INSTALACIÓN Y RENOVACIÓN DE CERTIFICADO SSL

Departamento de Firma Electrónica Avanzada UNAM

Manual de Instalación

Contenido del Documento

Ficha del Documento

Control de Versiones del Documento

Versión	Fecha	Autor	Motivo del Cambio
1.0	15/01/2017	Departamento de Firma Electrónica Avanzada	Creación del documento Inicial
1.2.1	30/07/2020	Departamento de Firma Electrónica Avanzada	Actualización de documento
1.3	22/08/2020	Departamento de Firma Electrónica Avanzada	Actualización de documento

Dirigido a

El presente documento está dirigido al personal técnico responsable de realizar la instalación y configuración de Certificados SSL proporcionados por la UNAM.

Alcance

El documento que a continuación se presenta, define de manera general el procedimiento a seguir para realizar la configuración e instalación de Certificados SSL en los sitios web de la UNAM.

Para obtener más información o asesoría técnica puede mandar un correo a firma.tic@unam.mx , llamar el 56 22 39 82 o visitar la página www.fea.unam.mx/SSL

Glosario y convenciones

Término	Definición	Convención en este documento
Certificados raíz e intermedio	Certificados proporcionados por el emisor del certificado SSL que validan la cadena de certificación de la CA raíz e intermedia.	`UNAM_Root_R3_raiz` `UNAM_RSA_OV_SSL_CA`
CSR (Certificate Signing Request)	Solicitud de certificado que contiene información codificada en un archivo de texto, requerido para la emisión del certificado SSL del sitio.	`solicitud.csr`
Certificado SSL	Certificado SSL del sitio web proporcionado por la UNAM.	`myservidorweb.cer`
DN *(Distinguished Name)*	Nombre de dominio de su sitio.	`DN miservidorweb.unam.mx`
Llave Privada (Private Key)	Llave privada del certificado digital	`myservidorweb.key`

<RUTA>	hace referencia al directorio donde se encuentran los archivos.	`<RUTA>`
JKS (*Java keyStore*)	Almacén de certificados y entidades de certificación usado por las aplicaciones Java para trabajar con SSL	`myservidorweb.jks`
Passsword Almacén de certificados	Contraseña que se asigno al crear el archivo jks	**`passwordmyservidorweb`**
Alias DN *(Distinguished Name)*	Alias que se asignó cuando se creó el almacén de llaves JSK (*Java keyStore*)	`aliasmyservidorweb`

Introducción

Para realizar la instalación del certificado se debe haber realizado previamente la solicitud oficial al Departamento de Firma Electrónica Avanzada de la DGTIC y enviado el archivo *CSR* correspondiente al correo electrónico (firma.tic@unam.mx).

Una vez que se han validado todos los elementos, la DGTIC le proporcionará el certificado SSL solicitado, así como un par certificados adicionales (raíz e intermedio) vinculados a la Autoridad Certificadora emisora de los certificados.

Acerca del certificado raíz e intermedio

Cada certificado SSL emitido tiene su propia autoridad raíz e intermedia, los navegadores validan la cadena de certificación correspondiente, por lo que en cada integración de un certificado SSL nuevo o renovado, se deberá realizar el proceso de integración de los certificados raíz e intermedio.

Con cada solicitud de emisión de un certificado SSL, se recibirán 3 archivos comprimidos (.zip), dos de los cuales corresponden al certificado raíz e intermedio.

Si se omite la instalación de los certificados raíz e intermedio, no se validará la cadena de certificación completa y algunos navegadores enviarán una advertencia de seguridad. Deberá asegurarse de que estos se encuentren instalados.

Instalación de Certificado SSL por primera vez

Instalación de SSL en Apache2 Server

Dependiendo de la versión que se encuentre instalada de Apache y el sistema operativo, se tendrán que modificar los siguientes archivos:

```
httpd.conf, apache2.conf o ssl.conf
```

Ejemplo:
Se asume que el certificado proporcionado por la DGTIC tiene el nombre de:

- myservidorweb.cer

Archivo de la llave privada, generado cuando creó el CSR:

- myservidorweb.key

Las directivas que se deben modificar se muestran en el siguiente ejemplo:

Inicio del proceso.
Ejemplo:

```
# Configuracion de SSL
SSLEngine on
SSLCertificateFile /<RUTA>/myservidorweb.cer
SSLCertificateChainFile /<RUTA>/UNAM_RSA_OV_SSL_CA.pem
SSLCertificateKeyFile /<RUTA>/myservidorweb.key
SSLCACertificatefile /<RUTA>/UNAM_Root_R3_raiz.pem
```

Nota: /<RUTA>/ hace referencia al directorio donde se encuentran los archivos.

