

PRÁCTICA 3: Servicio IIS en Windows Server 2022.

Servicios de Red e Internet

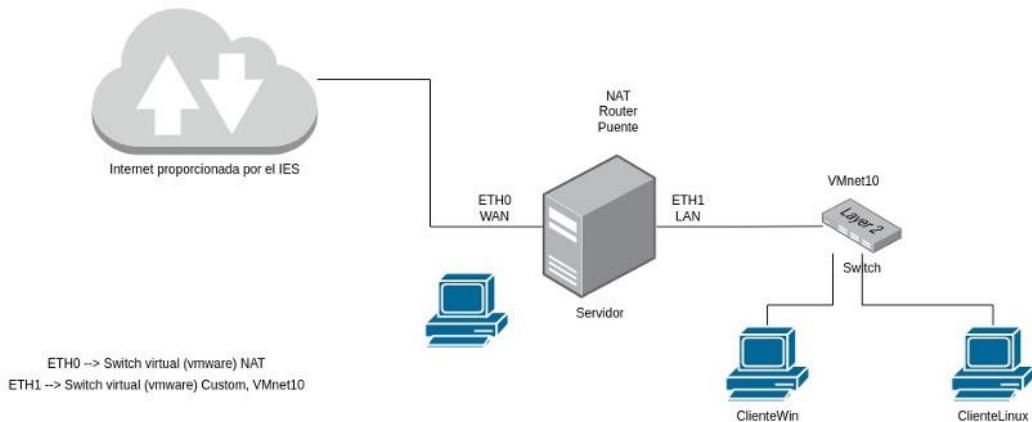
Ana María Serrano Pedrajas

Contenido

1.	Introducción.....	2
2.	Instala el rol IIS.....	3
3.	Crear un servidor compartido.....	5
a)	Sitios web virtuales	5
b)	Instalamos el rol de certificados.....	6
c)	Resto de la configuración.....	19
4.	A entregar las capturas de:.....	35
4.1.	Captura accediendo desde un cliente a http://www.1asir.local así como a https://www.1asir.local	35
4.2.	Captura accediendo a la sección de 1asir llamada FundamentosHardware, donde se aprecie que se ha logueado el usuario llamado “cliente”	36
4.3.	Captura accediendo a la sección de 1asir llamada Redes.....	36
4.4.	Captura accediendo desde un cliente a http://www.2asir.local así como a https://www.2asir.local	36
4.5.	Captura accediendo al sitio de 2asir.local desde un cliente con ip 10.0.0.35	39
4.6.	Captura accediendo desde un cliente a http://www.1daw.local así como a https://www.1daw.local	40
4.7.	Captura donde se muestre que se ha realizado la redirección hacia la sección de sistemas informáticos dentro del sitio 1daw.local	41

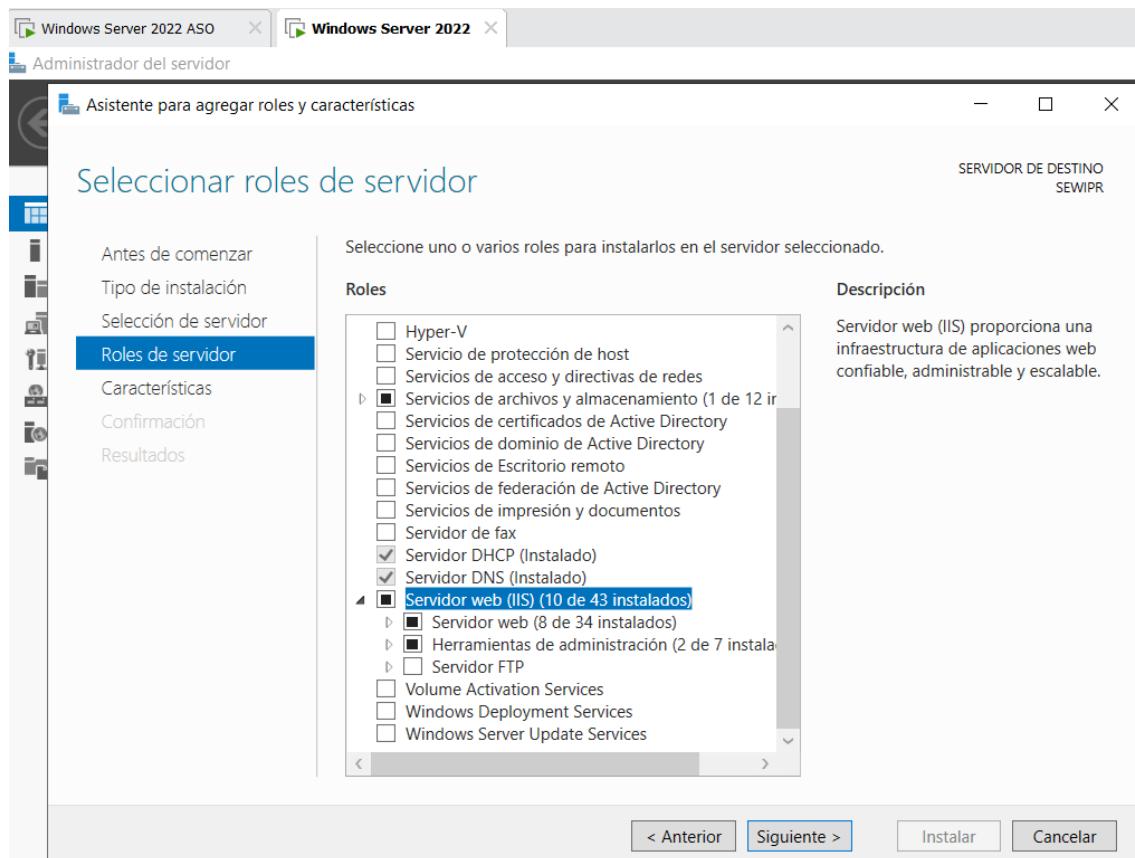
1. Introducción

Esta práctica se centra en la configuración de un servidor web utilizando Internet Information Services (IIS) en un entorno virtualizado. El objetivo principal es comprender los pasos necesarios para instalar, configurar y asegurar un servidor web capaz de alojar sitios web y aplicaciones web.

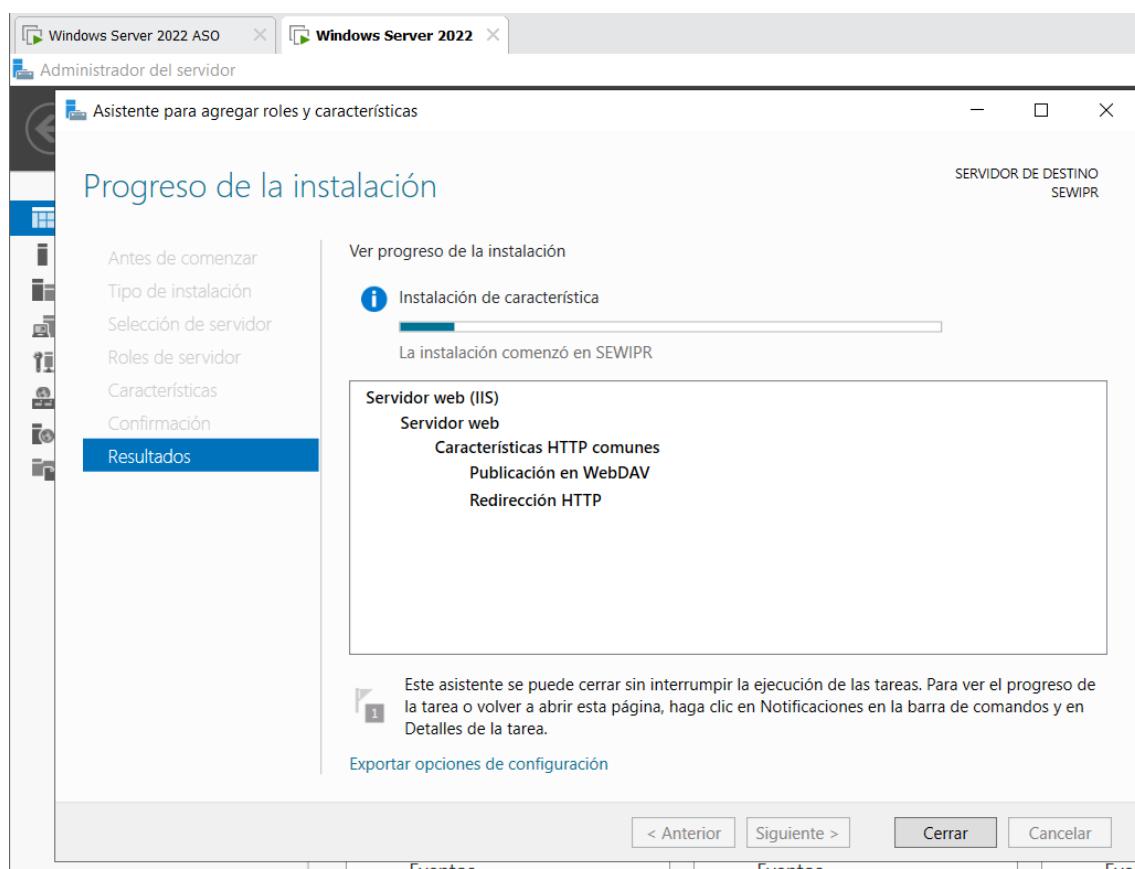
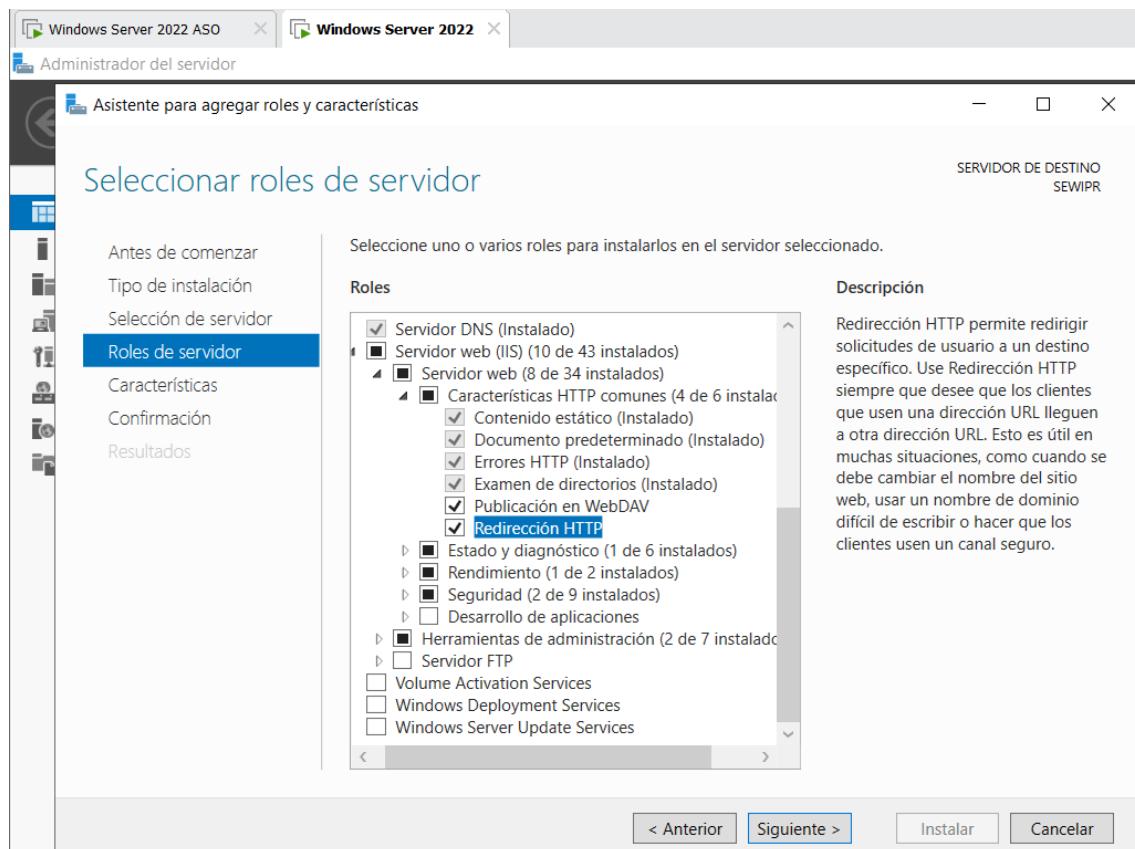


2. Instala el rol IIS

Para instalar el rol IIS, accede al Administrador del servidor. Localiza la sección "Administrar" y selecciona "Aregar roles y características" para iniciar el asistente de instalación. En el apartado "Roles de servidor", marca "Servidor web (IIS)" e instala las características requeridas. Procede con la instalación y verifica la correcta implementación del rol.



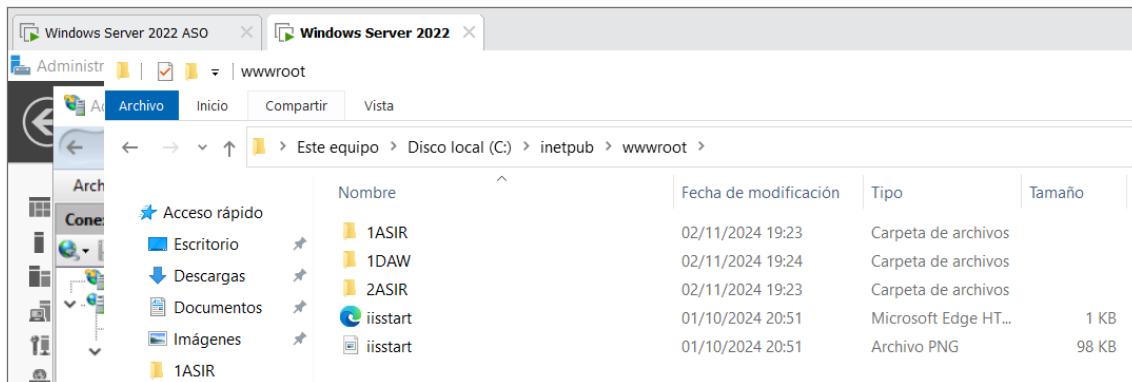
Es importante instalar Redirección HTTP, ya que será una característica que utilizaremos más adelante.



3. Crear un servidor compartido

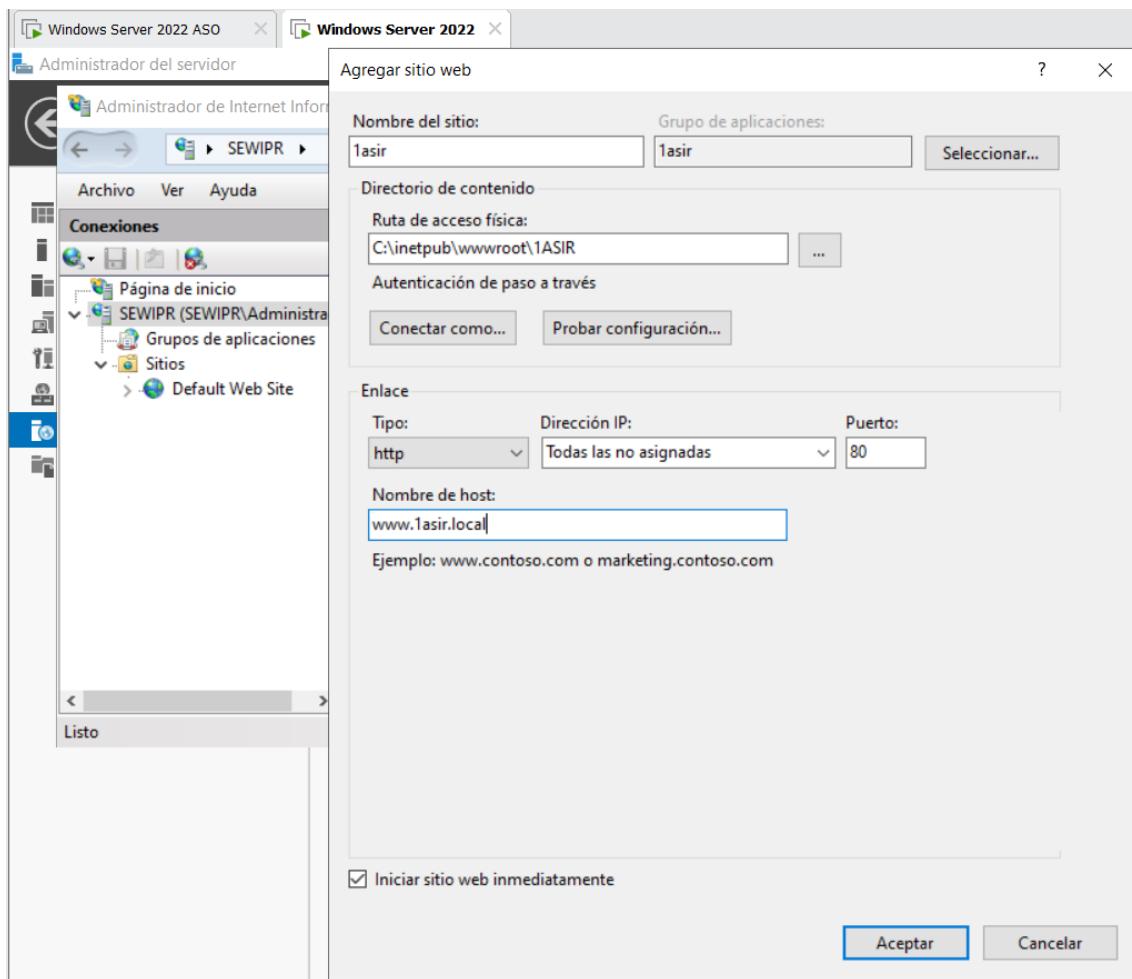
a) Sitios web virtuales

Para configurar los sitios web virtuales, primero creamos las carpetas 1asir, 2asir y 1daw en la unidad C:\. Dentro de cada carpeta, creamos un archivo Default.htm con un mensaje de bienvenida.



