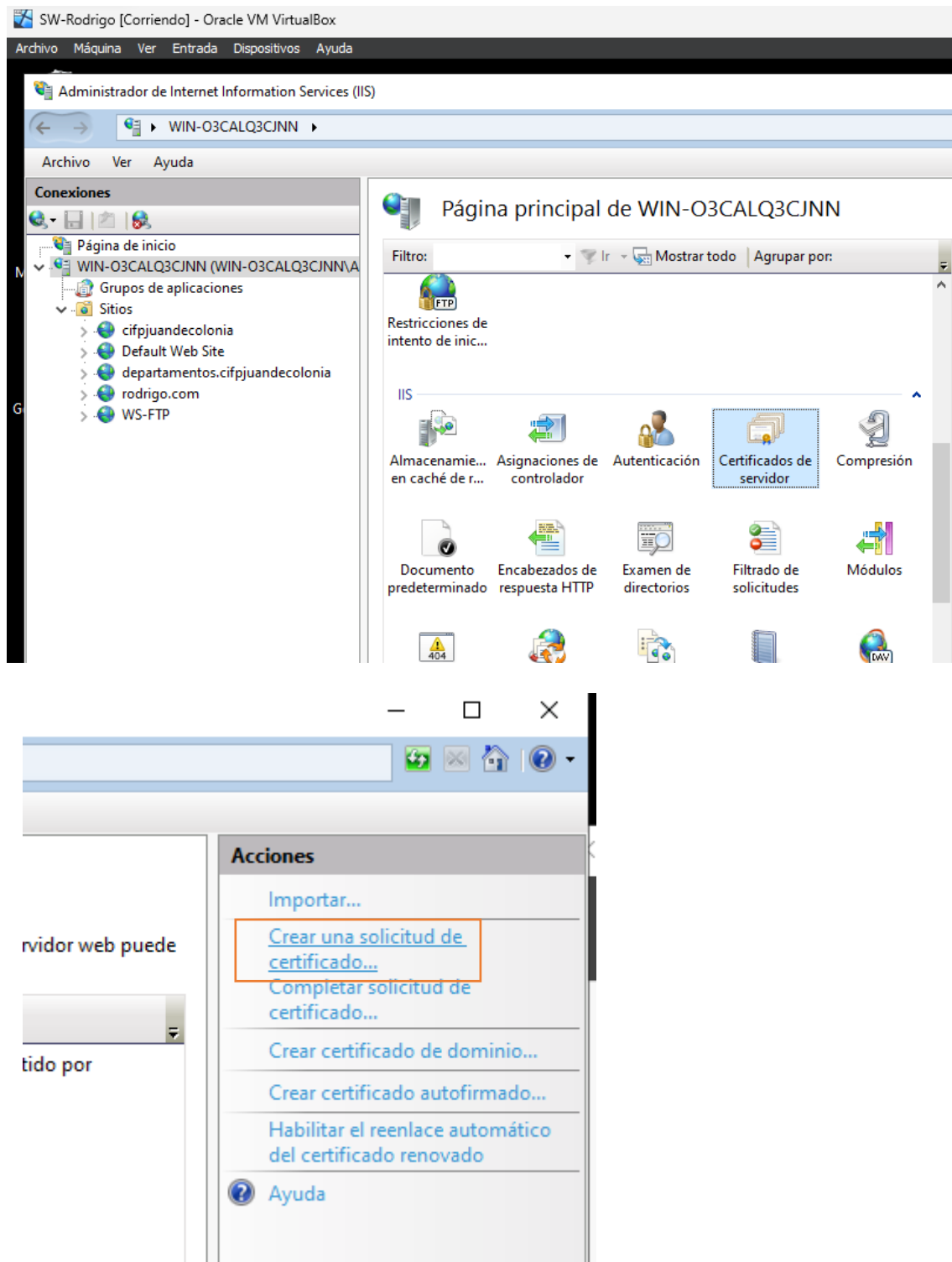


## SERVIDOR ISS: UTILIZACIÓN DE HTTPS

En este ejercicio dejaremos constancia en un documento PDF de haber creado un sitio web seguro, para ello en nuestro documento dejaremos constancia de haber:


1.) Dado los pasos para crear un certificado de dominio. Señalando como nos pide una CA (autoridad de certificación).



Solicitar certificado

?

×

**Propiedades de nombre distintivo**

Especifique la información requerida para el certificado. Estado o provincia y Ciudad o localidad deben ser nombres oficiales y no deben contener abreviaturas.

Nombre común:	<input type="text" value="www.rodrido.com"/>
Organización:	<input type="text" value="rodrido"/>
Unidad organizativa:	<input type="text"/>
Ciudad o localidad:	<input type="text" value="Burgos"/>
Estado o provincia:	<input type="text" value="España"/>
País o región:	<input type="text" value="ES"/>

Anterior

Siguiente


Finalizar

Cancelar

Solicitar certificado

?

×

**Nombre de archivo**

Especifique un nombre para la solicitud de certificado. Esta información se puede enviar a una entidad de certificación para que la firme.

Especificar un nombre de archivo para la solicitud de certificado:

