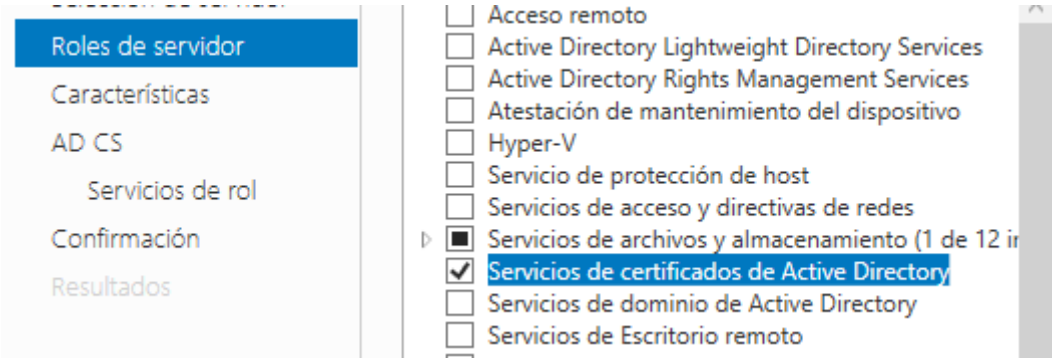
TEMA 2: Administración de credenciales de acceso a sistemas

Práctica 2.7: Creación de una PKI en Windows

En este caso vamos a mostrar como instalar una CA en un entorno Windows para poder emitir certificados y utilizarlos en los servicios de Windows.

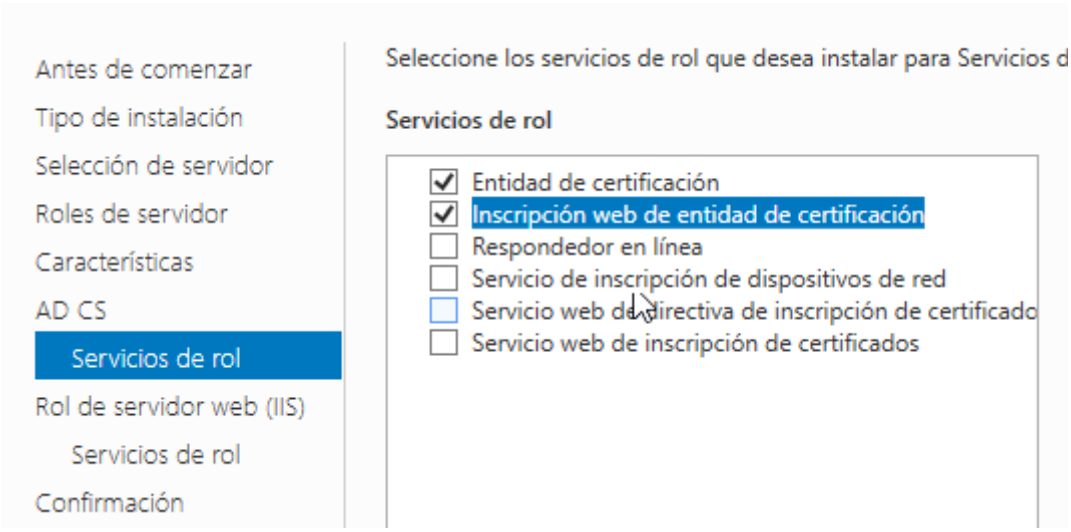
Desde el panel de administrador del servidor haremos una nueva instalación basada en características o en roles.

Y seleccionaremos “Servicios de certificados de Active Directory”

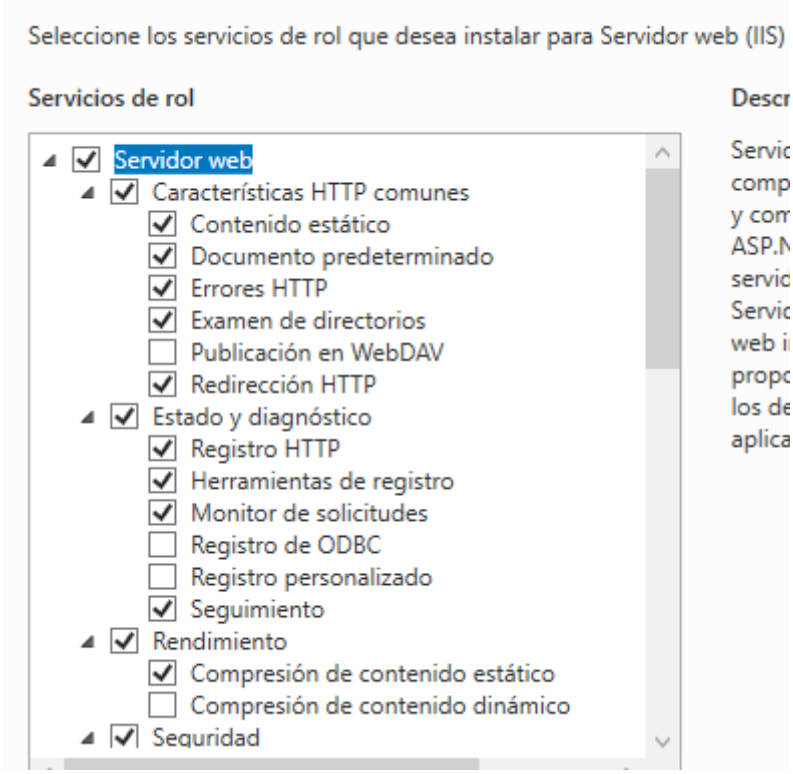


Servicios de certificados de Active Directory (AD CS) proporciona la infraestructura de certificados para habilitar escenarios como redes inalámbricas seguras, redes privadas virtuales, IPSec, protección de acceso a redes (NAP) y el sistema de cifrado de archivos (EFS).

