



FACULTAD DE INGENIERÍA Escuela de Computación

G3_AUTORIDAD_CERTIFICADORA



COMPETENCIAS

- El estudiante crea una entidad certificadora.
- El estudiante genera certificados Digitales.

MATERIALES Y EQUIPOS

- Software virtual-box 7.0.4
- OVA de WS2019 22.04

INTRODUCCION

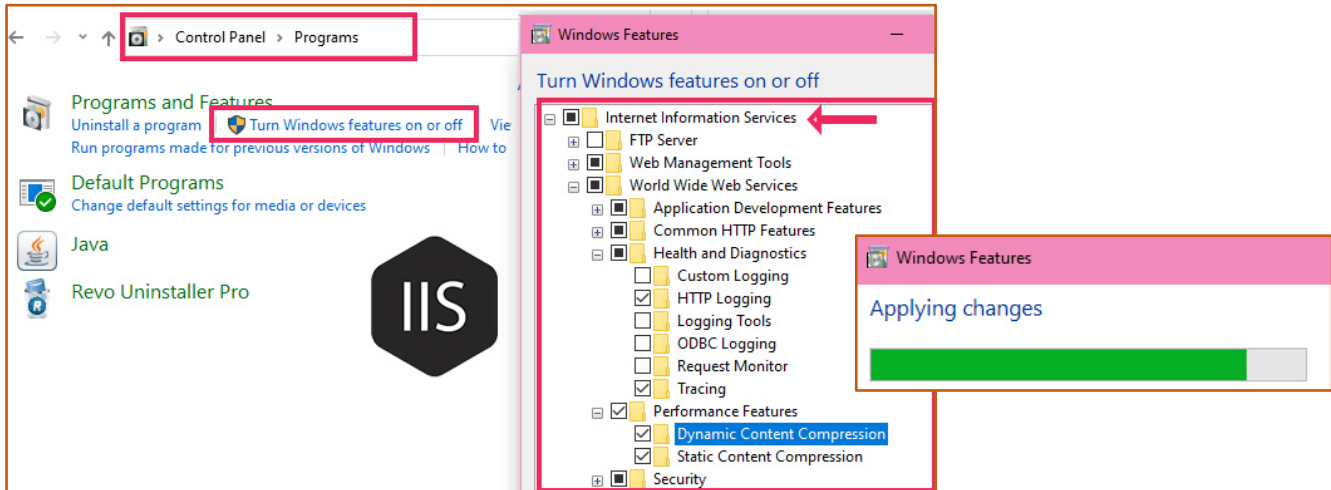
Autoridad Certificadora(CA): es una entidad confiable responsable de emitir y gestionar certificados digitales. Los certificados digitales son utilizados en la criptografía de clave pública para asegurar la autenticidad, integridad y confidencialidad de la información en línea, así como para establecer conexiones seguras a través de Internet.



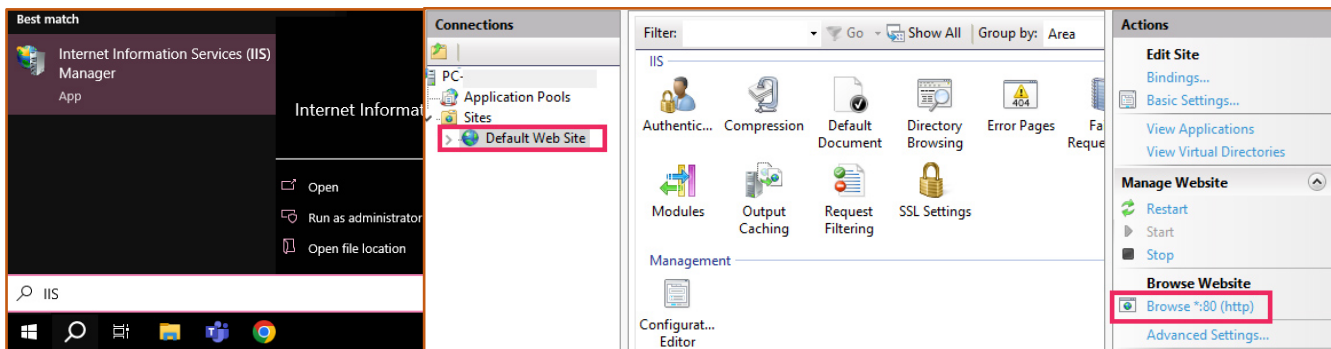
Para el desarrollo de la práctica se implementará la topología mostrada en la figura.