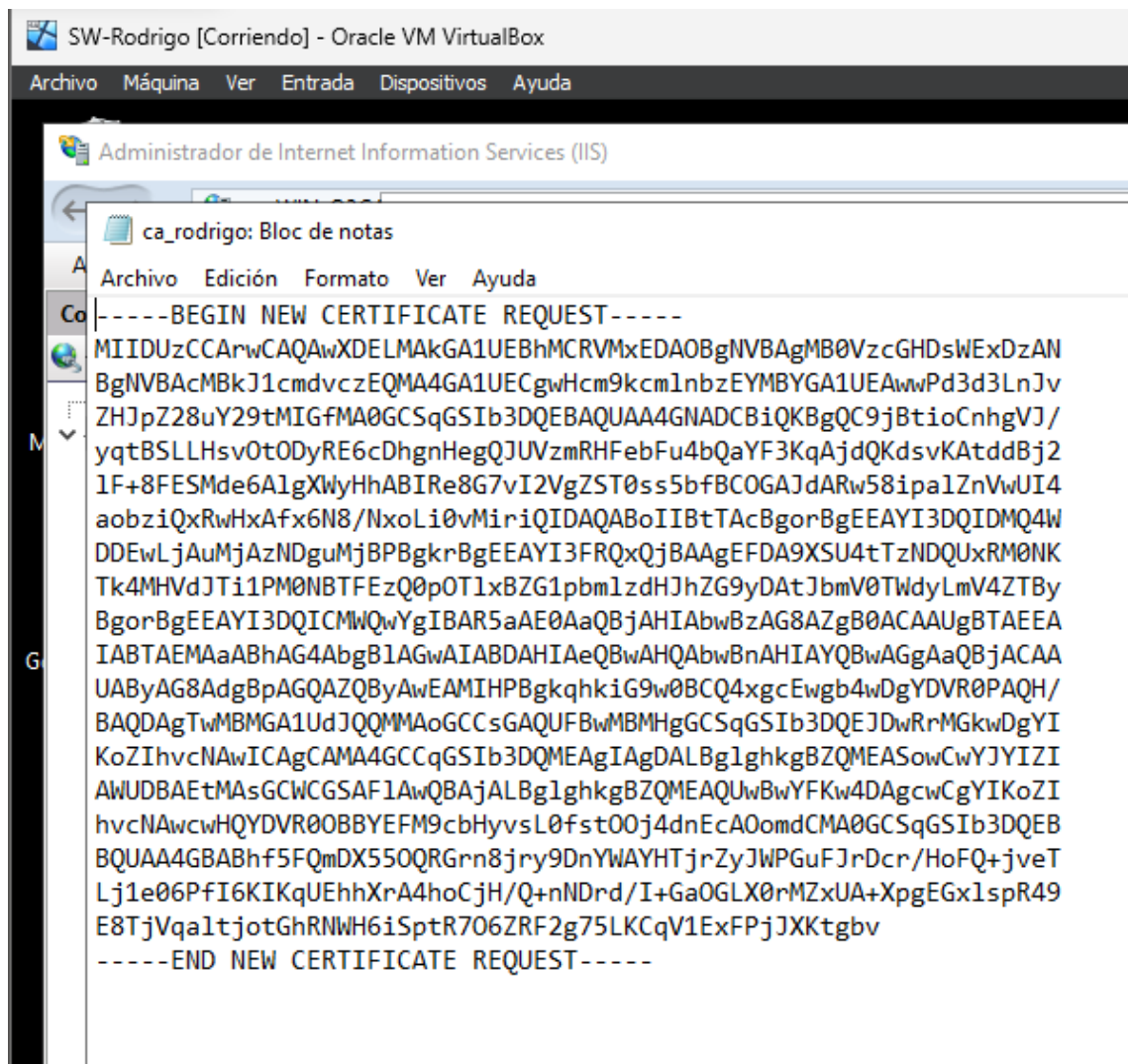
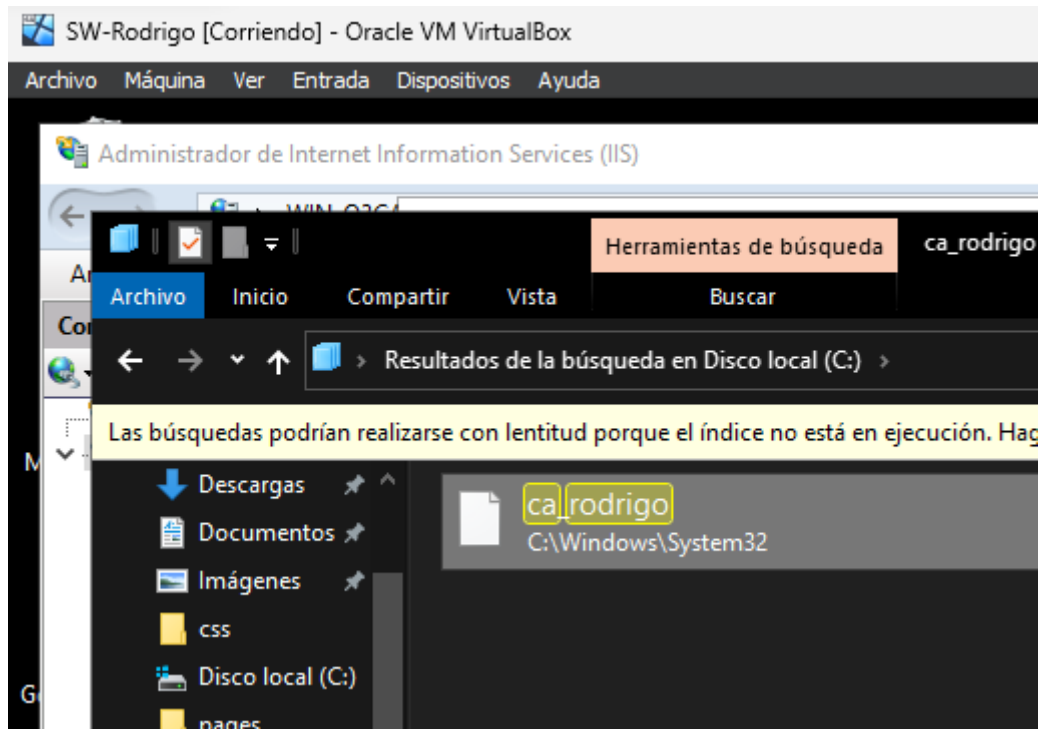
<input type="text" value="ca_rodrido"/>	<input data-bbox="981 1400 1034 1438" type="button" value="..."/>
---	---

