Protocolo TLS/SSL
Práctica 8

1. Objetivo

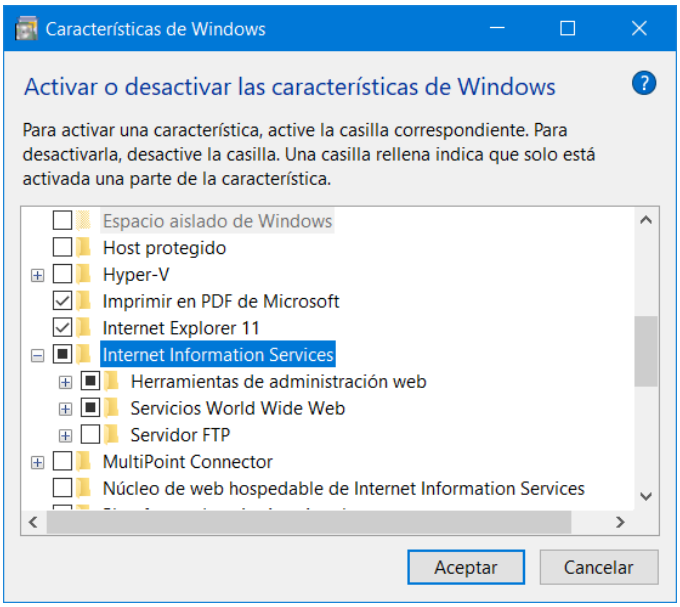
En esta práctica el alumno debe preparar un servidor web y un navegador web para que se puedan establecer comunicaciones seguras (cifradas) entre ellos usando el protocolo TLS/SSL. Habrá que crear o reutilizar los certificados necesarios que deberán ser instalados tanto en el servidor web como en los 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 Puente (Bridge).

2. Preparación del servidor web

Para utilizar un servidor web es muy cómodo activar el IIS 10 (Internet Information Server) que viene integrado en Windows 10.

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:

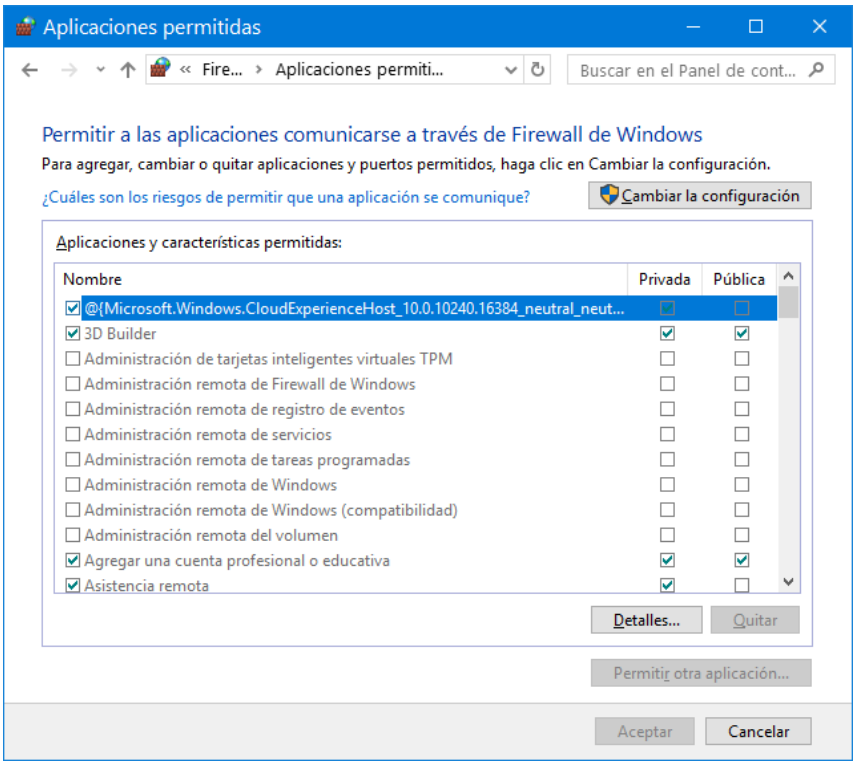


Selecciona la casilla de Internet Information Services, con las opciones que vienen preseleccionadas por defecto.

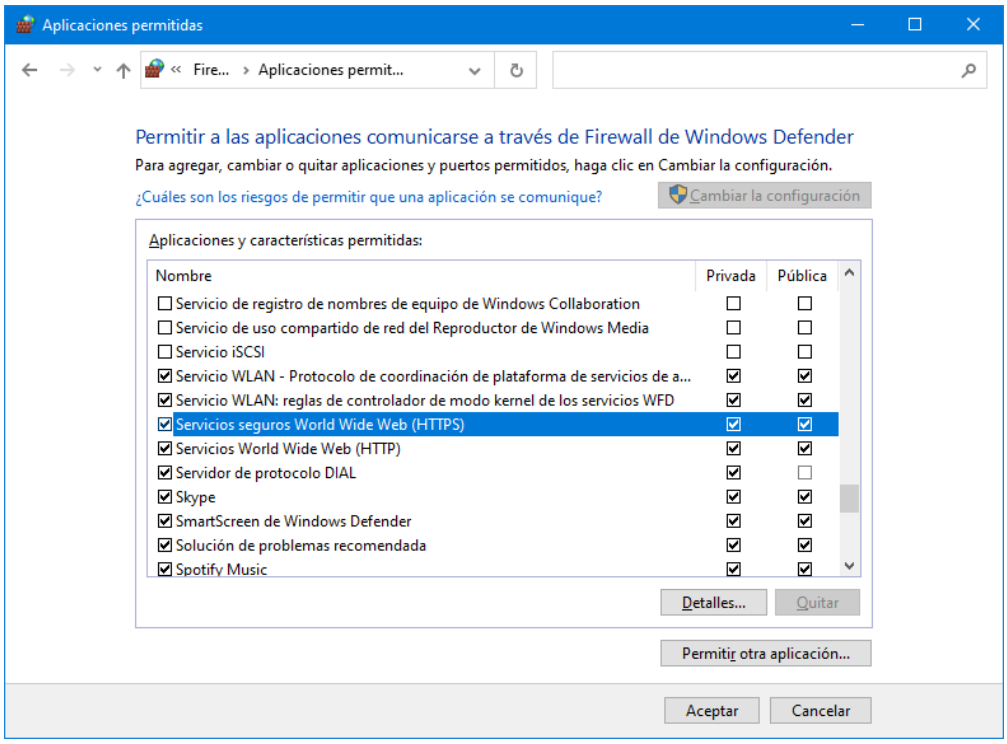
Para que el servidor sea accesible desde otros computadores es necesario abrir los protocolos y puertos adecuados en el **Firewall de Windows**. Windows 10 realiza esta operación automáticamente. Para comprobar esta operación hacer:

Inicio > Panel de control > Firewall de Windows Defender

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



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



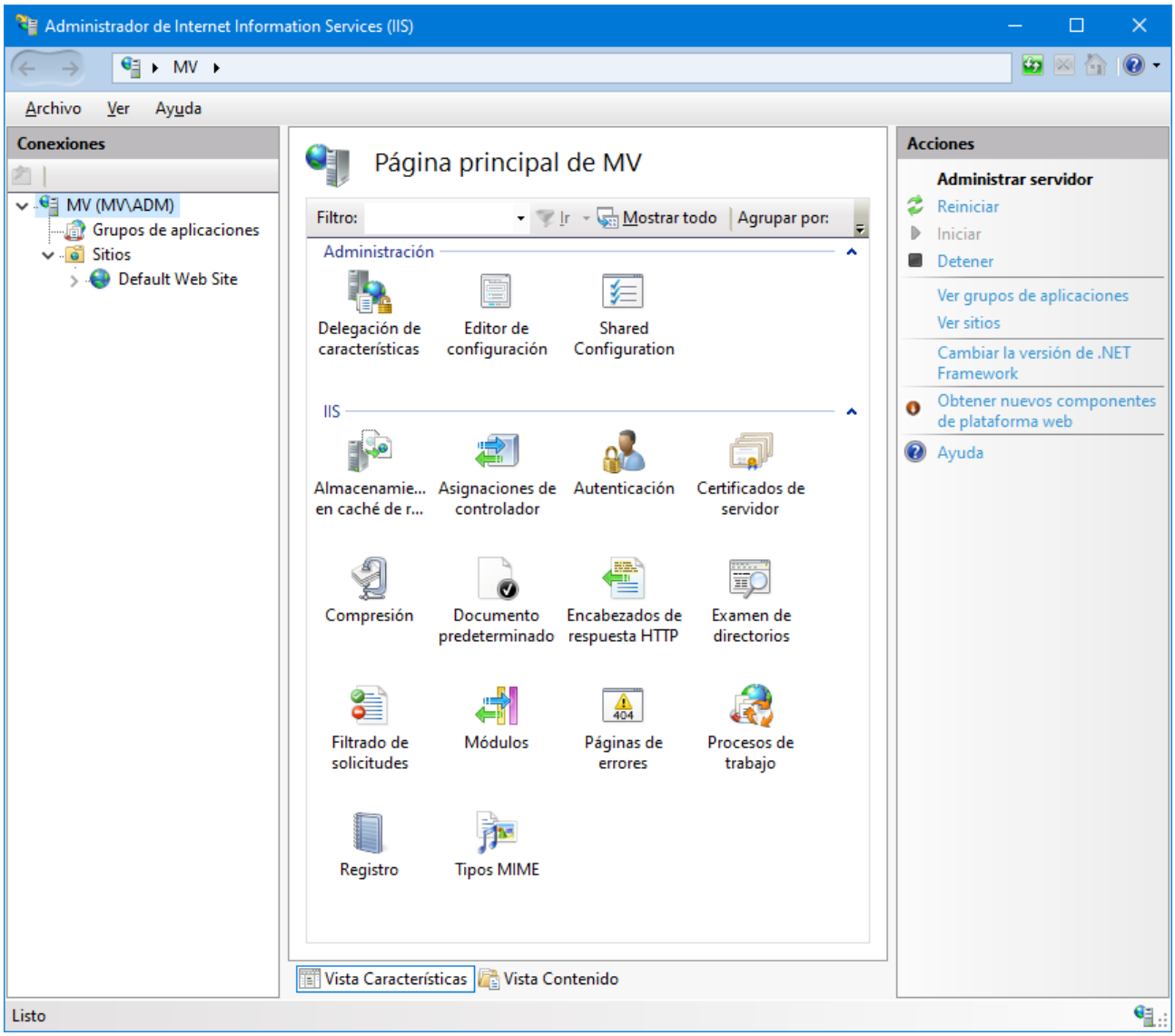
Para arrancar la herramienta de administración del IIS hacer:

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**

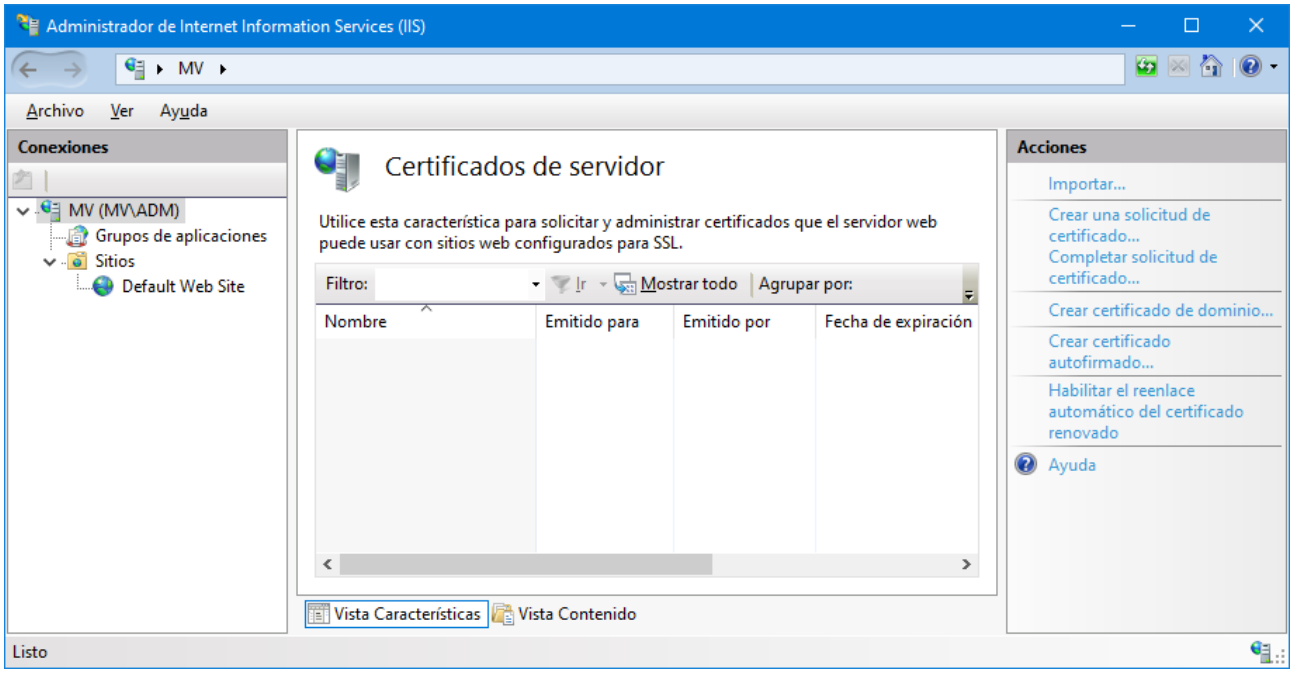
Aparece la siguiente consola de administración:



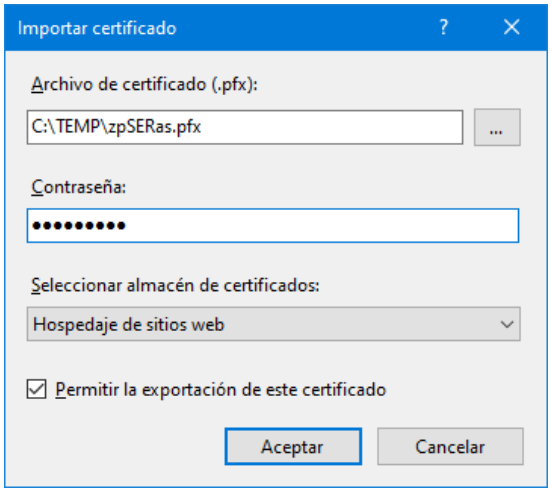
En la que se ha desplegado el árbol de conexiones en el panel izquierdo. En este panel se puede observar que hay un servidor IIS en el computador MV (nombre del equipo que se puede asignar en: Panel de control > Sistema) que aloja aplicaciones y sitios web. Un servidor IIS puede alojar varios sitios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

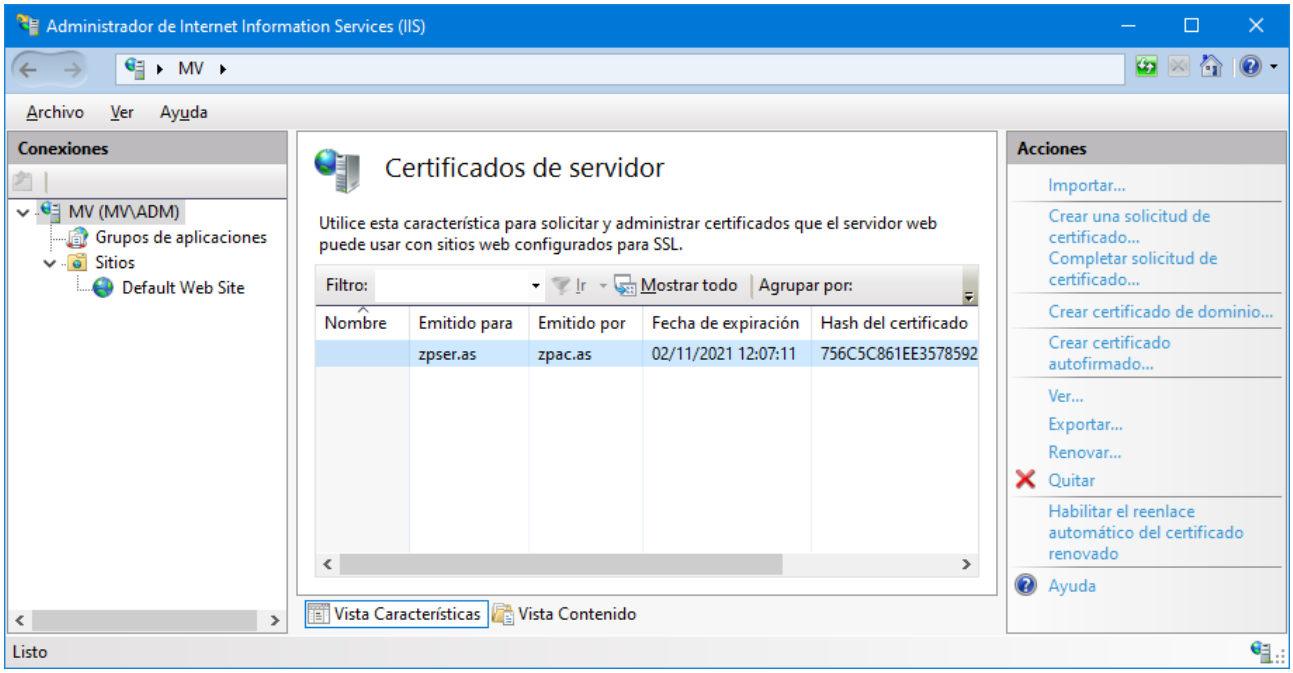


En el panel derecho de Acciones seleccionar "Importar...". En la ventana de selección de archivos que aparece seleccionar el certificado de servidor creado previamente: zpSERas.pfx y proporcionar la contraseña que permite la utilización del certificado, por ejemplo conserpfx.



En Windows 10 se permite seleccionar el almacén de certificados “Personal” y 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 zpser.as, 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 zpser.as 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, zpac.as, 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 zpser.as 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 zpser.as**
- **zzACnombrealumno en vez de zpac.as**

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.

