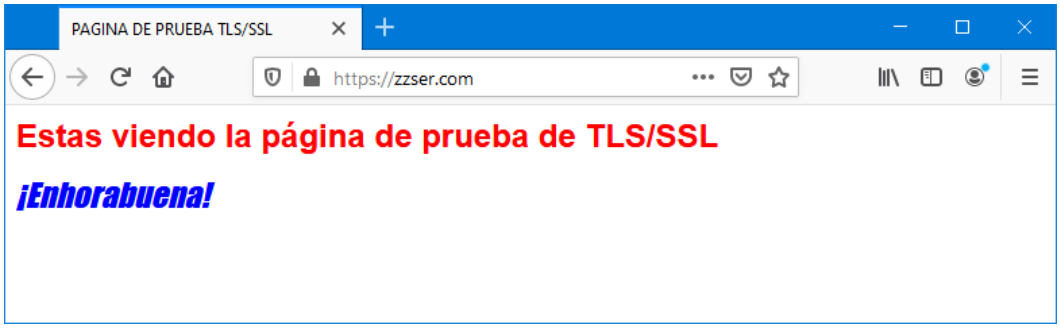


Tras marcar la primera opción pulsa el botón “Aceptar”.

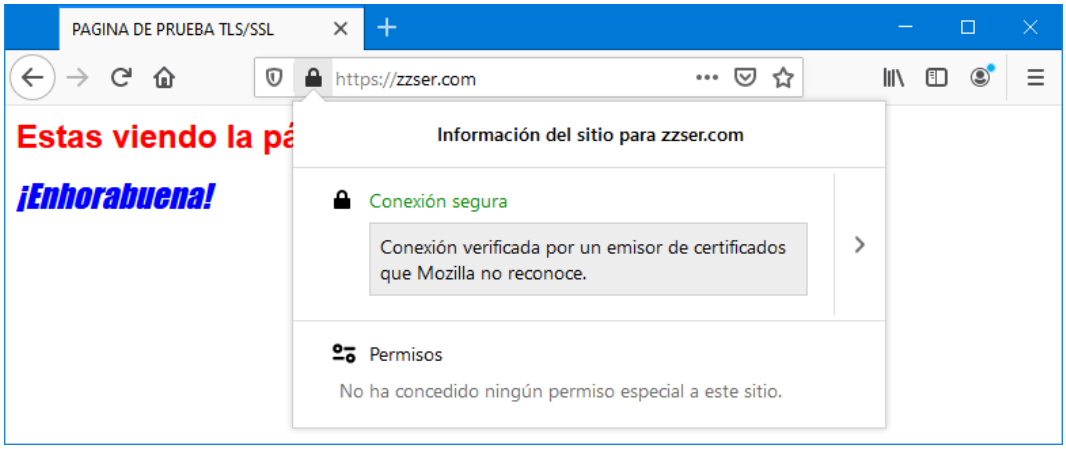
Ahora aparece el certificado en el almacén de Firefox.



Al acceder nuevamente a https://zzser.com se entra directamente al sitio tal como muestra la figura siguiente:

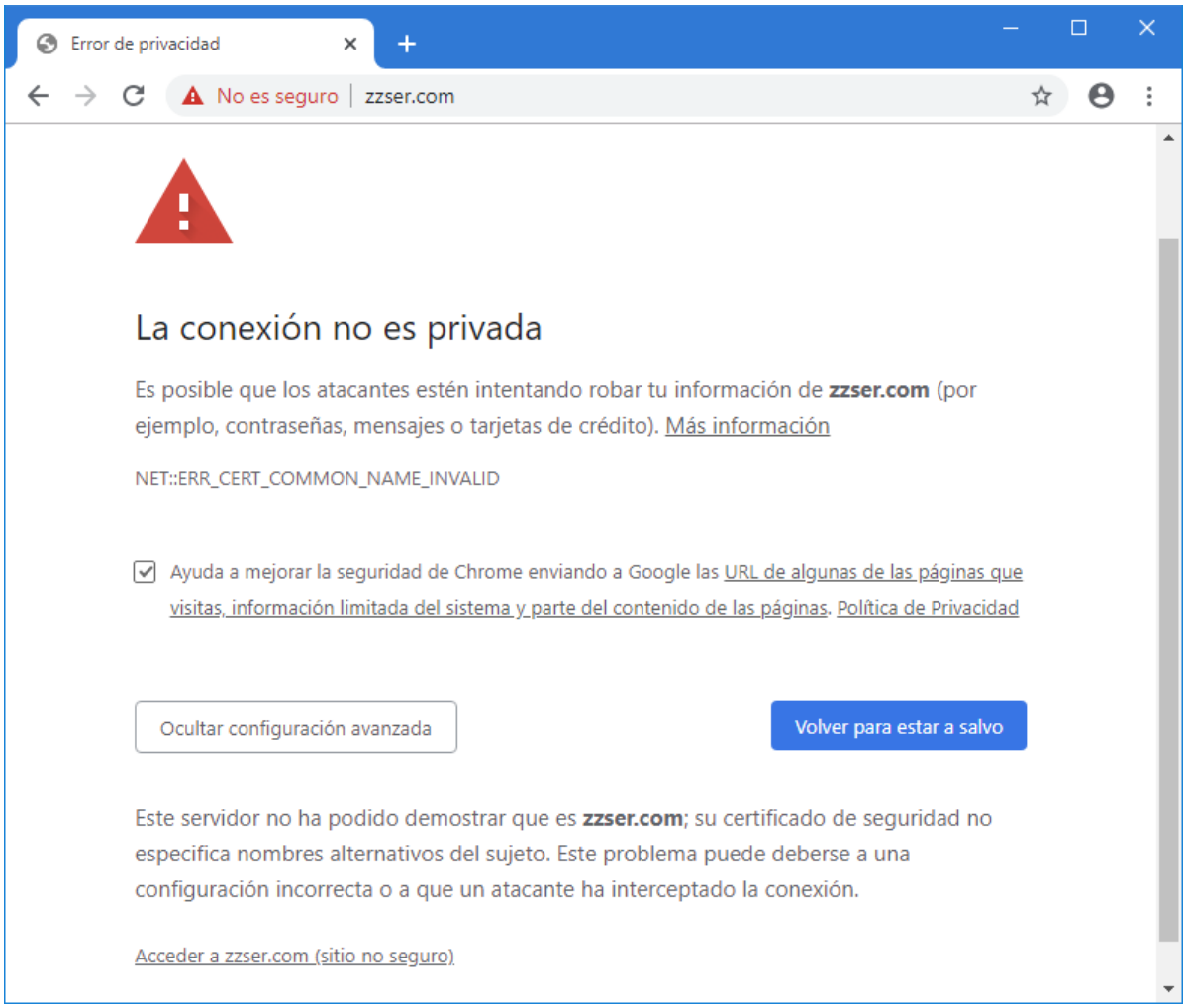


Haz clic sobre el candado verde para comprobar el estado de la conexión:

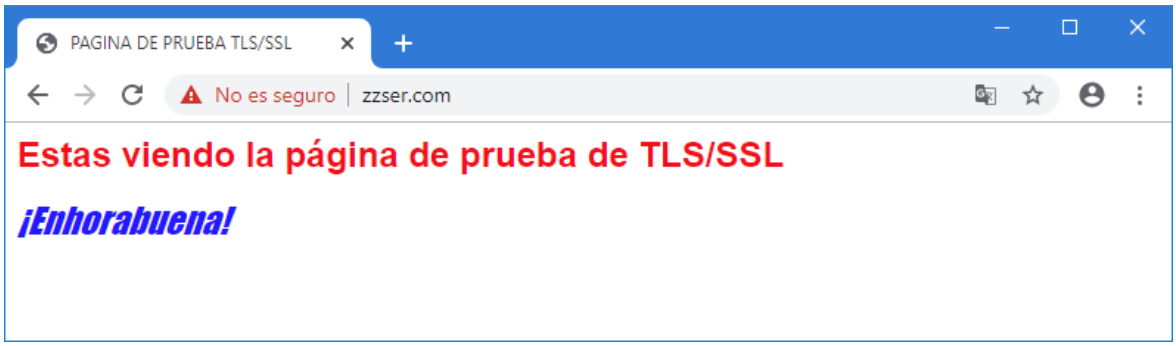


Accede con Chrome a https://zzser.com

Comprueba que se obtiene este error:



Si se usa el enlace “Acceder a zzser.com (sitio no seguro)” se accede al sitio:



Pero sin cifrar la conexión.

Este comportamiento se obtiene con la versión actual de Chrome, pero con versiones anteriores a la 58 el comportamiento era diferente.

NOTA: Antes de acceder al sitio web es conveniente borrar el historial de navegación de Chrome. Ir a Configuración > Privacidad y seguridad > Borrar datos de navegación.

El motivo del fallo al usar Chrome está muy claro: **su certificado de seguridad no especifica nombres alternativos del sujeto**. Se puede encontrar una explicación del error en:

https://support.google.com/chrome/a/answer/7391219?hl=en

La versión 58 y posteriores del navegador Chrome solo comprueban que algún SubjectAternativeName (SAN) incluido en el certificado enviado desde el sitio web coincide con el nombre del sitio web al que se ha accedido con Chrome.

Esta política se basa en una aplicación "excesiva" de la RFC 2818 que dice:

```
If a subjectAltName extension of type dNSName is present, that MUST
be used as the identity. Otherwise, the (most specific) Common Name
field in the Subject field of the certificate MUST be used. Although
the use of the Common Name is existing practice, it is deprecated and
Certification Authorities are encouraged to use the dNSName instead.
```

¡Chrome no usa el CommonName del certificado si no encuentra un SubjectAlternativeName!.

Los nombres alternativos de sujeto se almacenan en las extensiones en los certificados X509v3. MakeCert no permite crear certificados con extensiones, sino solo certificados básicos. Para crear certificados con extensiones habría que utilizar una herramienta como OpenSSL. También se podrían obtener certificados de una autoridad certificadora en los cuales se repita el CommonName en la extensión SubjectAlternativeName.

Pero Google previó que hasta la versión 65 de Chrome se pudiese configurar la política EnableCommonNameFallbackForLocalAnchors que permite a Chrome usar el commonName de un certificado si éste no tiene una extensión subjectAlternativeName.

En la siguiente sección de la práctica se proporciona una solución basada en la utilización de PowerShell y el comando New-SelfSignedCertificate.

5. Instalar un nuevo servidor usando los certificados generados con PowerShell

Si no has realizado la parte opcional de la práctica de gestión de certificados debes realizarla ahora para generar certificados más completos para un servidor web. Puedes crearlos en tu máquina física.

Crea un certificado raíz con el siguiente script:

```
# ccpACcom.ps1
# Crea un certificado raíz
# El parámetro -TextExtension indica que es de una Autoridad Certificadora
# Es necesario para que el navegador Firefox lo admita en el almacén de raíces de confianza

$cert = New-SelfSignedCertificate -Type Custom `
-Subject "CN=zpac.com" `
-KeyAlgorithm RSA -KeyLength 2048 -KeyExportPolicy Exportable `
-KeyUsage CertSign, CRLSign, DigitalSignature, KeyEncipherment, DataEncipherment `
-NotBefore (Get-Date) `
-NotAfter (Get-Date).AddYears(10) `
-HashAlgorithm sha256 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-TextExtension @("2.5.29.19={critical}{text}ca=1")
```

Crea un certificado para autenticar el servidor web con el siguiente script:

```
# ccpSERcom.ps1
# Crea un certificado de servidor firmado por la AC zpac.com
# El parámetro -DnsName crea un nombre alternativo del sujeto del certificado
# Es necesario para que el navegador Chrome acepte el certificado como válido

New-SelfSignedCertificate -Type Custom `
-Subject "CN=zpser.com" -DnsName "zpser.com" `
-KeyAlgorithm RSA -KeyLength 2048 -KeyExportPolicy Exportable `
-HashAlgorithm sha256 `
-Signer $cert `
-CertStoreLocation "Cert:\CurrentUser\My"
```

Exporta el certificado raíz y su clave privada asociada al fichero **zpACcom.pfx** para disponer de una copia de seguridad de la Autoridad Certificadora. Exporta también el certificado de la Autoridad Certificadora al fichero **zpACcom.cer**.