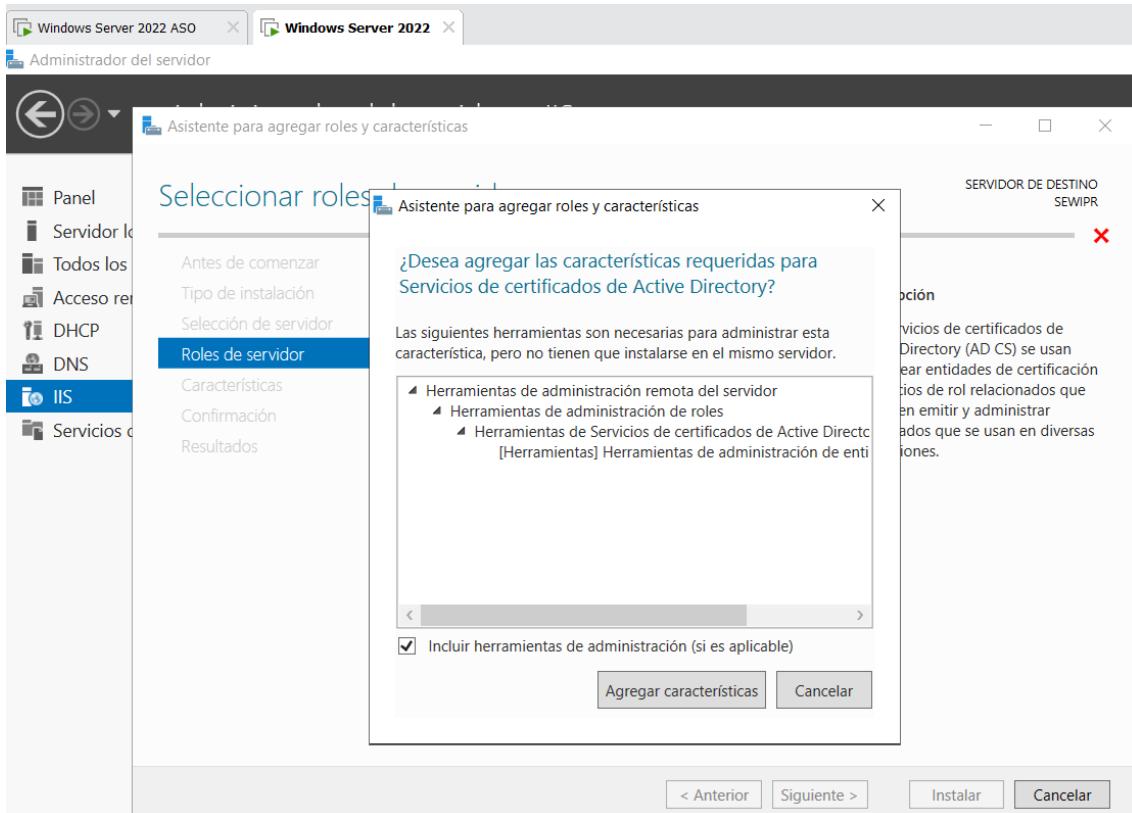
A continuación, abrimos el Administrador de Internet Information Services (IIS). Desplegamos el servidor en el panel "Conexiones" y vamos a "Sitios". Hacemos clic derecho y seleccionamos "Agregar sitio web...".

Creamos un nuevo sitio con el nombre "1asir", la ruta física C:\1asir, el tipo de enlace http y el nombre de host www.1asir.local. Repetimos el proceso para crear los sitios 2asir y 1daw con sus respectivas rutas, tipos de enlace y nombres de host. En esta tanda vamos a crear los sitios web con puerto 80, que no requieren certificados SSL para funcionar.

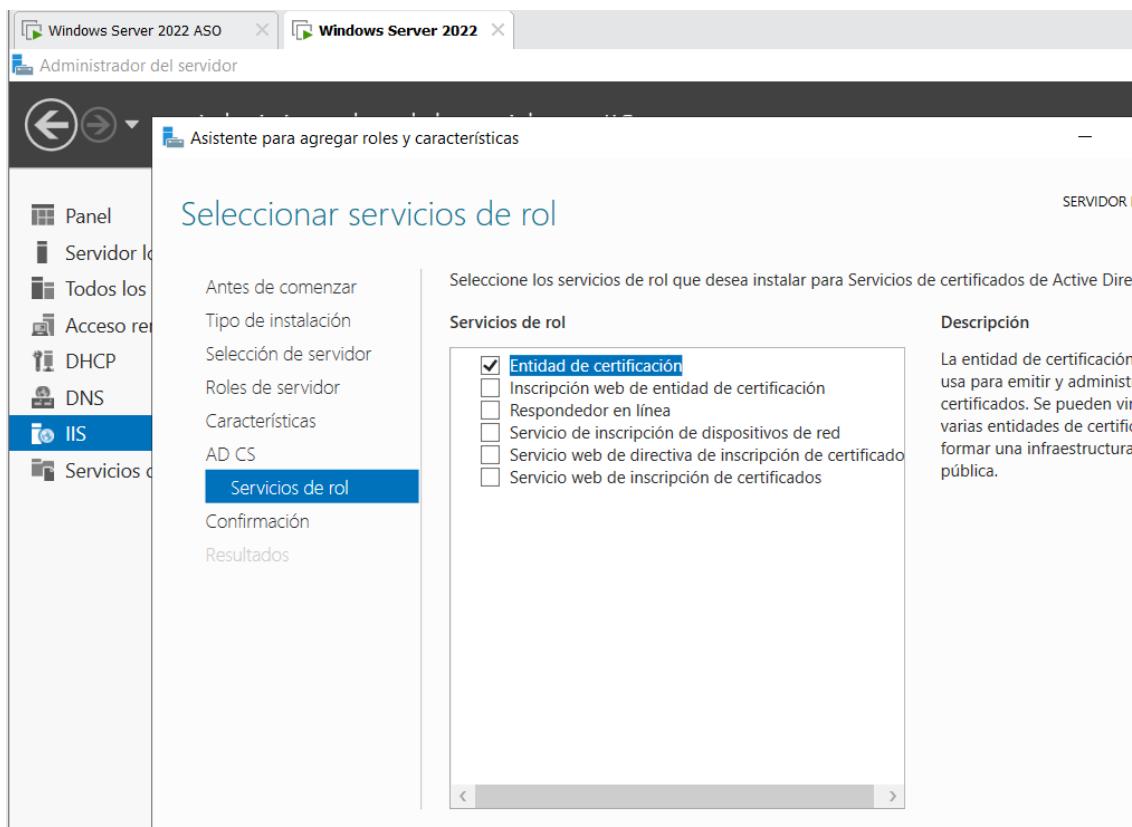


b) Instalamos el rol de certificados.

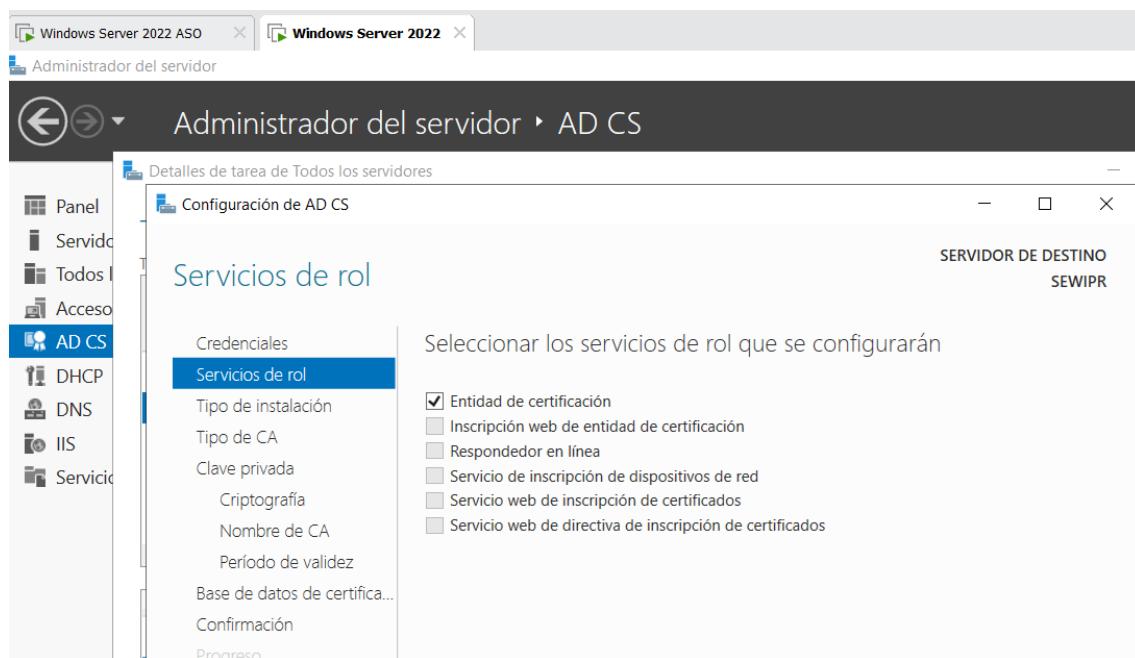
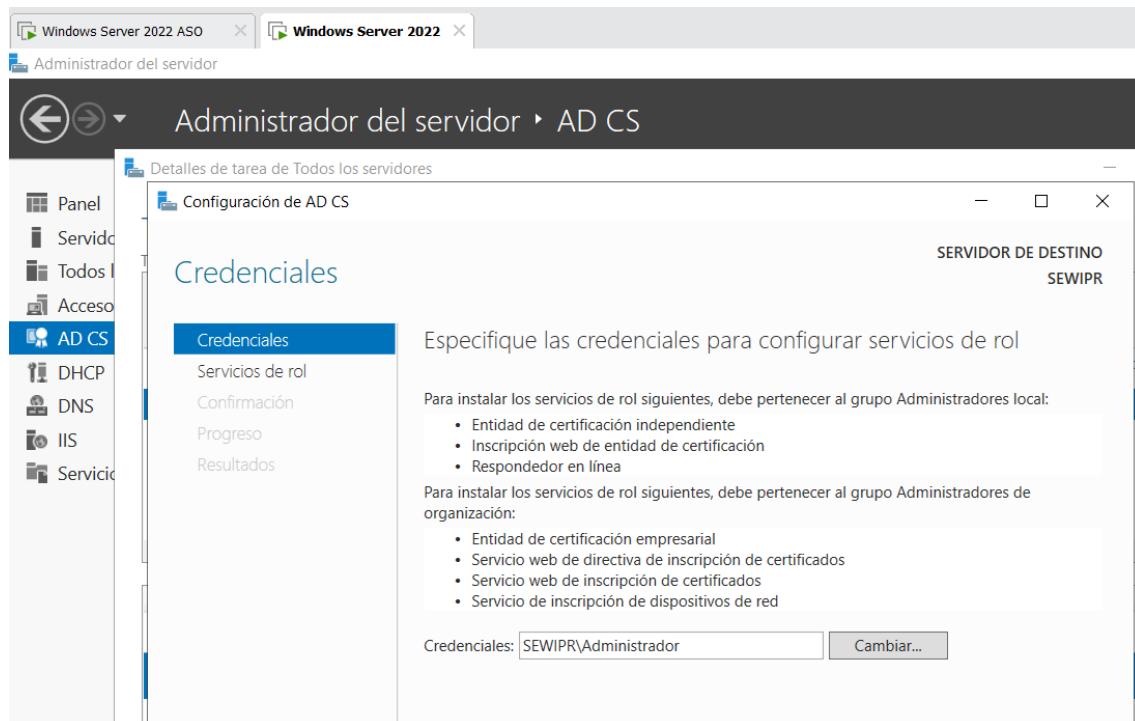
Ahora vamos a generar los sitios con acceso vía https. Para ello, necesitamos un certificado SSL y por tanto tenemos que instalar el rol de certificados en nuestro servidor. Podemos ver como el rol a instalar incluye la parte de Servicios de certificados de Active Directory.



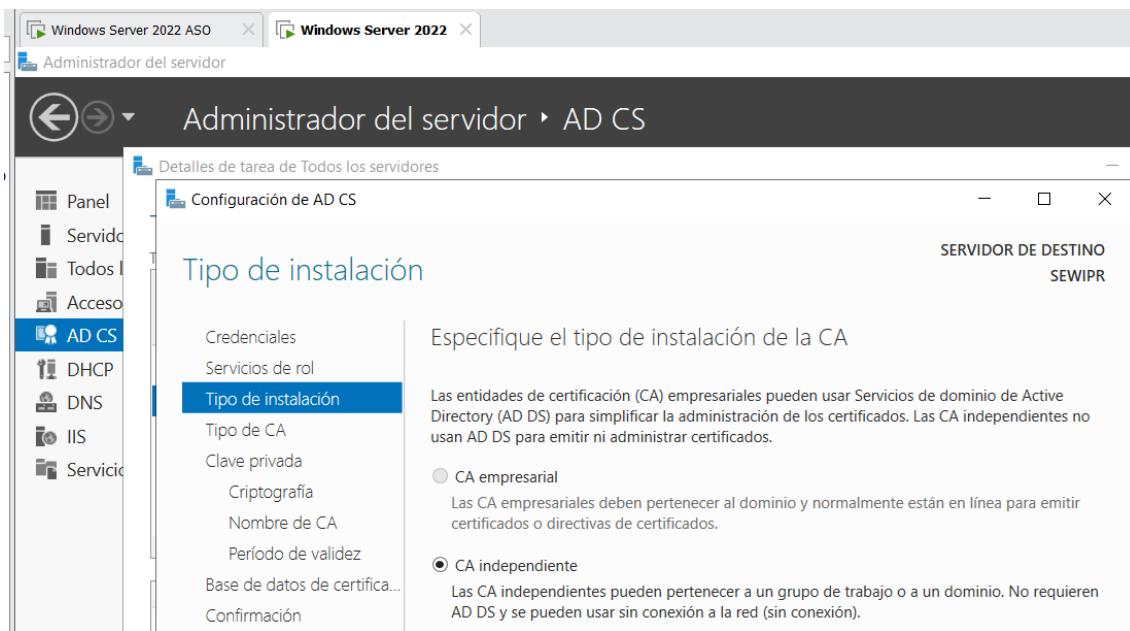
Al agregar las características, se nos abre una ventana con una serie de servicios a escoger, de los cuales escogeremos Entidad de certificación para instalar.



Ahora es turno de incluir las credenciales para configurar servicios de rol, que serán las mismas que las de nuestro usuario Administrador.



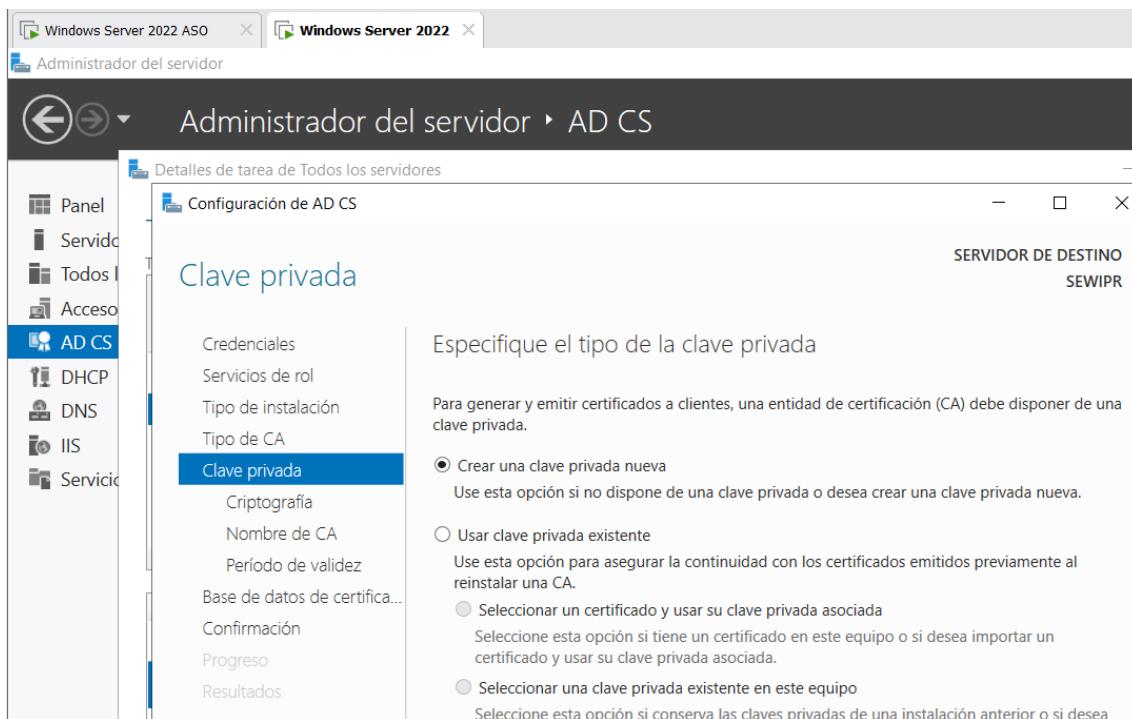
Como hemos seleccionado Entidad de certificación como servicio a instalar, se nos abre una ventana para que especifiquemos el tipo de instalación para la CA que queremos instalar. Podemos elegir entre CA empresarial o CA independiente. Escogemos esta última ya que la que queremos configurar está pensada a efectos de prueba y aprendizaje.



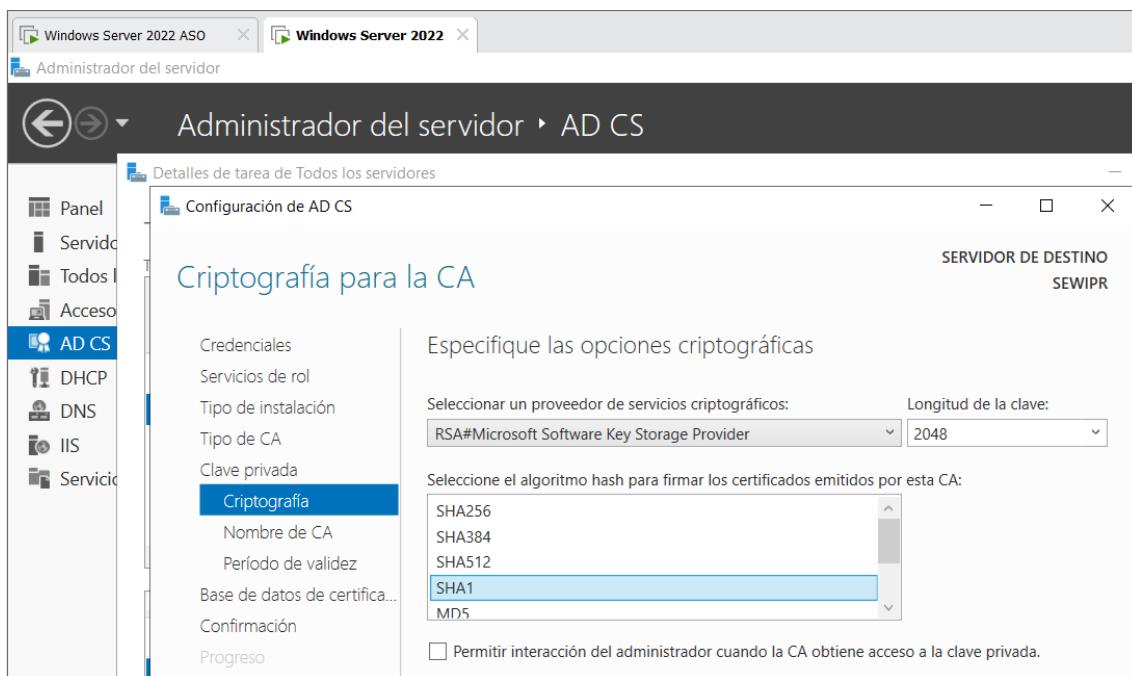
Una vez seleccionado el tipo de instalación que queremos para nuestra CA, ahora tenemos que elegir qué CA queremos generar, si una raíz o una subordinada. Todavía no tenemos una raíz, así que elegimos esta.