Anterior

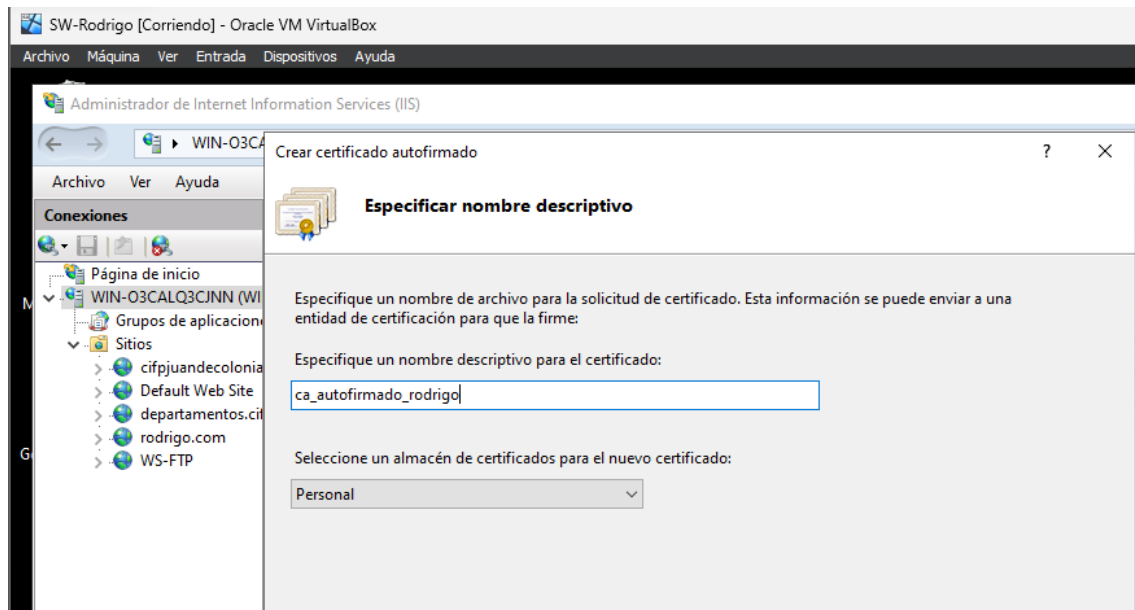
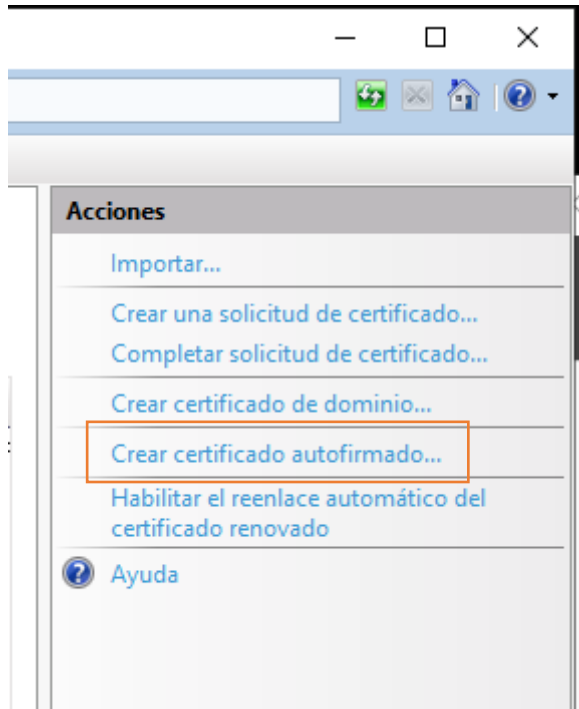
Siguiente