PARTE I HABILITAR IIS

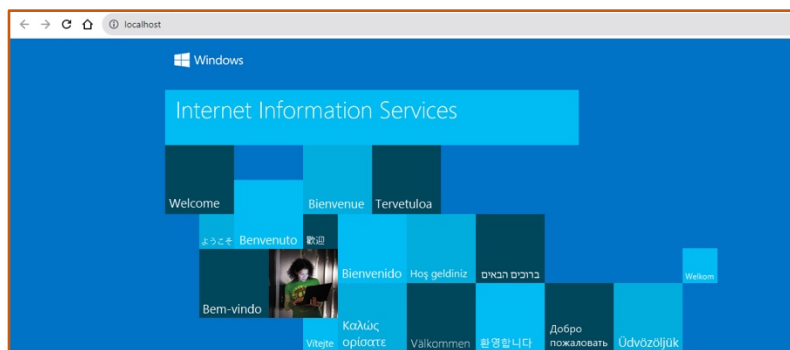
1. Abra la máquina anfitriona (maquina Física) y proceda con la activación de la característica de Windows IIS. Desde el panel de control abra las características de Windows y seleccione los campos exactamente como se muestran.



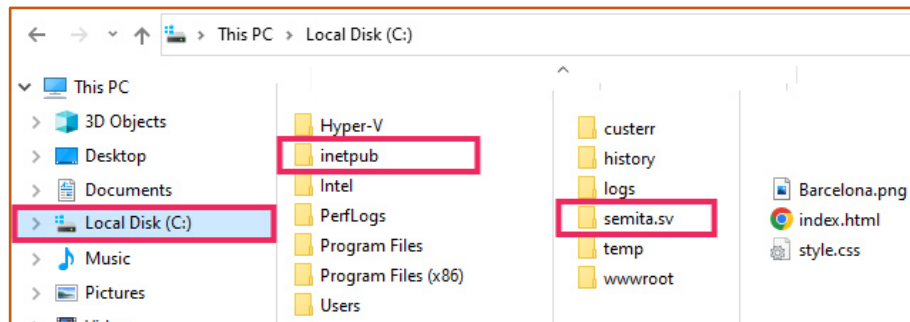
2. Abra la característica (IIS) desde el buscador de Microsoft y observe el entorno de configuración. Haga clic en **default Web Site** y posteriormente en **Browse*80 http**



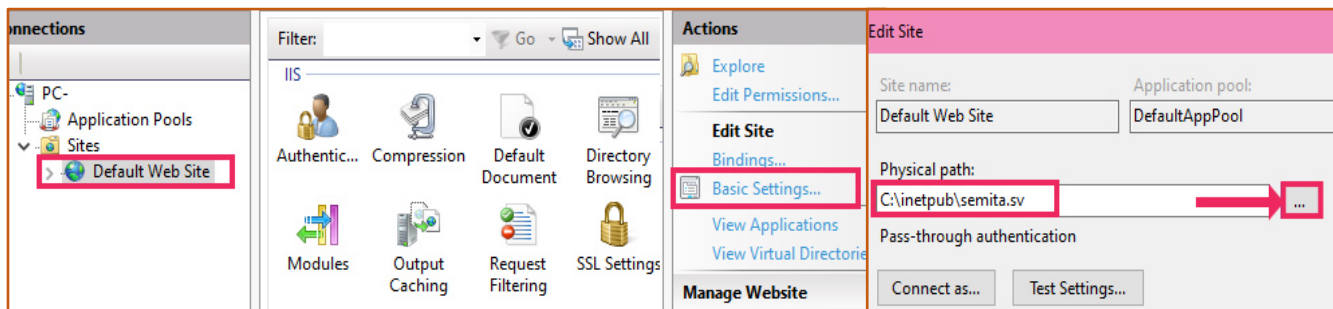
3. Le abrirá el navegador y le desplegará la página web por defecto.