Seleccionaremos los servicios de rol siguientes



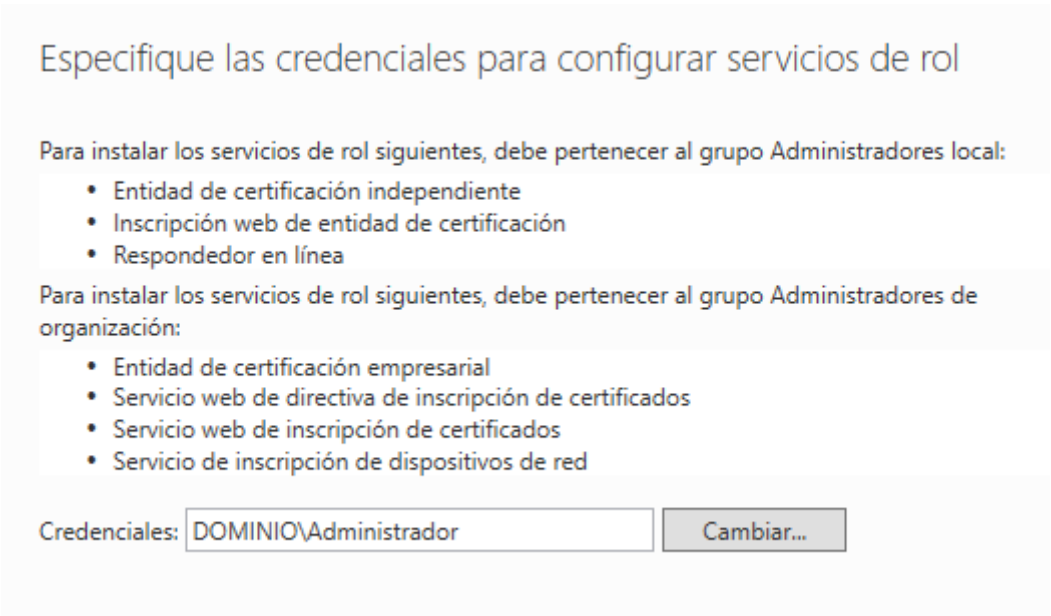
Dejaremos los servicios de rol para el Servidor web (IIS) como vienen por defecto.



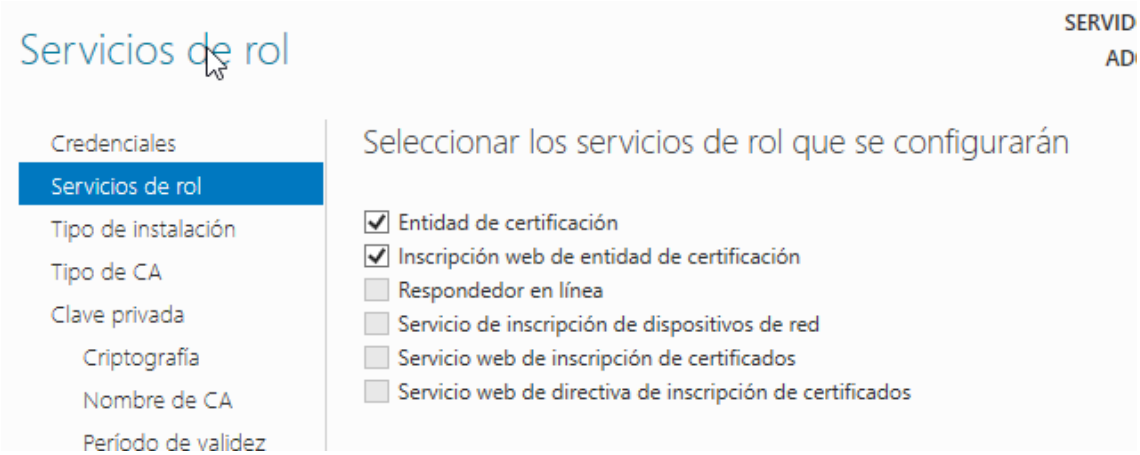
Y procedemos a instalar.

Seguidamente procedemos a configurar los servicios de rol instalados.

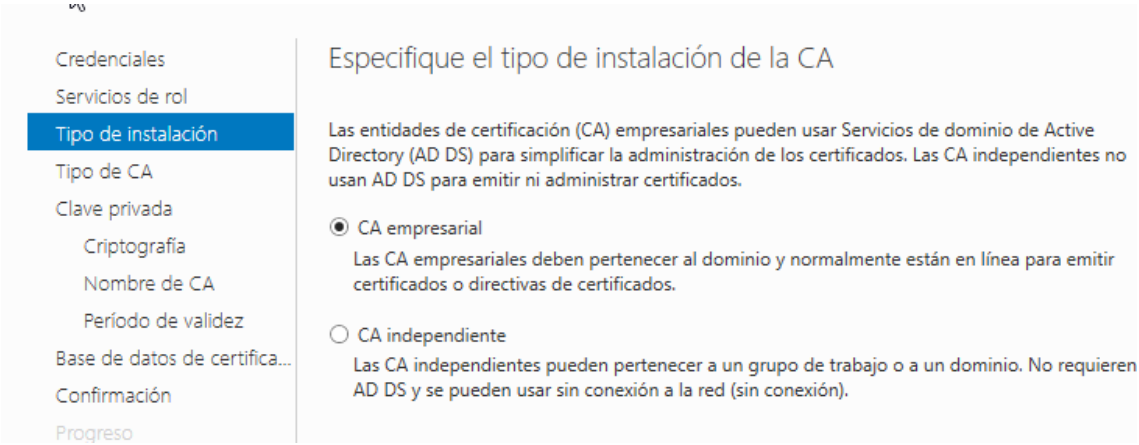
Durante el asistente dejamos las opciones por defecto



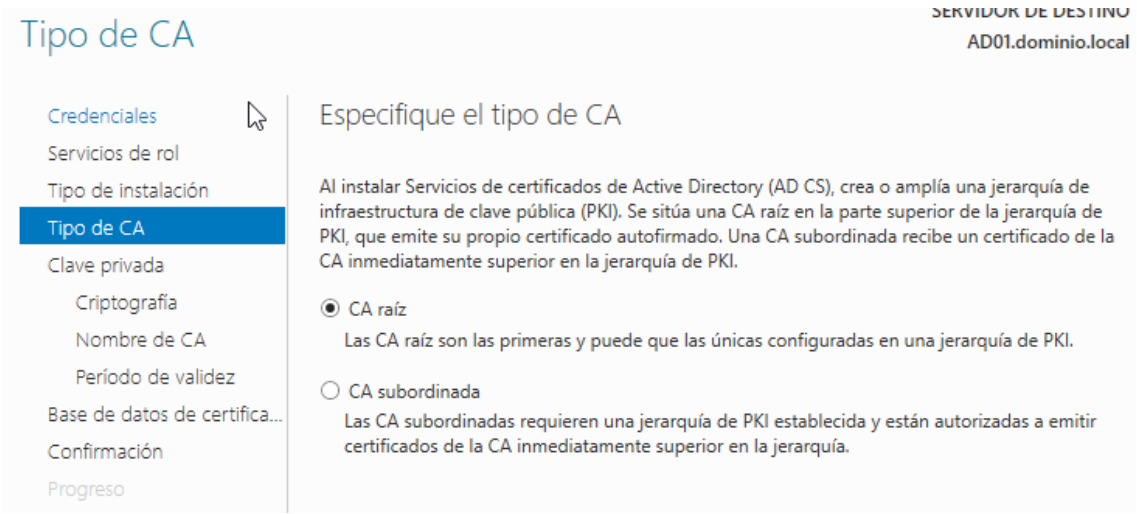
Y seleccionamos los servicios a configurar