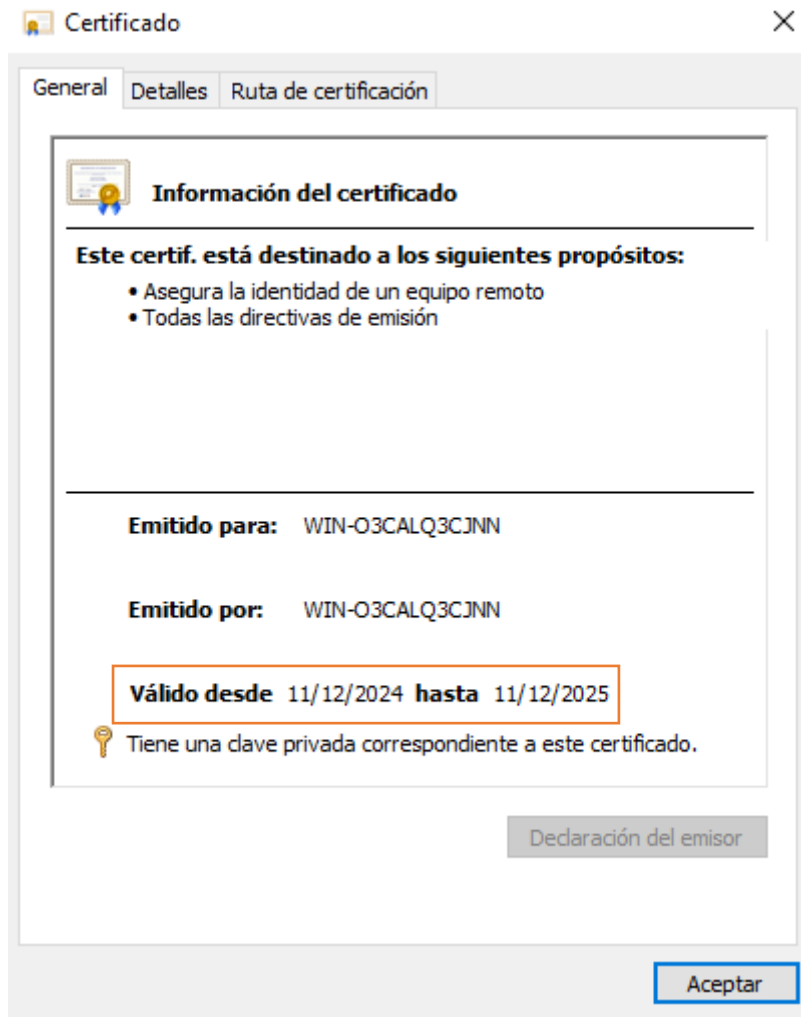
Finalizar

Cancelar

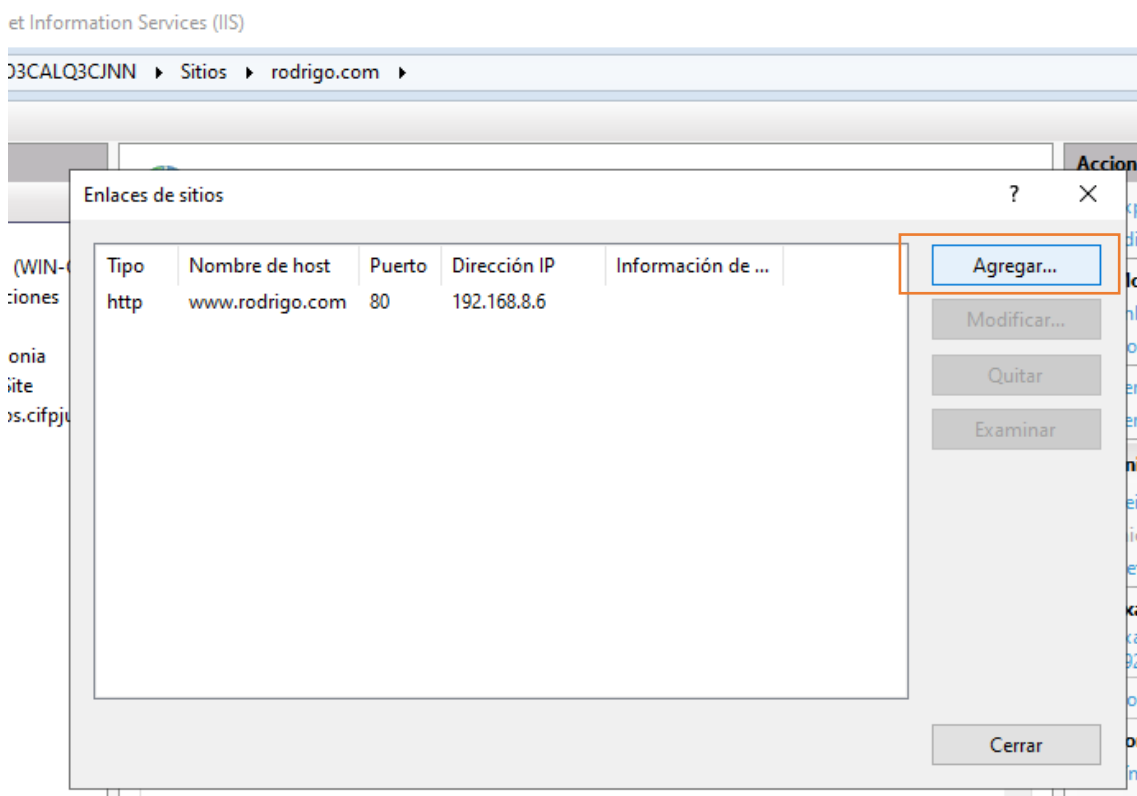
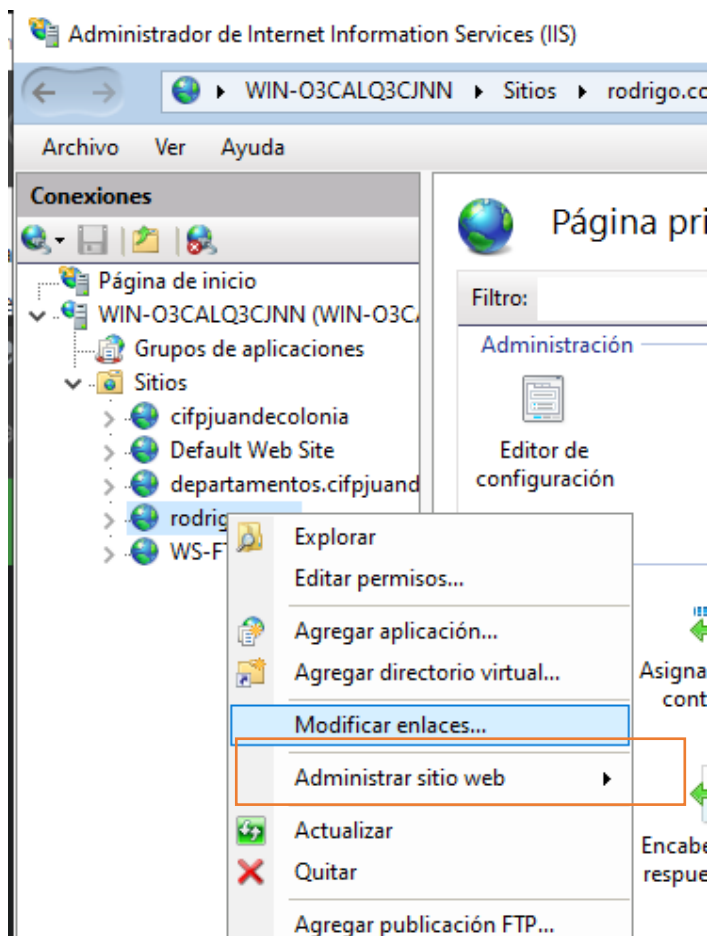