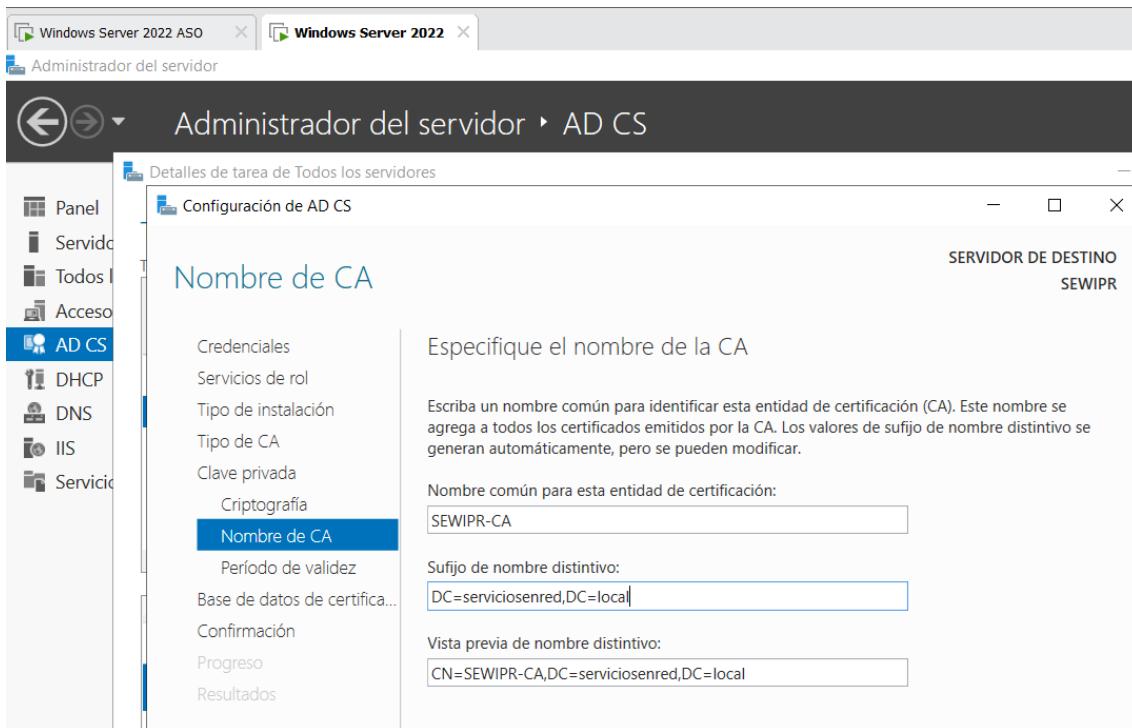
Ahora se nos pregunta si ya disponemos de una clave privada o si por el contrario queremos crear una nueva. Elegimos crearla.



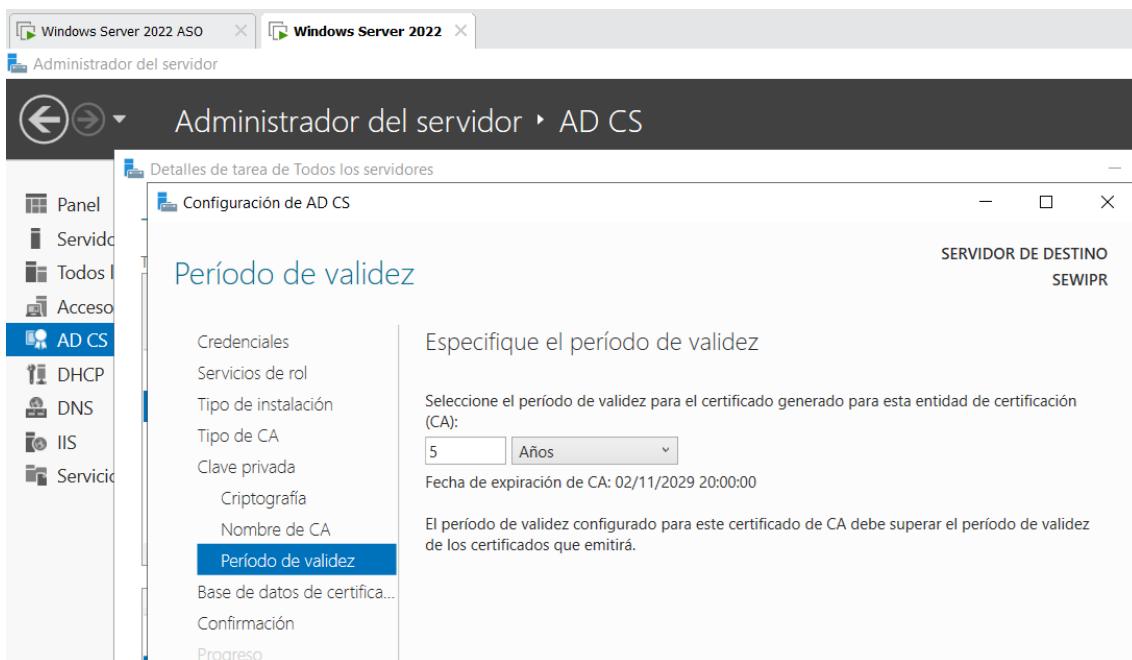
A continuación, se muestra la ventana para seleccionar el proveedor de servicios criptográficos (RSA 2048) y la longitud en bits de la clave de cifrado, que determina la seguridad del certificado.



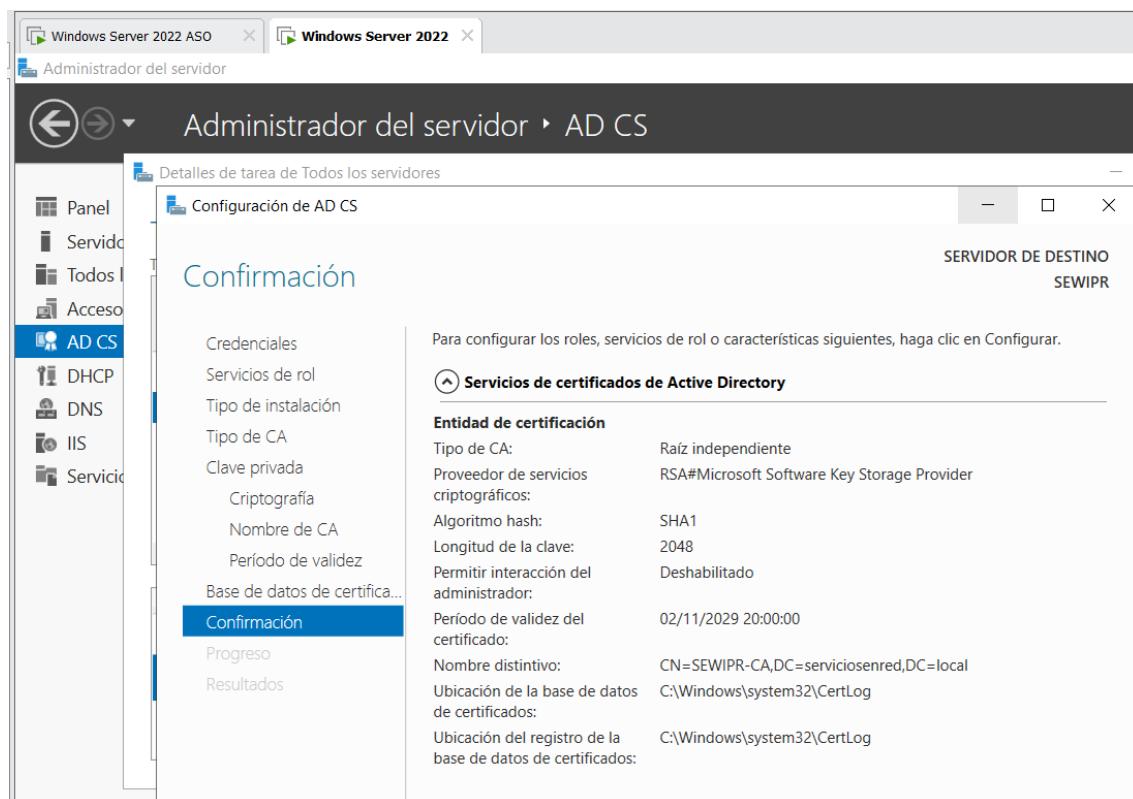
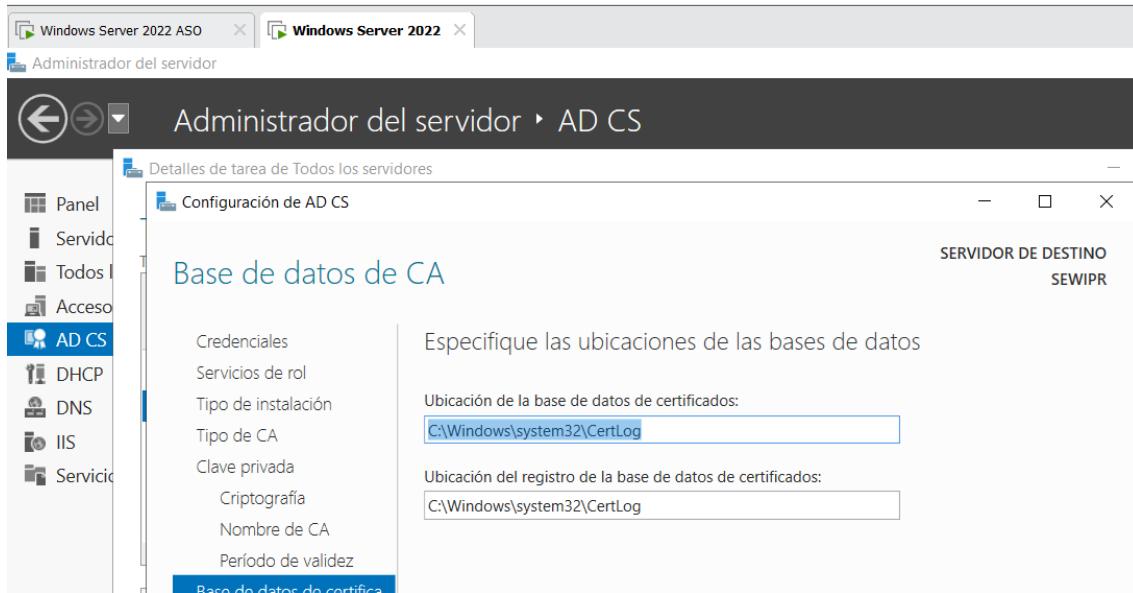
Ahora se deben especificar las propiedades del nombre distintivo para el certificado, que se conforma con el nombre común junto con el sufijo de nombre distintivo. En la vista previa vemos como queda nuestro nombre distintivo.



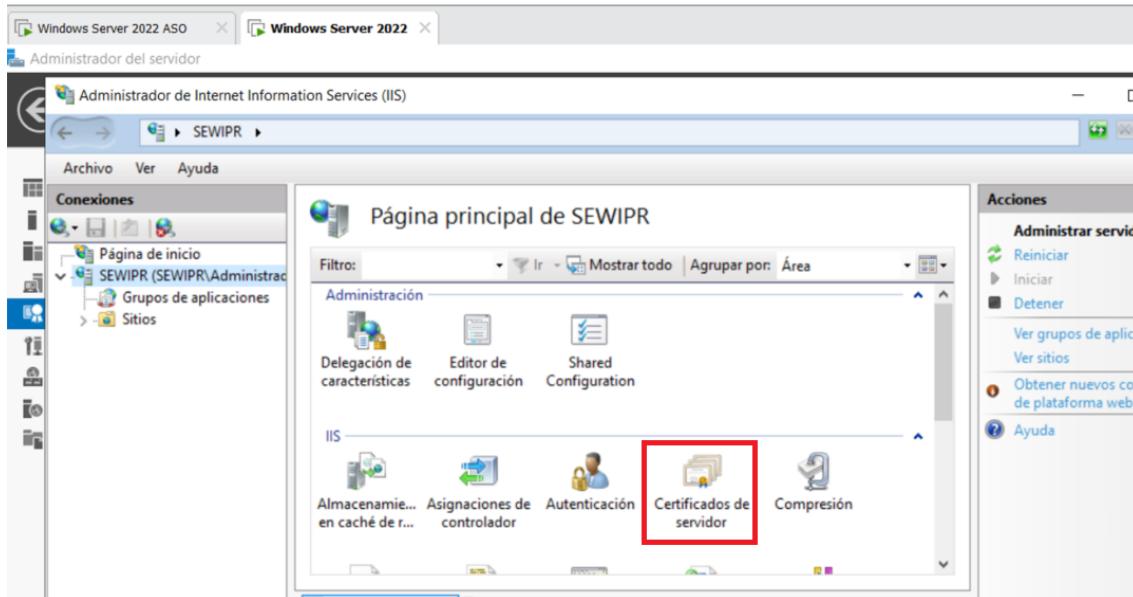
Ahora vamos a especificar el período de validez para nuestra CA a 5 años.



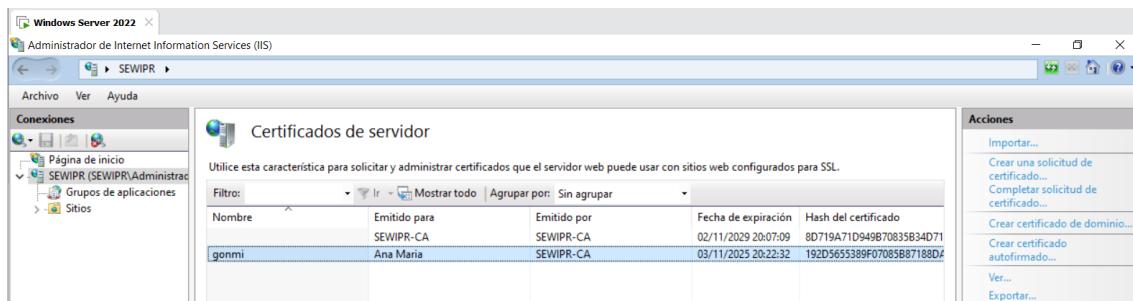
Ahora escogemos las rutas dónde se guardará la base de datos y los registros de log de los certificados.



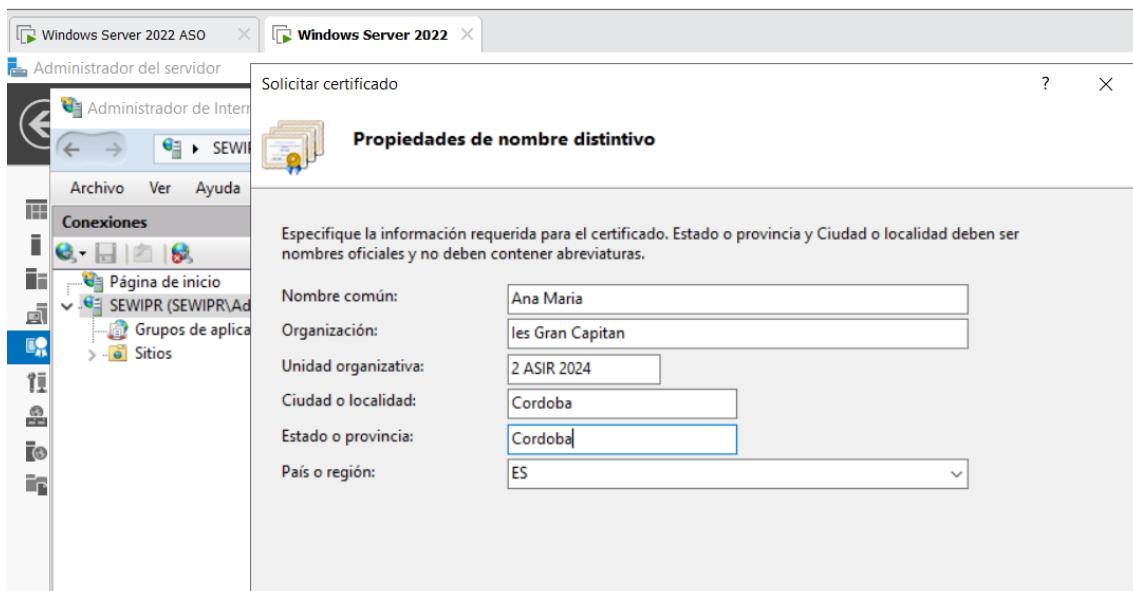
Una vez configurada nuestra CA, vamos a la sección Certificados de Servidor.



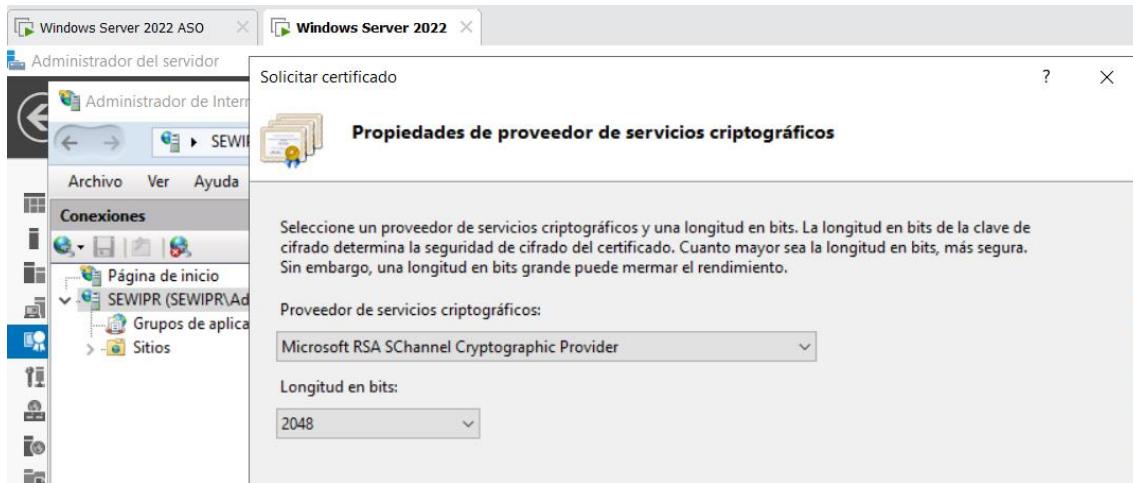
Y crearemos una solicitud de certificado haciendo clic derecho y seleccionando “Crear una solicitud de certificado...”.



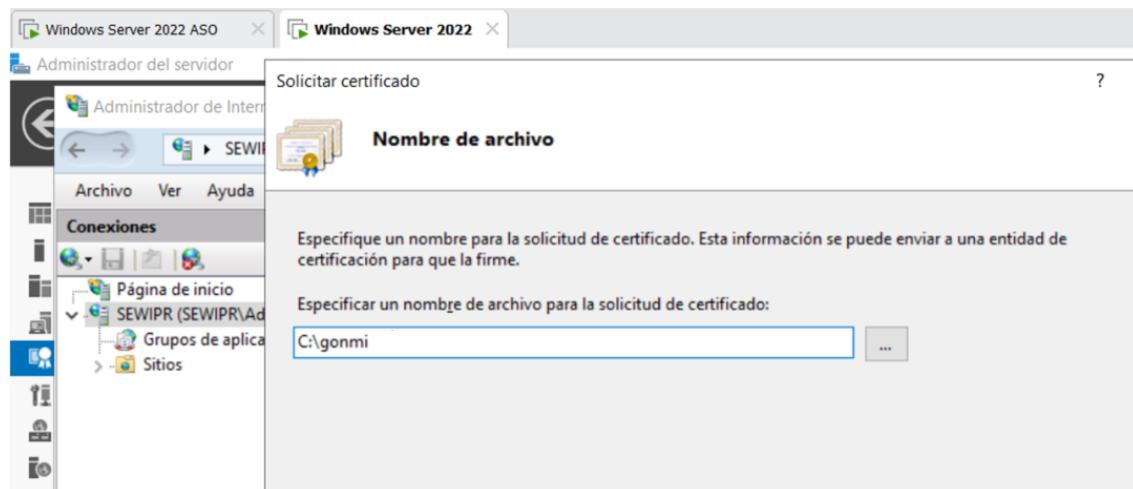
Añadiremos todos los datos solicitados para crear nuestra solicitud de certificado a partir de nuestra CA.