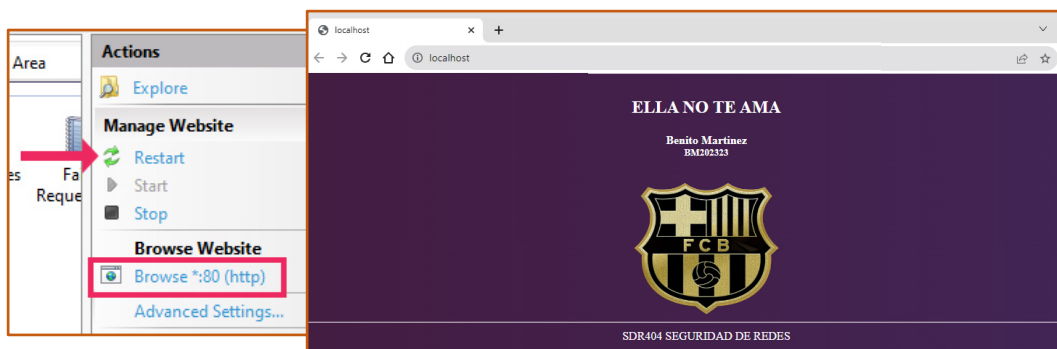
4. Copie la carpeta **semita.sv** exactamente en la ruta mostrada. (La carpeta **semita.sv** contiene el cuerpo de una nueva página web)



5. Entre nuevamente en la configuración de IIS, haga clic sobre **Basic Settings** y en la ventana desplegada, seleccione la carpeta **semita.sv**