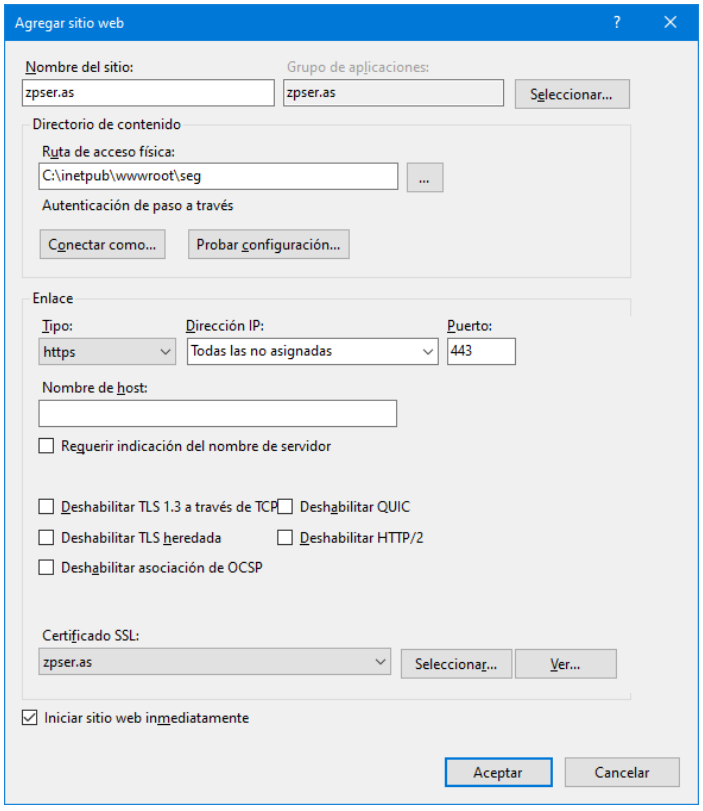
La utilización de cualquier directorio, como por ejemplo C:\Temp\ puede dar problemas de acceso con usuarios no autenticados, esto es, usuarios que acceden a la página principal del servidor seguro sin tener que autenticarse proporcionando un nombre de usuario y una contraseña.

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.

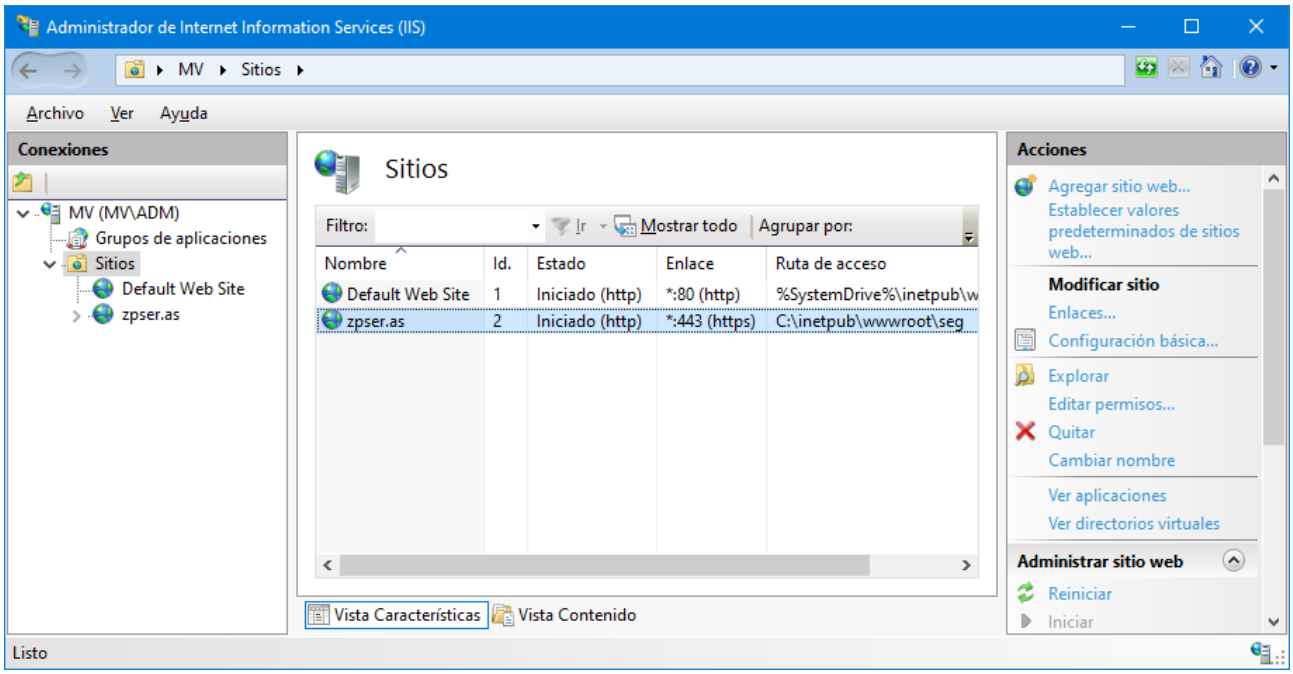
Seleccionar Sitios, hacer clic en el botón derecho del ratón y en el menú contextual seleccionar "Agregar sitio web...". En el cuadro de dialogo que aparece seleccionar las opciones que se indican a continuación:



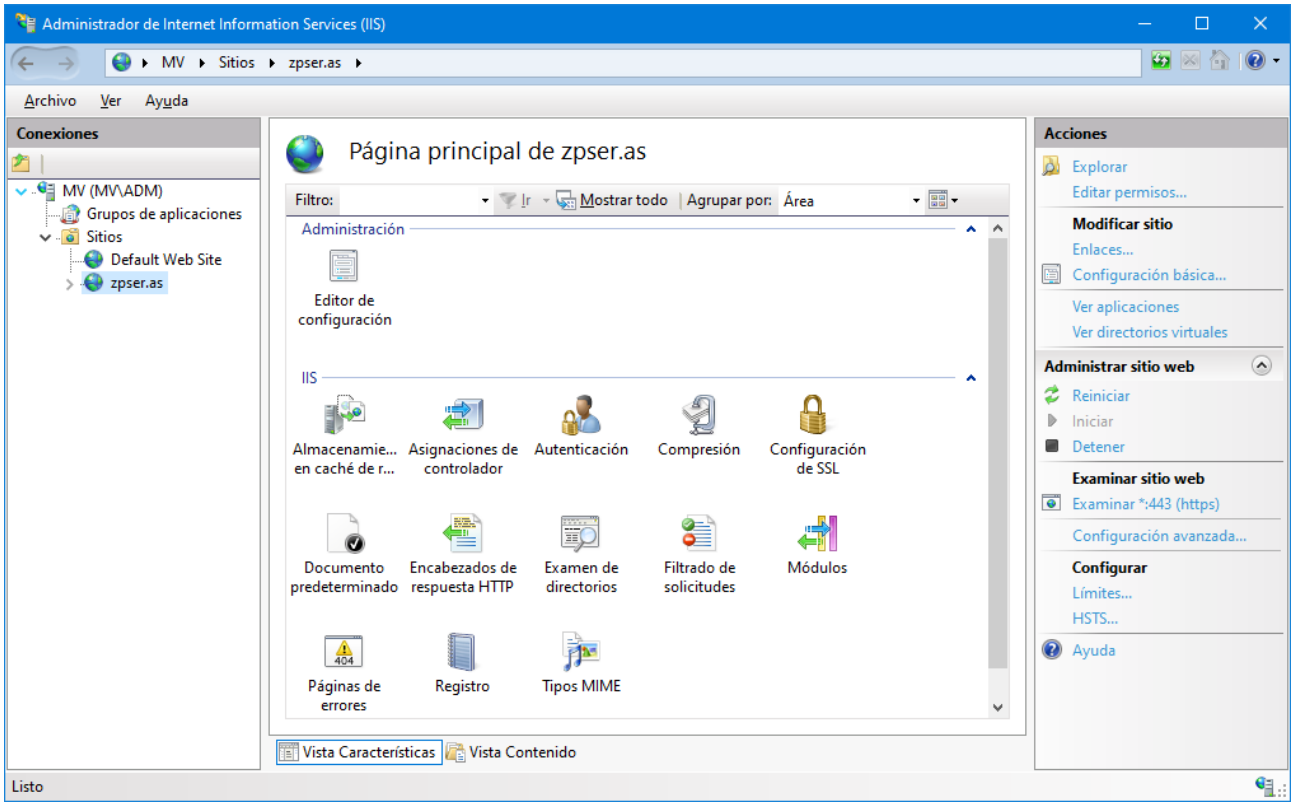
Observar cómo se elige el nombre del sitio zpser.as para que coincida con uno de los mostrados en el menú de opciones Certificado SSL. Observar que en el cuadro de diálogo previo en Certificado SSL se muestran los certificados disponibles en el almacén de certificados del IIS mostrándolos por el campo "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 zpser.as basado en TLS/SSL y aparece así en la página principal del Administrador de IIS.

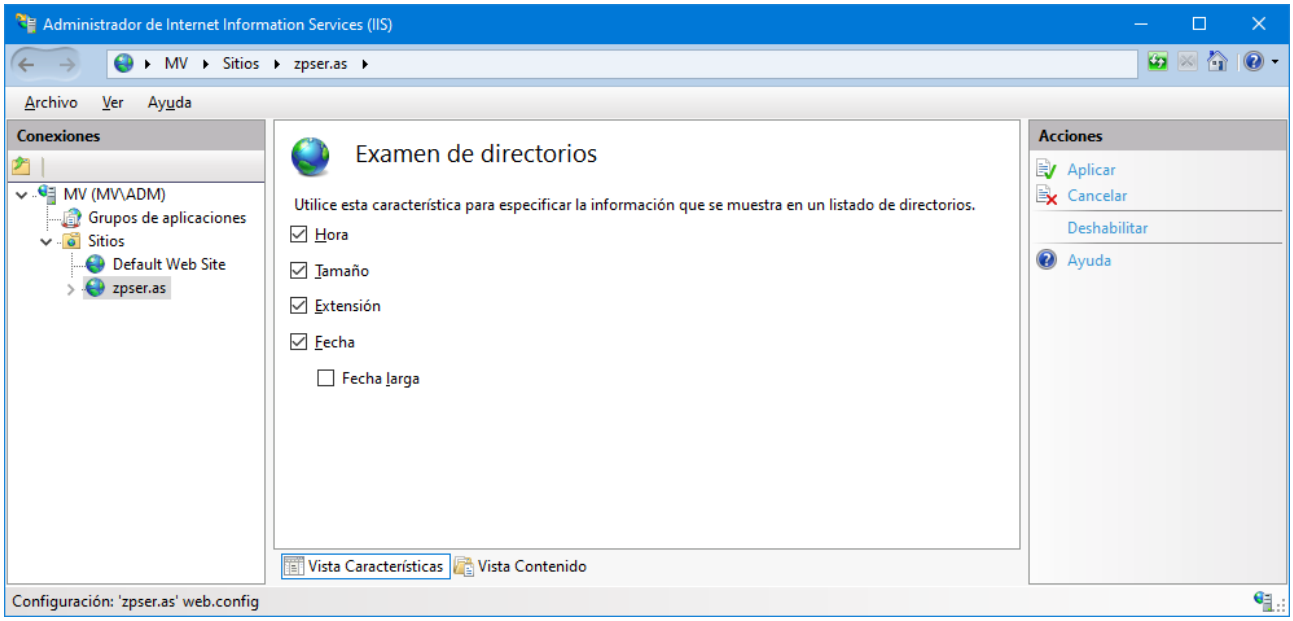


La configuración del sitio web puede incluir muchísimos aspectos y constituirían materia suficiente para una o más prácticas. A continuación se explican solo los aspectos más importantes para los objetivos de esta práctica. Si seleccionamos zpser.as en el panel izquierdo de Conexiones aparece la página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



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.

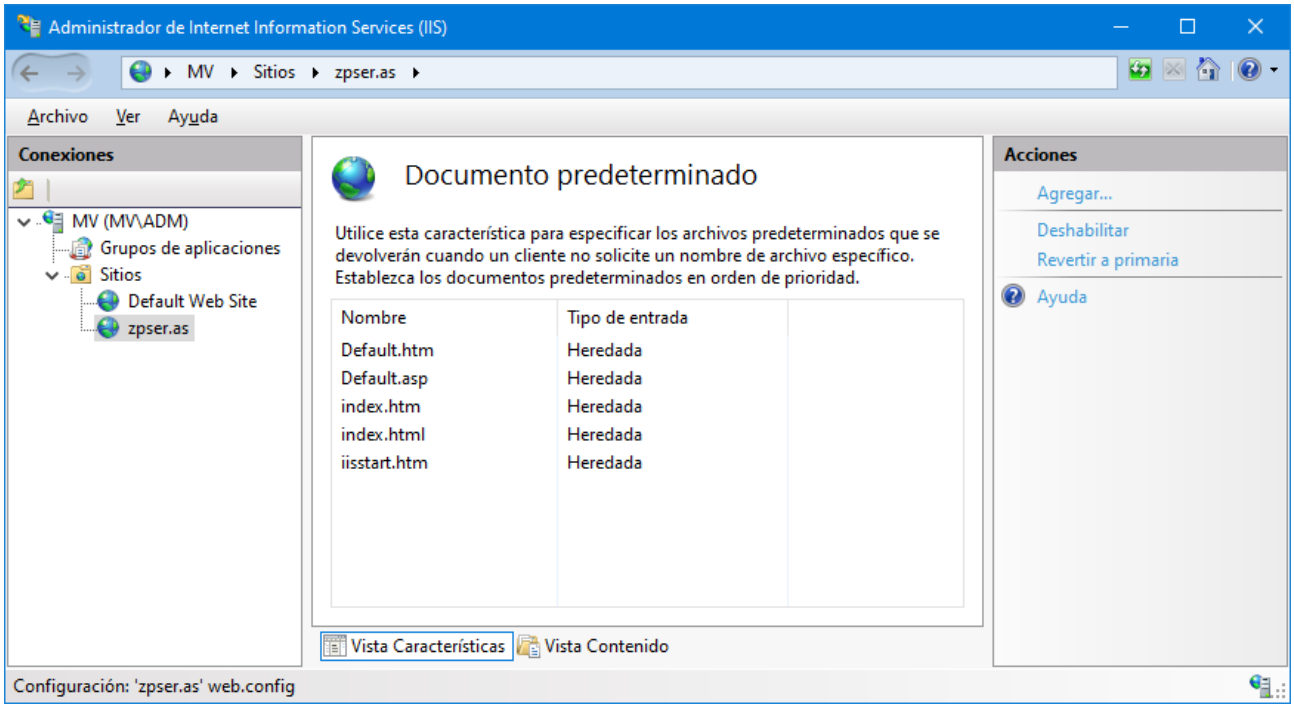
En el panel derecho hacer clic en la opción "Habilitar" y luego en el panel central seleccionar todas las opciones para que muestre la máxima información posible y finalmente en el panel derecho hacer clic en "Aplicar".



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 zpser.as, 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 Default.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.