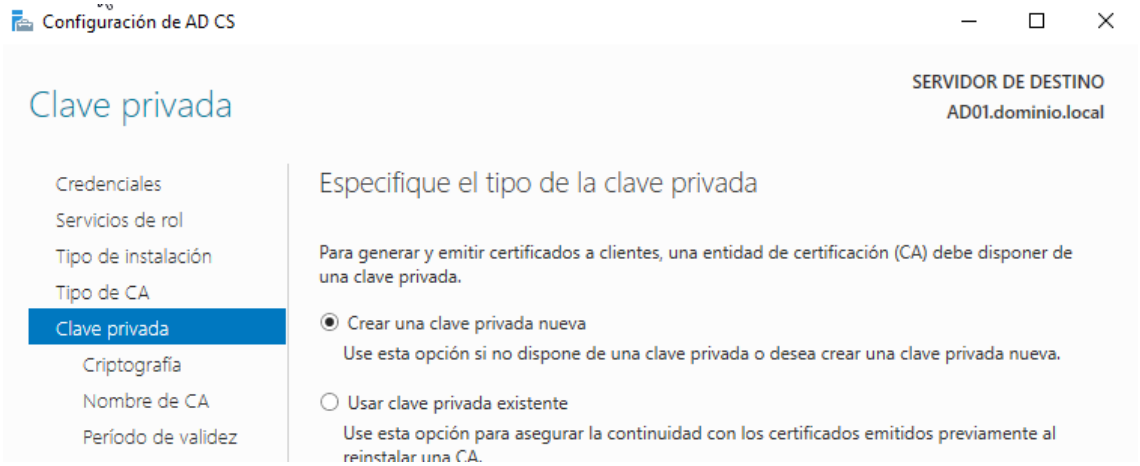
Realizamos una instalación de CA empresarial



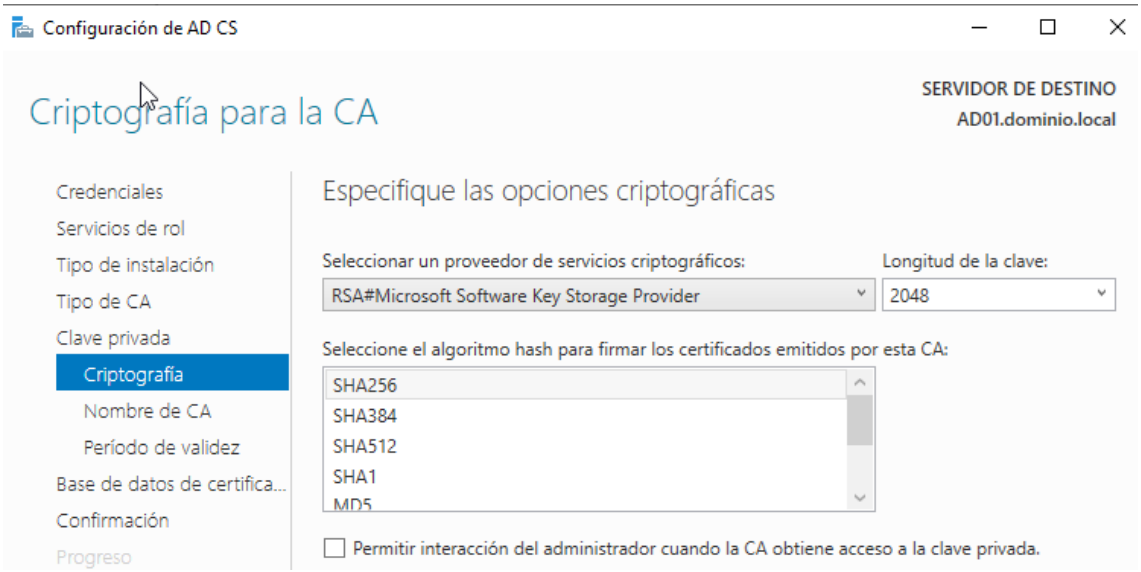
Y seleccionamos el tipo de CA raíz.



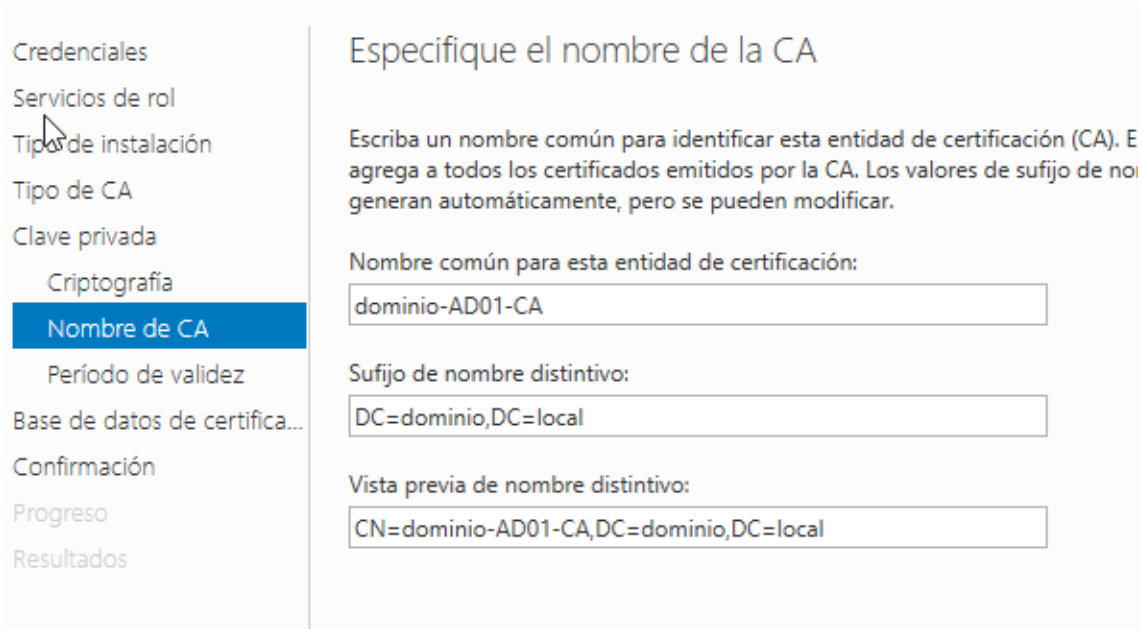
Seleccionamos crear una clave privada nueva.



Y dejamos las opciones criptográficas por defecto



Y especificamos un nombre para la CA. En este caso lo dejamos por defecto.