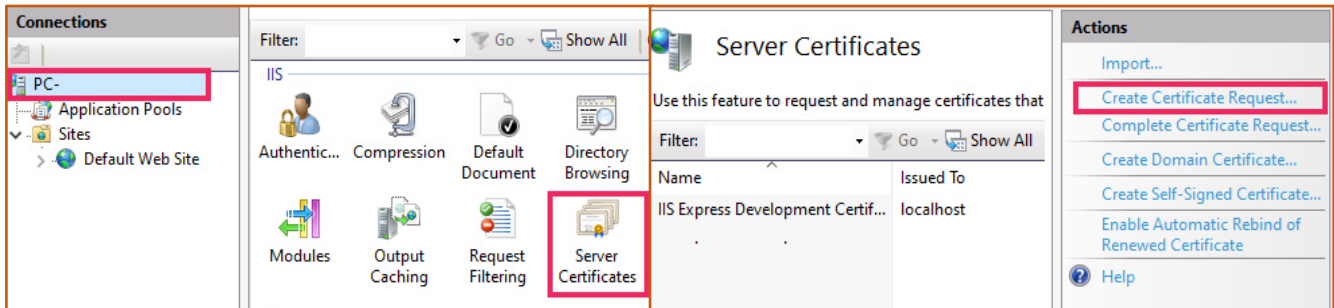


6. Reinicie el servicio IIS y verifique la nueva página web.

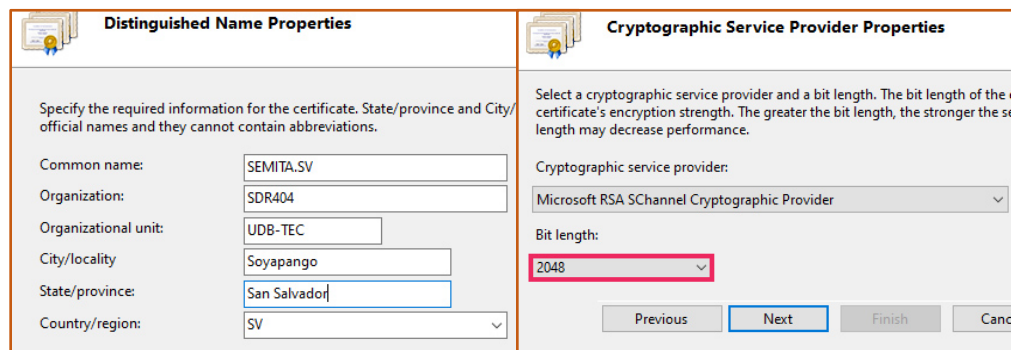


PARTE II EMISION DE SOLICITUD DE CERTIFICADO

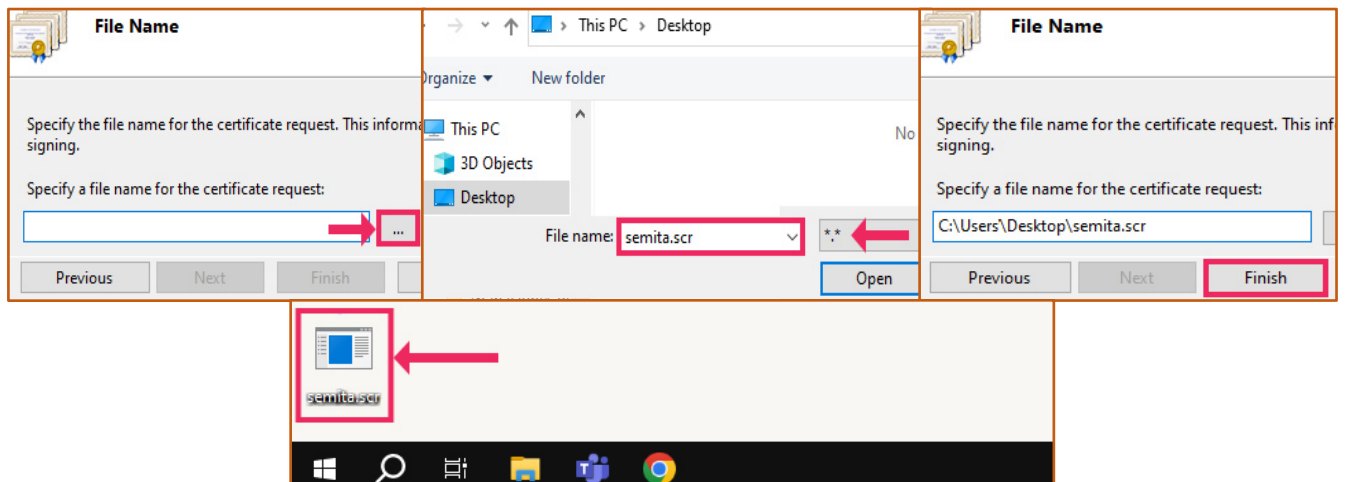
7. Desde la administración de IIS, haga clic sobre el servidor y seleccione la opción certificados de servidor. En el menú de acciones seleccione **crear solicitud de certificado**.



8. Llene los campos de la solicitud como se muestra en la figura, también deberá seleccionar la opción **2048 bits de longitud**

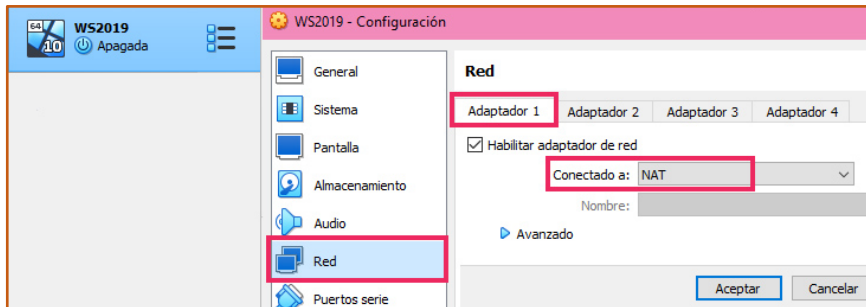


9. Asigne a la solicitud de certificado el nombre de **semita.scr** y ubique el archivo en el escritorio de la maquina anfitrión (**Copie el archivo semita.scr en una USB**)



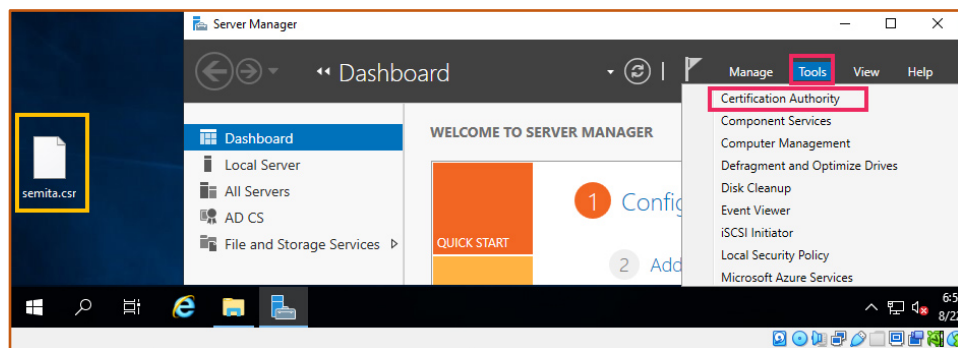
PARTE III EMISION DE DE CERTIFICADO

10. Haciendo uso de **virtualbox** importe la ova WS2019, posteriormente con WS2019 apagado configure el adaptador de red en modo NAT