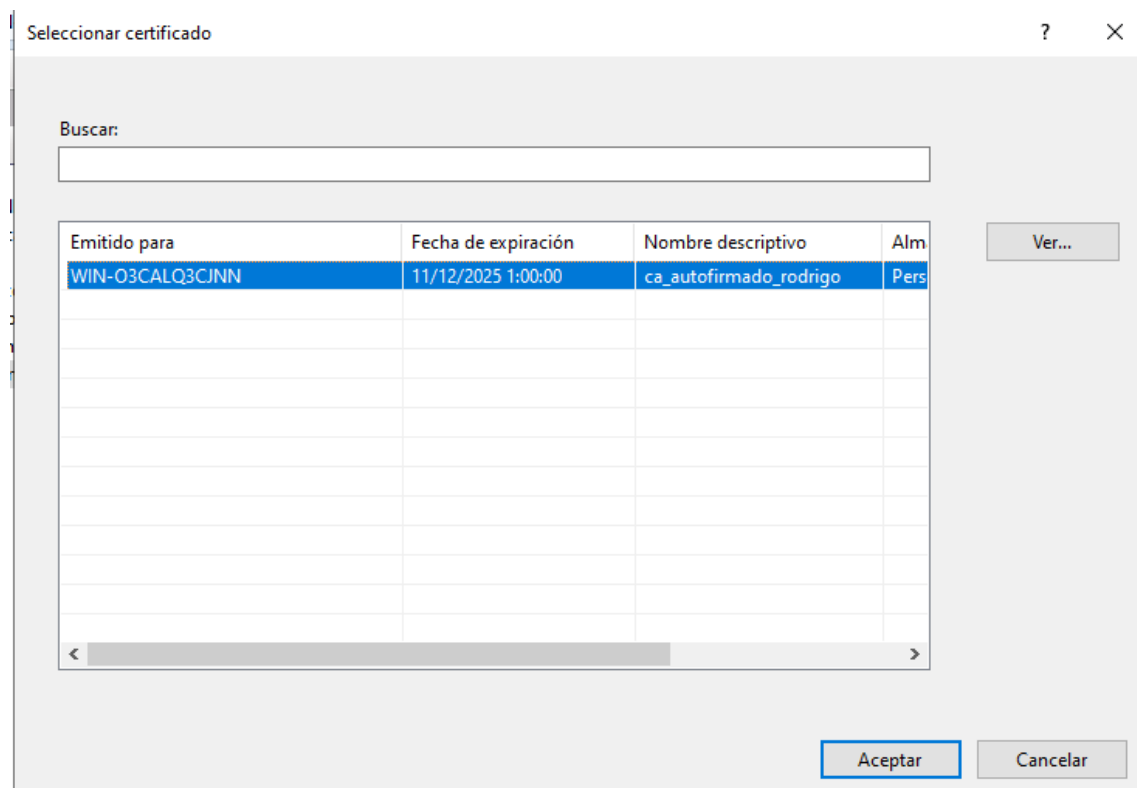
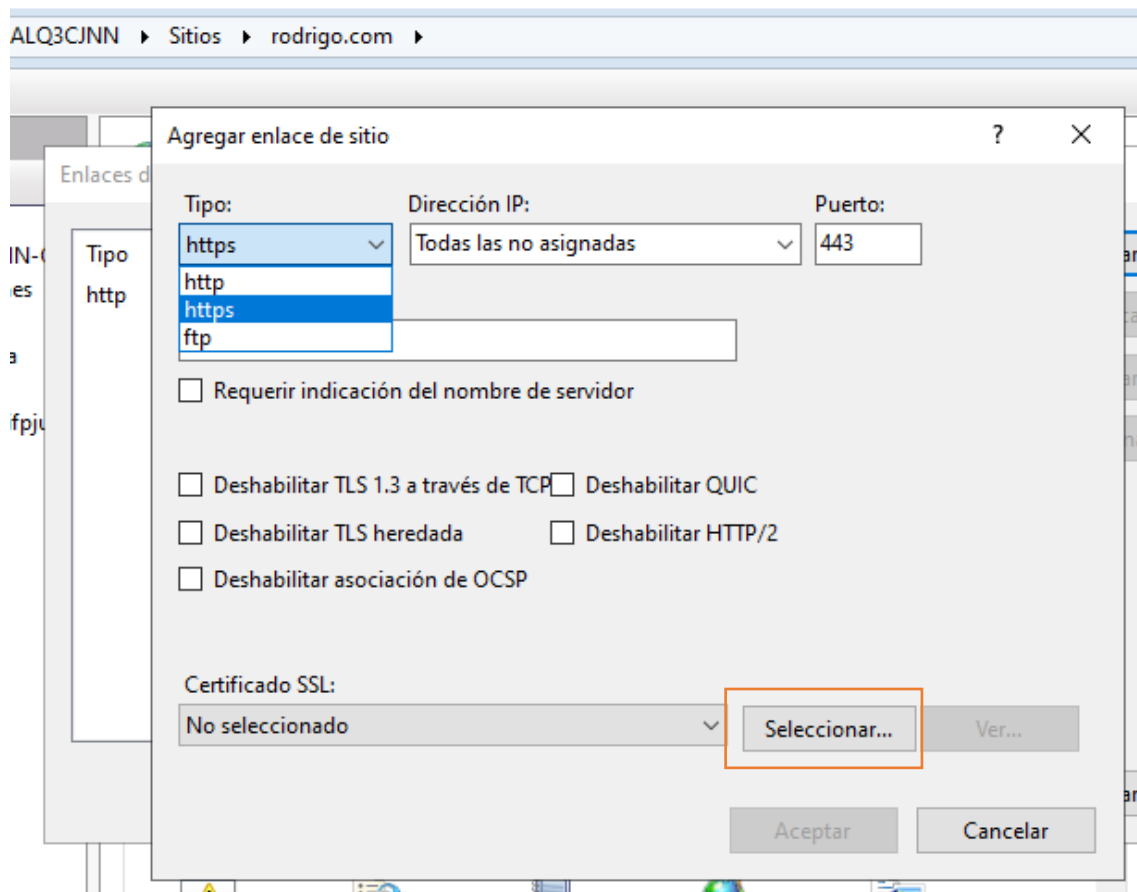
2.) Creado un certificado autofirmado, dejamos constancia de sus propiedades como la validez.