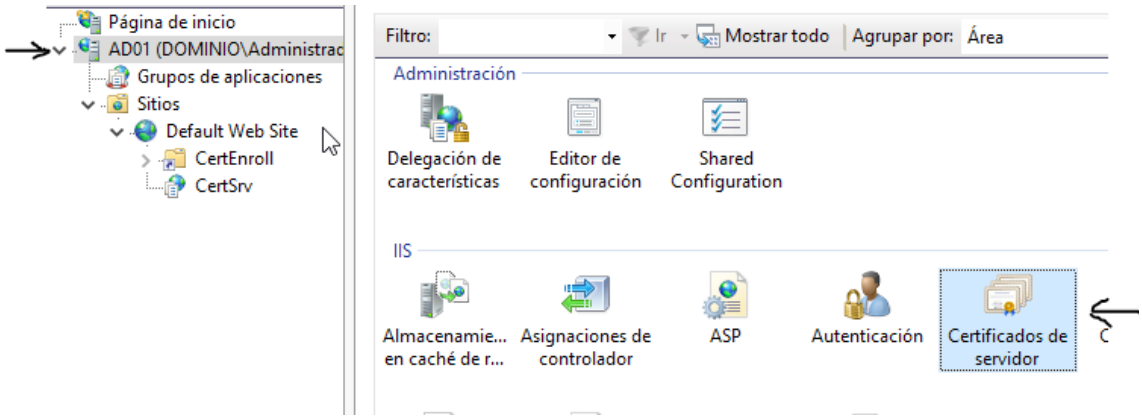
Seguimos el asistente hasta finalizar la instalación.

Cuando finalice tendremos instalada nuestra CA y podremos crear certificados mediante un explorador web entrando en la dirección http://localhost/certsrv

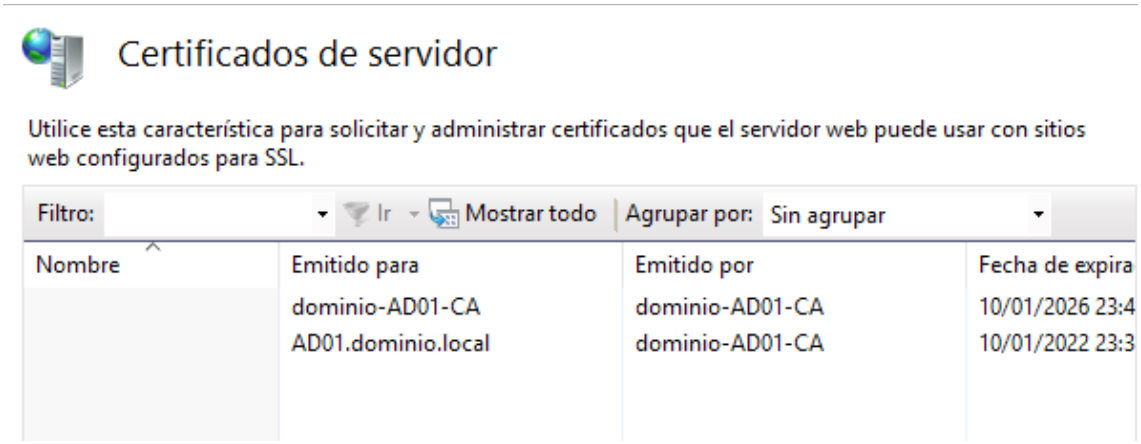
Si intentamos crear un certificado vía web, nos aparecerá un mensaje de advertencia que nos dice que nuestro sitio web necesita estar configurado para usar https.

Vamos a proceder a solucionar esto.

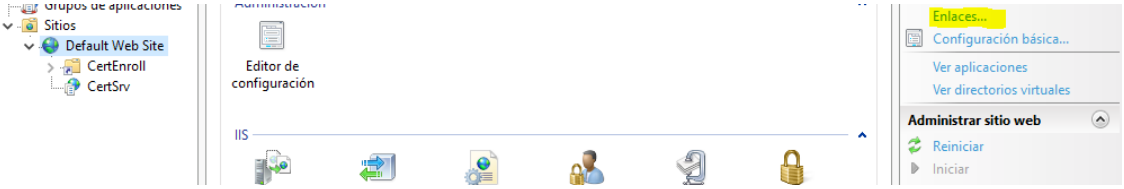
Nos dirigimos a nuestro servidor IIS y si seleccionamos “Certificados de servidor” dentro de “AD01”.



Vemos que tenemos un certificado AD01.dominio.local emitido por nuestra propia CA.



Vamos a asignar ese certificado a la página por defecto en el puerto 443. Para ello, seleccionamos “Default Web Site” y pinchamos sobre Enlaces…

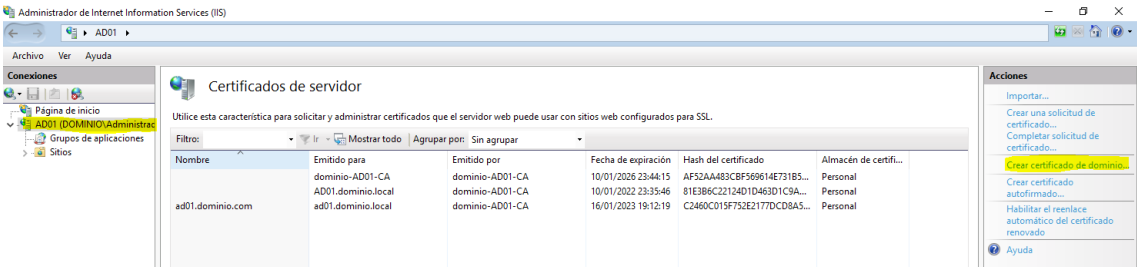


Y ahora si accedemos con un explorador a https://localhost/certsrv vemos que nos aparece la misma página desde la que podremos emitir certificados autofirmados.

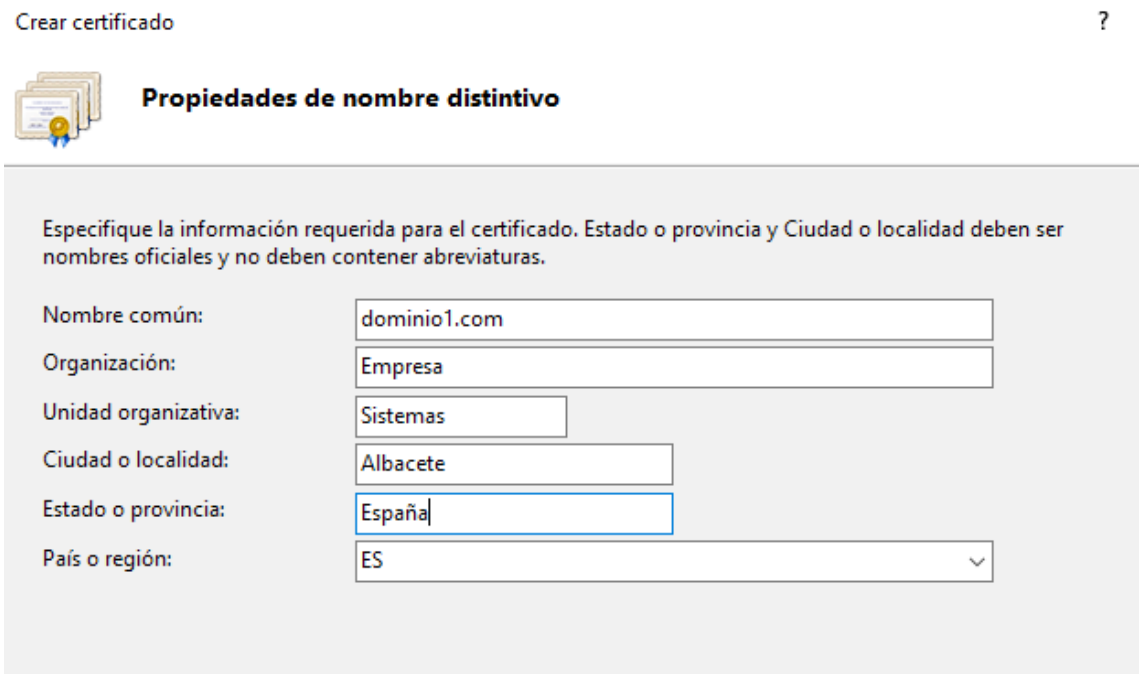
Practica 2.8: Configuración de dominios en IIS con SSL