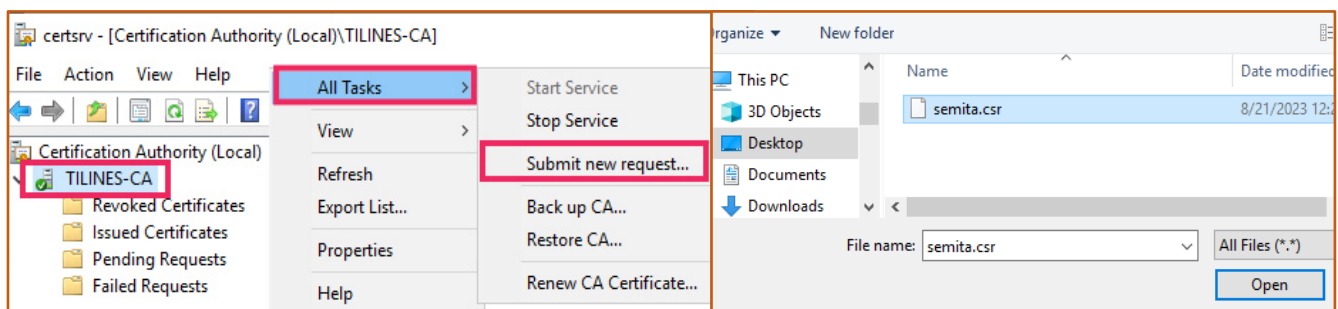


Usuario: Administrador
Password: Pa\$\$w0rd

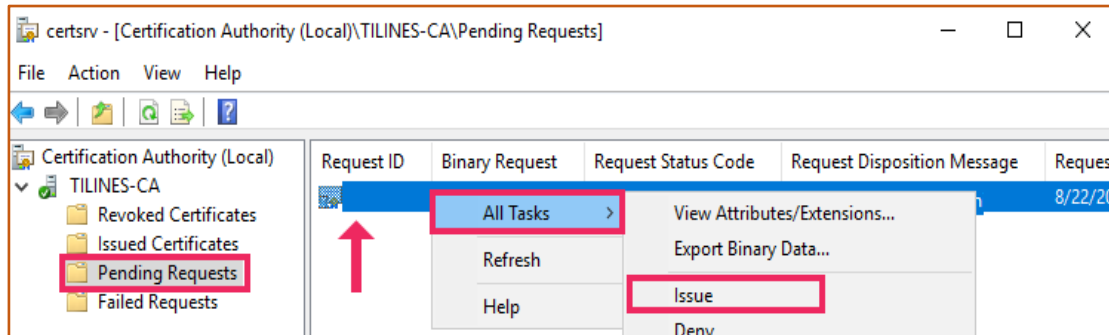
11. Inicie el servidor (utilice las credenciales mostradas), debe colocar el archivo **semita.scr** en el escritorio del servidor y abrir la característica **Autoridad certificadora**.



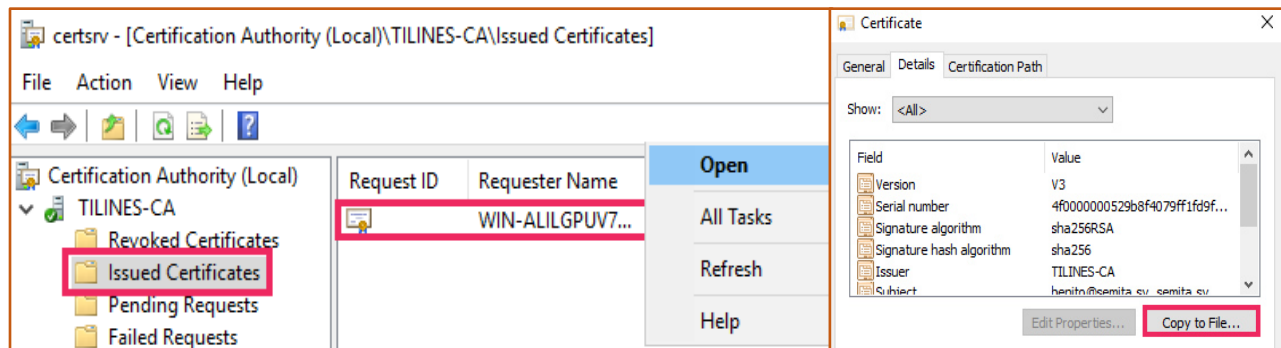
12. Se abrirá la Interfaz de la Autoridad Certificadora, posicione sobre el servidor **TILINES-CA**, haga clic derecho seleccione **todas las tareas** y la opción **submit new request**, habrá la solicitud de **semita.sv**