### 3.) Creado el sitio web seguro.





Agregar enlace de sitio

Tipo:  Dirección IP:  Puerto:

Nombre de host:

☐ Requerir indicación del nombre de servidor

☐ Deshabilitar TLS 1.3 a través de TCP ☐ Deshabilitar QUIC

☐ Deshabilitar TLS heredada ☐ Deshabilitar HTTP/2

☐ Deshabilitar asociación de OCSP

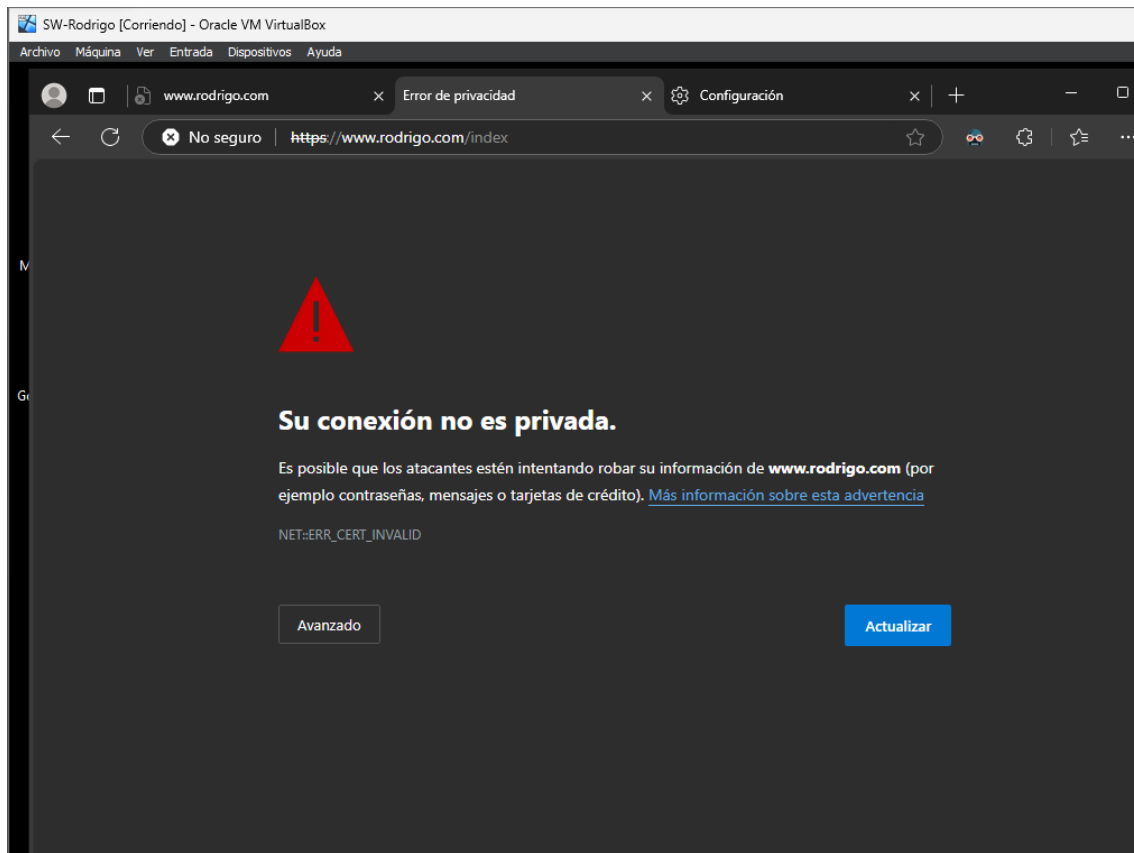
Certificado SSL:

Enlaces de sitios

Tipo	Nombre de host	Puerto	Dirección IP	Información de ...
http	www.rodrido.com	80	192.168.8.6	
https	www.rodrido.com	443	*	



4.) Comprobación de que el sitio funciona dándonos un mensaje previo de aviso de seguridad.



5.) ¿Porqué nos da este aviso?

Indica un problema con el certificado SSL/TLS del sitio web, el navegador no puede verificar la validez del certificado autofirmado. Debemos instalar un certificado emitido por una CA reconocida.

6.) Mostrar las CA de nuestro navegador.

Certificado

94a513a2-4254-456f-b830-2747e13ae617

Nombre del asunto

Nombre común

94a513a2-4254-456f-b830-2747e13ae617

Nombre del emisor

net  
windows

Nombre común  
MS-Organization-Access

Unidad organizativa  
82dbaca4-3e81-46ca-9c73-0950c1eaca97

Validez

No antes

Fri, 13 Sep 2024 08:29:19 GMT

No después

Wed, 13 Sep 2034 08:59:19 GMT

Información de clave pública

Algoritmo

RSA

Tamaño de la clave

2048

Exponente

65537

Módulo

B8:53:C2:26:F5:97:72:7F:C8:78:A8:E0:B8:8C:A1:C3:AF:97:F6:96:17:E4:F1:F1:C0:C1:7E...

Misceláneo

Número de serie

37:43:FC:4E:B8:FA:D0:9C:4C:32:D5:B4:1C:D5:35:73

Algoritmo de firmas

SHA-256 with RSA Encryption

Versión

3

Descargar

[PEM \(cert\)](#) [PEM \(cadena\)](#)

Huellas digitales

SHA-256

D2:B3:71:E9:B1:A6:14:C2:81:13:75:80:E7:29:E3:BF:E2:07:43:2D:78:28:D5:0A:A7:72:8...