Vamos a crear dos certificados para los dominios “dominio1.com” y “dominio2.com” de dos maneras distintas.

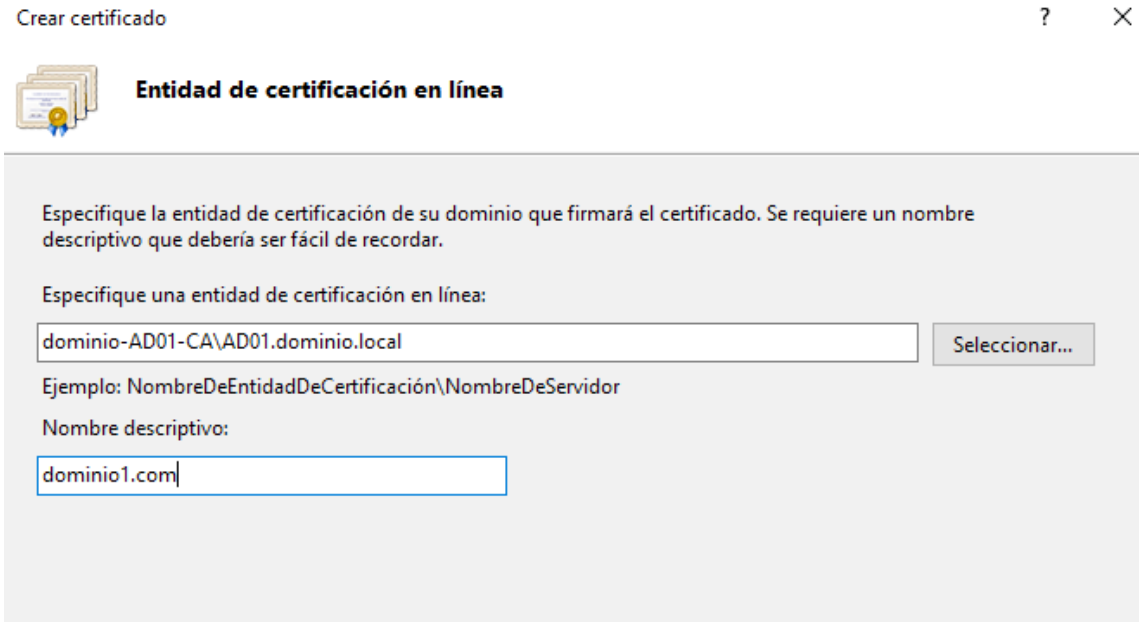
La primera será desde el servidor IIS mediante la opción “Crear certificado de dominio”. Para ello nos dirigimos al IIS y pinchando sobre el nombre, en las acciones disponibles seleccionamos “Crear certificado de dominio…”



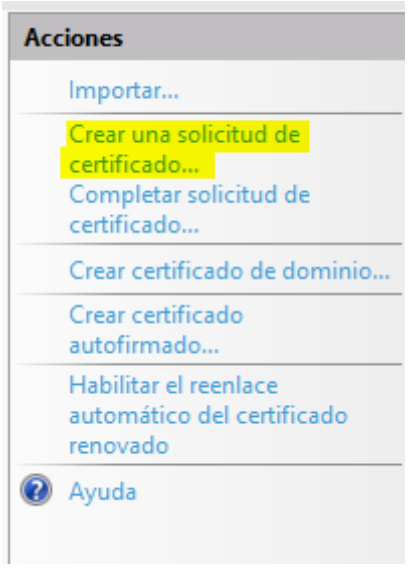
En el asistente rellenamos los campos con los datos sobre el dominio1.com



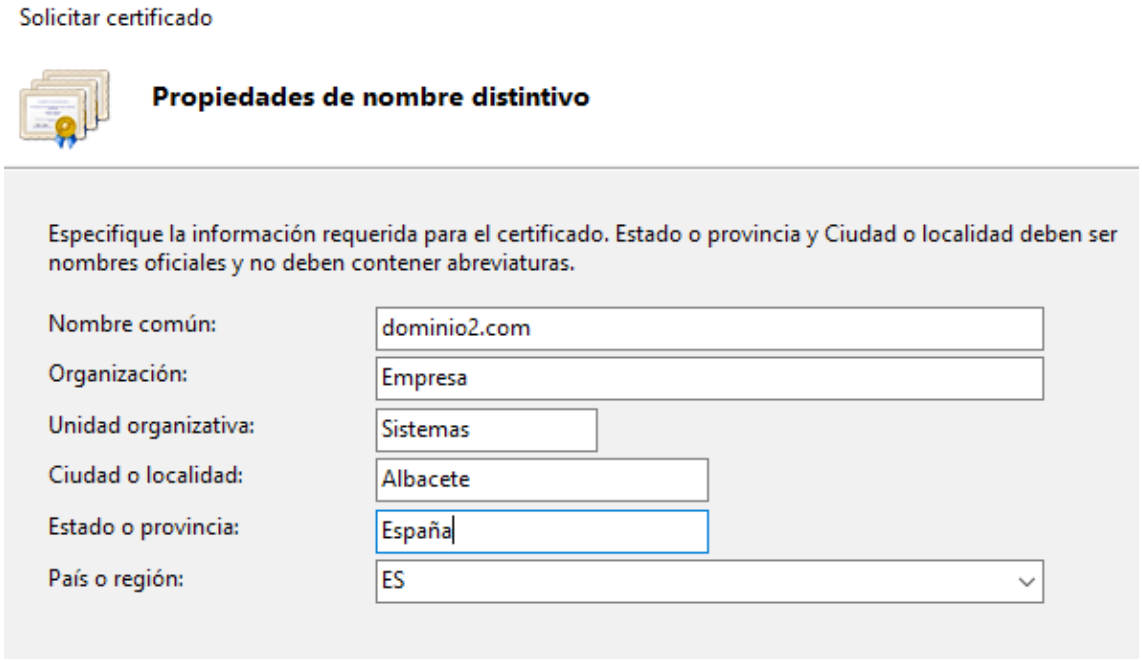
Y seleccionamos la entidad certificadora que hemos instalado en el servidor.