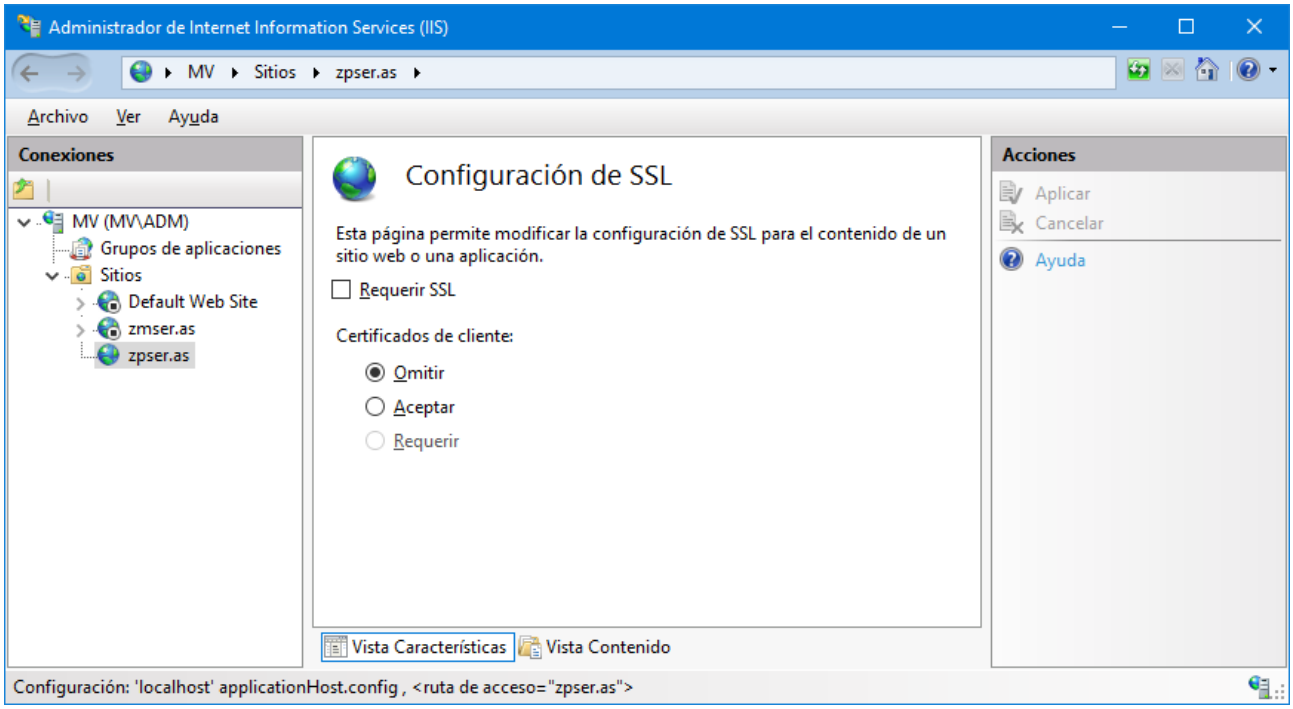
Para acelerar el desarrollo de la práctica, el fichero "Default.htm" con el código HTML se puede descargar del Campus Virtual.

```
<!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 zpser.as 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.

Inicialmente, no selecciones el uso de la tecnología SSL especifica de 40 bits.

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.

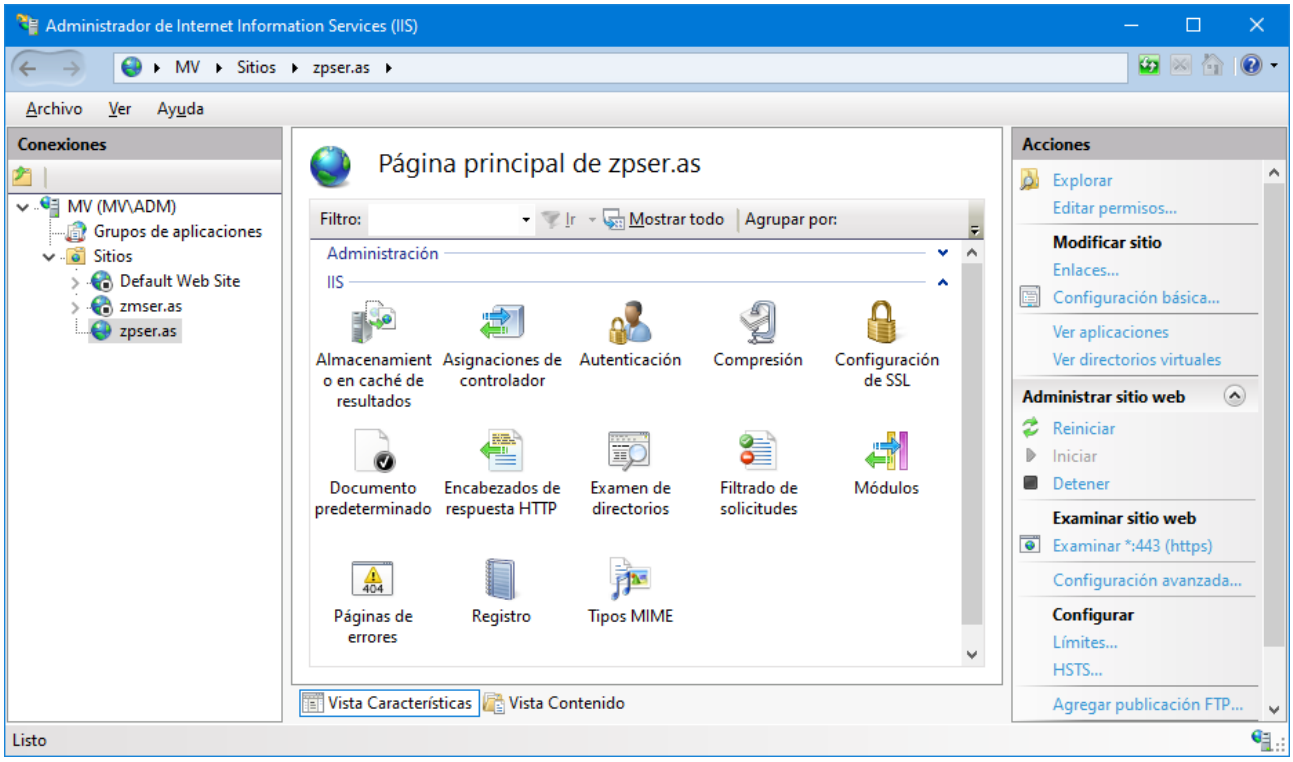
Inicialmente utiliza la opción predeterminada de Omitir. Posteriormente podrás experimentar con las otras opciones.

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 para probar el funcionamiento del servidor.

Observa el panel derecho de **Acciones** de la página principal del sitio web zpser.as:



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. También puedes acceder tú mismo desde tu propia máquina física.

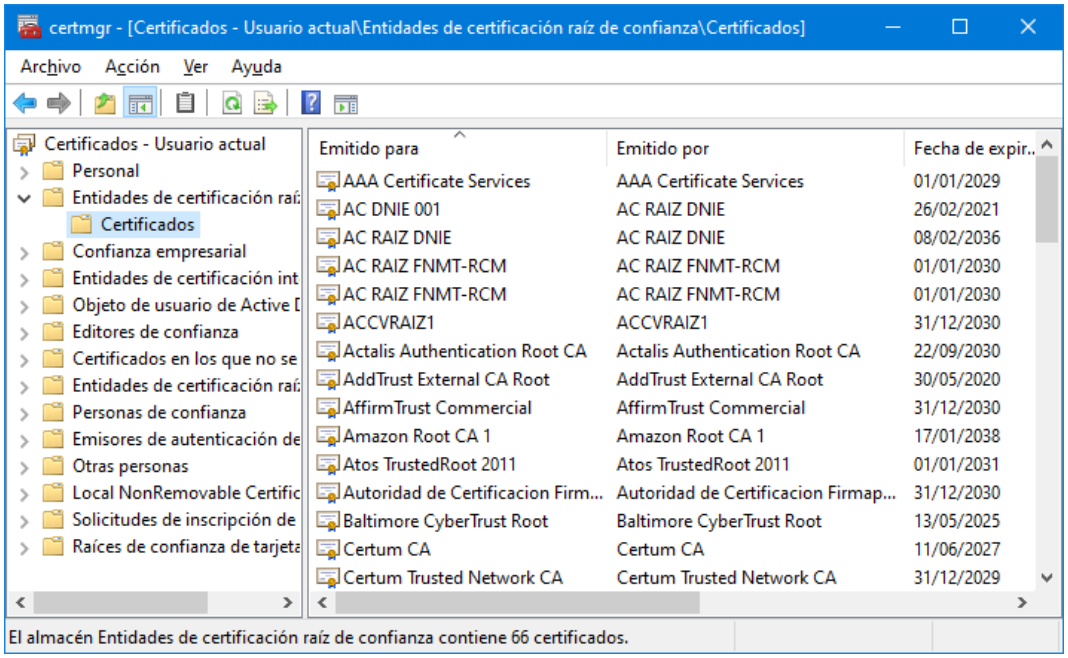
Aunque los navegadores indiquen que hay problemas, continuar el acceso hasta visualizar la página de bienvenida. Es lógico que haya problemas, pues aún no se han configurado los navegadores. Después de configurarlos, se harán pruebas de funcionamiento más detalladas.

PARAR LOS SERVIDORES WEB

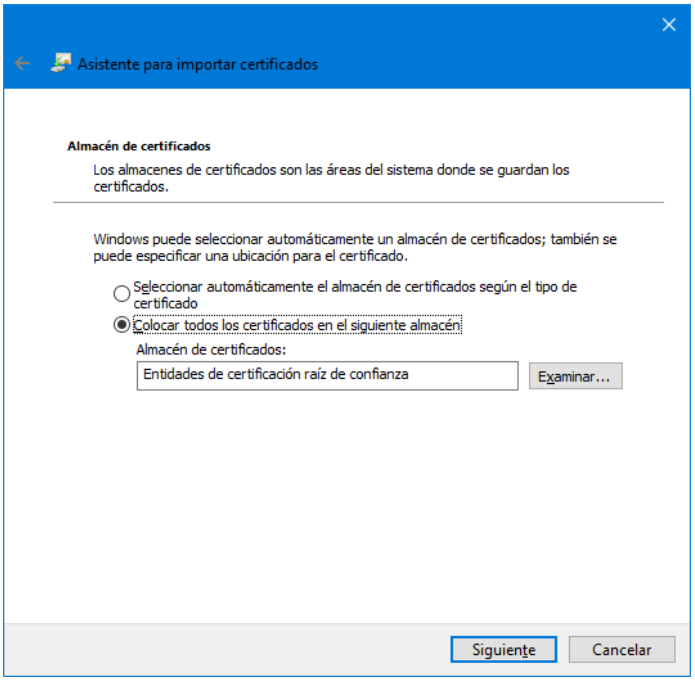
Observa que tras la instalación realizada hay dos servidores IIS en funcionamiento. Aunque no consumen muchos recursos, conviene detenerlos cuando no se vayan a utilizar e iniciarlos para realizar las pruebas. Las opciones Reiniciar/Iniciar/Detener están en el panel derecho de Acciones.

3. Preparación del navegador web

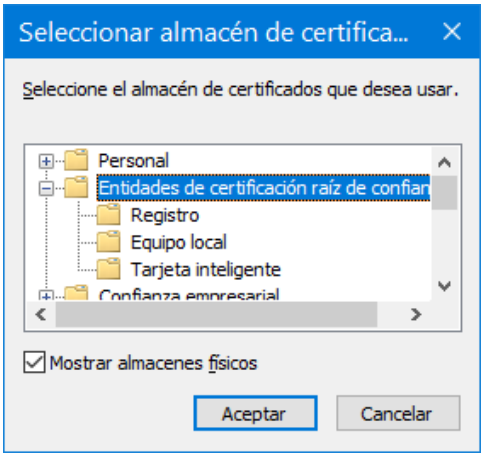
Para que el navegador pueda conectarse con éxito al sitio web debe tener instalado el certificado de la autoridad certificadora raíz de confianza que también ha emitido (firmado) el certificado del sitio web. Abrir la consola de administración de certificados tecleando en Inicio > Buscar programas y 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 zpACas.cer. Después elegir el almacén de certificados en el que se desea importar el certificado.

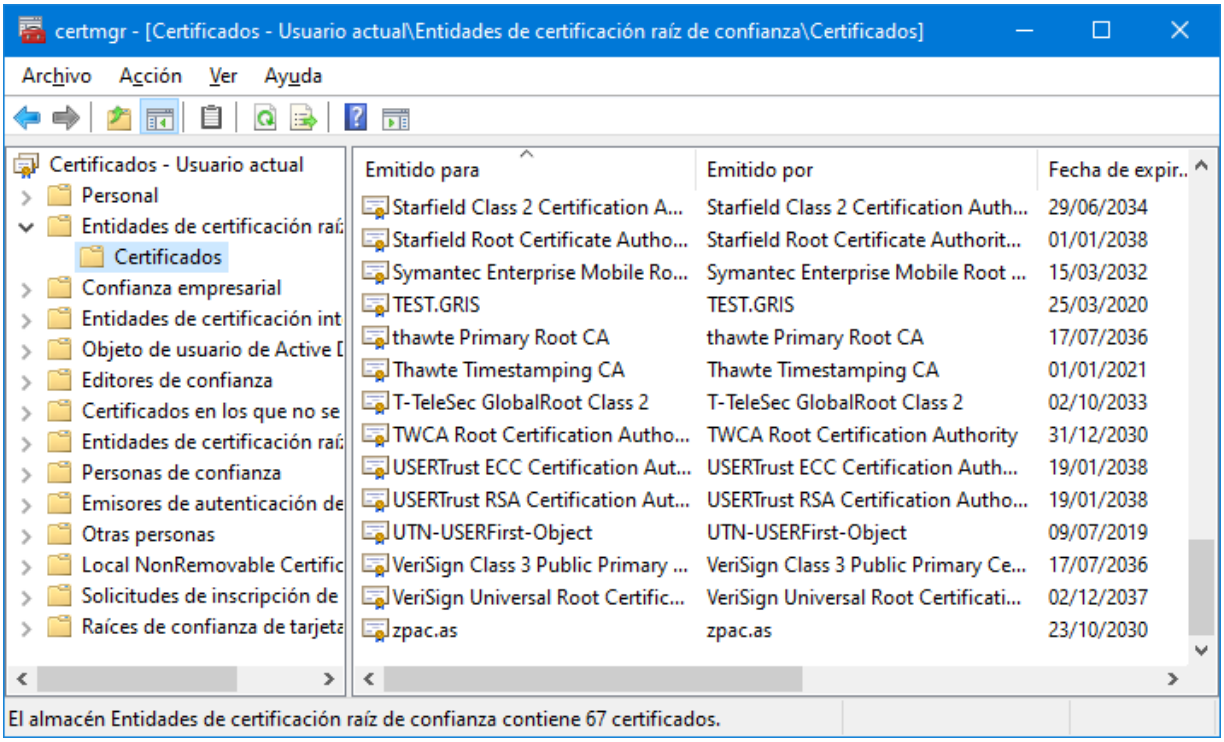


Si se desea tener un control mayor del almacén en el que se importa el certificado conviene pulsar el botón Examinar... y se despliega el cuadro de dialogo "Seleccionar almacén de certificados" en que se puede marcar la opción "Mostrar almacenes físicos".



Por ejemplo, elegir Equipo local.

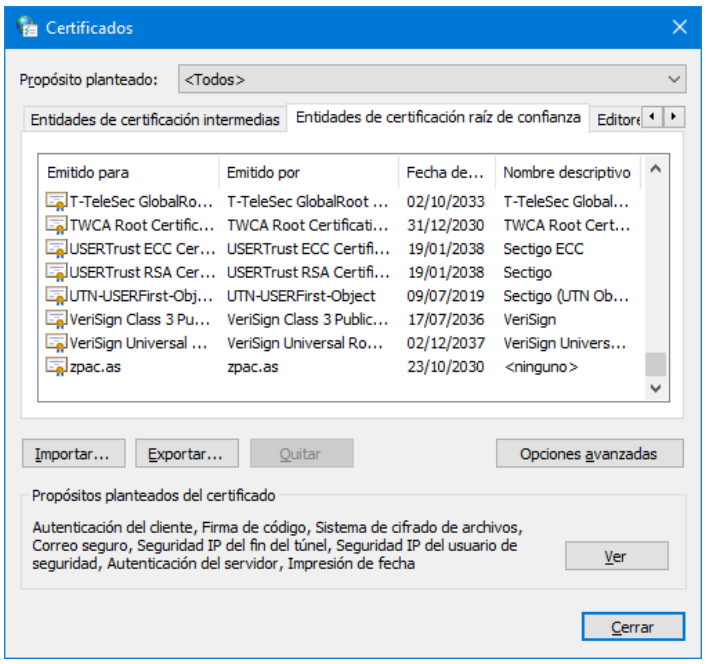
Para que la consola de administración de certificados muestre el nuevo certificado es preciso pulsar el botón Actualizar (sexto empezando por la izquierda, es una flecha circular verde).



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

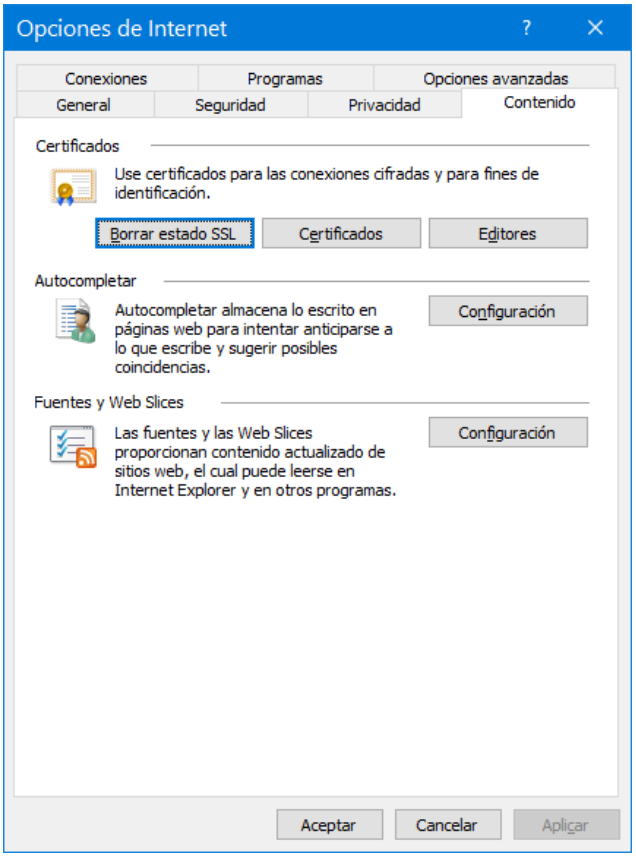
Comprueba ahora que el navegador Microsoft EDGE tiene acceso a los certificados.

Pulsa el botón “Configuración y más” (Alt+F), representado por ···, en la esquina superior derecha de la ventana de navegación. En el panel que aparece seleccionar la antepenúltima opción “Configuración”. En la nueva pestaña que aparece, selecciona en el panel izquierdo la opción “Privacidad, búsqueda y servicios”. Ahora, en el panel derecho, avanza hasta la sección “Seguridad” que contiene la opción “Administrar certificados”. Al seleccionar esta opción se abre el cuadro de diálogo “Certificados” que se muestra a continuación.



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

A este cuadro de dialogo también se puede acceder abriendo el “Panel de Control” y seleccionando “Opciones de Internet” para que aparezca la ventana siguiente.



En esta ventana, pulsando el botón “Certificados” aparece el cuadro de dialogo “Certificados”.

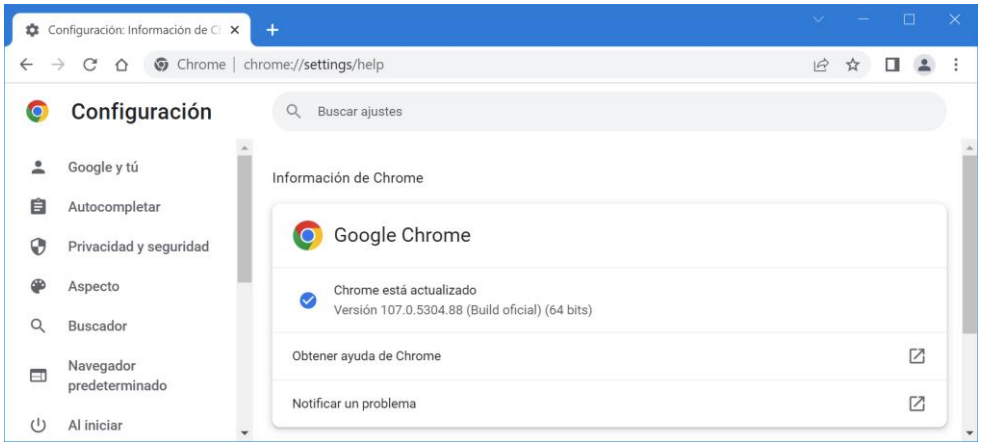