SHA-1

E6:1A:36:83:48:27:66:8A:0C:7B:34:00:B5:DF:D0:07:3E:8E:D3:27

1

Restricciones básicas

Autoridad de certificación

No

1

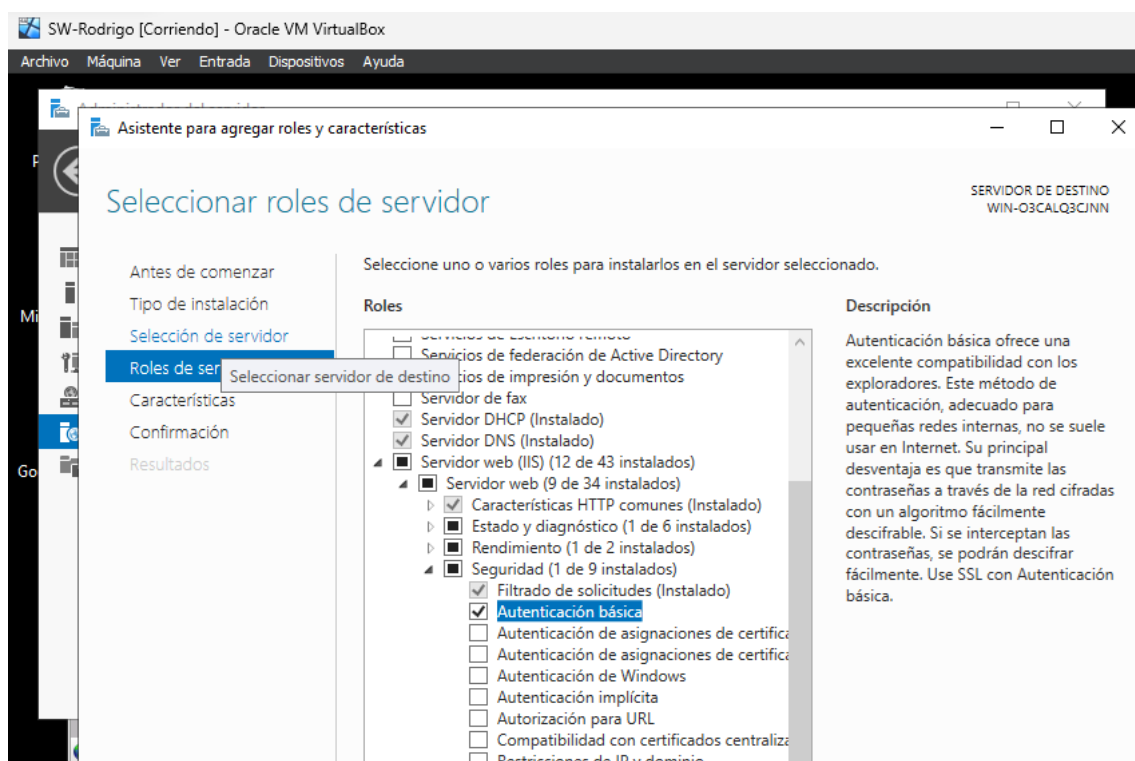
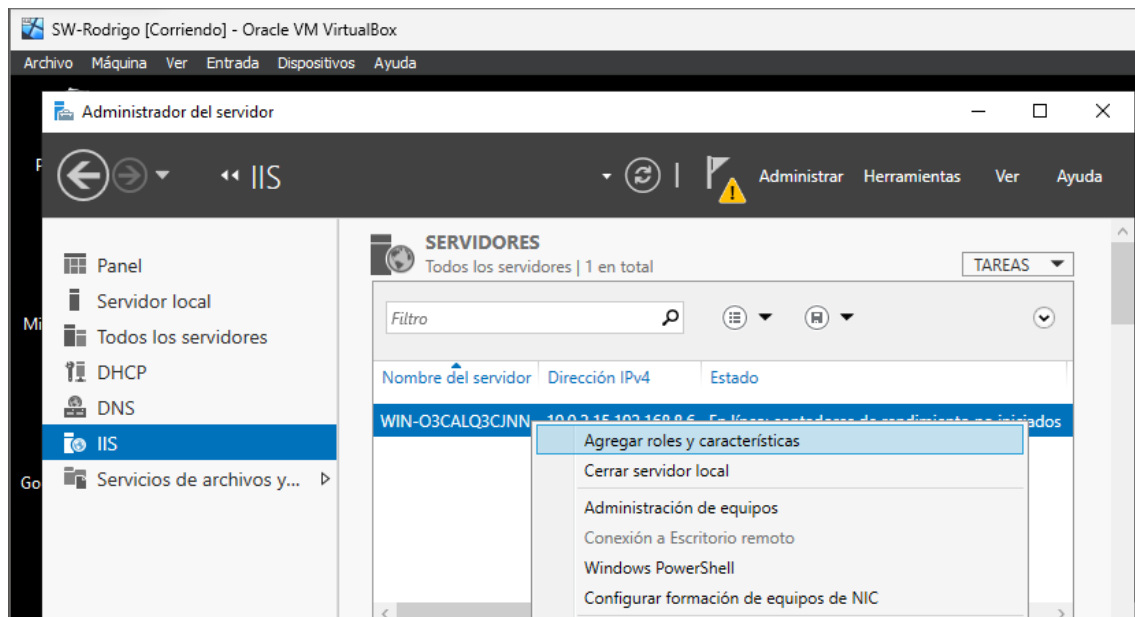
Usos extendidos de la clave