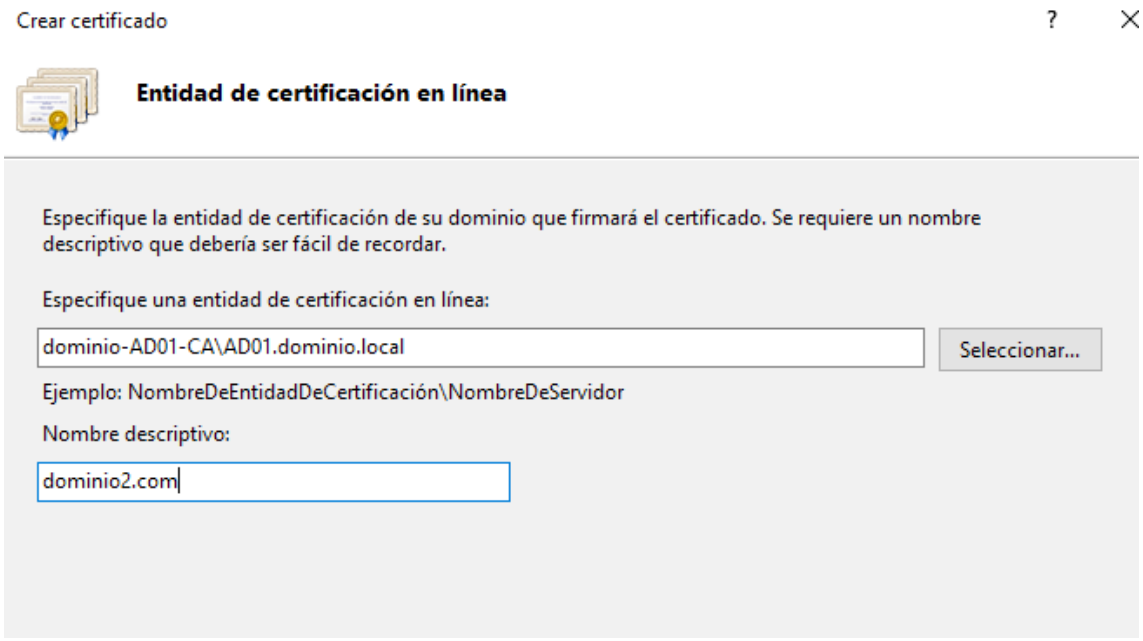


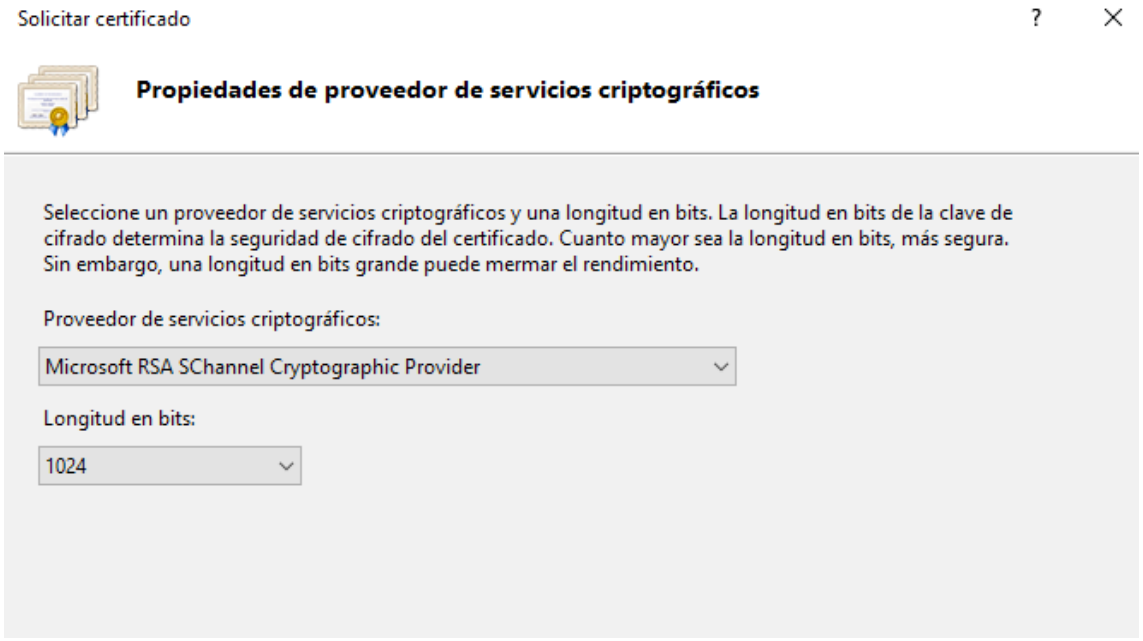
Para el segundo certificado, en este caso, nos dirigimos a nuestro IIS y pinchando sobre el nombre del servidor, en la sección “Acciones”, seleccionamos “Crear solicitud certificado”