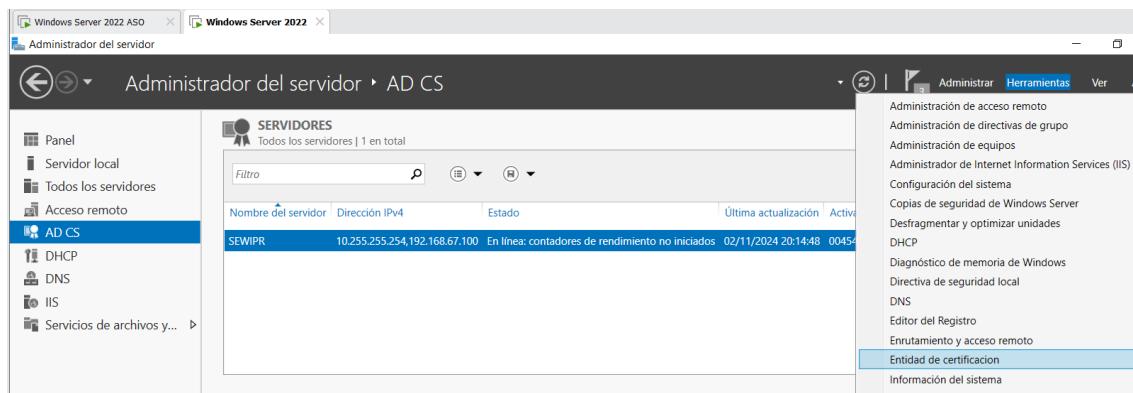
En las Propiedades de proveedor de servicios criptográficos es muy importante cambiar la Longitud de Bits por 2048.



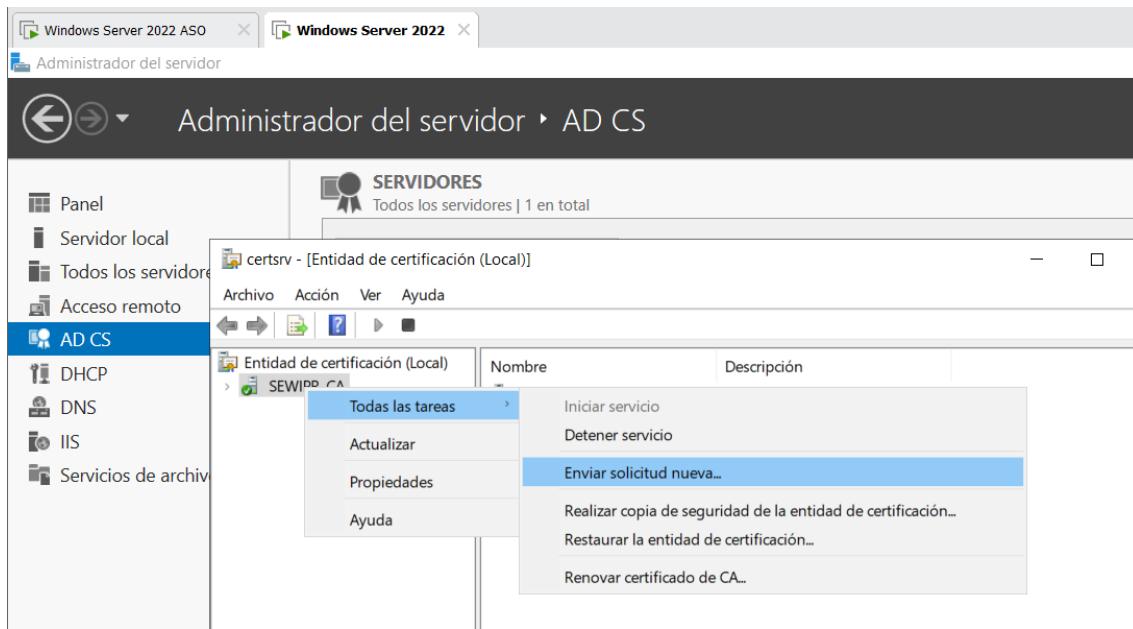
Y, a continuación, especificamos un nombre de archivo para la **solicitud** del certificado.



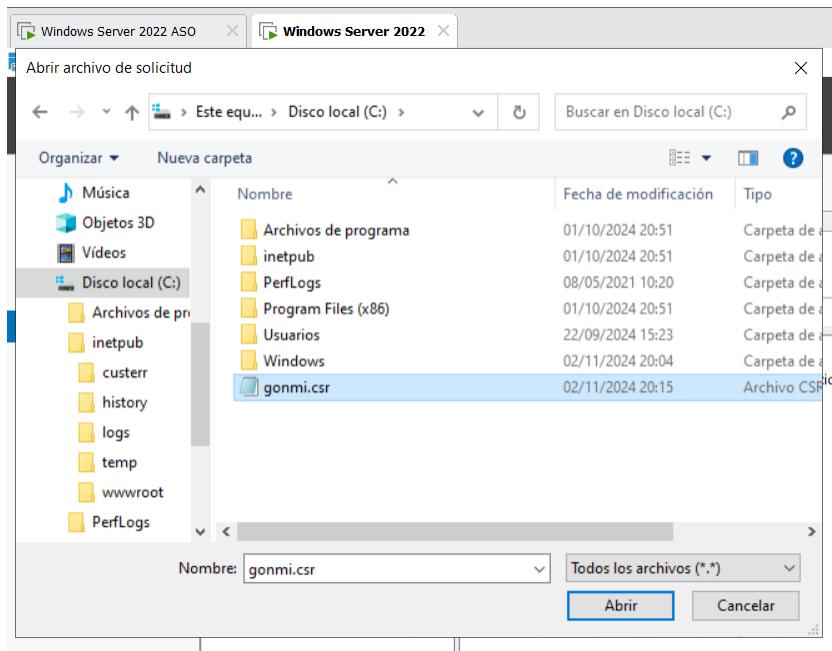
Completaríamos la solicitud volviendo a herramientas y clicando en Entidad de certificación.



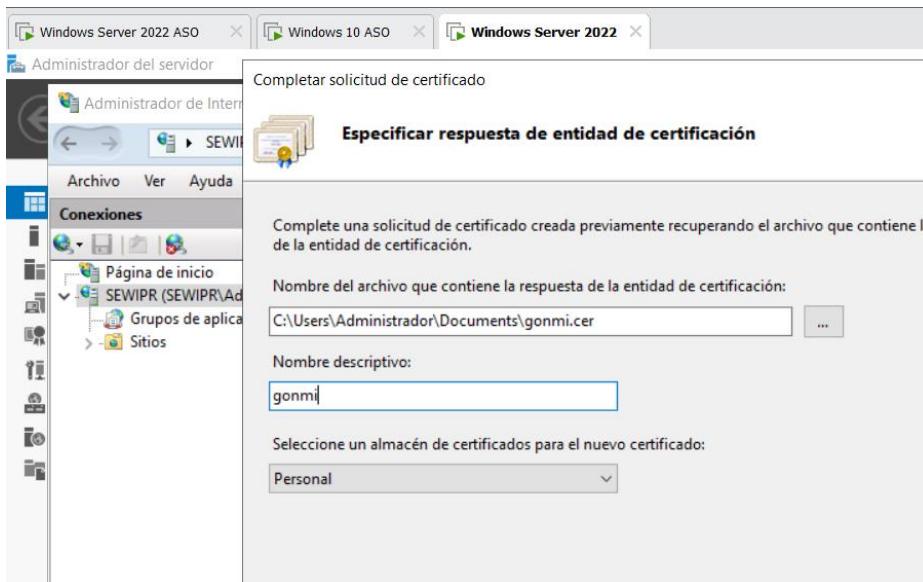
Una vez que clicamos en Entidad de Certificación, se nos abre una ventana con nuestro SEWIPR-CA. Hacemos clic derecho > Todas las tareas > Enviar solicitud nueva...



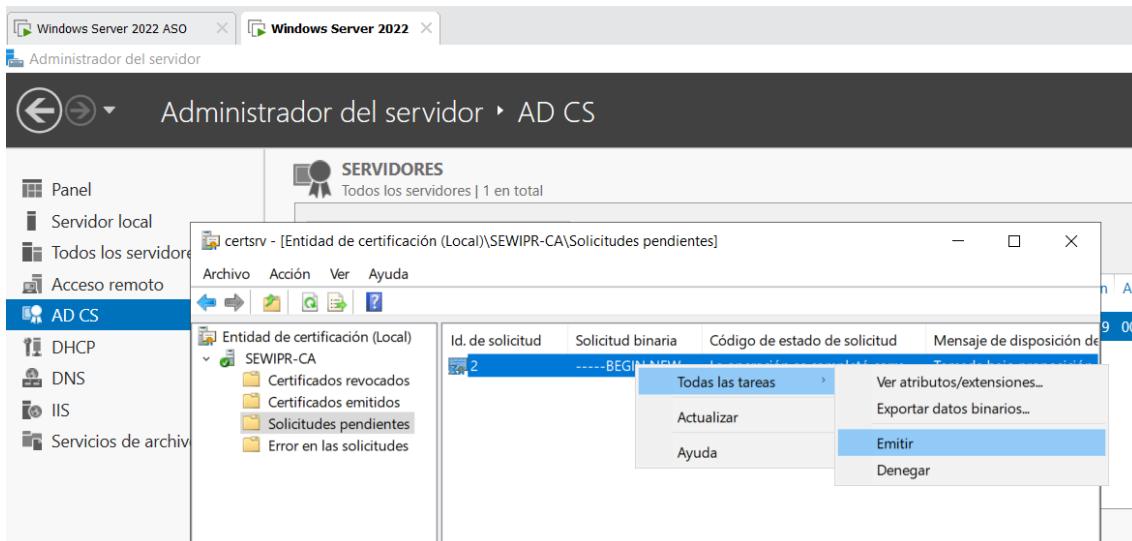
Le proporcionaremos nuestro archivo con la solicitud de certificado que generamos anteriormente.



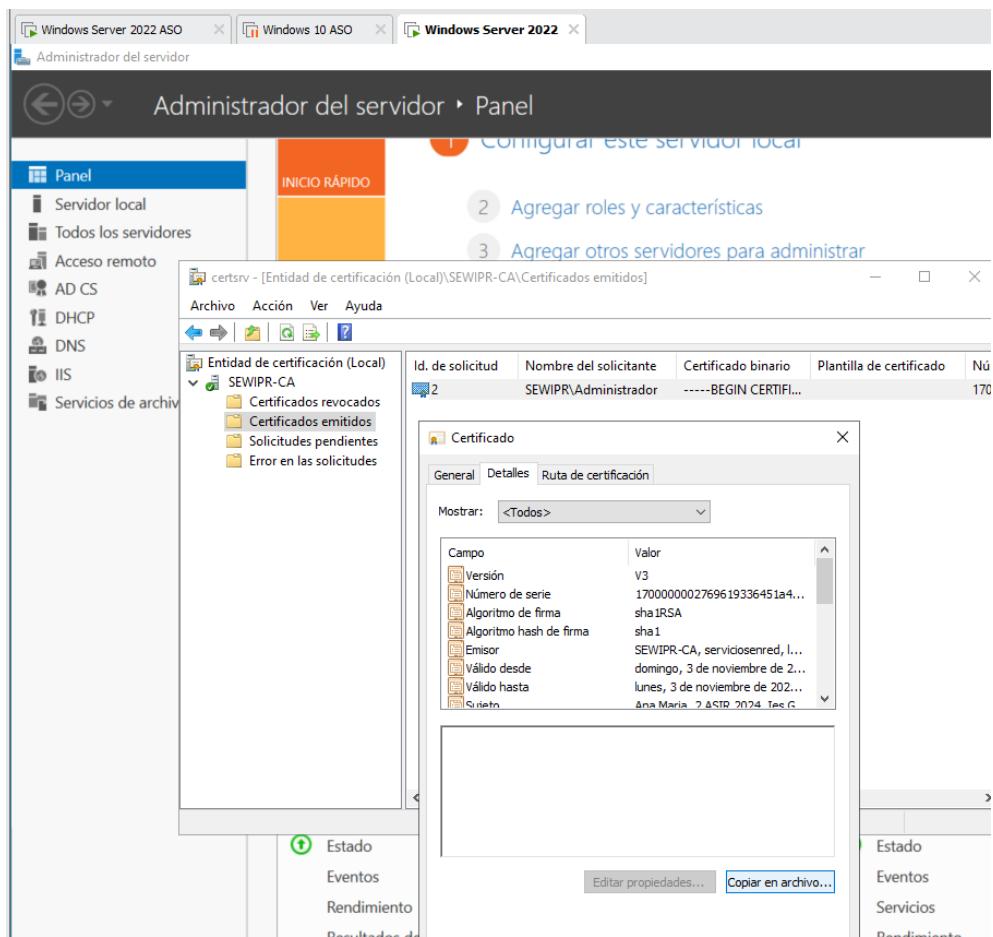
Desde el menú principal de servicios de certificados, hacemos clic en el elemento "Completar solicitud de certificado" de la columna derecha.



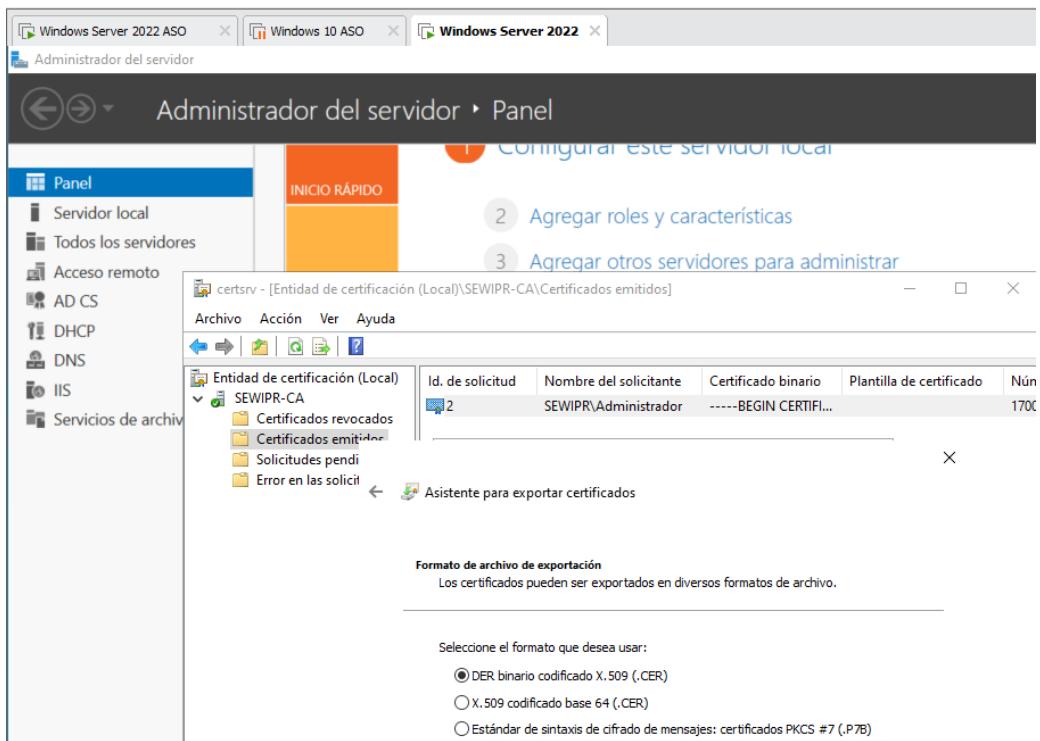
En nuestro Administrador del servidor de Windows Server 2022, podemos ir a Herramientas > Entidad de certificación para abrir la vista de Entidad de certificación local, vamos a Solicitudes pendientes y podemos encontrar la nuestra. Clic derecho en la solicitud > Todas las tareas > Emitir para emitir nuestro certificado.

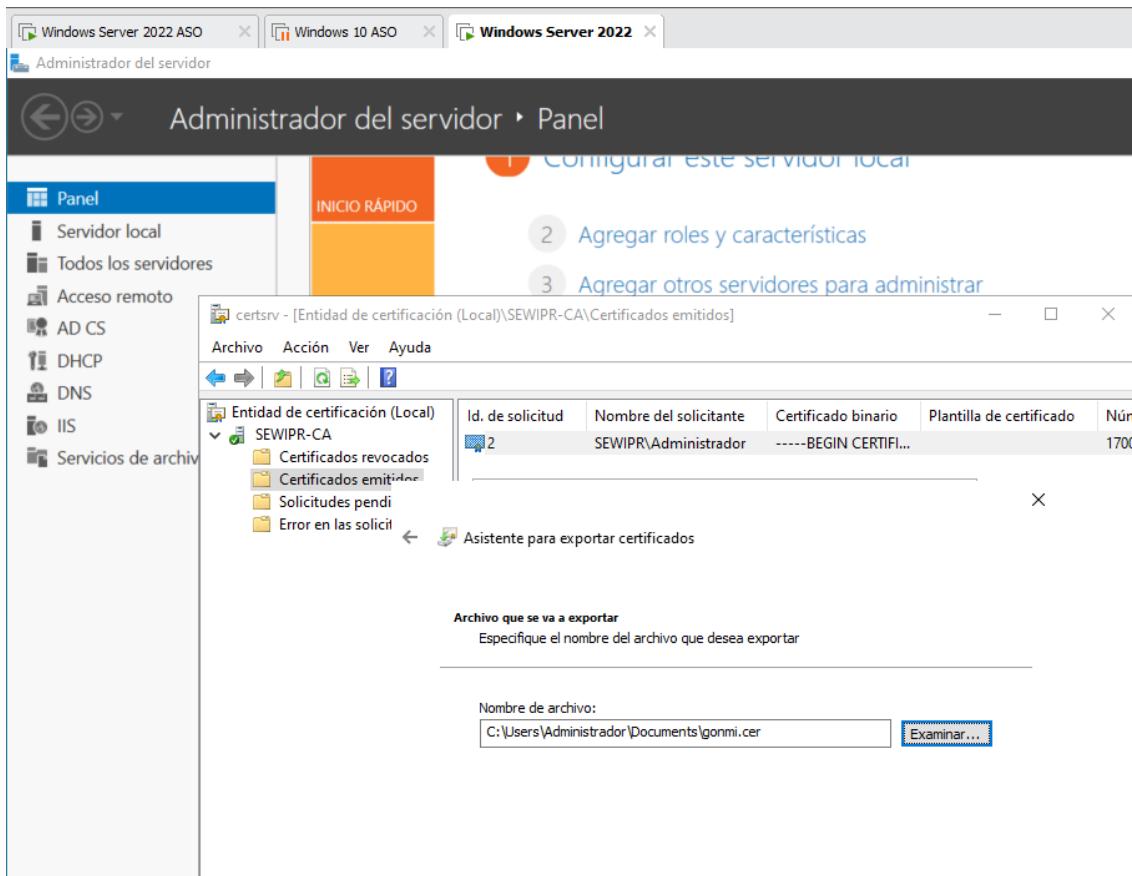


Ahora ya podemos encontrar nuestro certificado generado en la sección de Certificados emitidos.