Configuración adicional de EDGE: En la sección “Borrar datos de exploración” utiliza la opción “Elegir que se debe borrar cada vez que se cierra el explorador” y selecciónalo todo. Con esta configuración, basta con cerrar el explorador y abrirlo nuevamente para realizar cada prueba.

ACTUALIZACIÓN DE LOS NAVEGADORES

Conviene tener los navegadores actualizados entes de realizar las pruebas.

El navegador **EDGE** se actualiza mediante las actualizaciones de Windows. Para comprobar la versión pulsa el botón "Configuración y más" (Alt+F), representado por ···, en la esquina superior derecha de la ventana de navegación. En el panel que aparece seleccionar la antepenúltima opción "Configuración". En la nueva pestaña que aparece, observar en la parte inferior la sección "Acerca de Microsoft Edge".

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 muestra una página en la que muestra la versión actual y la actualiza automáticamente.



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 panel 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.

4. Pruebas en la Máquina Virtual

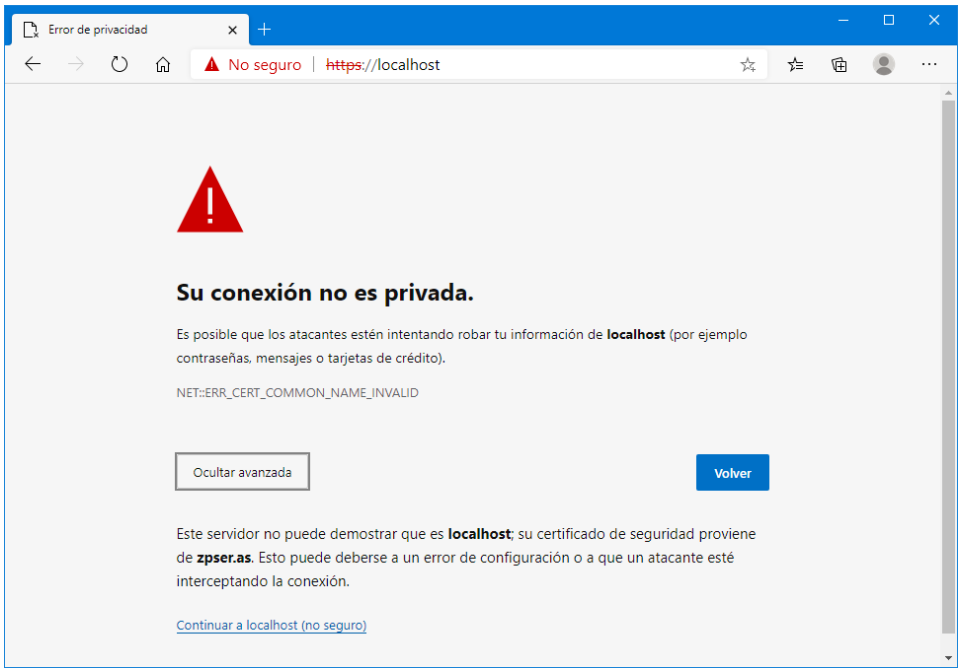
En la Máquina Virtual que funciona como servidor se puede abrir un navegador para usarlo también como cliente local.

Si dispones de poco tiempo, lee rápidamente esta sección y haz las pruebas solo con un navegador externo a la Máquina Virtual, tal como se indica en la sección siguiente.

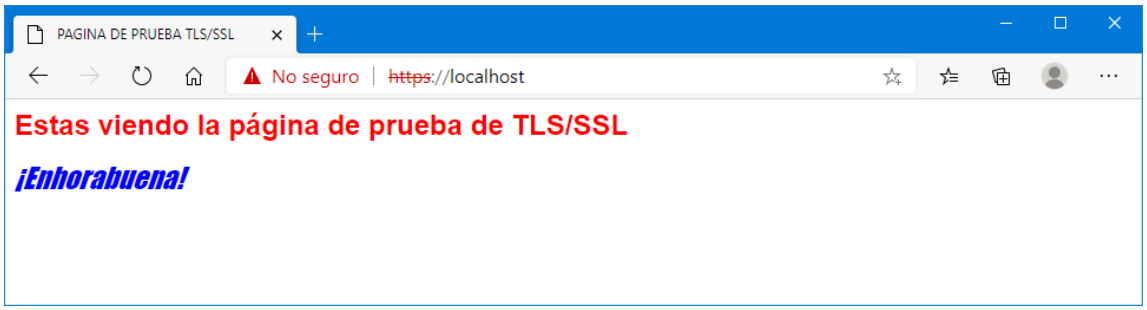
Primeramente, utiliza el navegador EDGE.

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

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

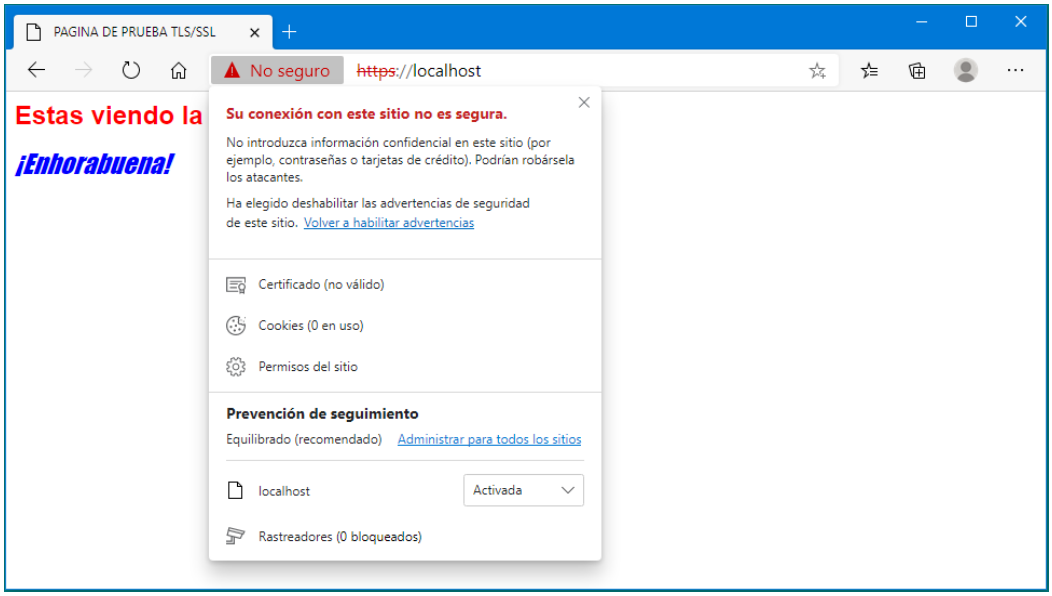


Seleccionado la opcion "Continuar a localhost (no seguro) se obtiene:



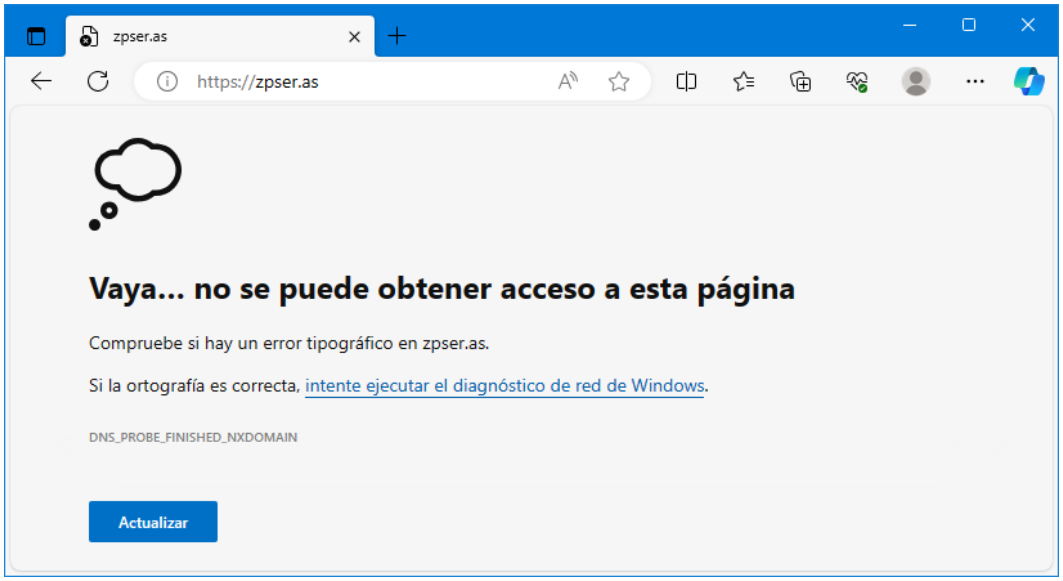
Se visualiza la página web de bienvenida del sitio seguro pero aparece un triángulo rojo indicando que el acceso no es seguro.

Al hacer clic sobre el triángulo se abre una ventana explicativa:



El certificado (no válido) ha sido emitido para zpser.as y no para localhost.

Comprueba que 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://zpser.as". 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 zpser.as

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

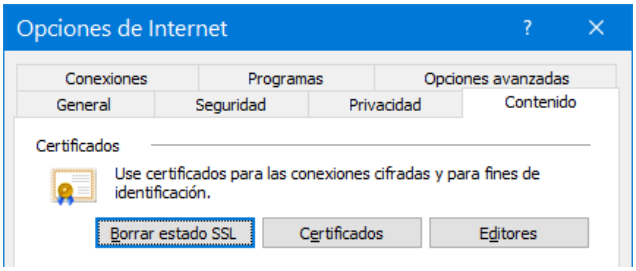
Para modificar el archivo hosts hay que ejecutar el editor como Administrador.

En Windows 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, tras navegar hasta el directorio indicado, cd simplemente teclear en la consola notepad hosts.

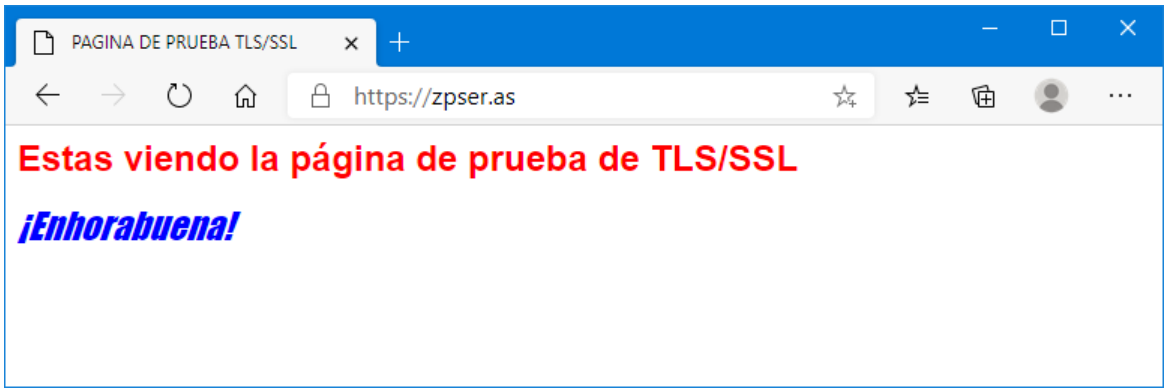
Tras incluircd divers\etc\hosts la línea en el archivo hosts, vuelve a acceder al sitio web seguro.

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.



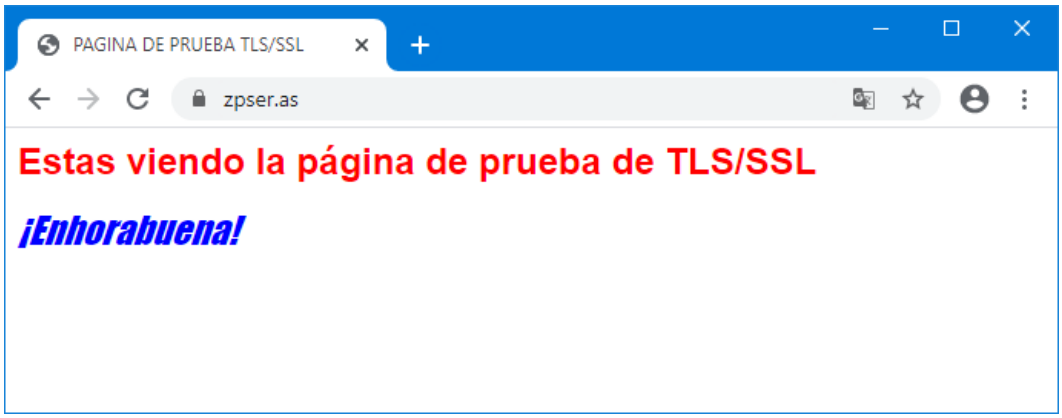
Acceder con EDGE a https://zpser.as

Se obtiene este resultado:



Accede con Google Chrome a https://zpser.as

Se obtiene este resultado:



5. Pruebas con un cliente (navegador) externo a la Máquina Virtual

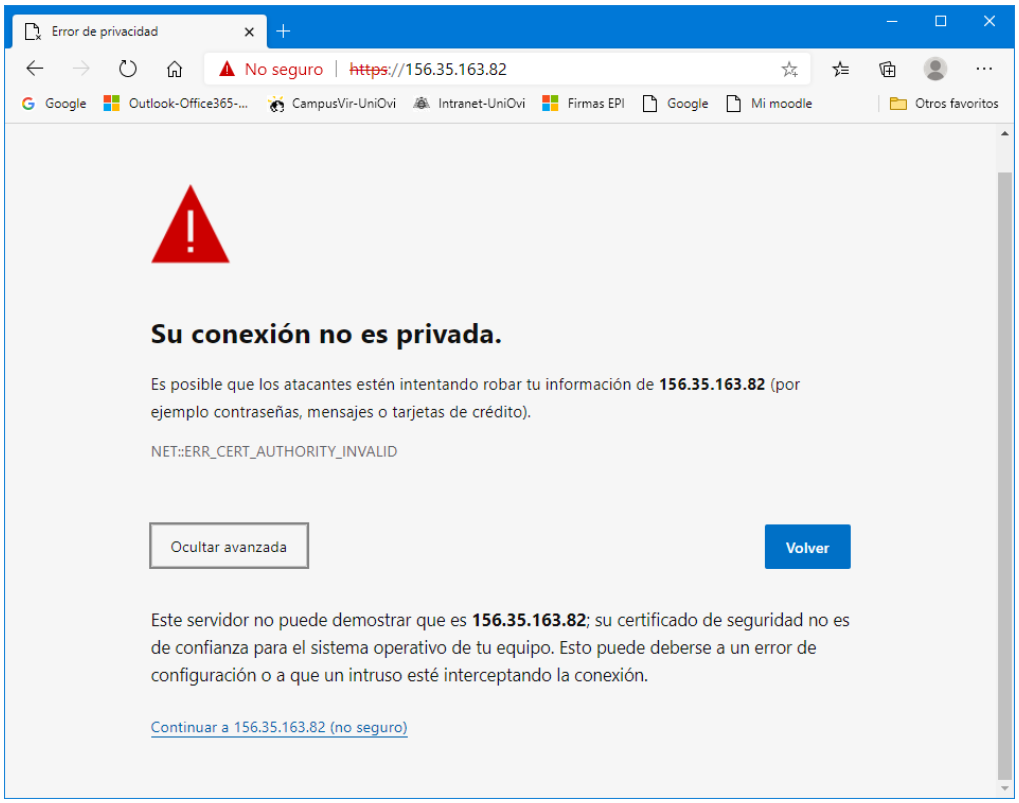
Realizar las mismas pruebas pero usando un cliente (navegador) en otro computador.

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.

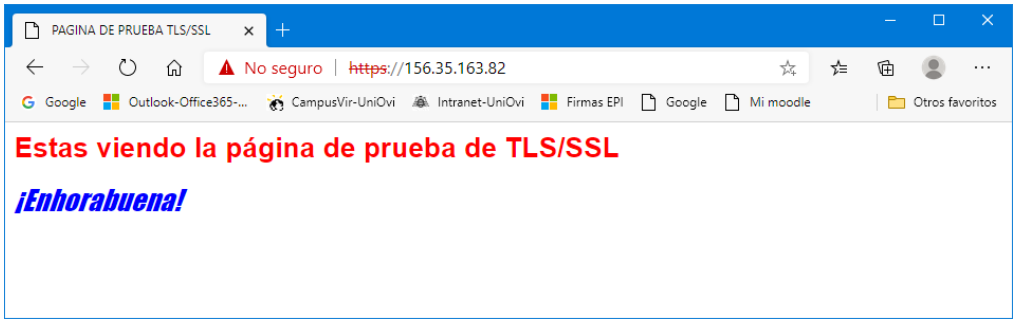
Recuerda que antes de realizar cada prueba conviene borrar el historial de navegación de los navegadores y el estado SSL.

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:



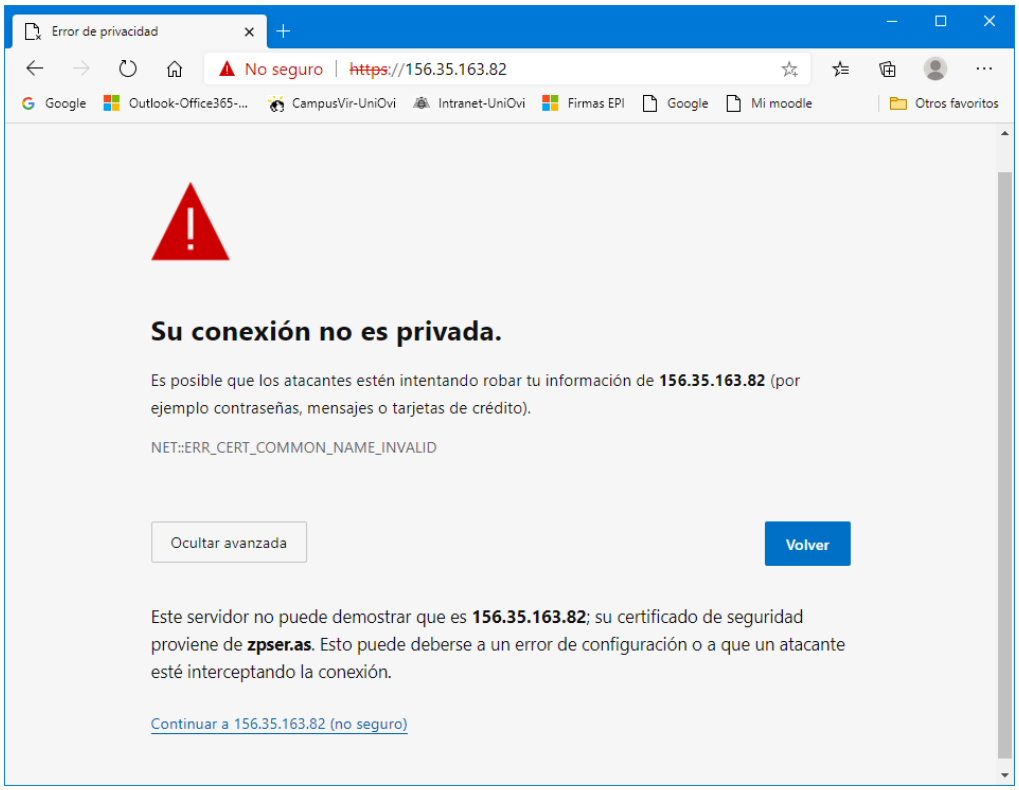
Tras seleccionar “Continuar a” se obtiene:



Observa que se indica la presencia del error “autoridad de certificación inválida”.

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: zpac.as.

Al volver a acceder a la dirección IP del servidor web seguro, tras instalar el certificado de zpac.as en el computador cliente, se obtiene:



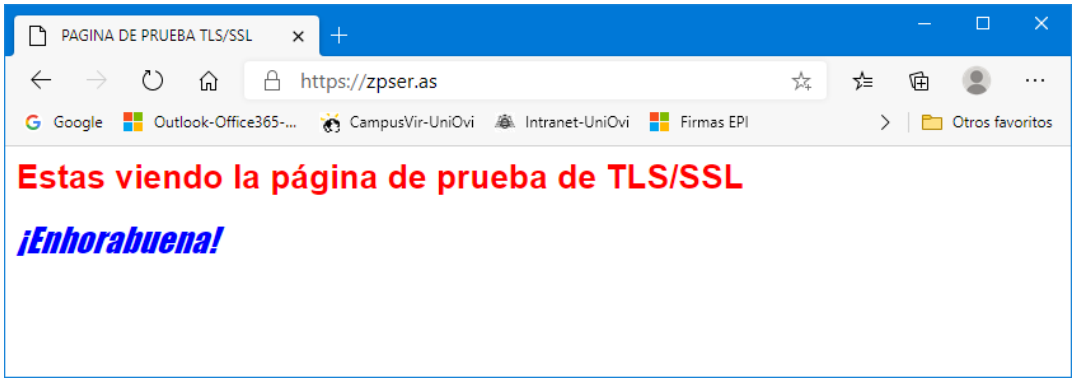