Rellenamos los campos, poniendo como nombre común dominio2.com

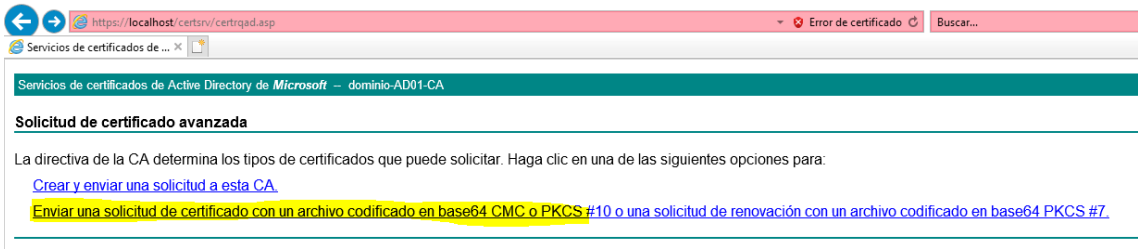




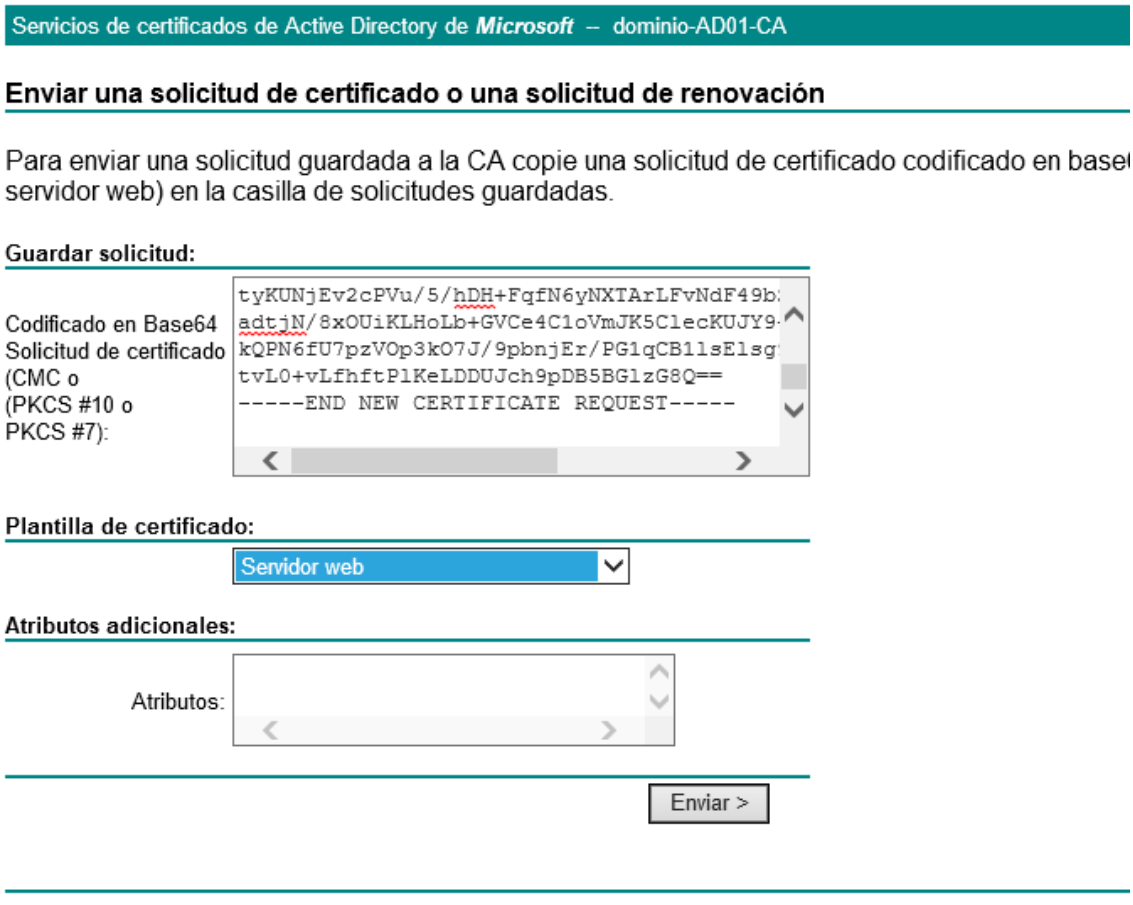


Le ponemos un nombre al archivo de la solicitud.

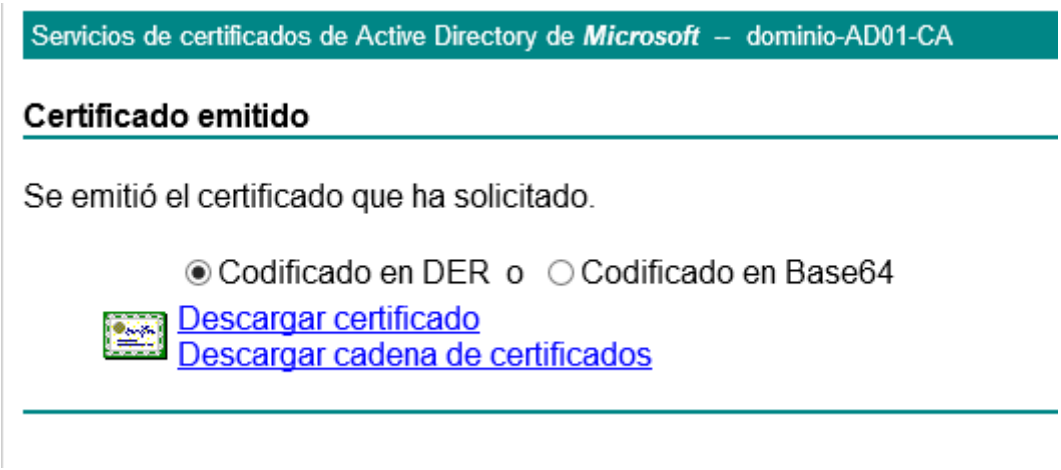
Seguidamente nos dirigimos a nuestro servidor de certificados vía web y seleccionamos la segunda opción.



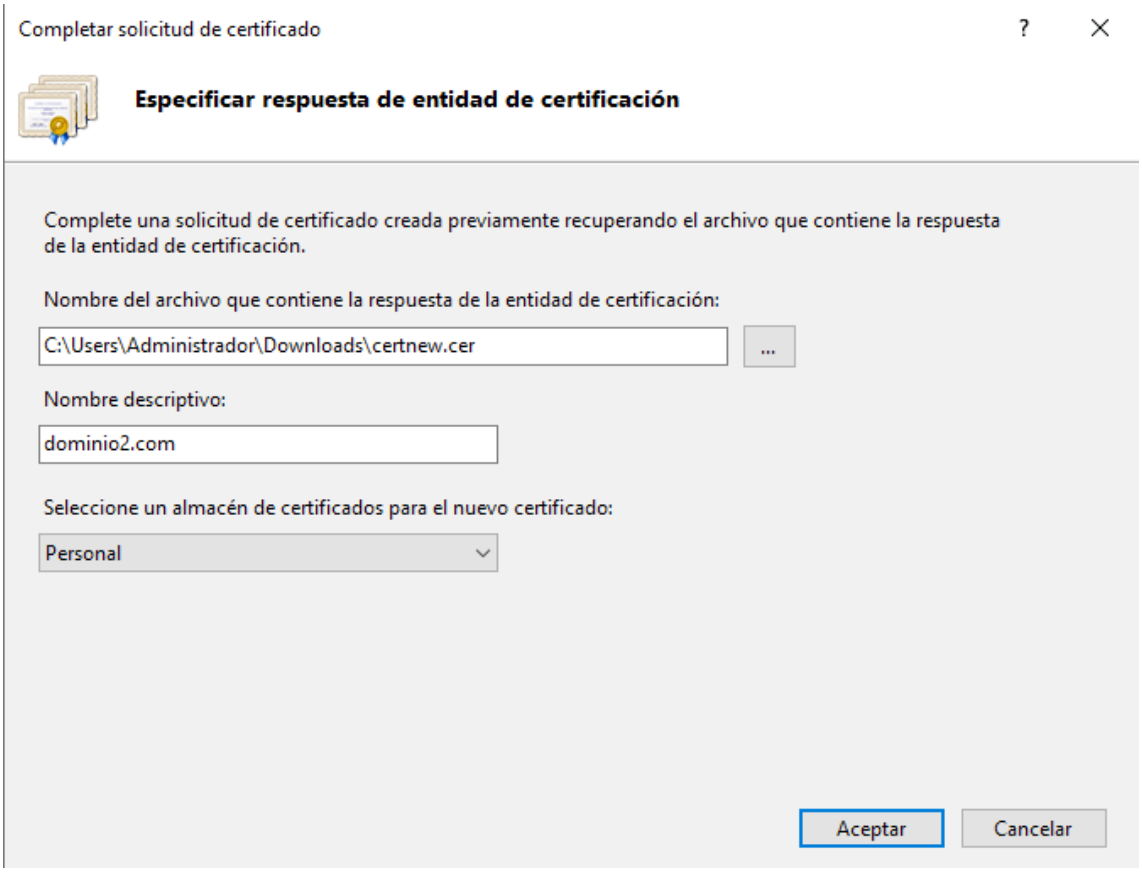
Copiamos el texto del archivo dominio2.com_csr.txt