Vamos a exportarlo para poder tener el archivo con el que poder configurar nuestros sitios web.

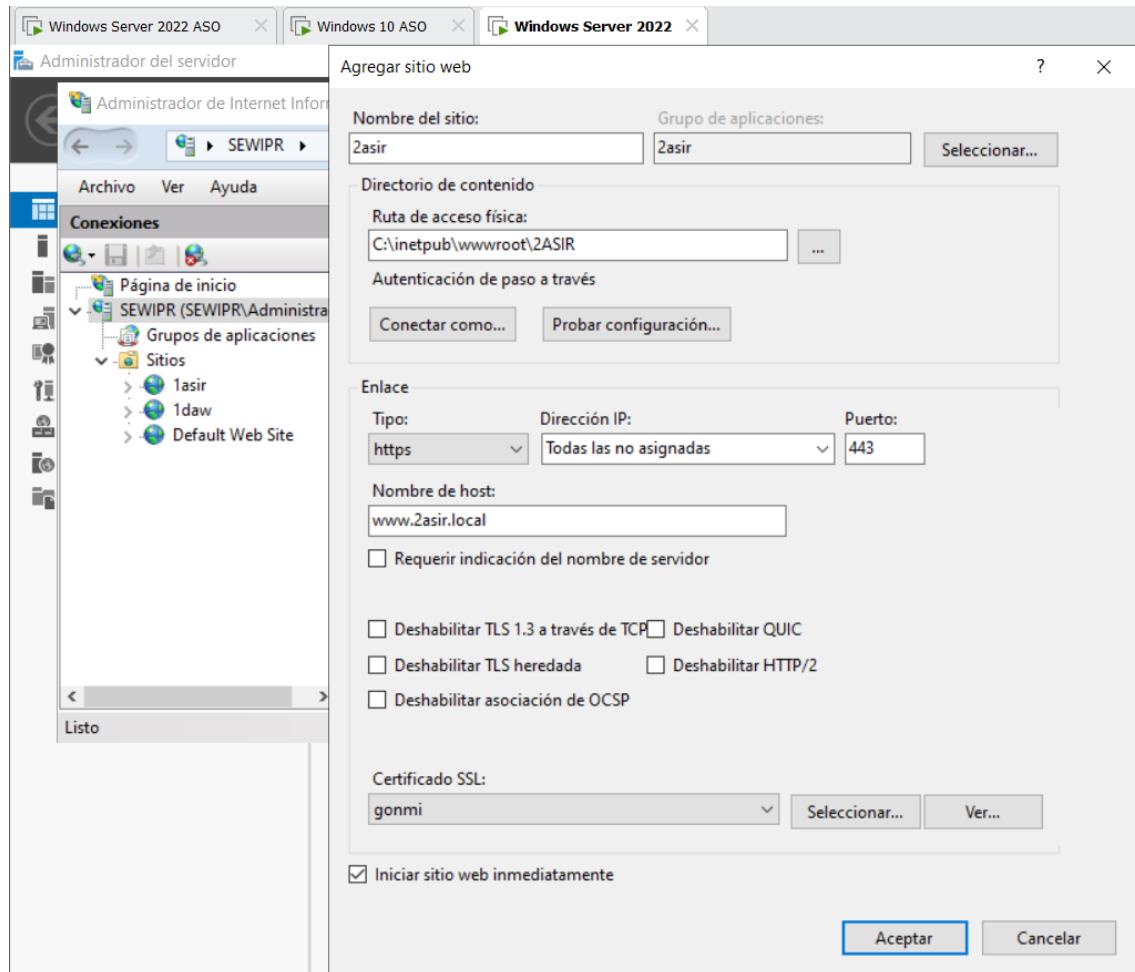




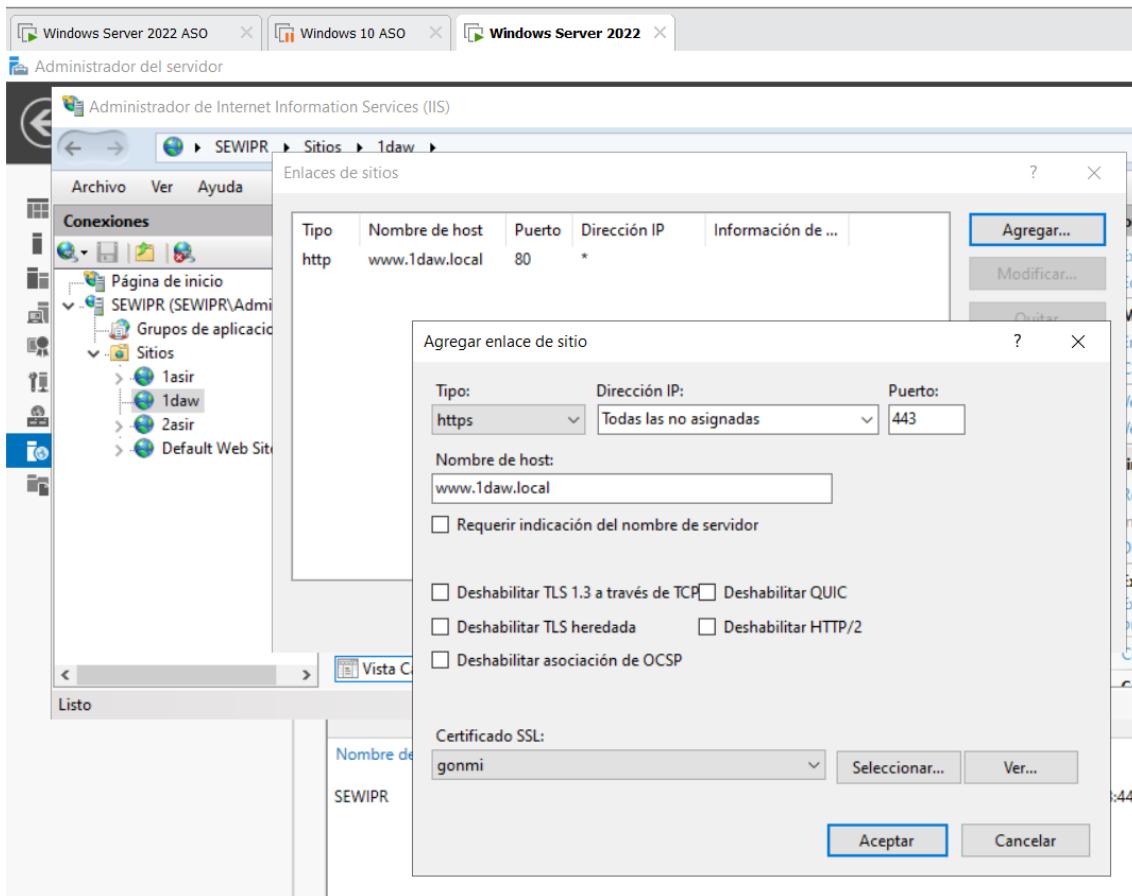
Con esto ya tendríamos nuestro certificado en la ruta indicada.

c) Resto de la configuración

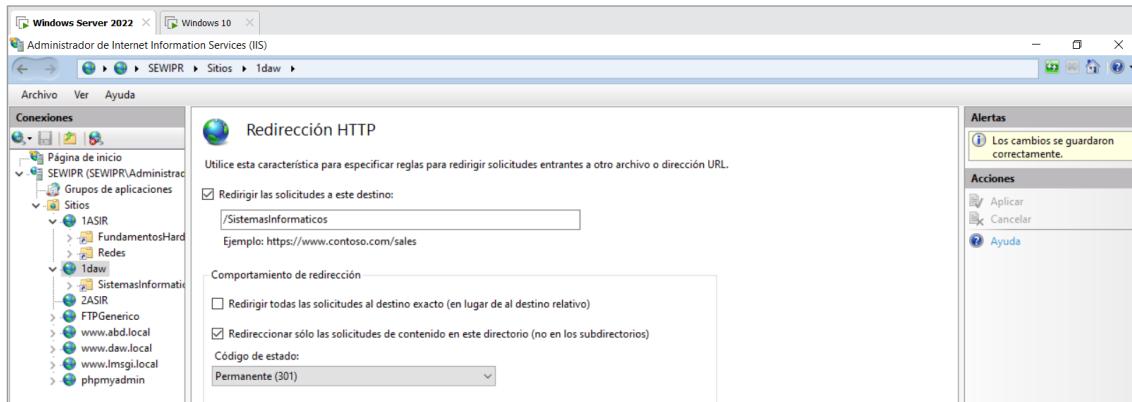
Podemos comenzar a generar los sitios virtuales que tendrán acceso vía https. Empezamos con el de **2asir**. Incluimos la ruta física, el tipo de autenticación a https como es requerido en el enunciado y el puerto 443. El certificado SSL es el que acabamos de generar que lo escogemos del listado.



Repetimos configuración para **1daw**.

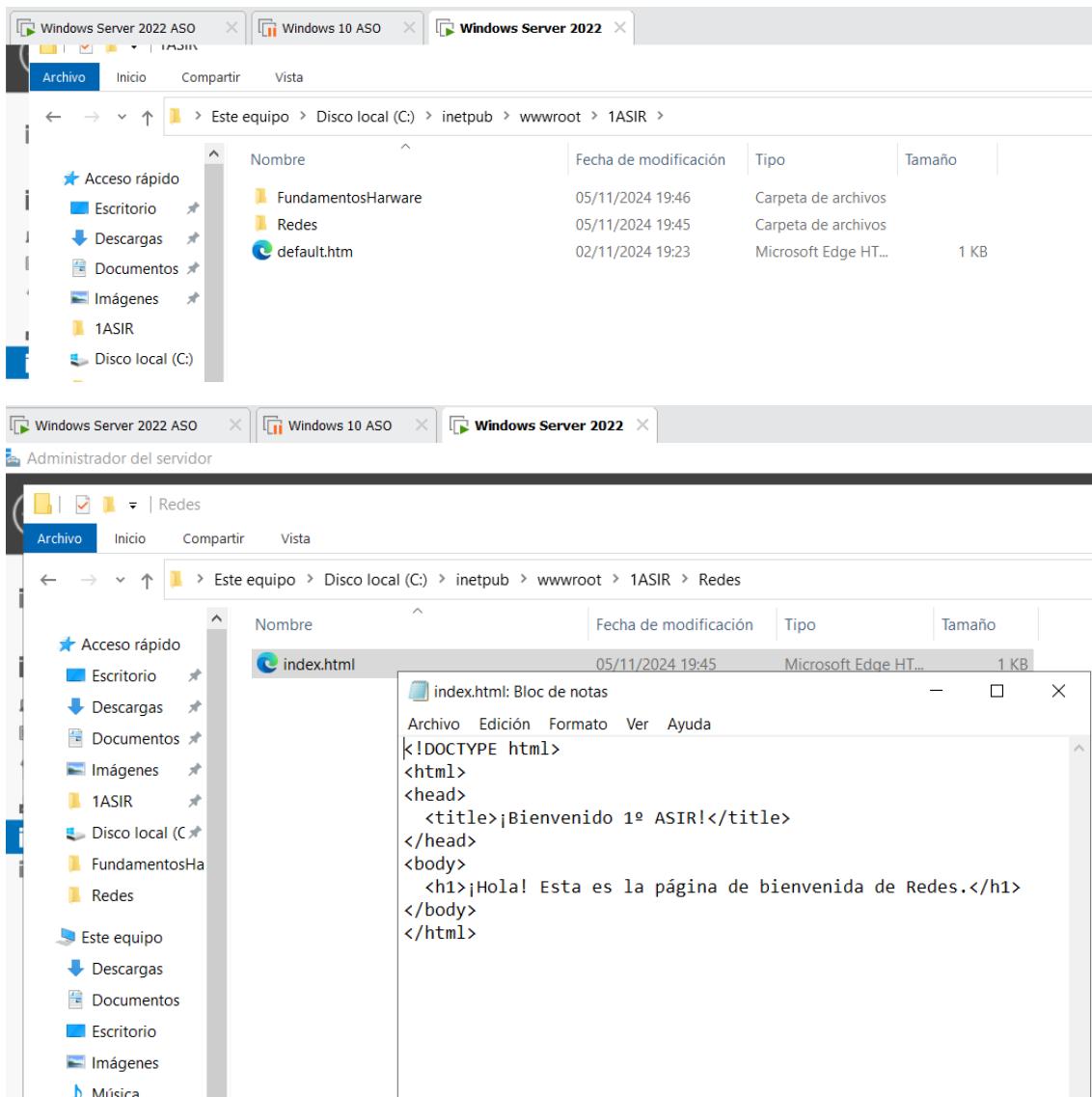


Este sitio requiere según el enunciado de una redirección a /SistemasInformaticos.

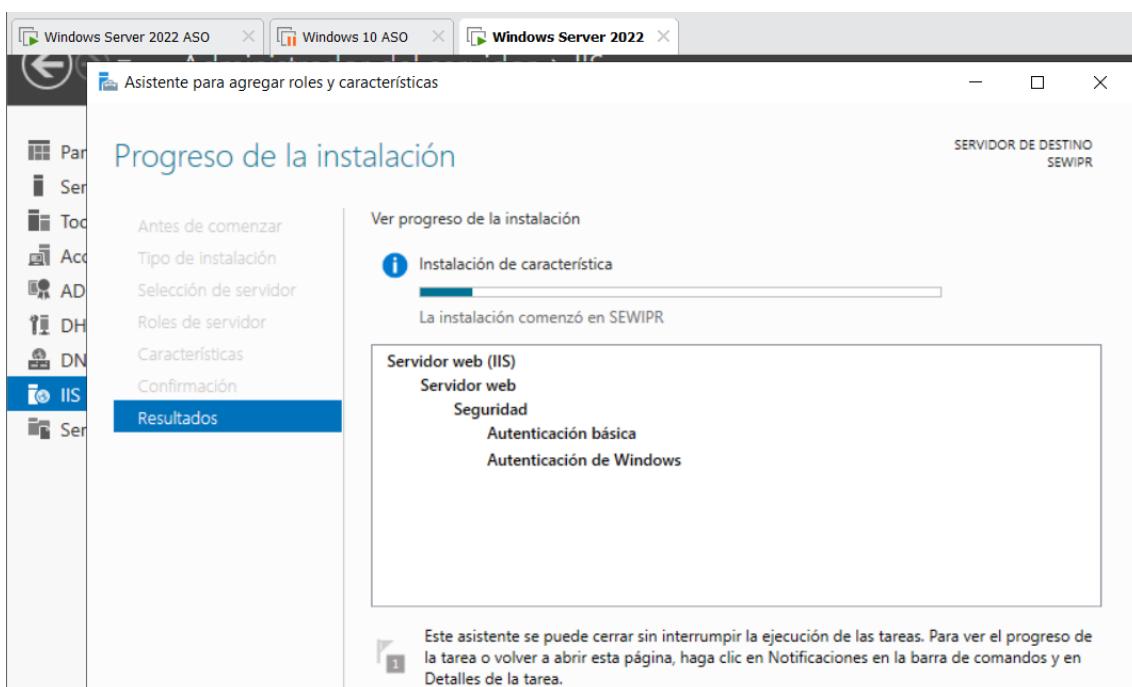
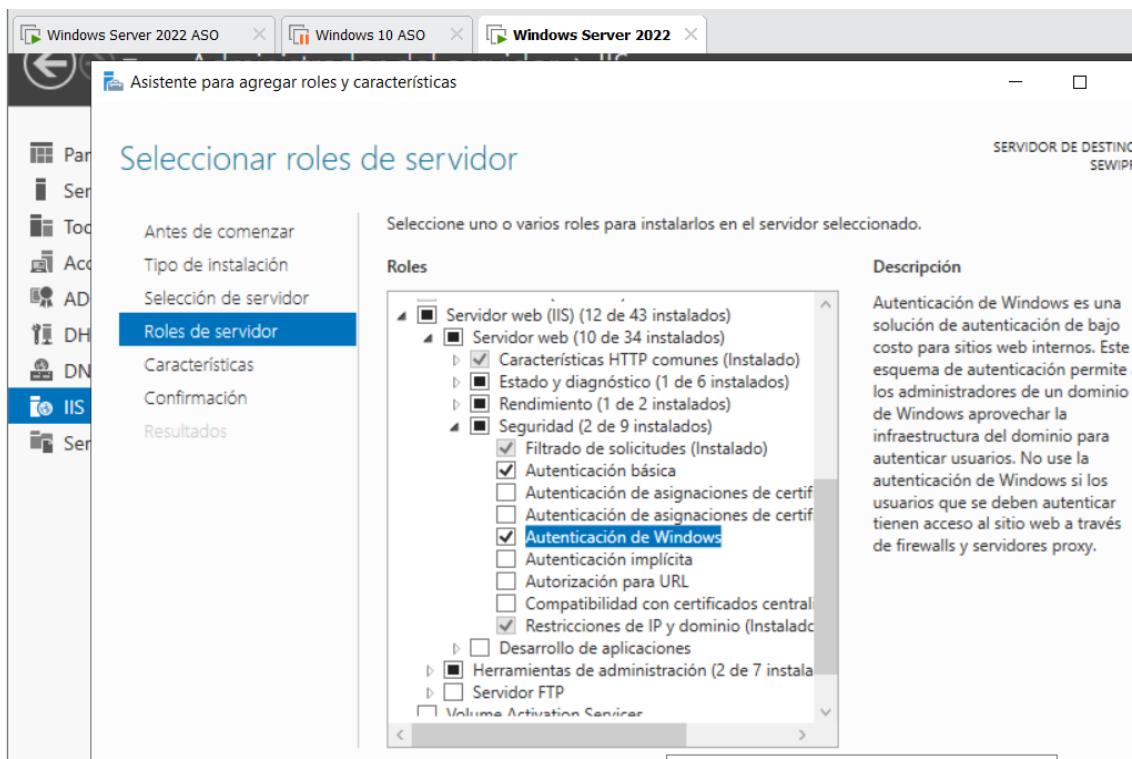


Una vez creados los directorios virtuales vamos a generar las páginas html.