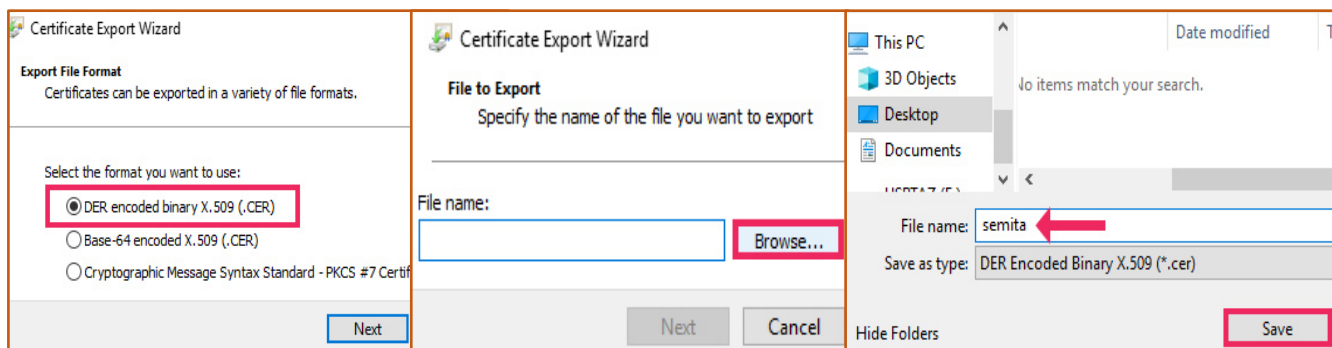
13. Haga clic sobre el menú solicitudes pendientes y sobre la solicitud [semita.sv](#) de un clic derecho y seleccione [todas las tareas](#) y la opción [issue](#)



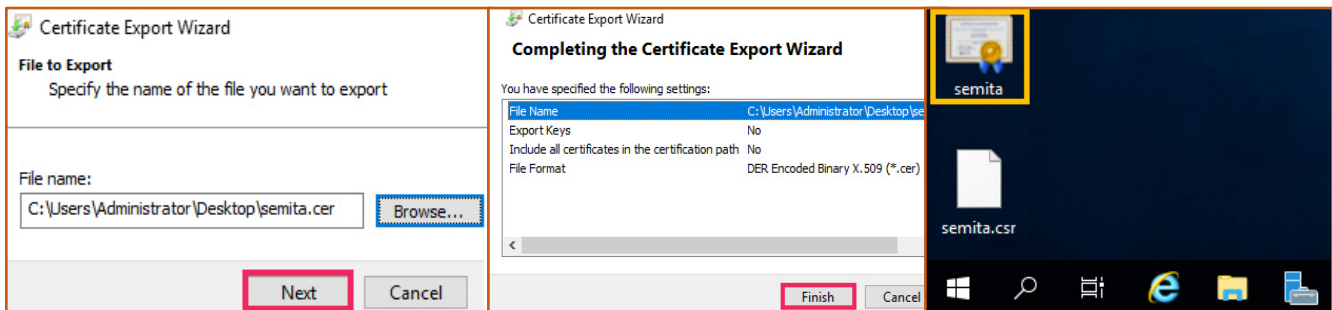
14. Ahora dirijase al menú [issued certificates](#) y haga clic sobre el certificado emitido. Seleccione la opción [abrir](#) y haga clic sobre [copiar como archivo](#).



15. Seleccione el formato X.509(.CER), luego debe especificar el nombre del certificado y ubicarlo en el escritorio del servidor.