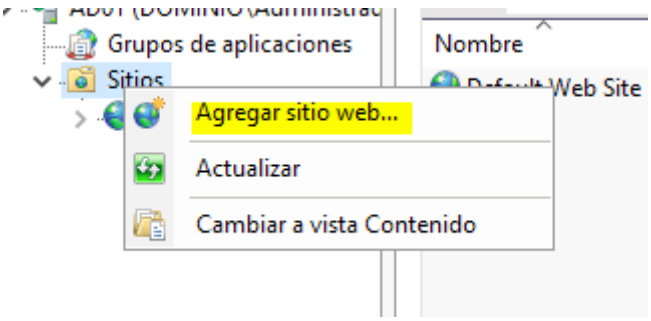
Y nos descargamos el certificado emitido en formato .cer

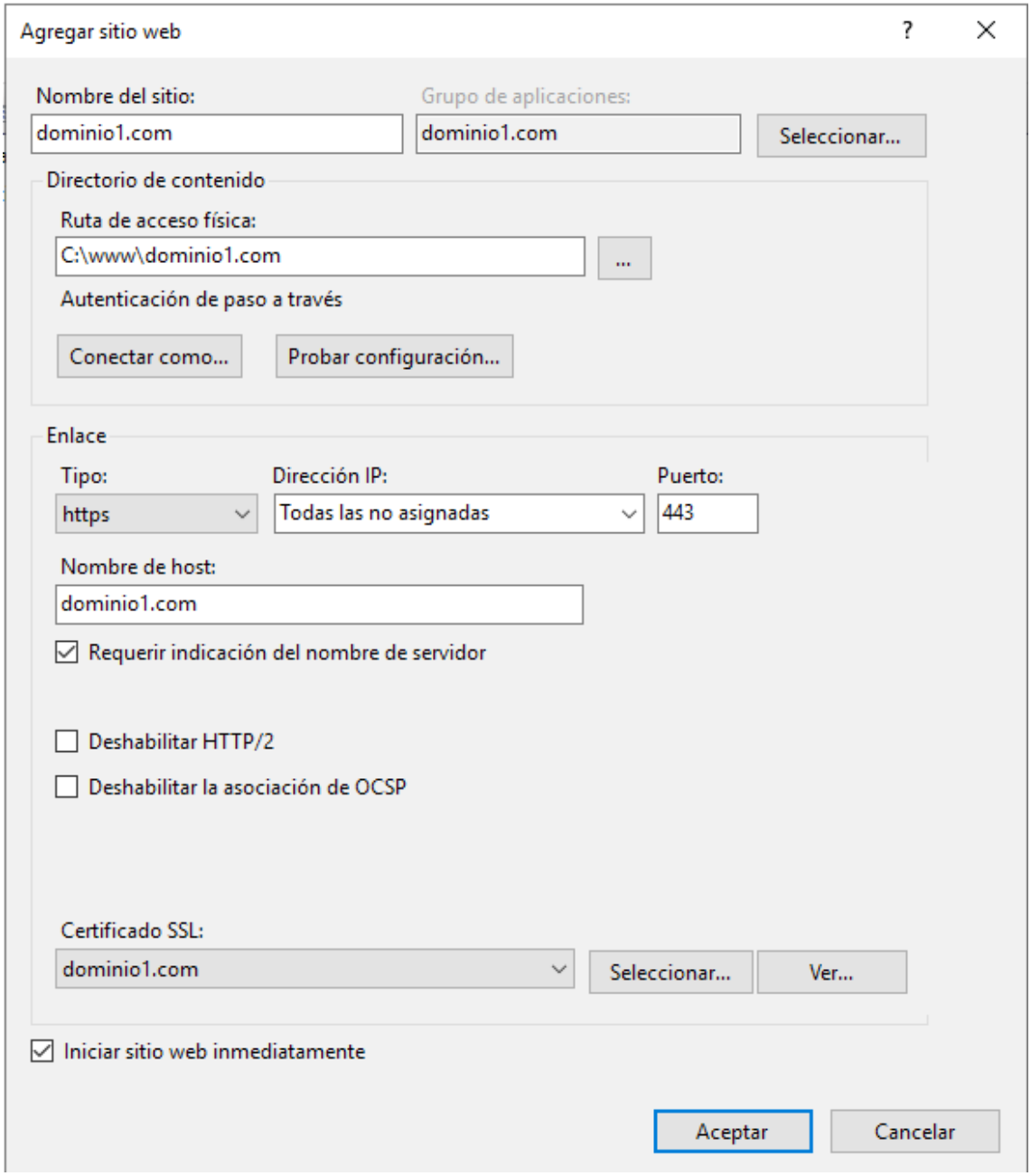


Para finalizar, nos dirigimos a nuestro IIS y completamos la solicitud del certificado.



Llegados a este punto solamente nos queda crear los sitios web y asignarles un certificado.




Agregar sitio web
Nombre del sitio:
dominio1.com
Grupo de aplicaciones:
dominio1.com
Seleccionar...
Directorio de contenido
Ruta de acceso física:
C:\www\dominio1.com
...
Autenticación de paso a través
Conectar como...
Probar configuración...
Enlace
Tipo:
https
Dirección IP:
Todas las no asignadas
Puerto:
443
Nombre de host:
dominio1.com
Requerir indicación del nombre de servidor
Deshabilitar HTTP/2
Deshabilitar la asociación de OCSP
Certificado SSL:
dominio1.com
Seleccionar...
Ver...
Iniciar sitio web inmediatamente
Aceptar
Cancelar