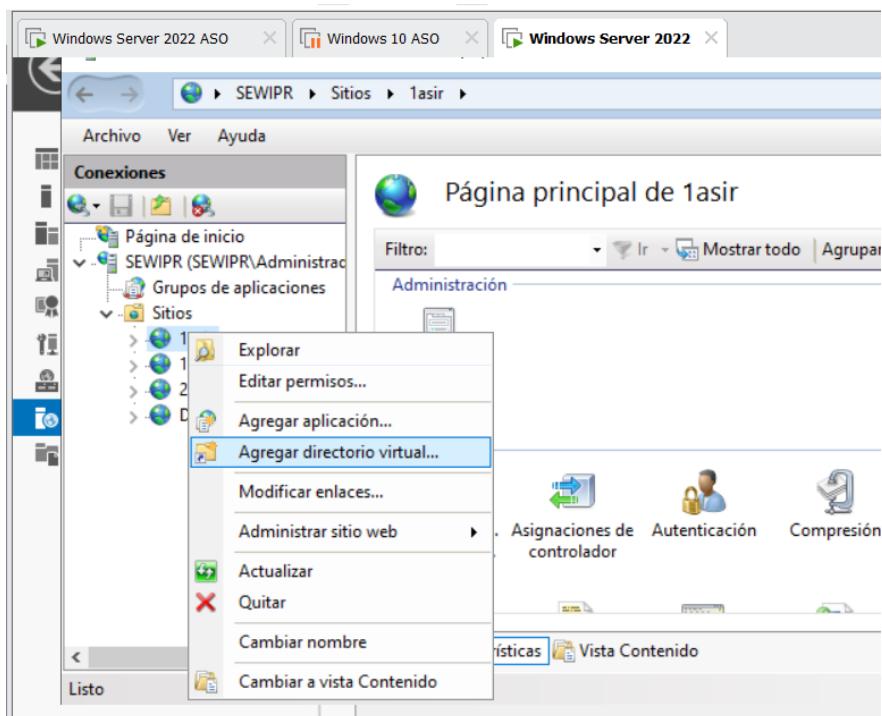
El orden que seguiremos será primero crear una carpeta, tanto de Redes como de Fundamentos Hardware y, cada una, tendrá su index correspondiente.



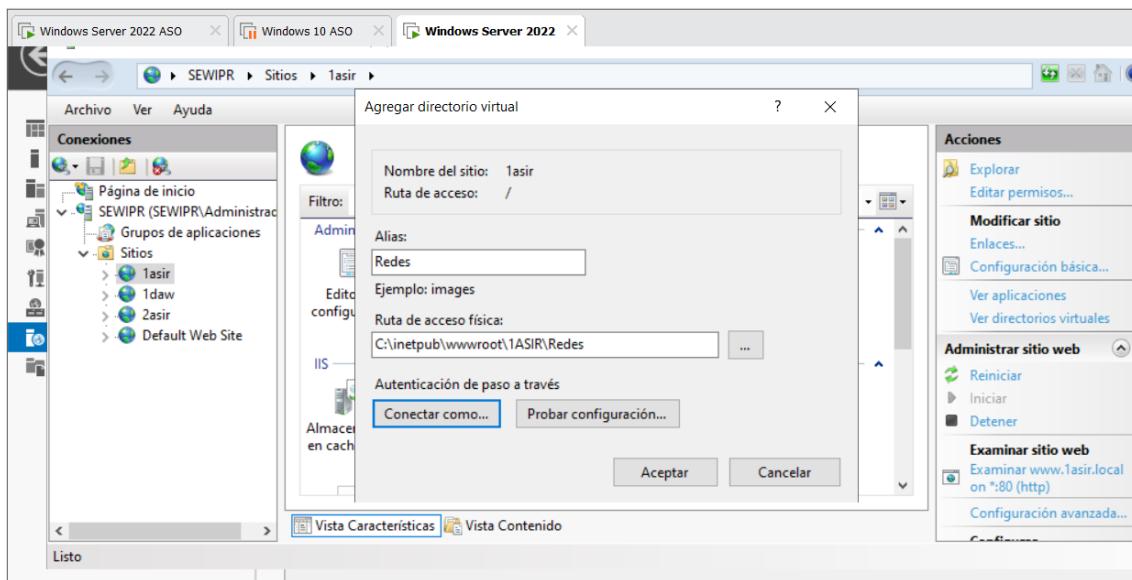
El enunciado nos solicita que la subpágina FundamentosHardware de la página 1asir tenga acceso restringido a un usuario llamado cliente. Por tanto, necesitamos tener autenticación básica para esta página. Continuaremos por tanto agregando los dos roles necesarios al servidor.



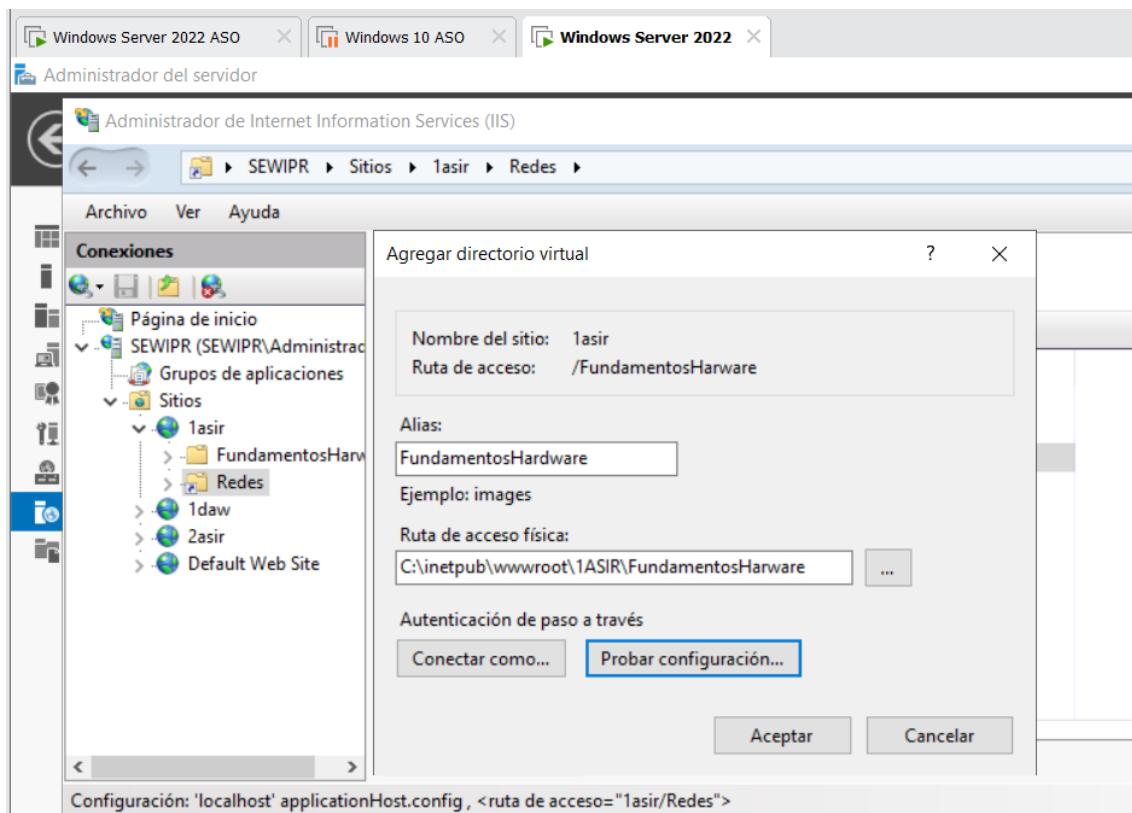
Crearemos un directorio virtual en 1ASIR de la siguiente manera.



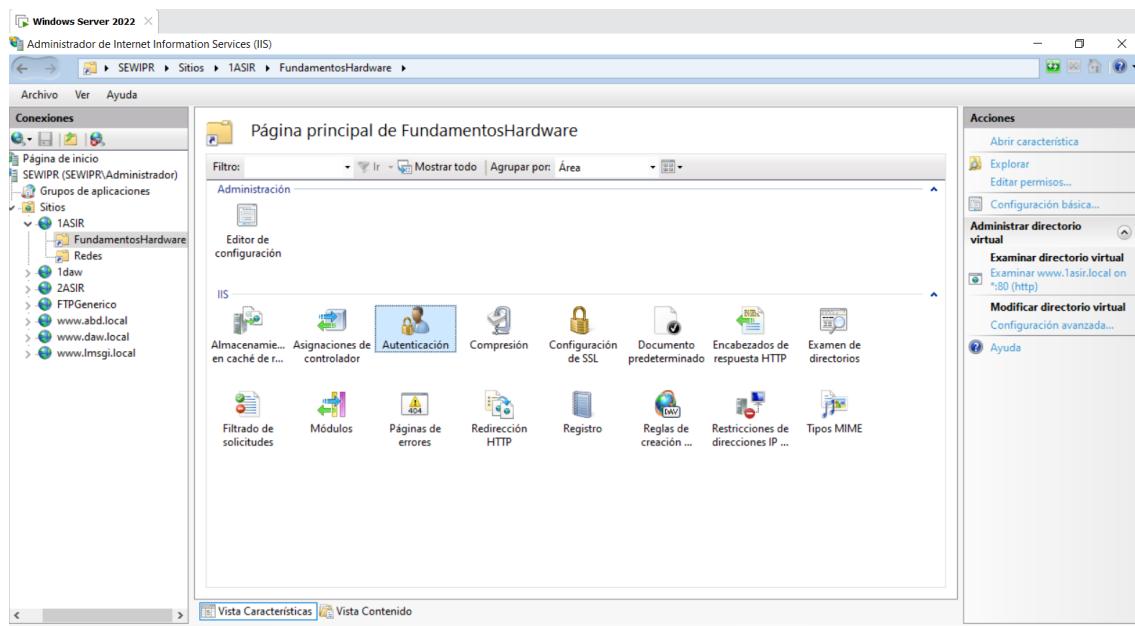
Configuraremos la ruta /redes, que no lleva autenticación básica.



Configuraremos ahora la ruta /FundamentosHardware, que sí lleva autenticación básica.



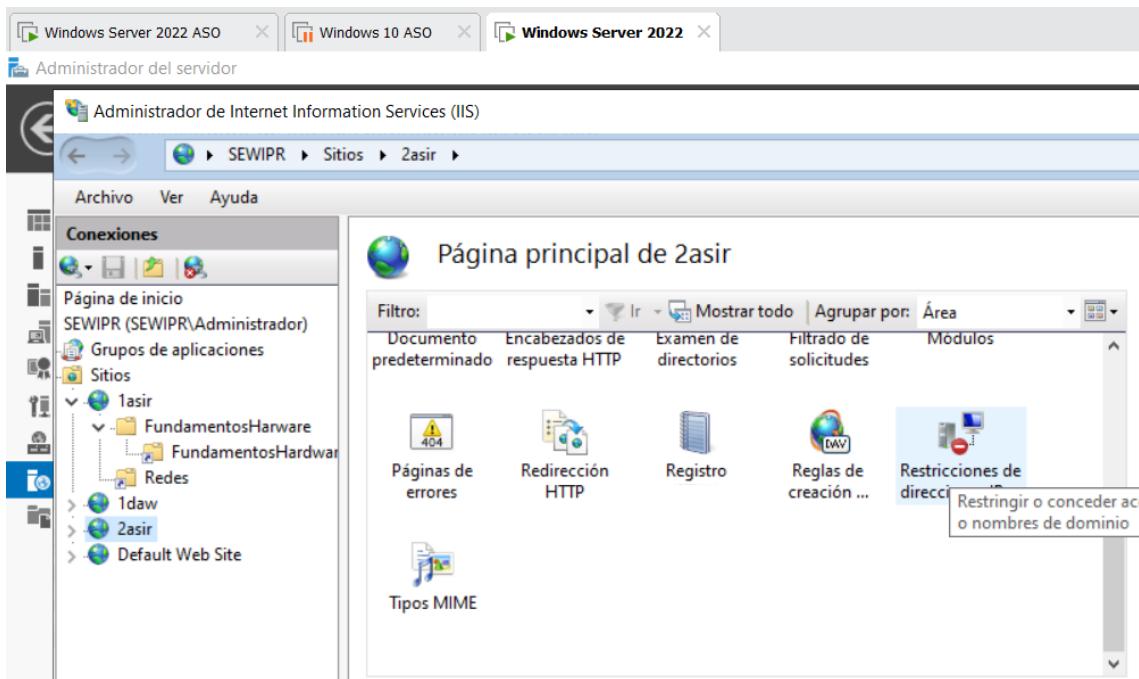
Seleccionamos el directorio virtual y hacemos doble clic en la opción de autenticación.



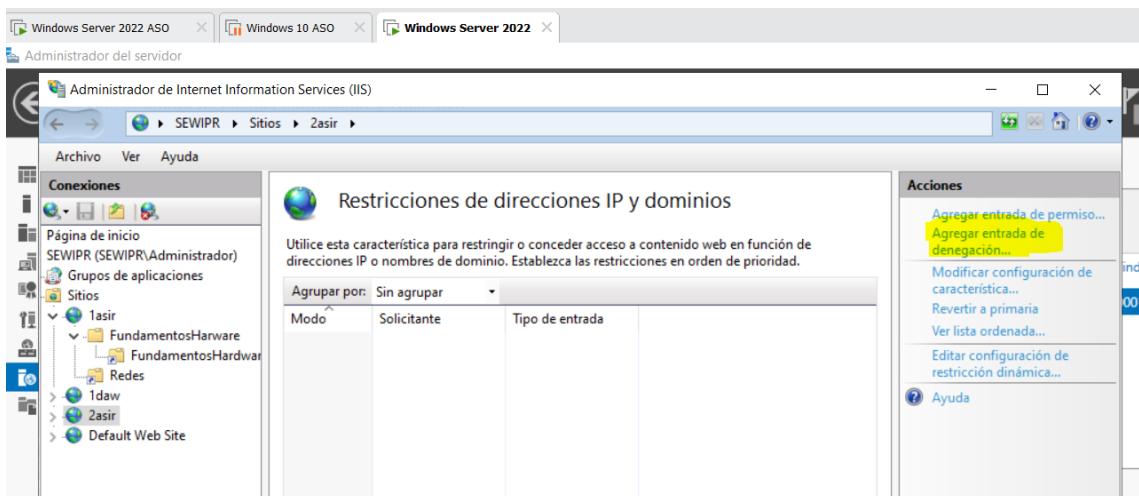
The screenshot shows the Windows Server 2022 Server Manager interface. The left navigation pane shows the site structure under 'Sitios' (Sites), with '2ASIR' selected. The main pane displays the 'Autenticación' (Authentication) configuration page. The 'Acciones' (Actions) pane on the right lists options like 'Examinar directorio virtual' (Examine directory virtual) and 'Modificar directorio virtual' (Modify directory virtual). The central pane shows a table of authentication methods:

Nombre	Estado	Tipo de respuesta
Autenticación anónima	Deshabilitada	
Autenticación básica	Deshabilitada	Desafío - HTTP 401
Autenticación de Windows	Habilitada	Desafío - HTTP 401
Suplantación de ASP.NET	Deshabilitada	

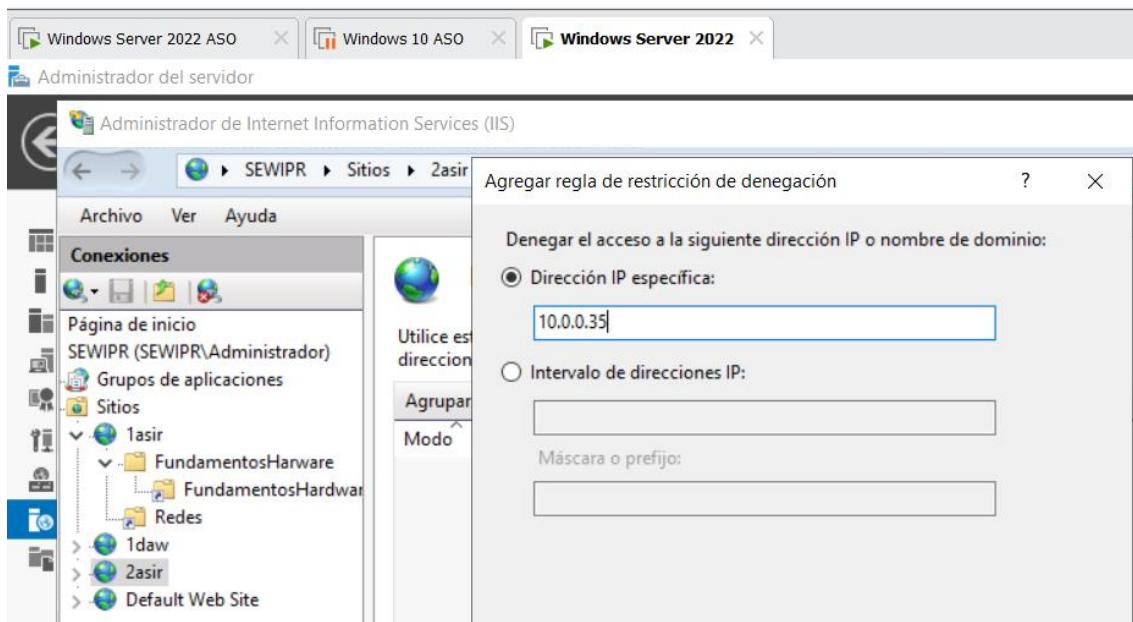
Continuamos con 2ASIR.



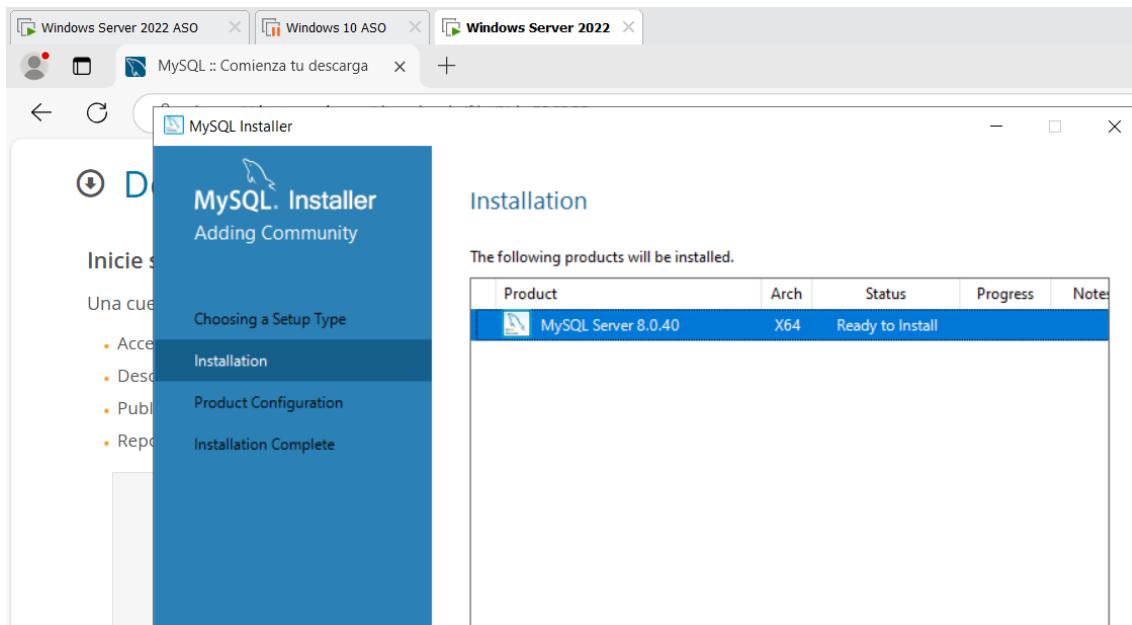
Hacemos clic con el botón derecho sobre las restricciones y le damos a abrir características. A continuación, agregamos entrada de denegación.



Y agregamos la ip 10.0.0.35 que es la que nos solicita el enunciado para bloquear.



Una vez realizado esto, continuamos con el montaje de Wordpress y, para ello, es necesario instalar primero un SQL <https://dev.mysql.com/downloads/installer/>



Instalaremos también el gestor de bases de datos PHPMyAdmin para tener acceso gráfico y una gestión más simple de nuestro sistema de bases de datos MySQL.