Observa que ahora se indica la presencia del error “nombre común del certificado inválido”.

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 realizada esta acción, se puede acceder directamente al sitio sin errores.

Accede con EDGE a https://zpser.as

Este el resultado al acceder:

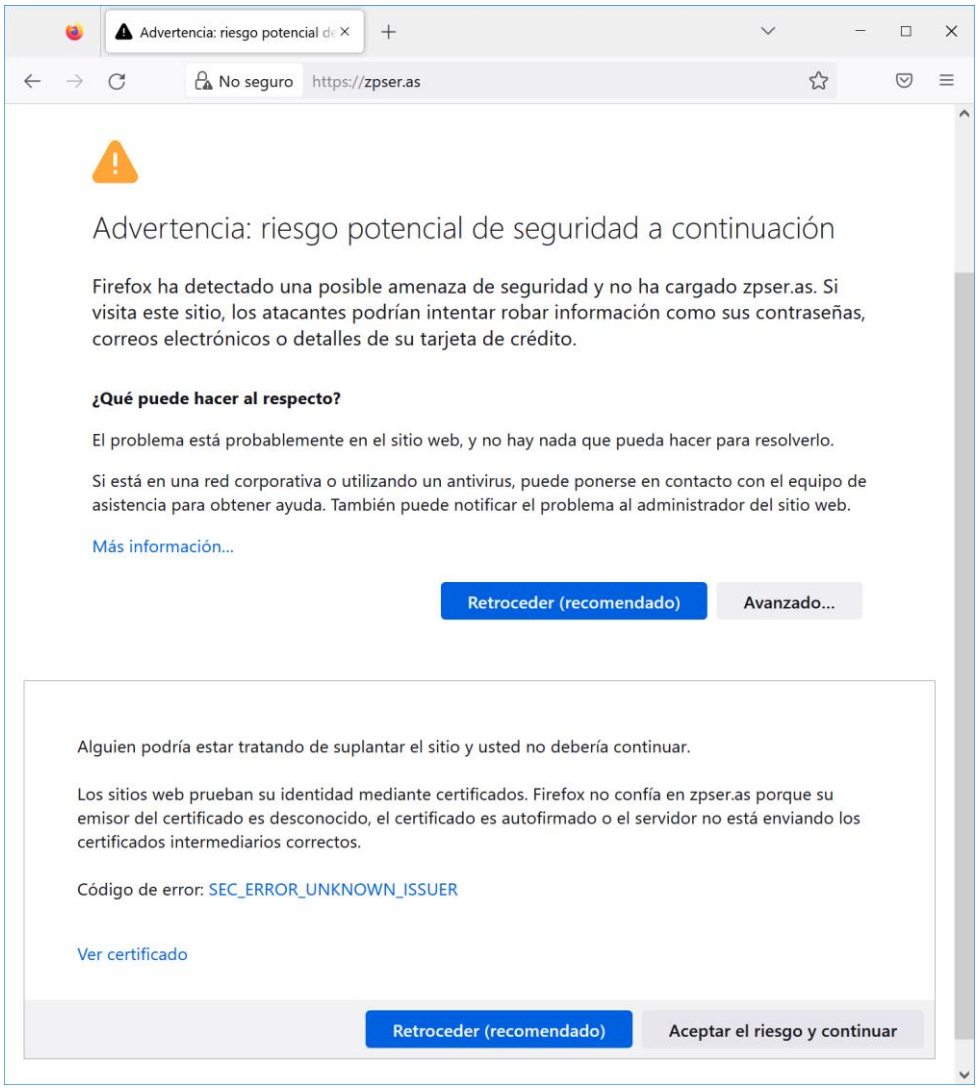


Pulsa en el candado que aparece a la izquierda del URL para ver la información del sitio web.

Accede con Firefox a https://zpser.as

Antes elimina el certificado de zpac.as del Almacén de Entidades de certificación raíz de confianza.

Dependiendo de la configuración del computador cliente, probablemente el navegador mostrará la siguiente ventana con una advertencia:



Esta advertencia se produce porque Firefox no reconoce el certificado emisor del certificado que ha recibido del servidor. Este problema surge porque Firefox utiliza su propio almacén de certificados, aunque las últimas versiones pueden usar los certificados del sistema operativo, aunque no está bien documentado el uso.

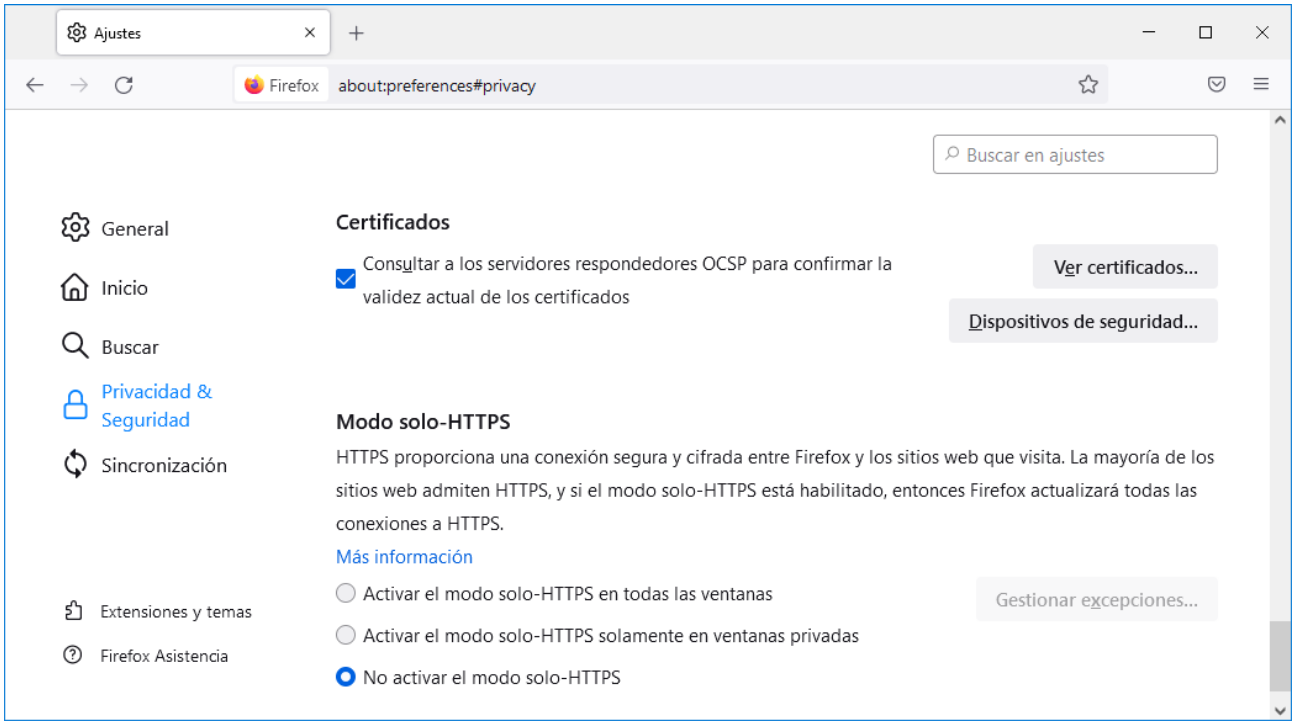
Para comprobar que Firefox utiliza sus propios certificados raíz de confianza, haz lo siguiente:

1) Borra el certificado de zpac.ser el almacén de entidades raíz de confianza de Windows.

2) Importa el certificado de la autoridad certificadora en el almacén de certificados de autoridades de Firefox. Procede del modo siguiente:

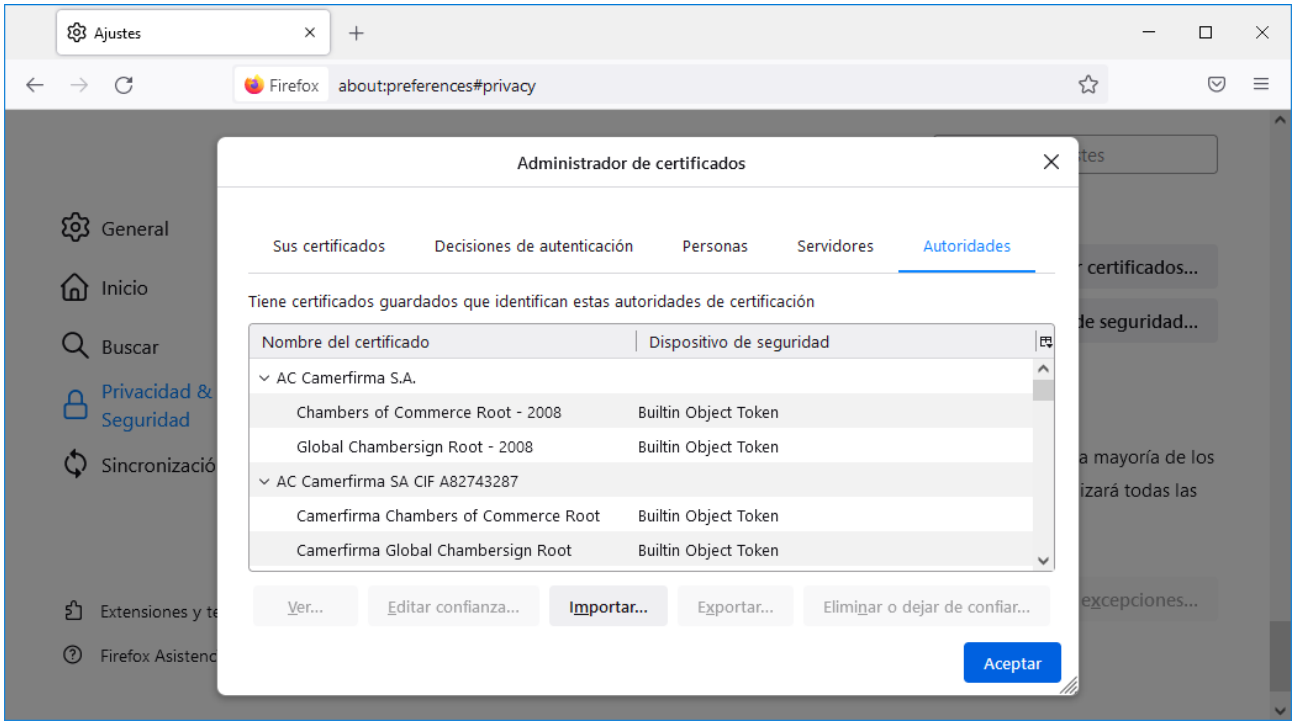
En cualquier página del navegador Firefox haz clic en el botón “menú” (tres barras horizontales) en la esquina superior-derecha. En la ventana que se abre selecciona “Ajustes”. Entonces se abre la página about:preferences en una nueva pestaña. En la página about:preferences selecciona “Privacidad & Seguridad” 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.

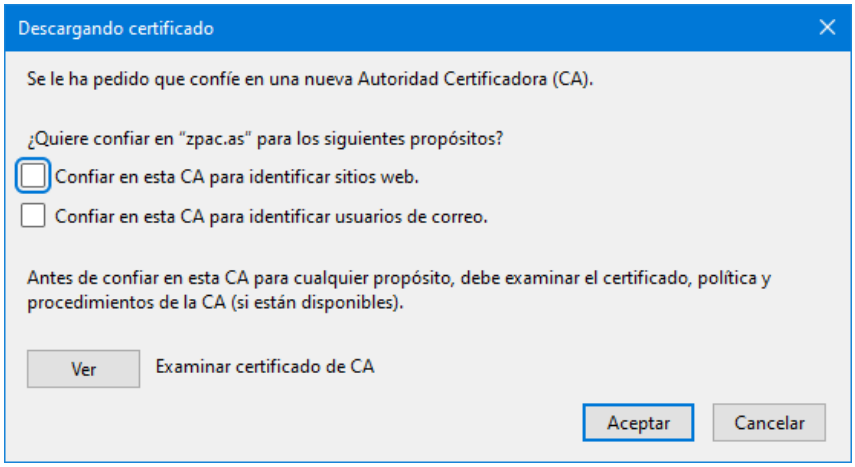
La figura siguiente muestra la ventana a la que hay que acceder.



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

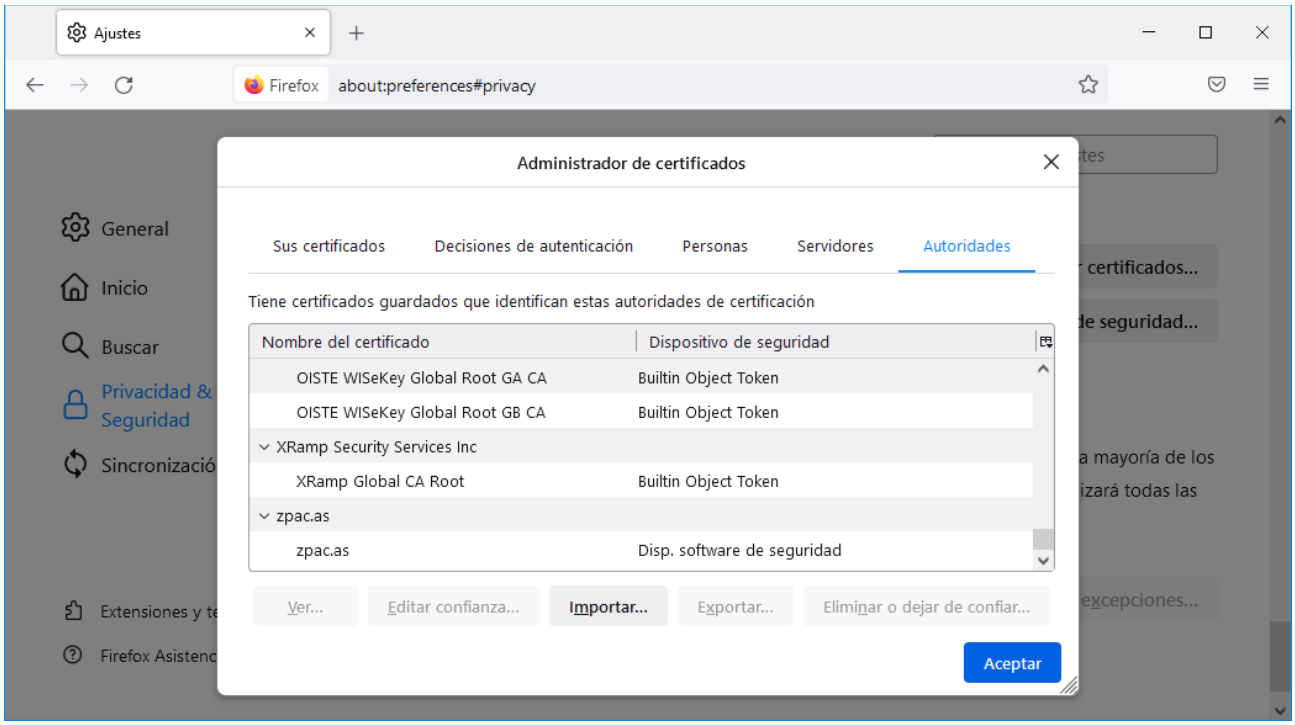
Pulsa el botón “Importar…” y se solicita un fichero con el certificado.

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

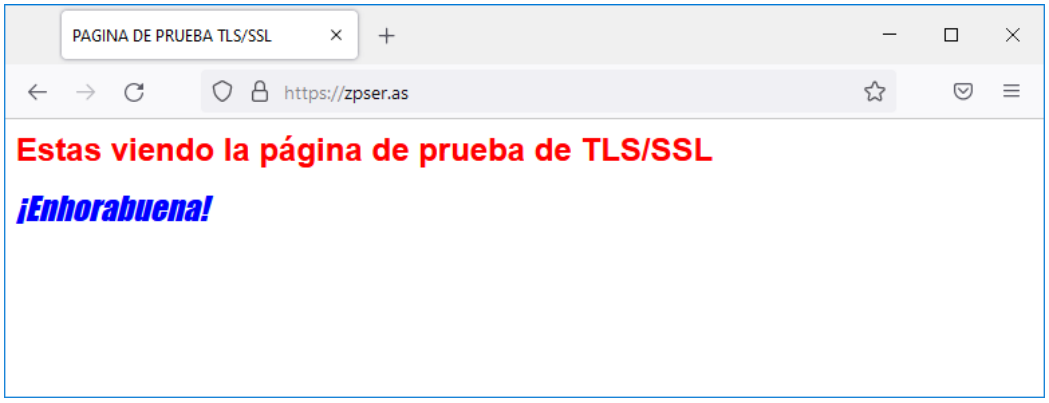


Tras marcar la primera opción pulsa el botón "Aceptar".

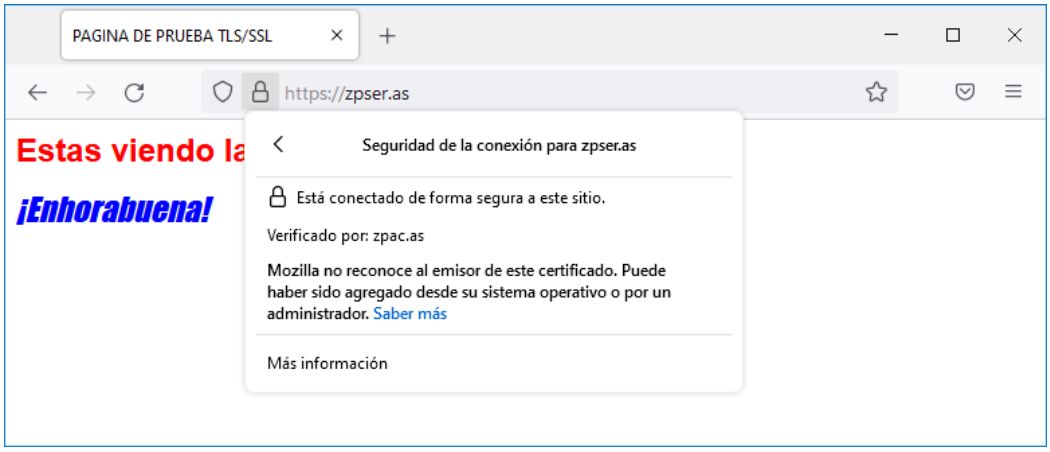
Ahora aparece el certificado en el almacén de Firefox.



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

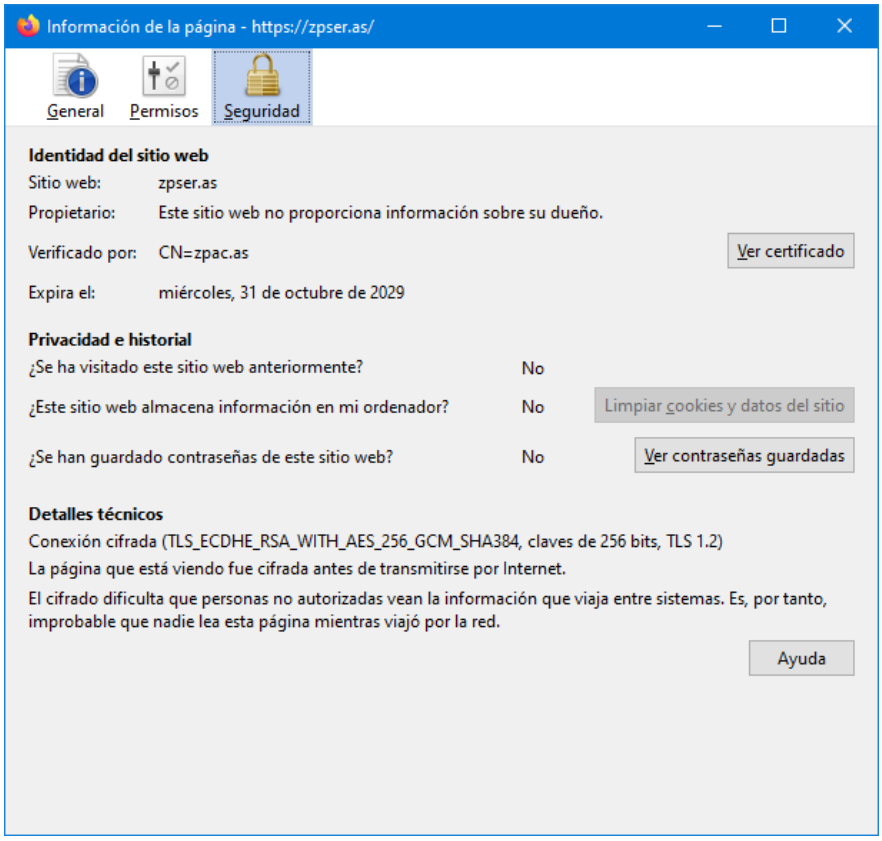


Haz clic sobre el candado para comprobar el estado de la conexión:



Selecciona el enlace “Más información” en la parte inferior de la ventana.

Firefox muestra la ventana siguiente con información detallada sobre el certificado, la conexión cifrada, etc.

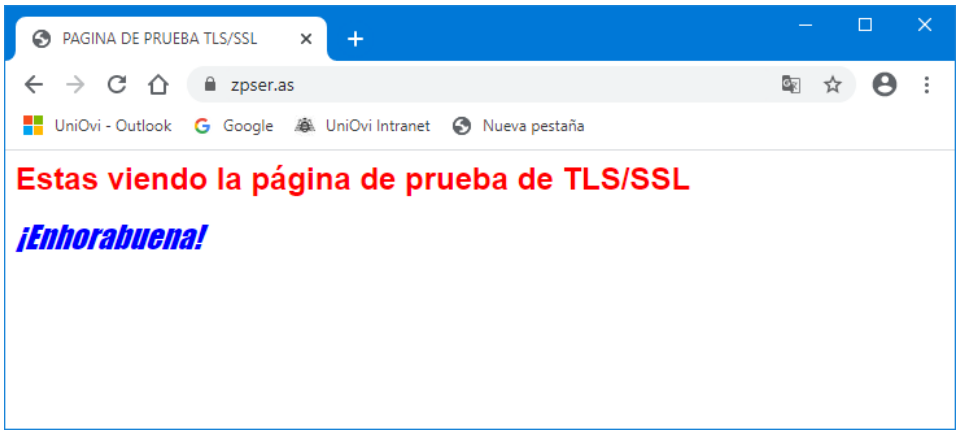


Accede con Chrome a https://zpser.as

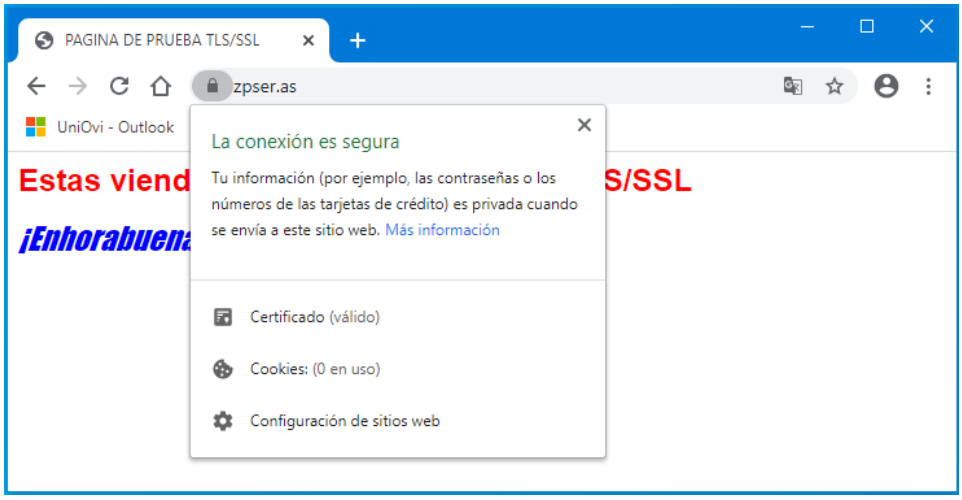
Antes de acceder al sitio web es conveniente borrar el historial de navegación de Chrome. Ir a Configuración > Privacidad y seguridad > Borrar datos de navegación.

Acuérdate de cargar nuevamente el certificado raíz de zpac.as en el almacén de certificados de las entidades raíz de confianza de Windows.

Comprueba que se accede directamente y sin problemas:



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

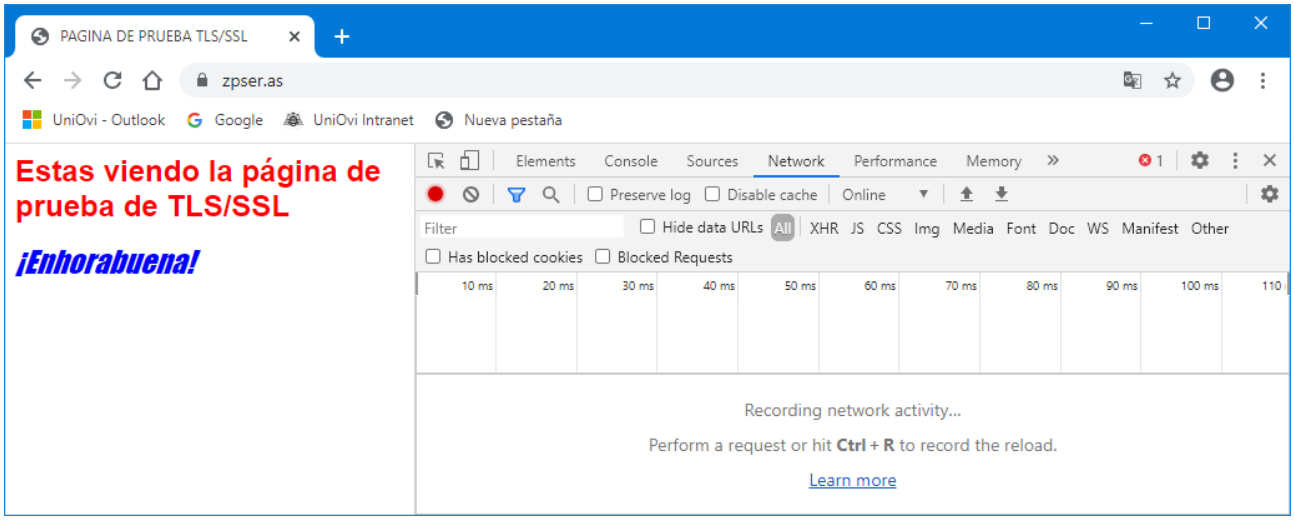


Este buen comportamiento del navegador Chrome se debe a que el certificado que envía el servidor incluye en la extensión “Nombre alternativo del titular” el valor “Nombre DNS=zpser.as”.

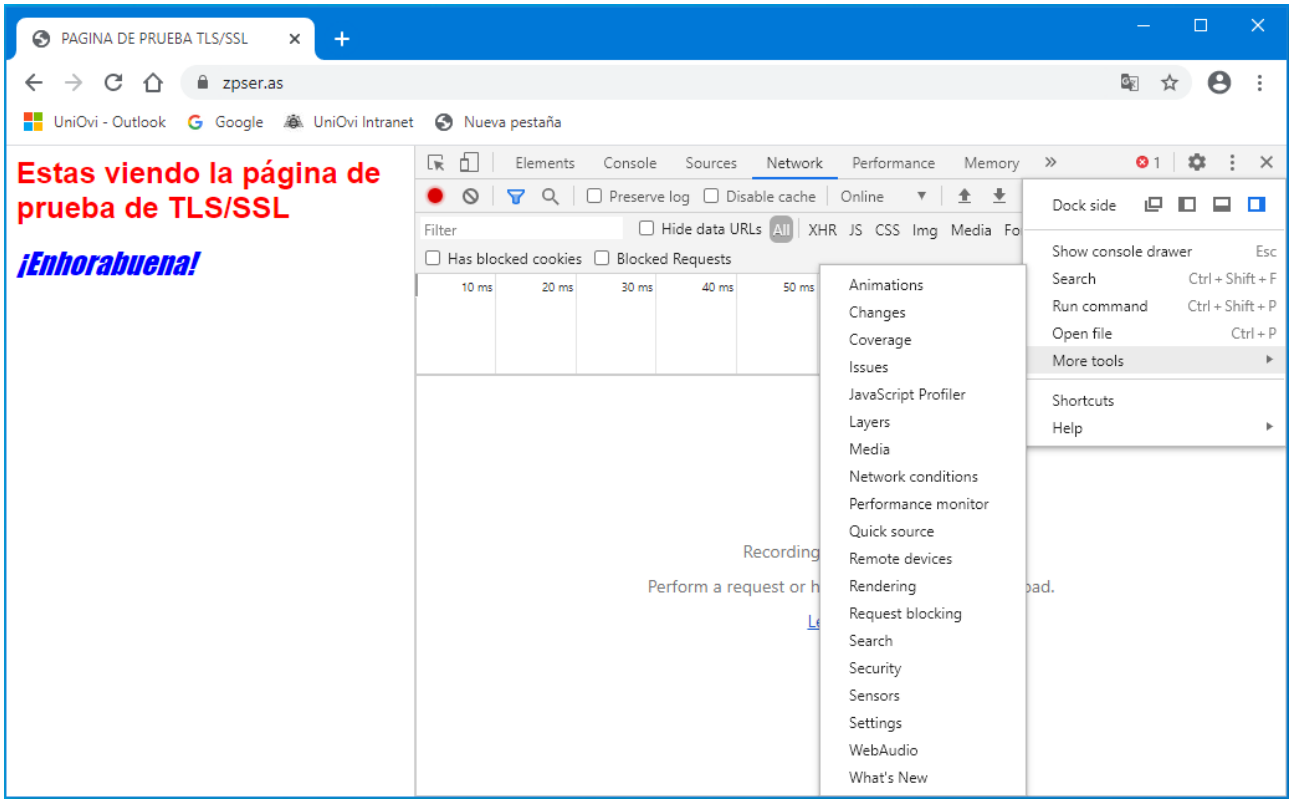
Este comportamiento se obtiene con la versión actual de Chrome, pero con versiones anteriores a la 58 el comportamiento era diferente: Chrome no utilizaba la extensión “Nombre alternativo del titular”.