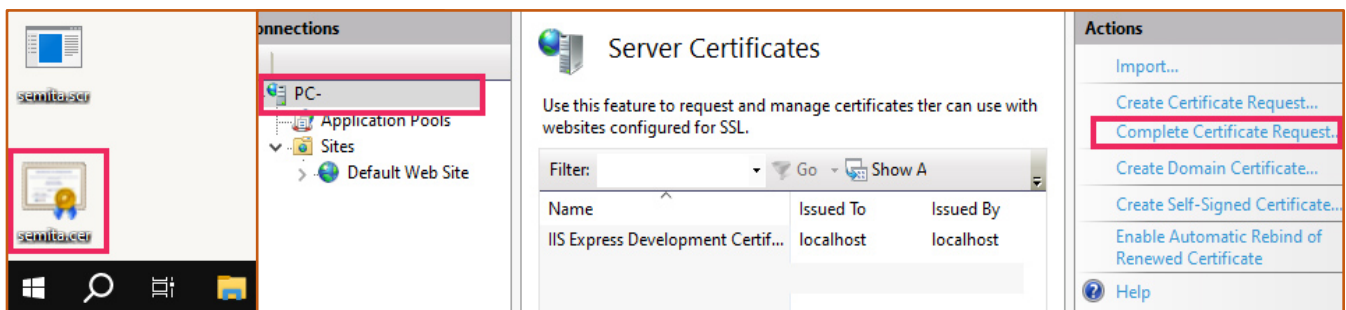
16. Después de establecer la ubicación de destino del certificado y su debido formato haga clic en siguiente y finalizar



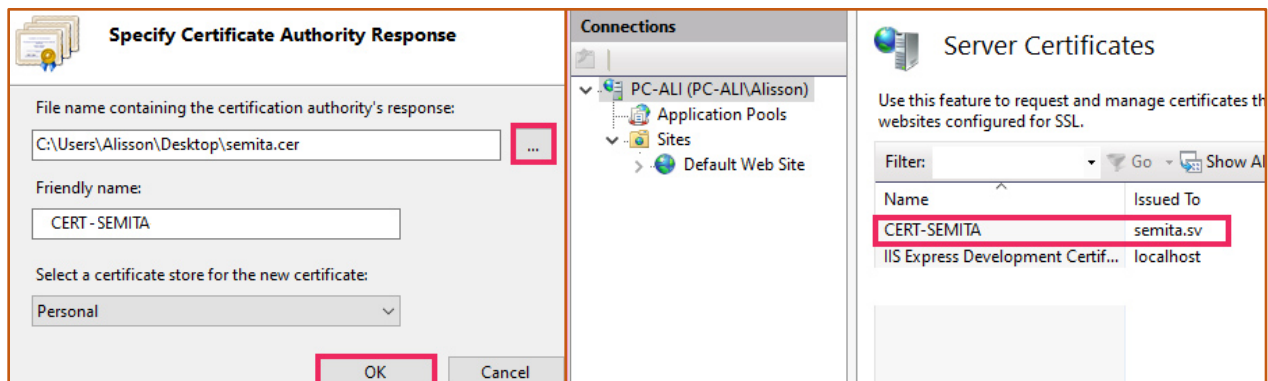
Debe extraer el certificado emitido por el servidor (USB o portapapeles compartido)

PARTE IV INSTALACION DE CERTIFICADO

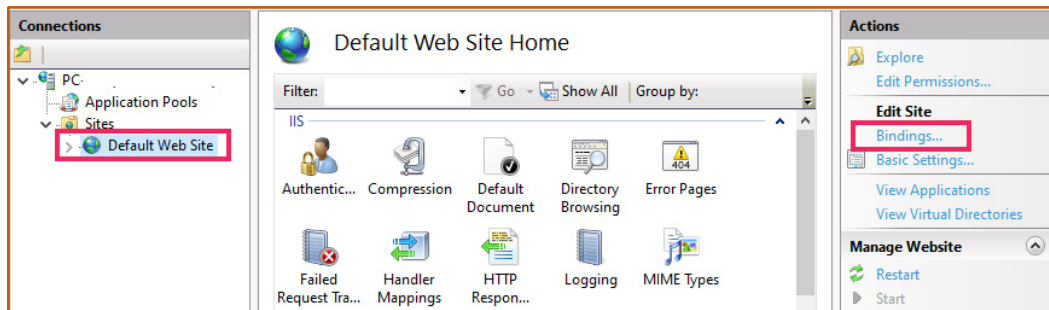
17. Coloque en el escritorio de la maquina anfitrión (Maquina Física) el certificado emitido el servidor y en el panel de IIS seleccione la opción **completar solicitud de certificado**.