Descargamos y extraemos la última versión de PHP, en este caso la 8.4.1.

The screenshot shows the PHP download page at <https://windows.php.net/download/>. The page title is 'downloaded right from the PECL website.' It includes instructions for 'Which version do I choose?' for IIS and Apache, and a list of download links for 'VS17 x64 Thread Safe (2024-Nov-20 11:18:26)'.

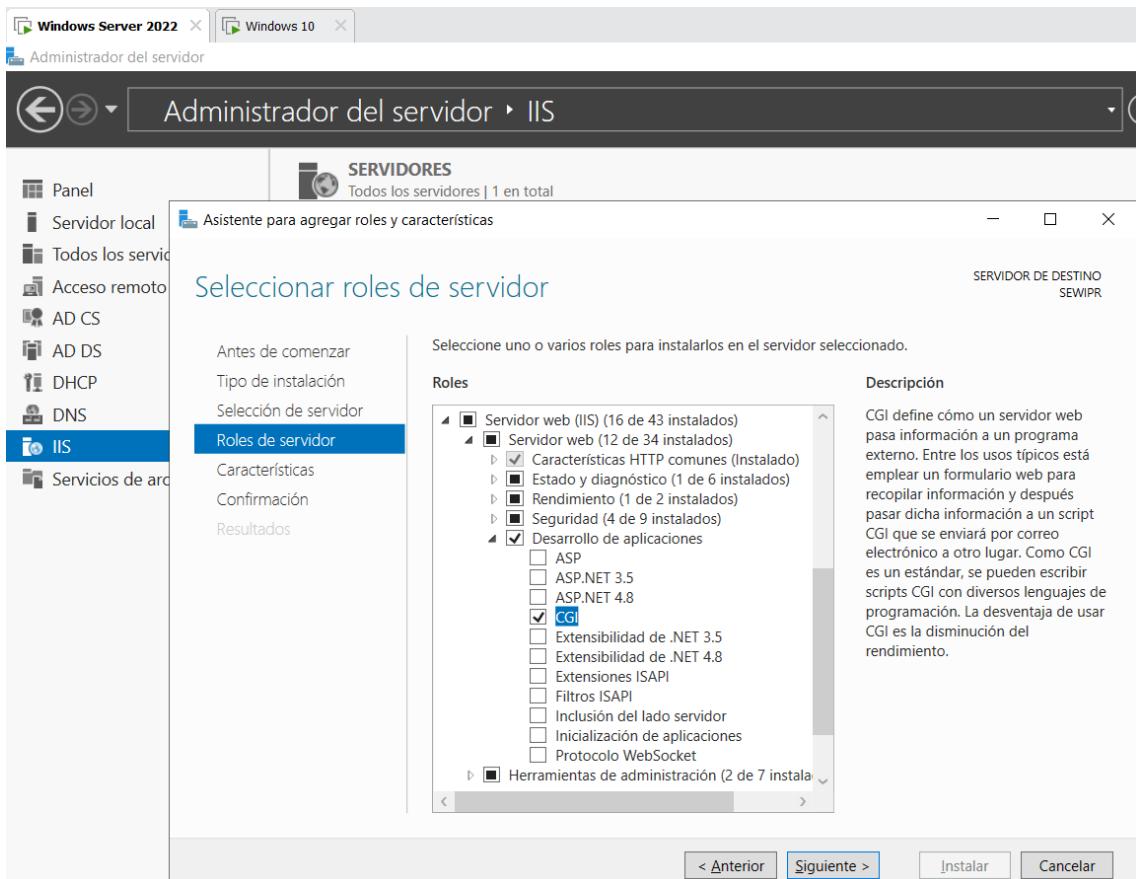
IIS
If you are using PHP as FastCGI with IIS you should use the Non-Thread Safe (NTS) versions of PHP.

Apache
Please use the Apache builds provided by [Apache Lounge](#). They provide VC15 and VS16 builds of Apache for x86 and x64. We use their binaries to build the Apache SAPIs.
With Apache, using the apache2handler SAPI, you have to use the Thread Safe (TS) versions of PHP

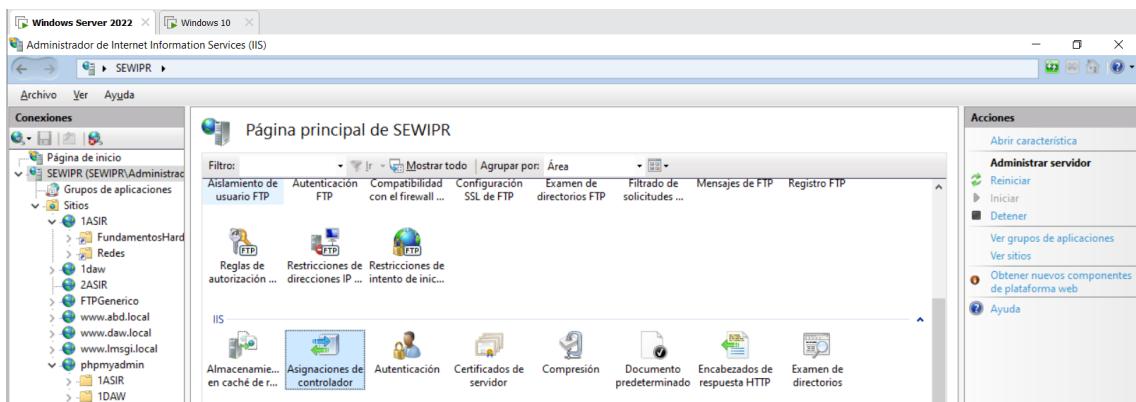
VS17 x64 Thread Safe (2024-Nov-20 11:18:26)

- [Zip \[32.33MB\]](#)
sha256: 020d265aa9aa2759dc527c16ce4749cb7b8b7f70ec13cac9237f428da2eb6ee
- [Debug Pack \[31.03MB\]](#)
sha256: 5fb9f657715931dabe055753eec99c71416b9d34ce20fe9e3424d497782bffde
- [Development package \(SDK to develop PHP extensions\) \[1.35MB\]](#)
sha256: 30327f2e746de1530c547e3ac71078f4c5e607b85ac0f60a4b154481c14892f0

PHP necesita del rol CGI para funcionar, así que instalamos este rol:



Tenemos que asignar el controlador descargado, seleccionamos nuestro servidor en IIS y clicamos la opción correspondiente:



Y pincharemos en “Aregar asignación de módulo” en el panel de la derecha:

The screenshot shows the IIS Manager interface. On the left, the 'Conexiones' pane lists several websites under 'SEWIPR (SEWIPR\Administrac...)'. The 'Sitios' section contains sites like 'FundamentosHard', 'Redes', '1daw', '2ASIR', 'FTPGenerico', 'www.abd.local', 'www.daw.local', 'www.lmsgi.local', 'phpmyadmin', '1ASIR', '1DAW', '2ASIR', and 'phpmyadmin'. The main pane displays a table titled 'Asignaciones de controlador' (Handler Mappings) with columns: Nombre (Name), Ruta de acceso (Access Path), Estado (Status), Tipo de ruta de... (Type of URL mapping), Controlador (Module), and Tipo de ent... (Type of entity). There are two sections: 'Deshabilitado' (Disabled) and 'Habilitado' (Enabled). Under 'Habilitado', there are entries for 'CGI-exe', 'OPTIONSVerbHandler', 'TRACEVerbHandler', 'WebDAV', and 'StaticFile'. The 'Acciones' (Actions) menu on the right includes options like 'Añadir controlador administrado...', 'Añadir asignación de script...', 'Añadir asignación de script comodín...', 'Añadir asignación de módulo...', 'Modificar permisos de características...', and 'Ver lista ordenada...'. The 'Añadir asignación de módulo...' option is highlighted with a red box.

Rellenamos el formulario indicando que queremos servir los archivos *.php con FastCgiModule y la ruta del ejecutable.

This screenshot shows the 'Agregar asignación de módulo' (Add module mapping) dialog box. It has fields for 'Ruta de acceso de solicitudes:' (Request path), which is set to '*.php'; 'Módulo:' (Module), which is set to 'FastCgiModule'; and 'Nombre:' (Name), which is set to 'PHP via FastCGI'. The dialog also includes a 'Ejecutable (opcional)' (Optional executable) field containing 'C:\php-8.4.1\php-cgi.exe'. At the bottom are 'Aceptar' (Accept) and 'Cancelar' (Cancel) buttons. The background shows the same IIS Manager interface as the previous screenshot, with the 'Sitios' list visible on the left.

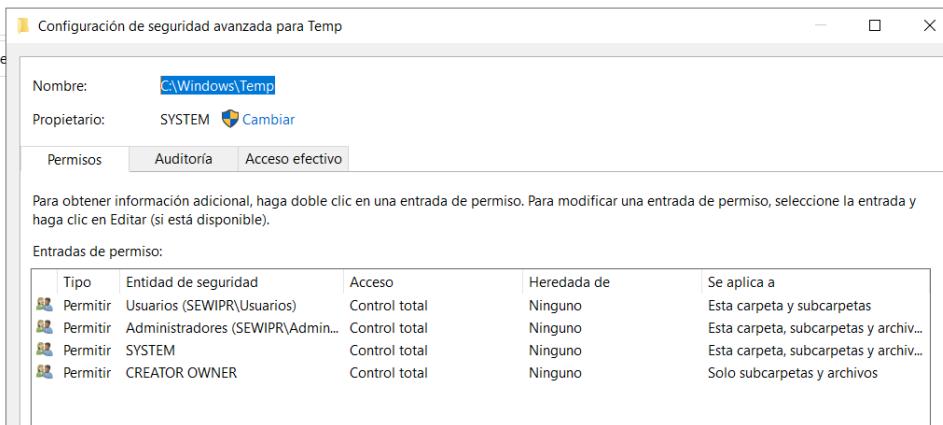
Necesitaremos instalar también Microsoft Virtual C++ Redistributable para que FastCGI funcione.

The screenshot shows a web browser window with the URL <https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170>. The left sidebar has a 'Version' dropdown set to 'Visual Studio 2022' and a 'Filter by title' input field. Below these are links for 'Redistribute an ATL application', 'Latest Supported Visual C++', and 'Redistributable Downloads'. The 'Redistributable Downloads' section lists three architectures: 'ARM64', 'X86', and 'X64'. The 'X64' section is expanded, showing a download link for 'Instalación de Microsoft Visual C++ 2015-2022 Redistri...' and a large preview image for 'Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.42.34433'. This preview image shows the 'TÉRMINOS DE LICENCIA DEL SOFTWARE DE MICROSOFT' (Microsoft Software License Terms) and 'MICROSOFT VISUAL C++ 2015 - 2022 RUNTIME' sections, along with a checked checkbox for 'Acepto los términos y condiciones de licencia' (I accept the terms and conditions of this license). At the bottom are 'Instalar' (Install) and 'Cerrar' (Close) buttons.

Necesitamos también descomentar y ampliar las siguientes líneas en el archivo C:\php-8.4.1\php.ini:

```
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT
session.save_path = "C:\Windows\temp"
extension_dir = "C:\php-8.4.1\ext"
extension=mysqli
```

A la carpeta C:\Windows\temp donde queremos guardar las sesiones le daremos control total a los Usuarios:



Y reiniciamos IIS:

```
C:\ Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.20348.587]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>iisreset

Intentando detener...
Servicios Internet detenidos correctamente
Intentando iniciar...
Servicios Internet reiniciados con éxito

C:\Users\Administrador>
```

Hecho todo esto, ya podemos acceder a phpmyadmin y crear una base de datos para nuestro wordpress:

```
1 create database wordpress;
2 create user 'wordpress'@'localhost' identified by 'usuario';
3 grant all privileges on wordpress.* to 'wordpress'@'localhost';
4 flush privileges;
```

Ya podemos descargar wordpress en un archivo zip:

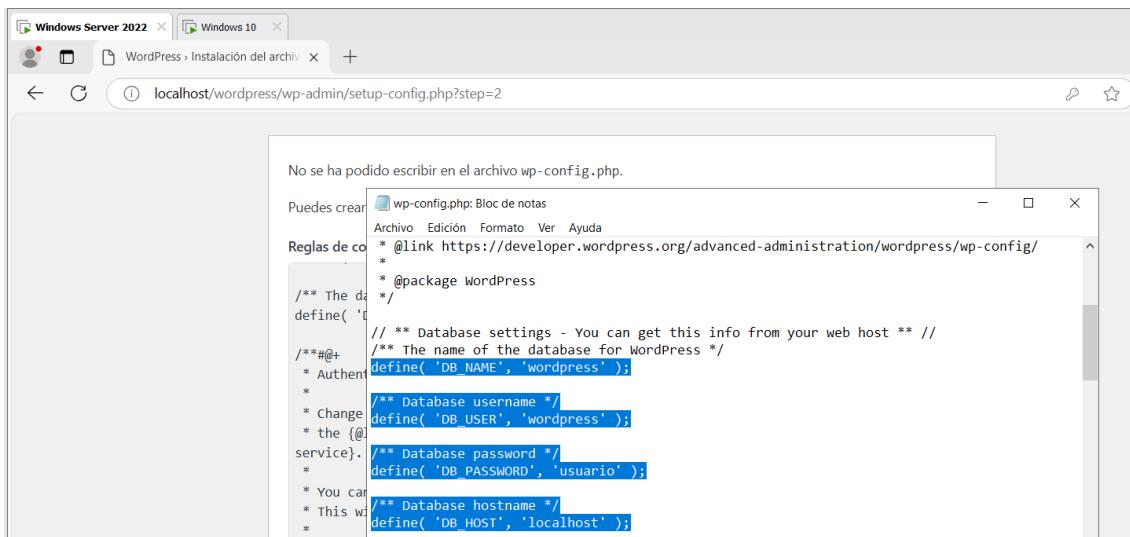
The screenshot shows a web browser window with the title "Descargar – WordPress.org Español". The URL in the address bar is "https://es.wordpress.org/download/". The page content includes the heading "Descárgalo e instálalo por tu cuenta" and the subtext "Para cualquiera que se sienta a gusto contratando su propio alojamiento y dominio." Below this are two main buttons: a large blue button labeled "Descarga WordPress 6.7.1" and a smaller white button labeled "Guía de instalación". Further down, there is a note about recommended PHP and MySQL versions, followed by links for "Versiones · Nocturnas · Contador · Origen".

Le daremos control total a los usuarios “IUSR” que son los de IIS:

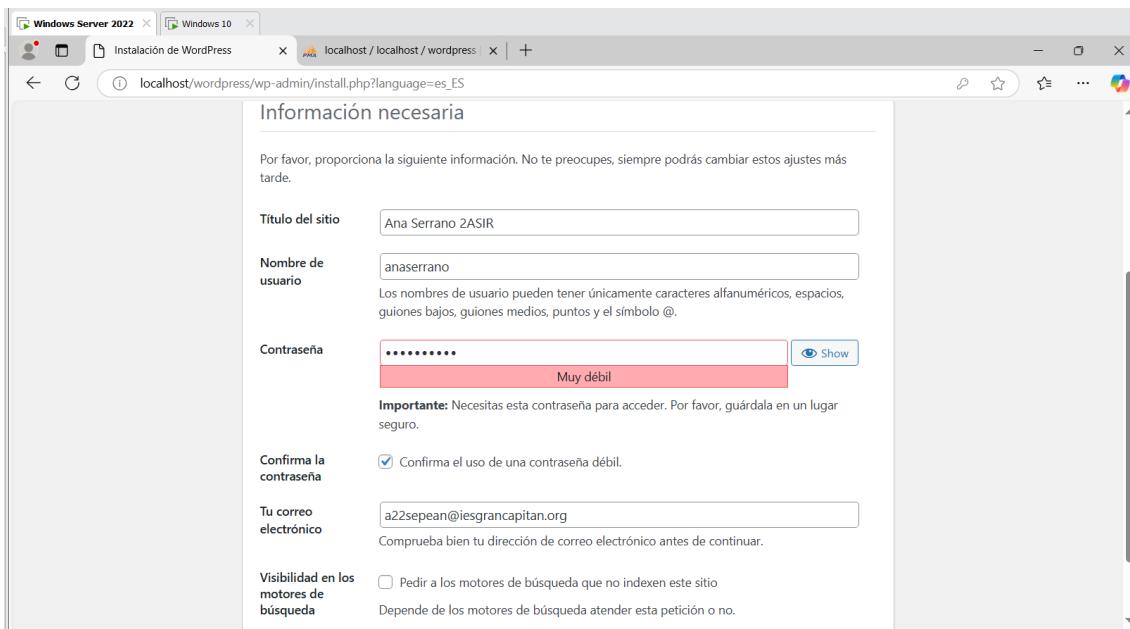
The screenshot shows a Windows File Explorer window with the path "Este equipo > Disco local (C:) > inetpub > wwwroot". A folder named "wordpress" is selected. A properties dialog box is open over the file list, specifically the "Seguridad" (Security) tab. In the "Nombres de grupos o usuarios:" (Names of groups or users:) list, the "IUSR" user is highlighted. The "Permisos de IUSR" (IUSR permissions) table shows the following settings:

Permiso	Permitir	Denegar
Control total	✓	
Modificar	✓	
Lectura y ejecución	✓	
Mostrar el contenido de la carpeta	✓	
Lectura	✓	
Escritura	✓	

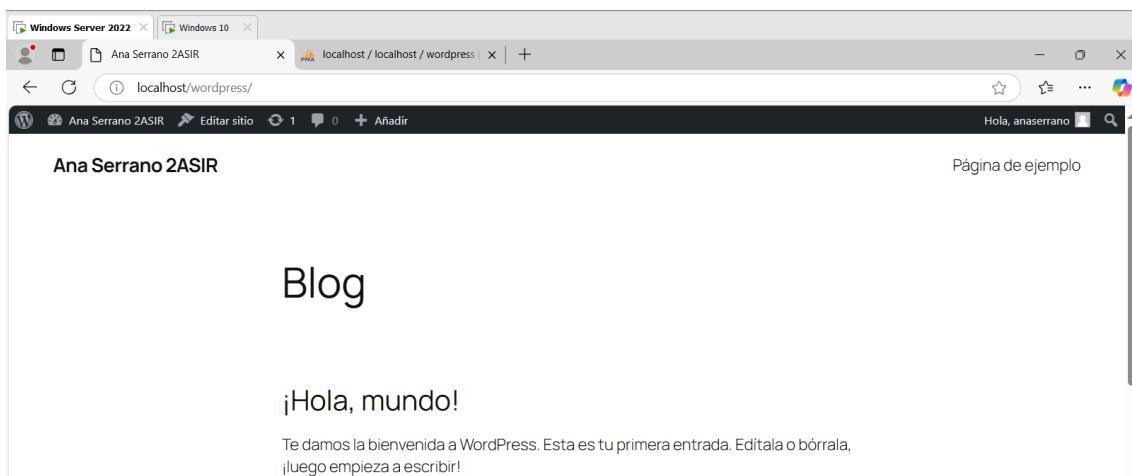
Accedemos a <http://localhost/wordpress> y ya vemos la página de instalación. Renombraremos wp-config-sample-inc.php a wp-config.php y le pondremos los datos de acceso a nuestra base de datos:



Y ya podemos continuar con la instalación:



Una vez terminada la instalación, vemos la página del blog de bienvenida de Wordpress:



4. A entregar las capturas de:

- 4.1. Captura accediendo desde un cliente a <http://www.1asir.local> así como a <https://www.1asir.local>

Comprobamos primero <http://www.1asir.local> en puerto 80:



A continuación, comprobamos <https://www.1asir.local> en puerto 443:



HTTP Error 404. The requested resource is not found.