Para ver más detalles sobre la conexión debes abrir las herramientas para desarrolladores de Chrome. Pulsa el botón “Personaliza y controla Google Chrome” representado por tres puntos verticales en la esquina superior derecha de la ventana de Chrome. En el menú emergente selecciona: Más herramientas > Herramientas para desarrolladores (Ctrl + Mayús + i). Para abrir/cerrar rápidamente las herramientas pulsa F12.

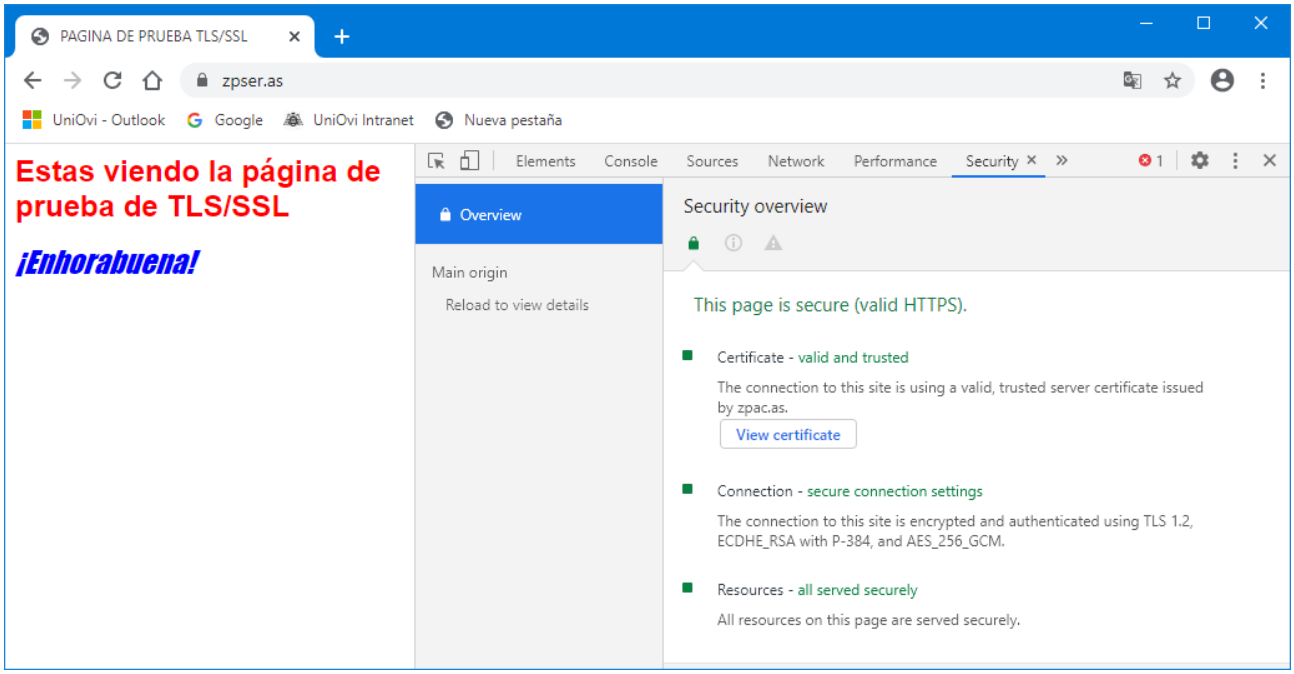
Se puede ver una ventana como la siguiente:



En el menú horizontal de herramientas busca la herramienta "Security". En la figura previa está abierta la herramienta Network. Selecciona >> en la barra horizontal para ver más elementos ocultos del menú. Si entre los nuevos elementos mostrados no está Seguridad, pulsa el botón con tres puntos verticales de la barra horizontal de herramientas y en el menú emergente selecciona "More tools". Tal como se ve en la figura siguiente, se muestran todas las herramientas disponibles, y puedes seleccionar la herramienta Seguridad.



Al seleccionar la herramienta Seguridad se muestra la ventana siguiente:



Observa que la conexión utiliza TLS 1.2 y un conjunto de algoritmos de cifrado concreto que usa DH, RSA y AES.

NOTA: El navegador EDGE (la nueva versión basada en chromium) se comporta exactamente igual que el navegador Chrome. Puedes comprobarlo si dispones de tiempo.

TAREA ADICIONAL:

Comprueba que **Chrome utiliza todos los nombres alternativos** del titular del certificado del servidor. Para ello accede al servidor utilizando:

https://www.zpser.es

https://www.zpser.com

Y comprueba que no es posible acceder con ellos.

Ahora edita el fichero hosts del computador cliente de modo que contenga las tres líneas siguientes:

A.B.C.D zpser.as

A.B.C.D www.zpser.es

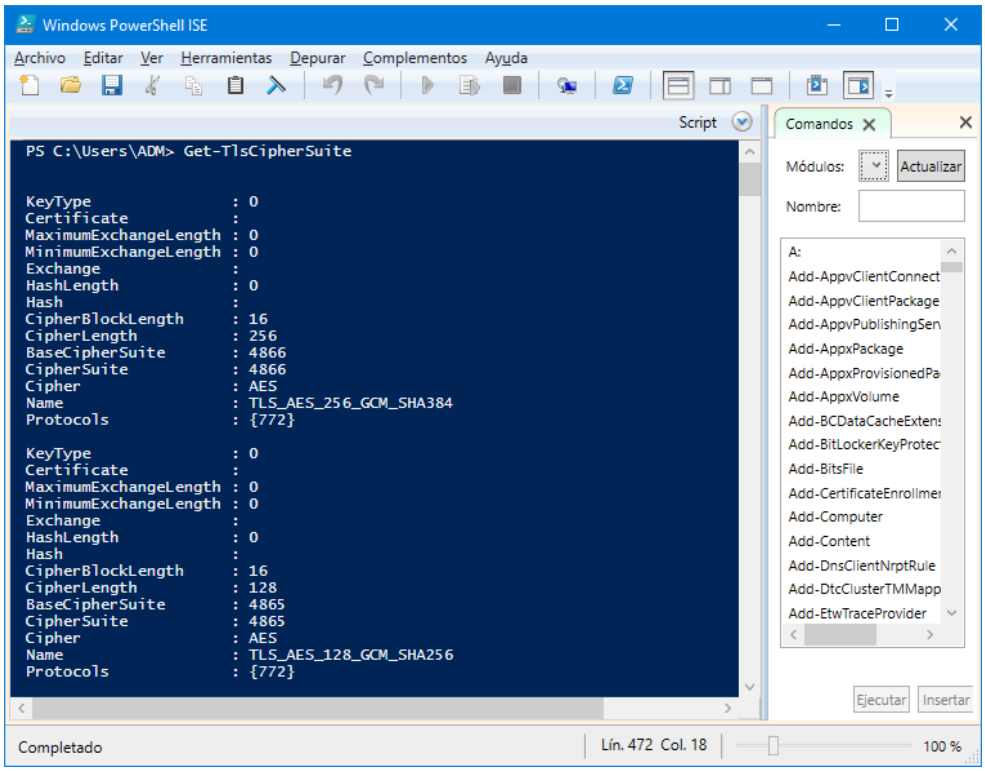
A.B.C.D www.zpser.com

Donde A.B.C.D es la dirección IPv4 del computador servidor.

Comprueba que ahora es posible acceder al servidor web seguro utilizando cualquiera de los tres nombres alternativos DNS.

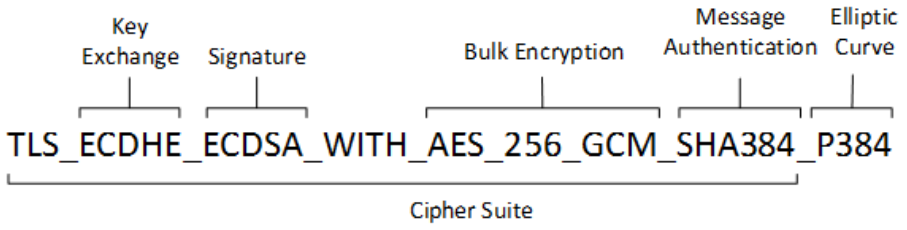
6. Visualizar los conjuntos de cifrado disponibles con PowerShell

Para visualizar los conjuntos de algoritmos de cifrado disponibles en un servidor se puede utilizar una consola de PowerShell y el cmdlet Get-TlsCipherSuite. La figura siguiente muestra un ejemplo de ejecución de este cmdlet, visualizando solo los dos primeros conjuntos.



Este cmdlet muestra los conjuntos de cifrado disponibles en orden de prioridad para establecer la conexión TLS.

El nombre del conjunto define los algoritmos de cifrado que están integrados en el conjunto. A continuación se muestra un ejemplo:



Observa que cada conjunto integra algoritmos para realizar diversas funciones:

- Intercambio de claves (*Key Exchange*)
- Firma (*Signature*)
- Cifrado masivo (*Bulk Encryption*)
- Autenticación de mensajes (*Message Authentication*)

Cada conjunto de cifrado se puede utilizar con unos protocolos determinados. Los protocolos se especifican mediante números decimales entre llaves. Cada número especifica una versión concreta

de un protocolo. Estos números se envían en los mensajes ClientHello y ServerHello en el handshake SSL/TLS. La tabla siguiente muestra los protocolos y los números utilizados para identificarlos.

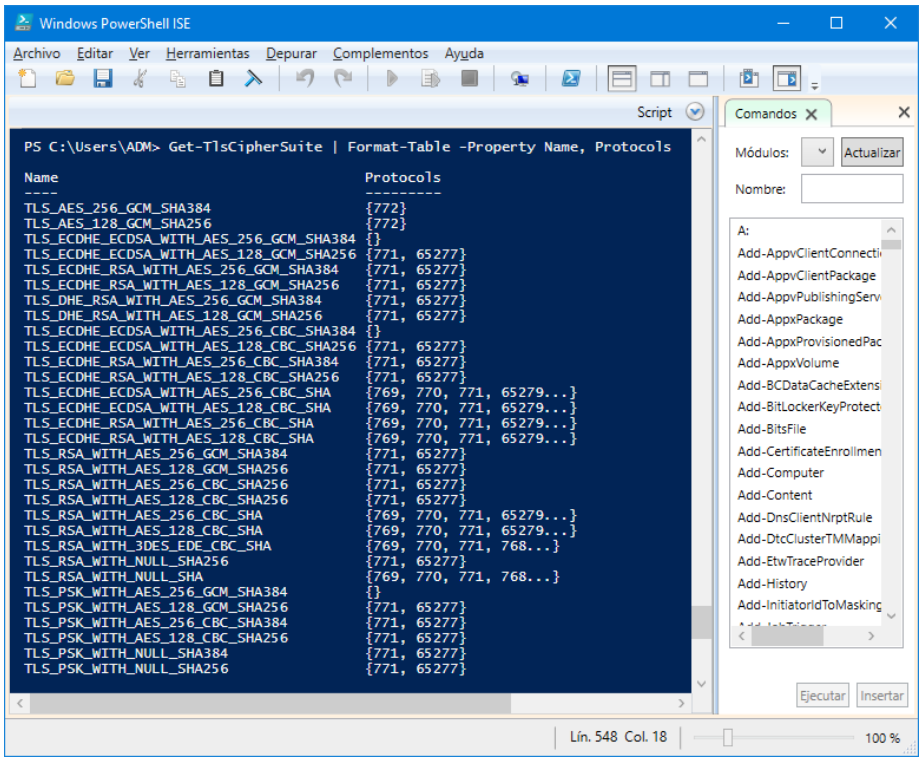
Protocolo	ID (hex)	ID (decimal)
SSL 2.0	0x0002	2
SSL 3.0	0x0300	768
TLS 1.0	0x0301	769
TLS 1.1	0x0302	770
TLS 1.2	0x0303	771
TLS 1.3	0x0304	772
DTLS 1.0	0xFEFF	65279
DTLS 1.1	0xFEFD	65277

NOTA: El protocolo DTLS proporciona privacidad en las comunicaciones para protocolos basados en datagramas, como UDP.

Ahora, genera nuevamente un listado de los conjuntos de cifrado, pero en un formato tabular, mostrando el nombre del conjunto y los protocolos que incluye. Utiliza el cmdlet siguiente:

```
Get-TlsCipherSuite | Format-Table -Property Name, Protocols
```

El resultado en un computador con Windows 10 puede ser el siguiente:



Observa los conjuntos de cifrado y los protocolos TLS y DTLS a los que se aplican.

7. Analizar el intercambio de paquetes con el protocolo TLS

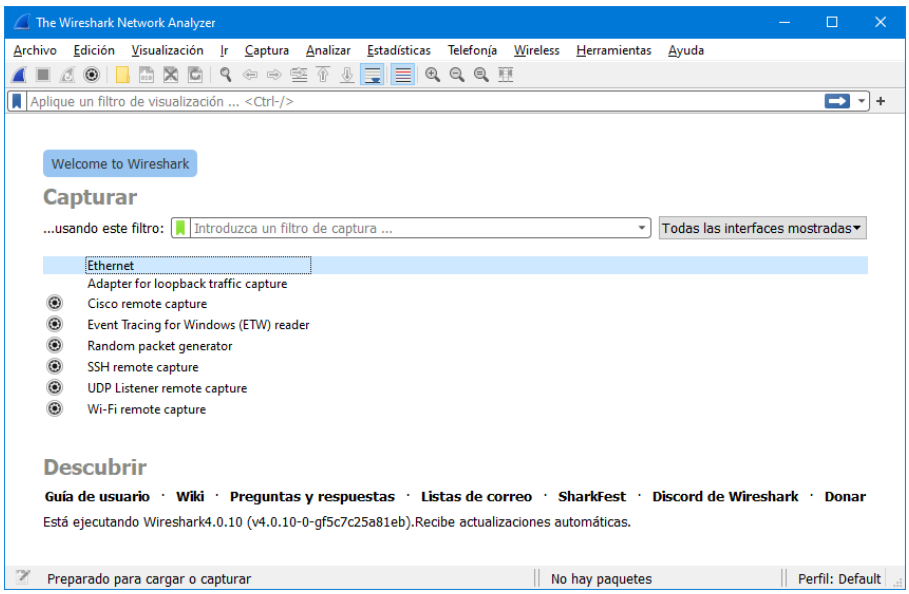
En esta sección de la práctica se analiza el intercambio de paquetes entre el servidor web y el cliente web (navegador web). Para ello, hay que utilizar un programa que permita analizar el tráfico entre el servidor y el cliente. Utilizar Wireshark que se debe descargar de su página web:

https://www.wireshark.org/download.html

Descargar y usar la versión portable para Windows x64 **en la Máquina Virtual de prácticas**. Para capturar paquetes de las interfaces de red Wireshark necesita el driver de red Npcap, que se debe descargar de su página web e instalar en la MV:

https://npcap.com/

Arranca Wireshark y podrás observar su interfaz:



Pulsa el primer botón por la izquierda (aleta de tiburón azul) para iniciar una captura.

Pulsa el segundo botón por la izquierda (cuadro rojo) para parar la captura.

En pocos segundos se pueden capturar miles de paquetes, sin generar tráfico deliberadamente usando aplicaciones.

Descarta los paquetes capturados que se muestran en la interfaz.

Desarrolla un filtro de captura de paquetes

El filtro es una línea que se introduce en el cuadro para el filtro en la interfaz de Wireshark que se muestra en la figura previa. Pulsa el botón verde en el extremo izquierdo del cuadro. Verás que puedes seleccionar uno de los filtros predefinidos disponibles, por ejemplo el denominado HTTP TCP port (80). Si arrancas la captura con este filtro es probable que se capturen pocos paquetes o incluso ninguno. Elimina el filtro pulsando el botón rojo en el extremo derecho del cuadro.

Un filtro de captura tiene el formato de una secuencia de primitivas conectadas por las conjunciones “and o or” y opcionalmente precedidas por “not”.

[not] primitiva [and|or [not] primitiva …]

Ejemplo: tcp port 23 and host 10.0.0.5

Este filtro captura todo el tráfico tcp con el puerto 23 (telnet) desde y hacia el host 10.0.0.5 y muestra el uso de dos primitivas y la conjunción and.

[tcp|udp] [src|dst] **port** <port>

> Esta primitiva permite filtrar por números de puerto. Usar tcp o udp para indicar el tipo de protocolo a considerar para el puerto indicado. Si no se usan se capturan paquetes para ambos protocolos. Usar src o dst para capturar solo los paquetes en los que aparece el puerto indicado como origen o como destino.

[src|dst] **host** <host_IP/name>

> Esta primitiva permite filtrar por la dirección IP o nombre de un host. Usando src solo se capturan los paquetes en los que la dirección IP aparece como origen y usando dst solo se capturan los paquetes en los que la dirección IP aparece como destino. Si no se especifica src o dst los paquetes en los que aparece la dirección IP, bien como origen o como destino, son capturados.

DESARROLLA un filtro que permita ver el tráfico entre el servidor web seguro y un navegador web, minimizando el número de paquetes capturado que no corresponden al tráfico de interés.

Una vez introducido y probado el filtro conviene guardarlo en un fichero.

Análisis de paquetes intercambiados con una configuración correcta

Configura correctamente los certificados en la máquina virtual (MV) y en la máquina física (MF).

Arranca el servidor web seguro en la MV.

Arranca el navegador web en la MF e introduce la URL del servidor web seguro, pero no la lances.

Borra el estado SSL en la MV y en la MF.

Arranca Wireshark en la MV y selecciona el filtro de paquetes desarrollado.

Lanza la petición desde el navegador web.

Para Wireshark después de que la página web se haya cargado en el navegador.

Analiza la secuencia de paquetes capturados que Wireshark muestra en su interfaz.

¿Puedes localizar ClientHello? ¿Qué versión de TLS se está utilizando?

¿Le sigue ServerHello? ¿Hay otros mensajes “lógicos” del protocolo TLS que han sido integrados en el mismo paquete TCP con el mensaje ServerHello?

¿Detectas luego el mensaje ClientKeyExchange? ¿Hay más mensajes del cliente integrados en el mismo paquete TCP?

¿Aparece finalmente el mensaje ChangeCipherSpec que envía el servidor?

Comprueba si hay fallos y reinicios del protocolo en la secuencia de paquetes.

Análisis de paquetes intercambiados con una configuración correcta

Elimina el certificado raíz de la MF y vuelve a repetir el proceso anterior. Comprueba si se aborta el handshake, y si se realicen varios intentos para establecer la conexión cifrada.

8. Crear un nuevo sitio web usando los certificados generados con MakeCert

El objetivo de esta sección de la práctica es comprobar la influencia de las características del certificado utilizado para crear un sitio web seguro.

Utiliza los certificados generados con MakeCert, disponibles en el Campus Virtual en la práctica 7. El nombre del servidor es zmSER.as y el de su raíz es zmAC.as.

Sigue los pasos ya explicados en esta práctica, que se recuerdan brevemente:

1.-Carga el certificado raíz de zmAC.as en el almacén de certificados "Entidades de certificación raíz de confianza". Cárgalo en el almacén de la máquina, no en el del usuario. Comprueba que el certificado raíz está disponible con la herramienta **Certlm.msc**, y NO con Certmgr.msc.

2.-Abre Inetmgr y úsalo para cargar el certificado de servidor de zmSER.as en el almacén de certificados "Hospedaje de sitios web" junto con su clave privada asociada, a partir del fichero zmSERas.pfx.

3.-Crea un directorio para los ficheros del nuevo sitio web. Ej.: C:\intepub\wwwroot\zmser

4.-Crea y configura un nuevo sitio web igual que el anterior pero usando como nombre del sitio el nombre del nuevo certificado: zmSER.as.

Conviene modificar el contenido del fichero Default.htm para ver que se accede al nuevo sitio. Modificar la línea de presentación y, por ejemplo, poner:

"Sitio web zmSER.as – Página de prueba TLS/SSL"

5.-Prepara el computador cliente.

Incluye en el fichero C:\Windows\System32\drivers\etc\hosts la línea:

A.B.C.D zmSER.as

Donde A.B.C.D es la dirección IPv4 del servidor web.

Carga el certificado de zmAC.as, raíz de zmSER.as, en el almacén de certificados "Entidades de certificación raíz de confianza". Cárgalo en el almacén del usuario, no en el de la máquina.

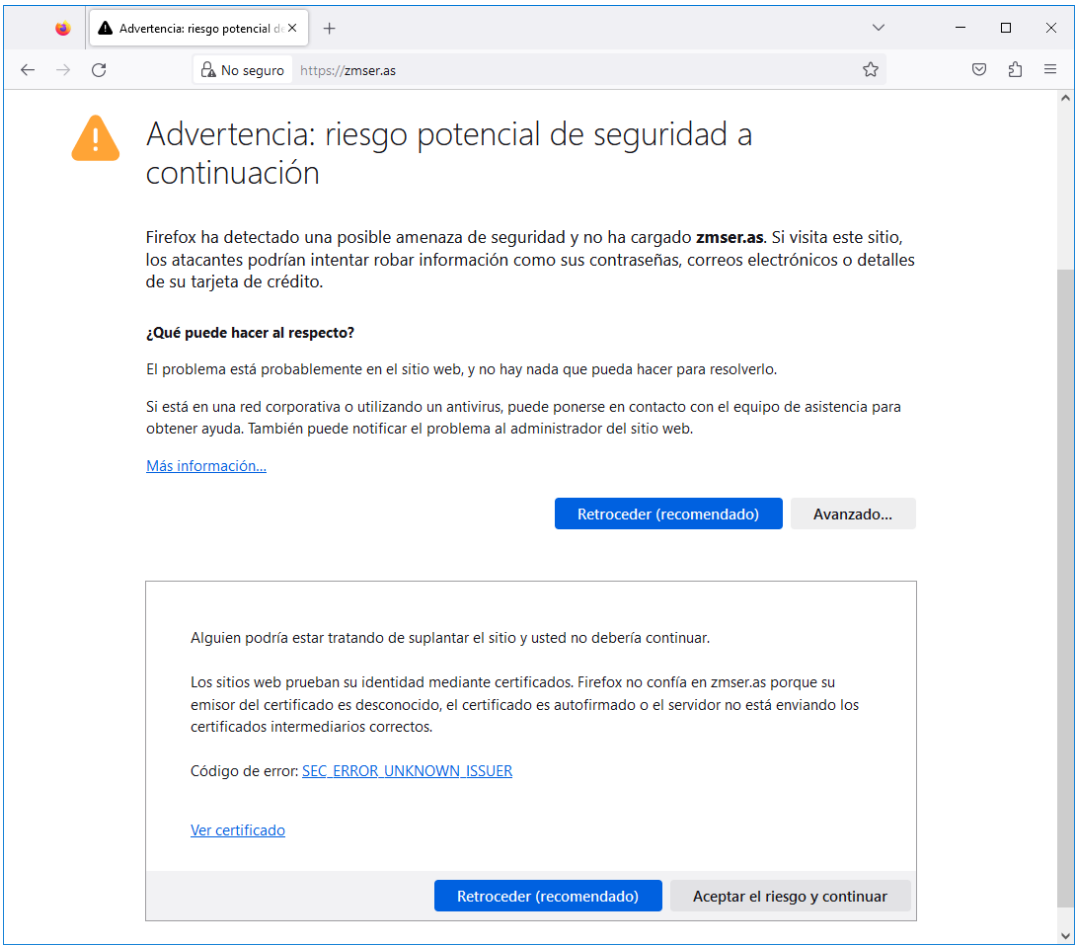
6.-Realiza pruebas de acceso al sitio web zmSER.as desde el computador cliente.

IMPORTANTE:

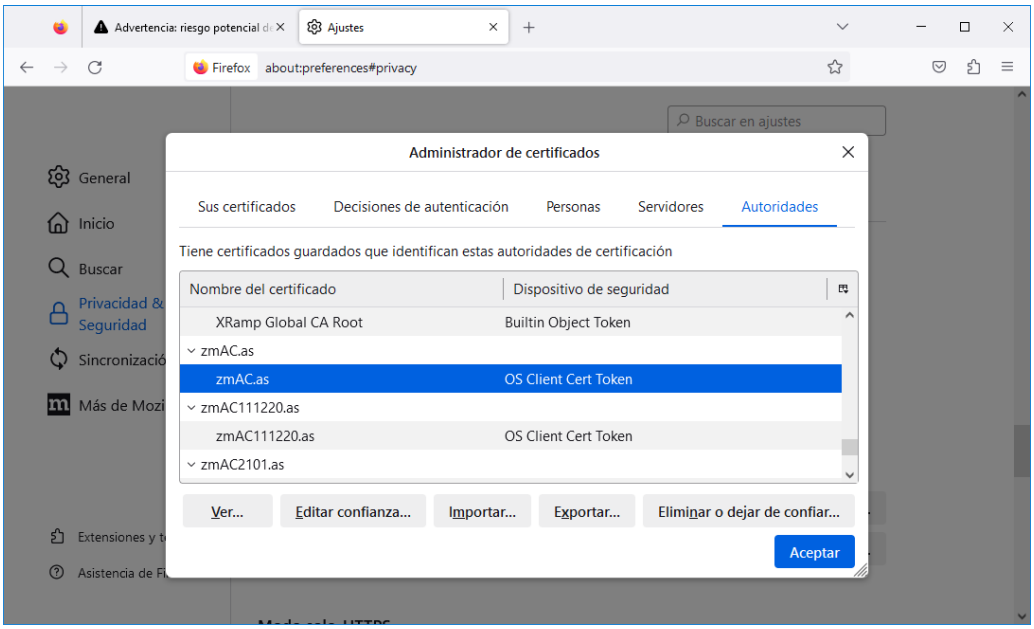
El servidor IIS puede almacenar múltiples sitios web, como zpser.as y zmser.as. Si estos dos sitios usan la misma IP y puerto no deben estar arrancados a la vez.
No debería haber ningún problema para usar un sitio web o el otro y tener los certificados de ambos sitios el almacén de certificados "Hospedaje de sitios web".

PERO…
Si se observan problemas, por ejemplo, que el servidor IIS cuando tiene arrancado el sitio zpser.as envía el certificado de zmser.as, o viceversa, lo mejor es tener en el IIS solo uno de los servidores y solo su certificado para hacer las pruebas.

El **acceso con Firefox** puede generar problemas, porque Firefox no reconoce a la autoridad certificadora que ha emitido el certificado de zmSER.as.

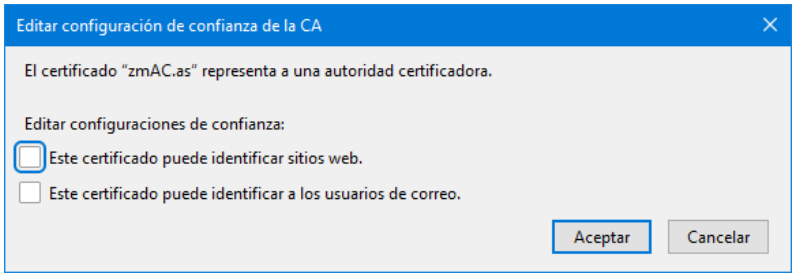


Accede al almacén de certificados de Autoridades de Firefox:



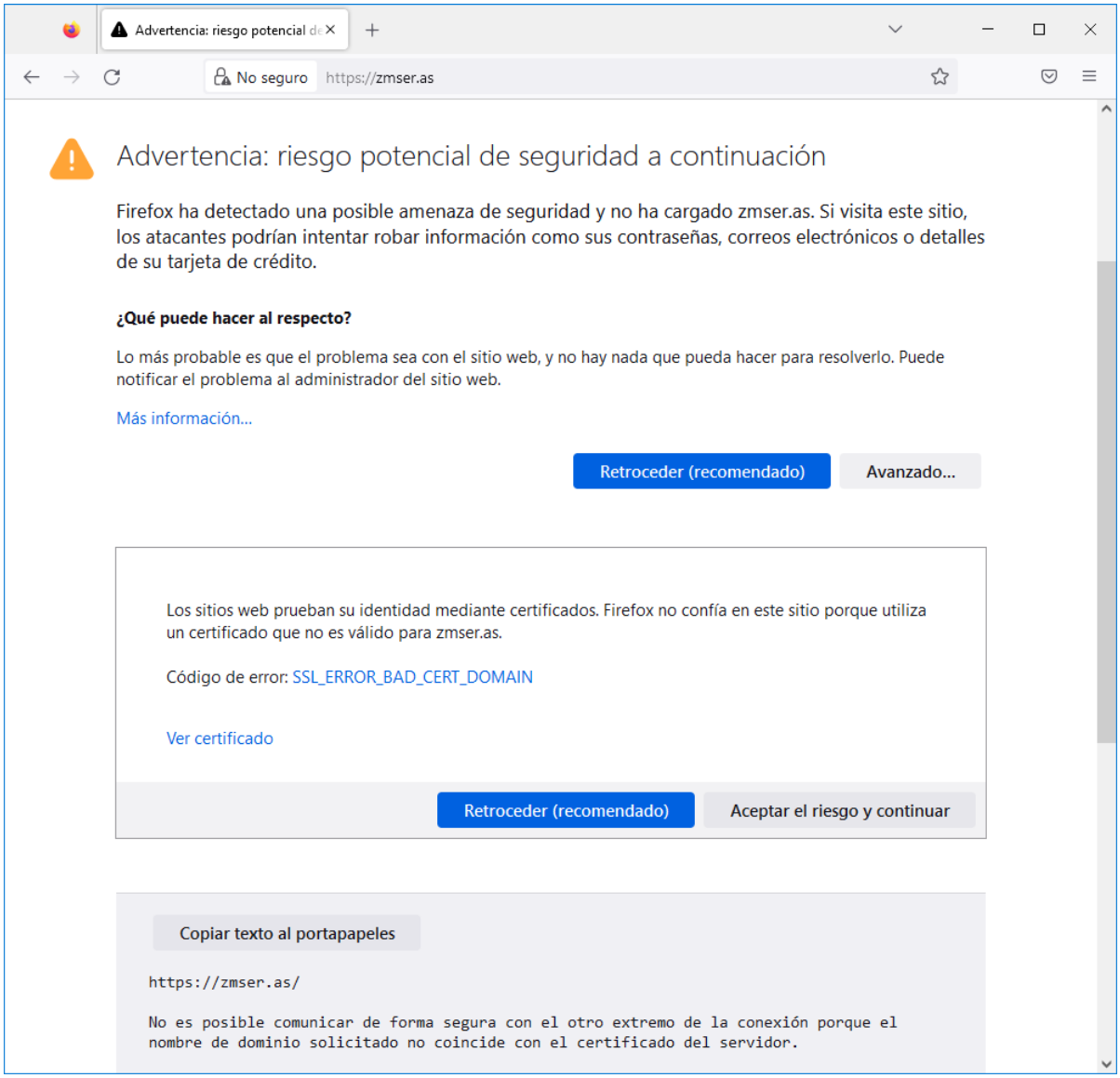
Se puede observar que Firefox tiene acceso al certificado emisor (zmAC.as) del certificado recibido del servidor web (zmSER.as), pero a través del almacén de certificados del sistema operativo Windows (OS Client Cert Token), ya que el certificado de zmAC.as no está instalado en el almacén de certificados de Firefox (Builtin Object Token).

Pulsa el botón “Editar confianza…” y aparece la ventana:

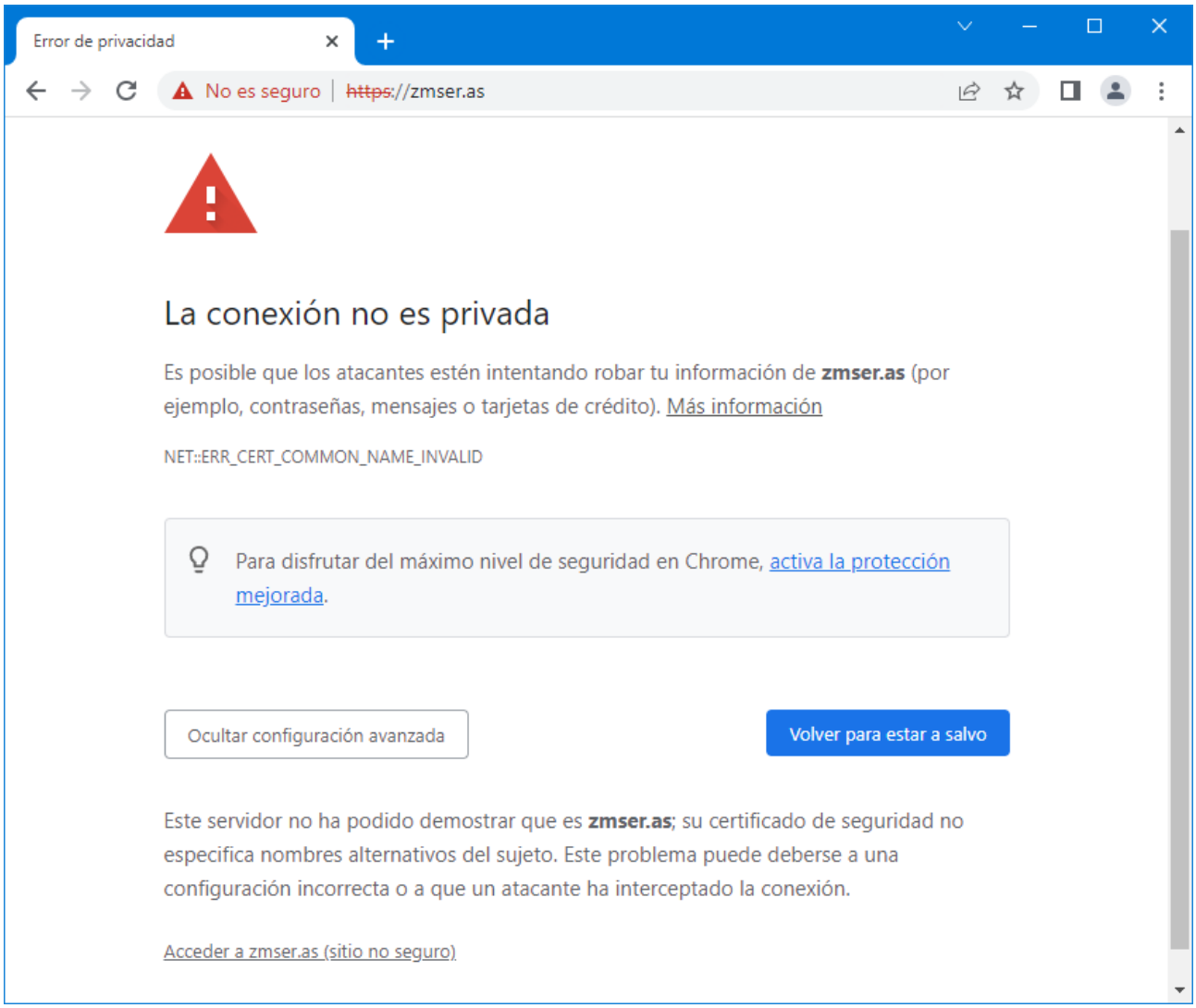


Selecciona la opción “Este certificado puede identificar sitios web”.

Ahora, limpia el historial de navegación y vuelve a acceder al servidor. Aparece un problema con el nombre de dominio del certificado.



El **acceso con Chrome** genera un error. Lee el último párrafo de la ventana siguiente, que se muestra después de pulsar el botón "Configuración avanzada".



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.

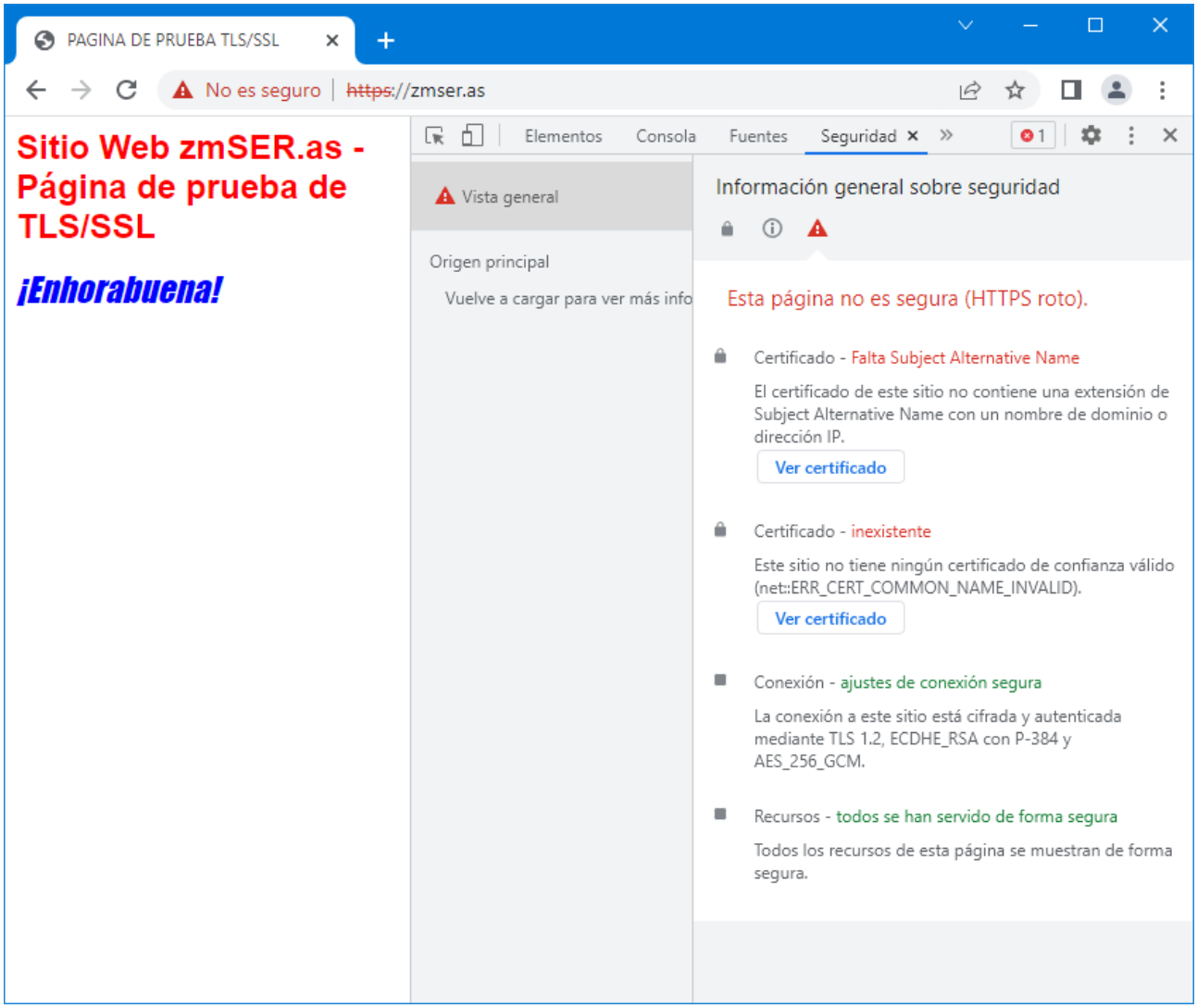
Esta política se basa en una aplicación "excesiva" de la RFC 2818 que dice:

```
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.
```

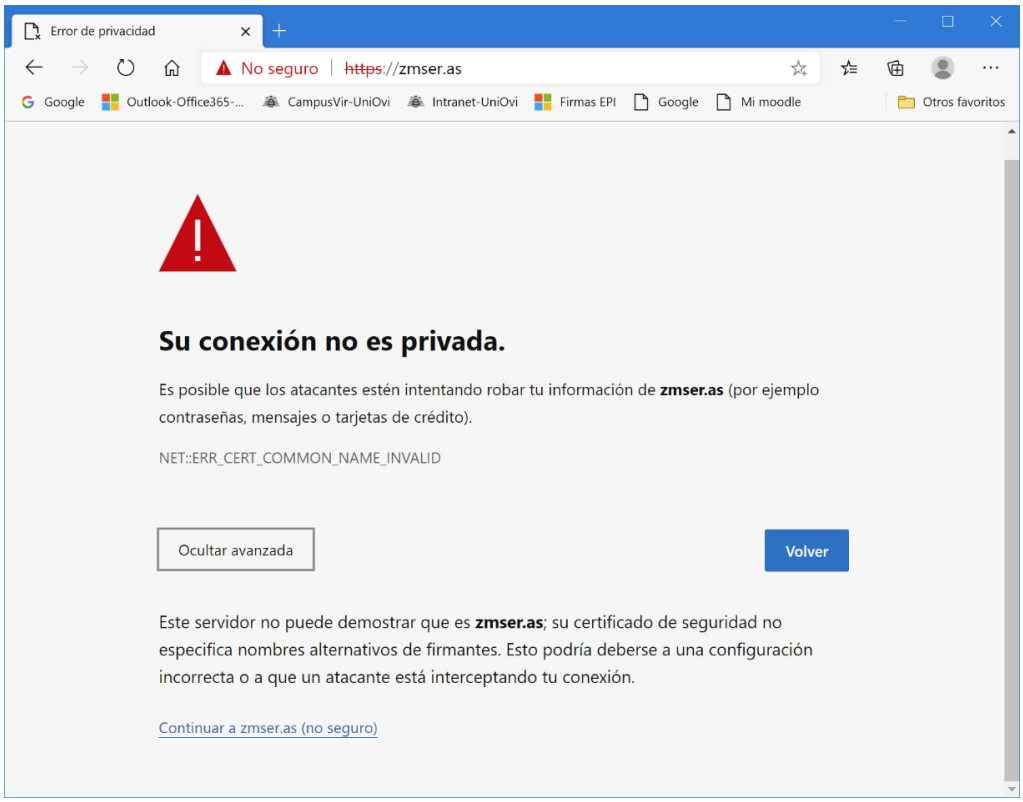
¡Chrome no usa el CommonName del certificado si no encuentra un SubjectAlternativeName!.

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 o PowerShell. También se podrían obtener certificados de una autoridad certificadora en los cuales se repita el CommonName en la extensión SubjectAlternativeName.

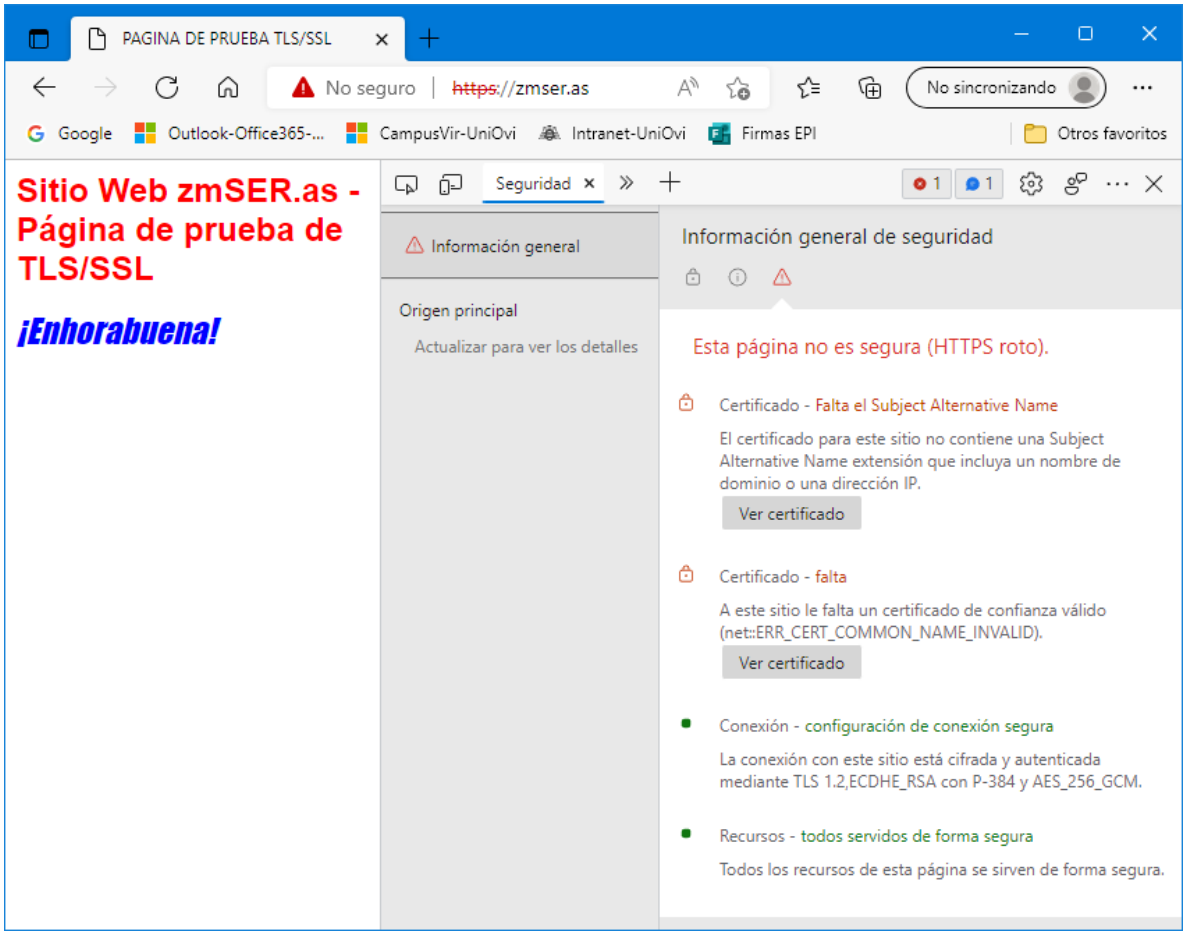
Se puede acceder a zmSER.as usando el enlace disponible al final de la página anterior, y aunque Chrome indica que el acceso no es seguro la conexión está cifrada.



El **acceso con EDGE** genera el mismo error que Chrome. Es lógico pues ahora el navegador EDGE se basa en el navegador Chromium:



Al acceder a zmSER.as se obtienen los mismos resultados que con el navegador Chrome:



9. 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 está 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/