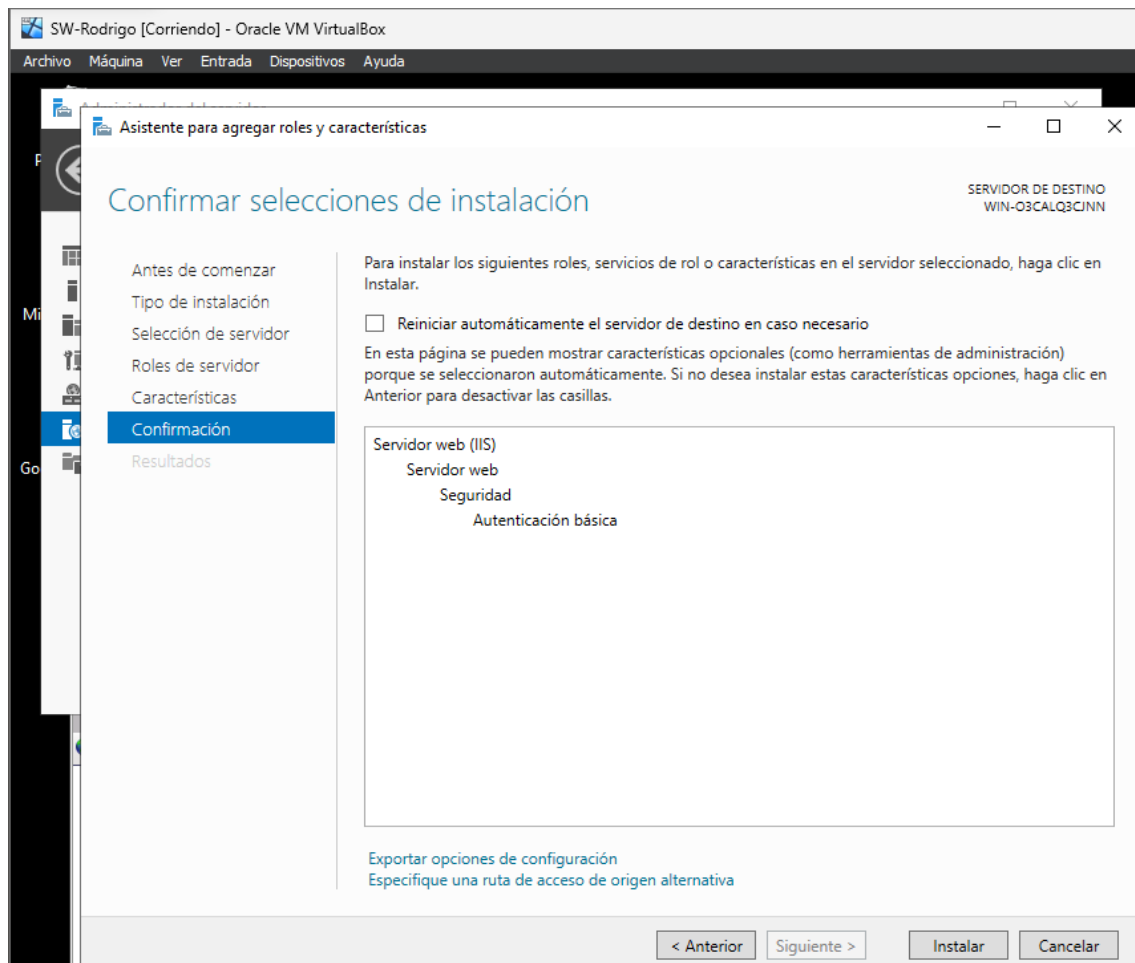
Propósitos

Client Authentication

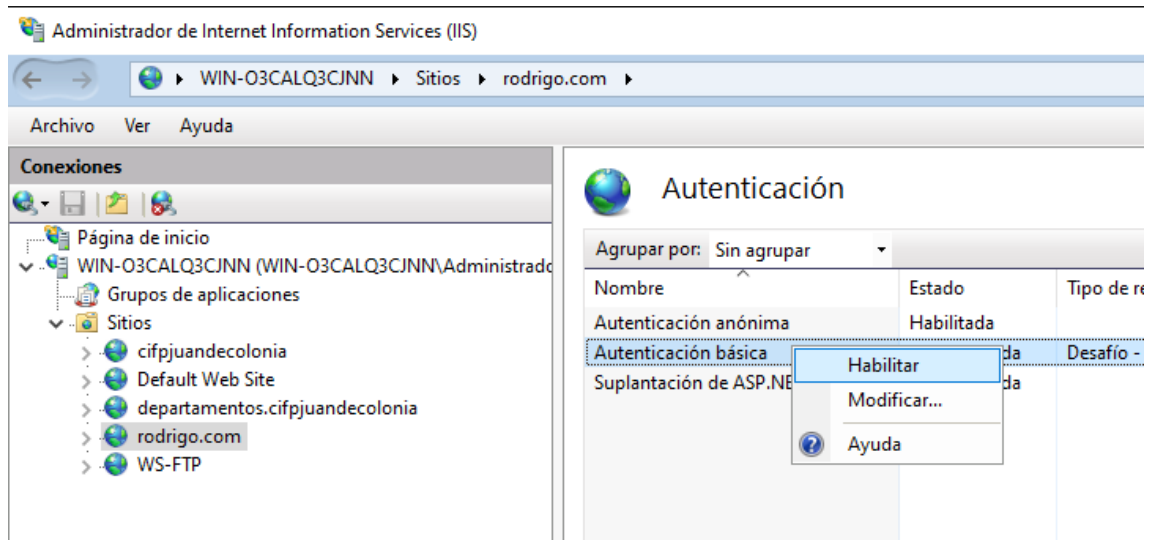
## 7.) Extra: Autenticación básica instalación en IIS y funcionamiento.

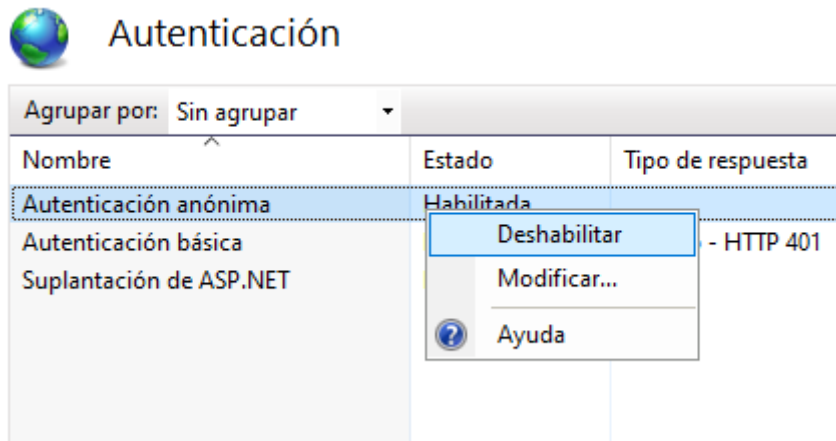
### Instalación:





## Funcionamiento:





Deshabilitamos la anónima.