Esto es lo esperado porque se requiere en el enunciado que este sitio sólo esté disponible en el puerto 80 (protocolo http).

4.2. Captura accediendo a la sección de 1asir llamada FundamentosHardware, donde se aprecie que se ha logueado el usuario llamado “cliente”

The screenshot shows a Windows Server 2022 desktop environment with two windows open: 'Windows Server 2022' and 'Windows 10'. The 'Windows 10' window is active and displays a browser with the URL 'www.1asir.local/FundamentosHardware/'. A 'Seguridad de Windows' (Windows Security) dialog box is overlaid on the browser. The dialog title is 'Inicie sesión para obtener acceso a este sitio' (Log in to access this site). It says 'Autorización requerida por http://www.1asir.local'. There are two input fields: the top one contains 'cliente' and the bottom one contains a password represented by '*****'. At the bottom are 'Aceptar' (Accept) and 'Cancelar' (Cancel) buttons.

¡Hola! Esta es la página de bienvenida de Fundamentos Hardware.

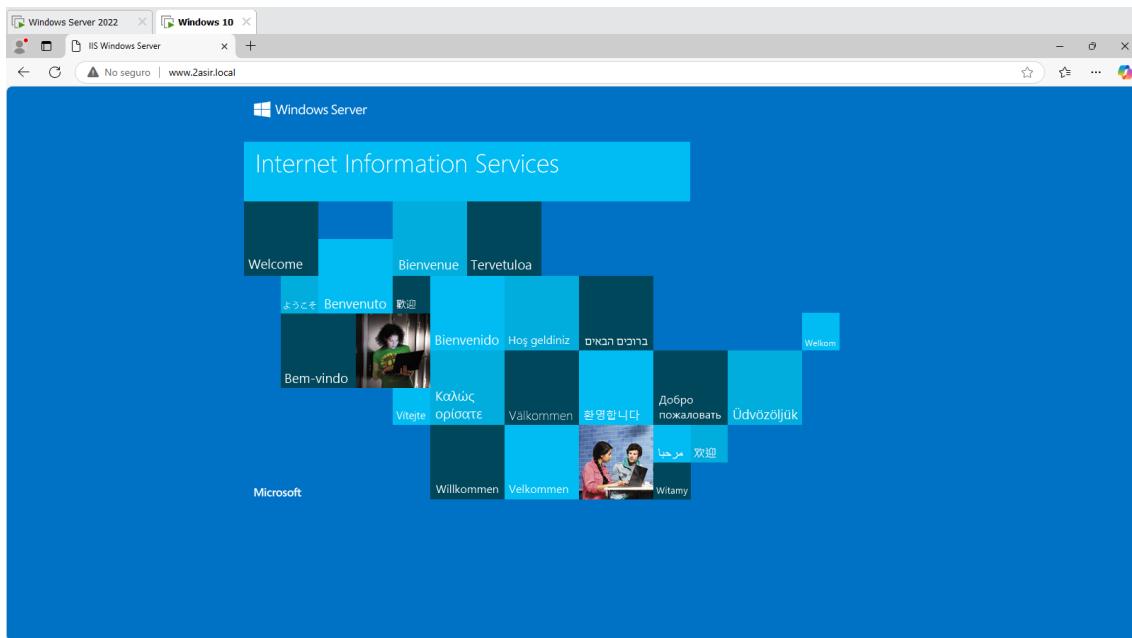
4.3. Captura accediendo a la sección de 1asir llamada Redes

The screenshot shows a Windows Server 2022 desktop environment with two windows open: 'Windows Server 2022' and 'Windows 10'. The 'Windows 10' window is active and displays a browser with the URL 'www.1asir.local/Redes/'. A 'Seguridad de Windows' (Windows Security) dialog box is overlaid on the browser. The dialog title is 'Inicie sesión para obtener acceso a este sitio' (Log in to access this site). It says 'Autorización requerida por http://www.1asir.local'. There are two input fields: the top one contains 'cliente' and the bottom one contains a password represented by '*****'. At the bottom are 'Aceptar' (Accept) and 'Cancelar' (Cancel) buttons.

¡Hola! Esta es la página de bienvenida de Redes.

4.4. Captura accediendo desde un cliente a <http://www.2asir.local> así como a <https://www.2asir.local>

Comprobamos primero <http://www.2asir.local> en puerto 80:



Esto es lo esperado porque se nos pide en el enunciado que solo configuremos el puerto 443 (protocolo https).

A continuación, comprobamos <https://www.2asir.local> en puerto 443:



Para que se cargue por defecto wordpress tenemos que poner index.php en primer lugar de los documentos predeterminados a buscar.

The screenshot shows the IIS Manager interface. On the left, the 'Conexiones' pane lists several sites, including '1ASIR' and '2ASIR'. The '2ASIR' site is selected. On the right, under 'Documento predeterminado', it says: 'Utilice esta característica para especificar los archivos predeterminados que se devuelven. Establezca los documentos predeterminados en orden de prioridad.' A table lists the default documents:

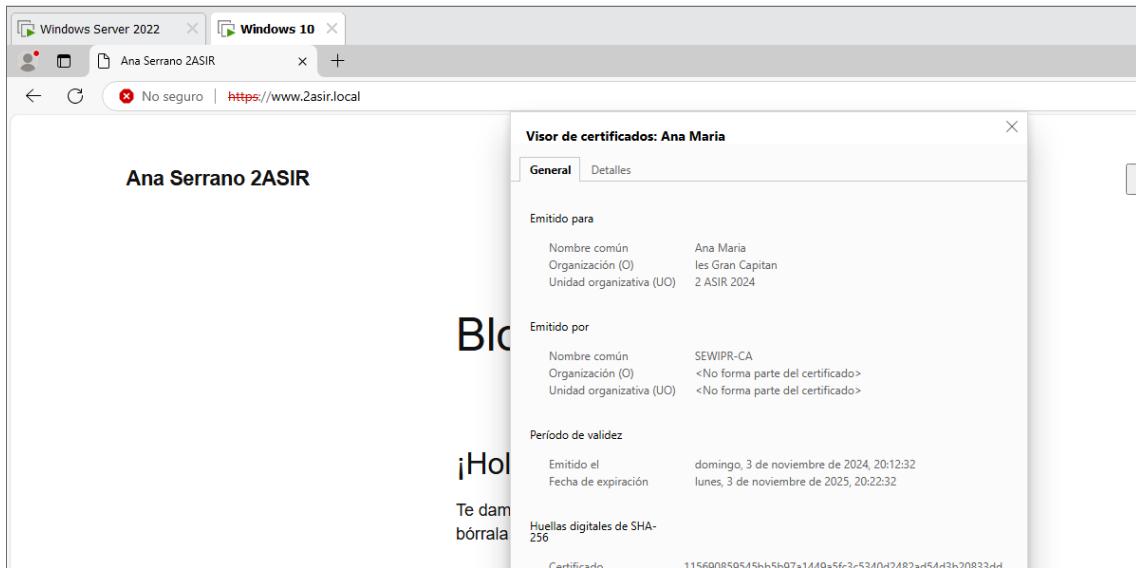
Nombre	Tipo de ent...
index.php	Heredada
Default.htm	Heredada
Default.asp	Heredada
index.htm	Heredada
index.html	Heredada
iisstart.htm	Heredada

Este sería el contenido completo de nuestra carpeta:

The screenshot shows the Windows File Explorer interface. The path 'Este equipo > Disco local (C:) > inetpub > wwwroot > 2ASIR' is selected. The left pane shows the file structure of the 2ASIR site. The right pane displays a list of files with their details:

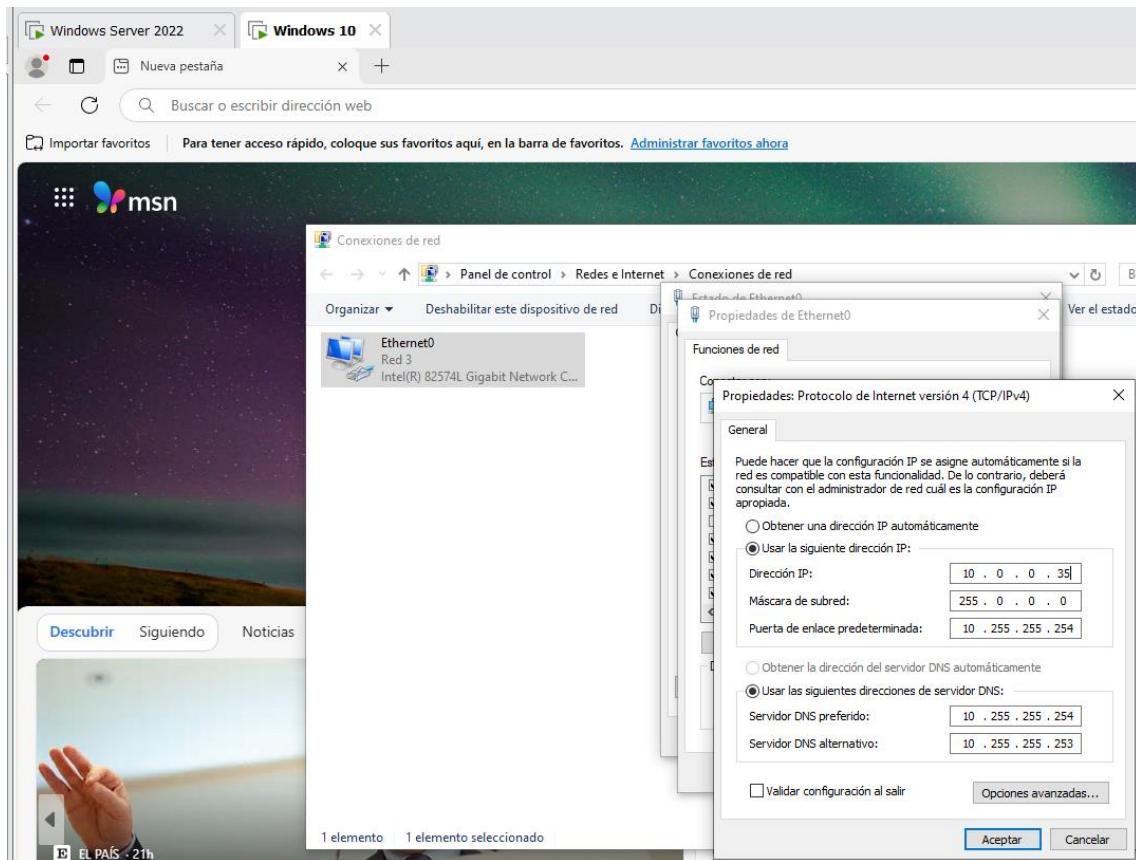
Nombre	Fecha de modificación	Tipo	Tamaño
wp-admin	07/12/2024 15:33	Carpeta de archivos	
wp-content	07/12/2024 15:34	Carpeta de archivos	
wp-includes	07/12/2024 15:35	Carpeta de archivos	
default.htm	02/11/2024 19:23	Microsoft Edge HT...	1 KB
index.php	07/12/2024 15:32	Archivo PHP	1 KB
license.txt	07/12/2024 15:32	Documento de tex...	20 KB
readme.html	07/12/2024 15:32	Microsoft Edge HT...	8 KB
web.config	07/12/2024 16:07	Archivo CONFIG	1 KB
wp-activate.php	07/12/2024 15:32	Archivo PHP	8 KB
wp-blog-header.php	07/12/2024 15:32	Archivo PHP	1 KB
wp-comments-post.php	07/12/2024 15:32	Archivo PHP	3 KB
wp-config.php	07/12/2024 15:47	Archivo PHP	4 KB
wp-config-sample.php	07/12/2024 15:32	Archivo PHP	4 KB
wp-cron.php	07/12/2024 15:32	Archivo PHP	6 KB
wp-links-opml.php	07/12/2024 15:32	Archivo PHP	3 KB
wp-load.php	07/12/2024 15:32	Archivo PHP	4 KB
wp-login.php	07/12/2024 15:32	Archivo PHP	51 KB
wp-mail.php	07/12/2024 15:32	Archivo PHP	9 KB
wp-settings.php	07/12/2024 15:32	Archivo PHP	29 KB
wp-signup.php	07/12/2024 15:32	Archivo PHP	34 KB

Comprobamos que el certificado SSL de la página es el generado durante la práctica.

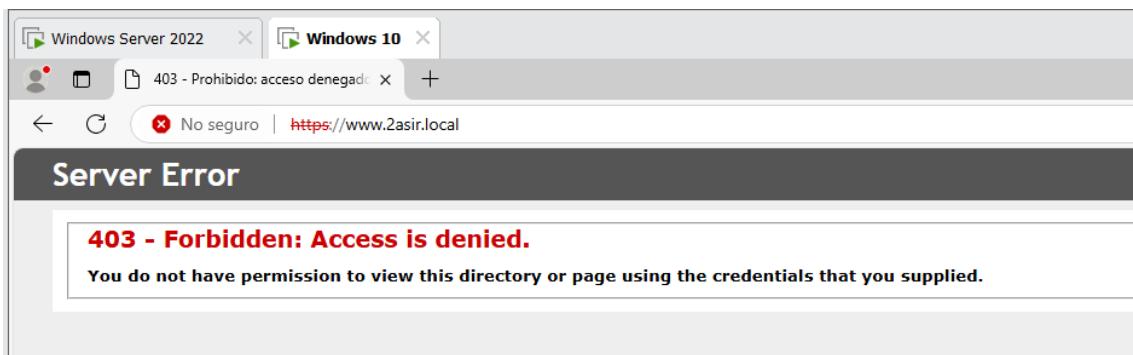


4.5. Captura accediendo al sitio de 2asir.local desde un cliente con ip 10.0.0.35

Cambiamos la IP del cliente:

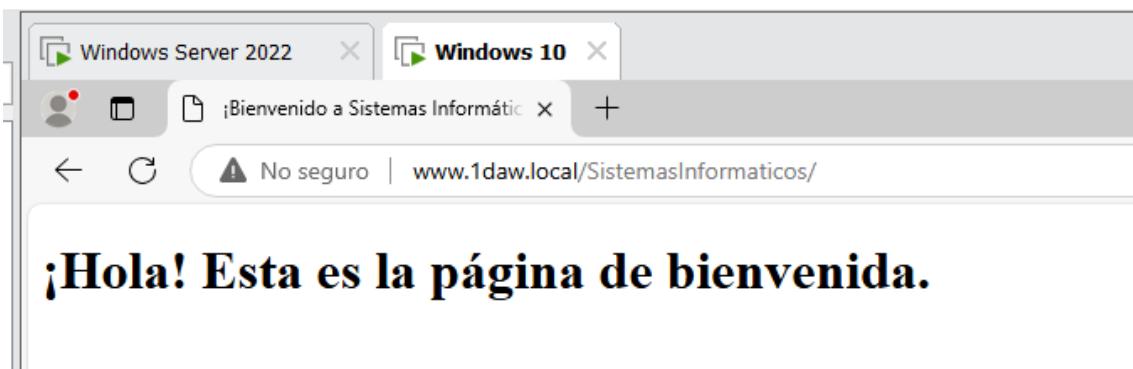


Intentamos acceder a <https://www.2asir.local> y vemos que no es posible.



4.6. Captura accediendo desde un cliente a <http://www.1daw.local> así como a <https://www.1daw.local>

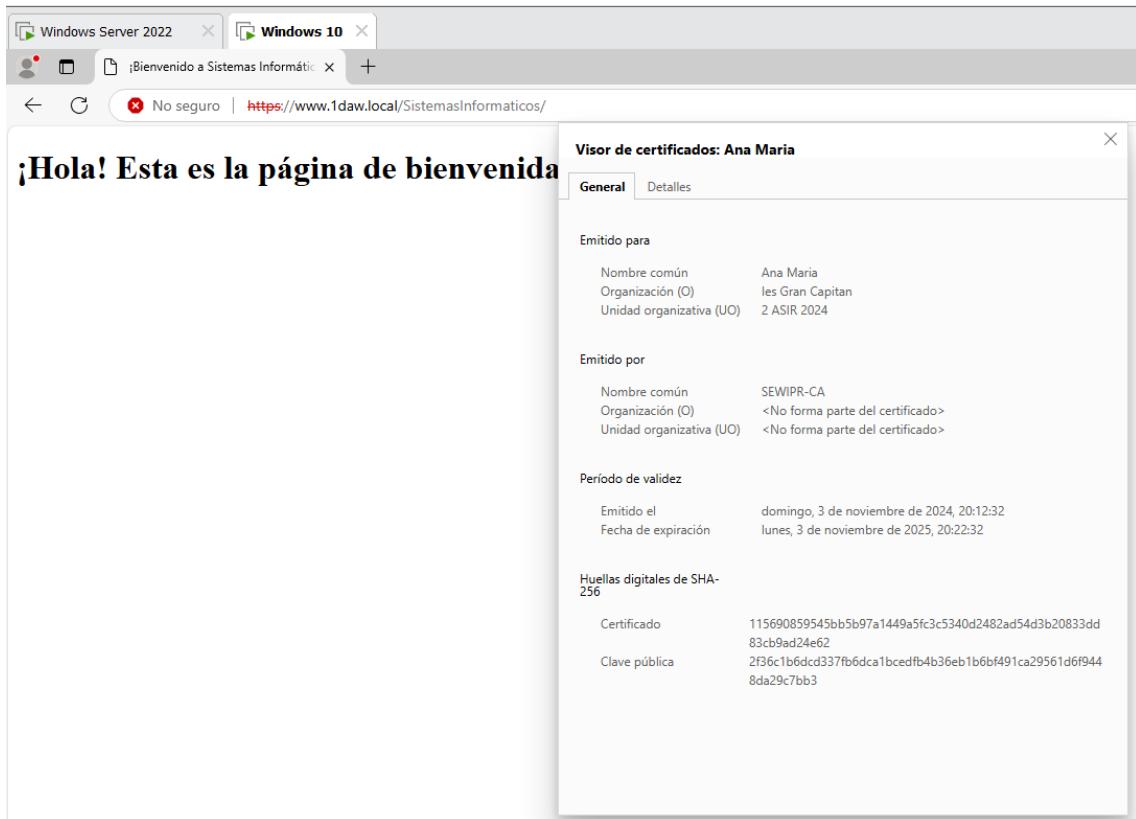
Comprobamos primero <http://www.1daw.local> en puerto 80. Comprobamos que se redirige correctamente a /SistemasInformaticos.



Vemos que ocurre lo mismo en la configuración con https.



Comprobamos también que el certificado SSL es el generado durante la práctica.



4.7. Captura donde se muestre que se ha realizado la redirección hacia la sección de sistemas informáticos dentro del sitio 1daw.local

Si abrimos el inspector web y nos vamos a "Red" podemos ver que se produce un 301 (redirección) hacia /SistemasInformaticos.