Exporta el certificado del servidor y su clave privada asociada al fichero **zpSERcom.pfx**.

Es importante exportar todas las propiedades extendidas. Usa las contraseñas habituales.

Copia los ficheros zpACcom.cer y zpSERcom.pfx a la máquina virtual en la que se ejecuta el servidor web.

Cargar los certificados en almacenes de la Máquina Local, NO en los del Usuario Actual.

Para ello utiliza la herramienta **Certlm.msc**, y NO la herramienta Certmgr.msc.

Carga el certificado raíz (zpACcom.cer) en el almacén "Entidades de certificación raíz de confianza".

Carga el certificado del servidor junto con su clave privada en el almacén "Hospedaje de sitios web".

Al cargar certificados, utiliza siempre como almacén físico el registro.

Ahora detén el servidor web seguro zzser.com y crea rápidamente el nuevo servidor zpser.com. Este nuevo servidor trabajará con los mismos directorios que el antiguo y el nuevo certificado.

En la máquina cliente desde la que va a acceder al servidor web seguro debes instalar el certificado de la Autoridad Certificadora zpACcom.cer en el almacén "Entidades de certificación raíz de confianza" del Usuario Actual usando la herramienta Certmgr.msc.

En el fichero "C:\Windows\system32\drivers\etc\hosts" añade la línea siguiente:

A.B.C.D zpser.com

Donde A.B.C.D es la dirección IPv4 del computador en el que se ejecuta el servidor web.

Esto es necesario para emular el registro del URL del servidor web en un servicio DNS.

Ahora se puede acceder al servidor web seguro con los navegadores EDGE, Internet Explorer 11 y Chrome directamente usando el URL **https://zpser.com**

Para acceder con ese URL directamente al servidor web seguro usando el navegador Firefox debes cargar previamente el certificado raíz zpACcom.cer en el almacén de Autoridades de Firefox.

6. Usar un servidor DNS en vez del archivo hosts

Si un servidor DNS ha asociado un nombre con la dirección IPv4 del computador en el que se ejecuta el servidor web, entonces se puede aprovechar el DNS y NO es necesario utilizar el archivo hosts del computador cliente.

Esta sección de la práctica solo se puede realizar si el servidor web se registra en un servicio DNS.

Para aprovechar el DNS y NO usar el archivo hosts.

Comprobar la dirección_IPv4 que tiene asignada el servidor web usando el comando ipconfig.

Hacer un "ping -a dirección_IPv4" desde otro computador para ver como el DNS resuelve la dirección devolviendo el nombre_DNS del servidor.

Si el comando ping indica que no hay acceso al servidor, comprueba si está habilitada la regla "Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)" del firewall. Habilítala, si es necesario. En algunos computadores, al habilitar esta regla, la dirección remota se restringe a "Subred Local". Si es así edita la regla para que la dirección remota sea "Cualquiera".

NOTA: Si se hace ping -a en el mismo computador en el que esta ejecutándose el servidor https, el comando ping -a nos devuelve el nombre del servidor que utiliza Windows, ej. PC-ES.

NOTA: Si se hace ping -a desde el computador en el que se modificó el fichero hosts para resolver localmente la dirección del servidor, hay que comentar la línea antes de ejecutar ping, pues si no el resolutor del DNS usa la información local.

Generar un nuevo certificado para el servidor usando como nombre del sujeto el que nos devuelve el DNS e instalarlo en el servidor.

Ahora es posible conectarse al servidor usando en el navegador la URL https://nombre_DNS/