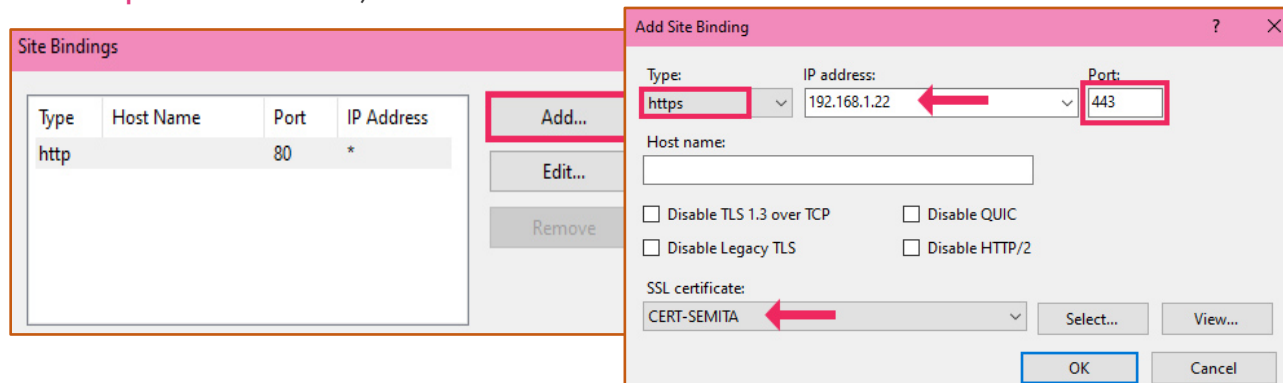
18. Especifique la ubicación del certificado y asigne un nombre representativo, deberá aparecer en el listado de certificados.



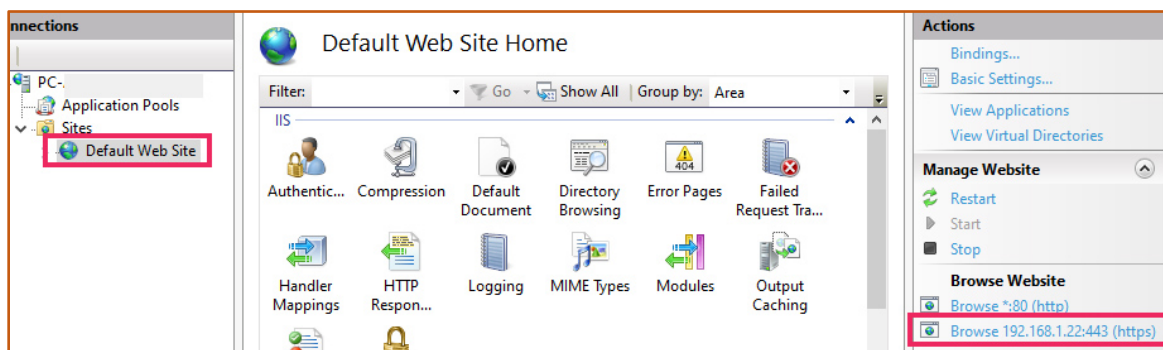
19. Ahora deberá crear un nuevo enlace que contenga el protocolo HTTPS para asegurar la página web.



20. Añada un nuevo enlace, pero con protocolo HTTPS para la pagina web empleando el certificado emitido por el servidor. (Asigne la dirección Ipv4 de su maquina anfitrión)



21. Verifique el funcionamiento del enlace con el certificado.



22. Observe los datos del certificado en el navegador.

192.168.1.22

No es seguro <https://192.168.1.22>

Visor de certificados: semita.sv

General Detalles

Enviado a

Nombre común (CN)	semita.sv
Organización (O)	SDR404
Unidad organizativa (OU)	UD8-TEC

Emitido por

Nombre común (CN)	TIUNES-CA
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez


Emitido el	lunes, 21 de agosto de 2023, 6:46:20
Vencimiento el	miércoles, 21 de agosto de 2024, 6:56:20

Huellas digitales

Huella digital SHA-256	C8 2E 0F 9D AF E8 18 98 FB E7 72 E7 6D A8 81 32 E2 1F A1 7D 2E CC FB DA CF 35 51 09 5C 21 D7 24
Huella digital SHA-1	7C 12 0A E5 58 AF 38 C7 09 4A CF 85 D9 15 C1 7E 7F 41 69 6C

ELLA NO TE AMA

Benito Martínez
BM202323



SDR404 SEGURIDAD DE REDES