Una vez modificadas las directivas se deberá de reiniciar el servicio de apache. El comando de reinicio depende de la versión del Sistema Operativo y la versión de apache.

Los certificados raíz e intermedio vienen comprimidos en un archivo .zip con nombres clave para una correcta identificación:

- UNAM_Root_R3_raiz.zip
- UNAM_RSA_OV_SSL_CA.zip

Fin del proceso.

Instalación de SSL en Zimbra

Se asume que el certificado proporcionado por la DGTIC tiene el nombre de:

- myservidorweb.cer

Los certificados raíz e intermedio vienen comprimidos en un archivo .zip con nombres clave para una correcta identificación:

- UNAM_Root_R3_raiz.zip
- UNAM_RSA_OV_SSL_CA.zip

Archivo de la llave privada, generado cuando creó el CSR:

- myservidorweb.key

La configuración de Zimbra usa nombres de certificados específicos, por lo que se deberán de renombrar los certificados enviados por parte de DGTIC para que la configuración de realice lo más trasparente posible.

Inicio del proceso.

Renombrar el certificado de su sitio myservidorweb.cer por comercial.crt, dicho certificado deberá de ser copiado a la siguiente ruta:

Nota: /<RUTA>/ hace referencia al directorio donde se encuentran los archivos.

```
cp /<RUTA>/myservidorweb.cer
/opt/zimbra/ssl/zimbra/commercial/comercial.crt
```

Renombrar el archivo de la llave privada myservidorweb.key y renombrarlo como comercial.key, dicho archivo deberá de ser copiado a la siguiente ruta:

```
cp /<RUTA>/myservidorweb.key
/opt/zimbra/ssl/zimbra/commercial/commercial.key
```

Para la configuración del certificado raíz e intermedio Zimbra usa un solo archivo que contiene los dos certificados:

- Se deberá ejecutar el siguiente comando para unir el certificado raíz UNAM_Root_R3_raiz.pem con el certificado intermedio UNAM_RSA_OV_SSL_CA.pem y generar el archivo commercial_ca.crt:

```
cat UNAM_Root_R3_raiz.pem UNAM_RSA_OV_SSL_CA.pem >
/opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt
```

Una vez renombrados los certificados, se deberá ejecutar el siguiente comando para la validación de dichos certificados (validar que la llave si corresponda al certificado del sitio y realizar una validación de que la cadena de certificación este completa).

```
/opt/zimbra/bin/zmcertmgr verifycrt comm
/opt/zimbra/ssl/zimbra/commercial/commercial.key
/opt/zimbra/ssl/zimbra/commercial/comercial.crt
/opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt
```

Una vez que los certificados fueron validados correctamente, se deberá ejecutar el comando para instalar el certificado SSL.

```
/opt/zimbra/bin/zmcertmgr deploycrt comm
/opt/zimbra/ssl/zimbra/commercial/comercial.crt
/opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt
```

Para concluir con la instalación del Certificado SSL de tendrá que reiniciar el servicio de Zimbra con el comando:

```
zmcontrol restart
```

Fin del proceso.

Instalación de SSL en NGINX

Se asume que el certificado proporcionado por la DGTIC tiene el nombre de:

- myservidorweb.cer

Los certificados raíz e intermedio vienen comprimidos en un archivo .zip con nombres clave para una correcta identificación:

- `UNAM_Root_R3_raiz.zip`
- `UNAM_RSA_OV_SSL_CA.zip`

Archivo de la llave privada, generado cuando creó el CSR:

- myservidorweb.key

Para instalar el Certificado SSL en Nginx, se deberá crear un paquete con los tres certificados entregados por parte de DGTIC.

Inicio del proceso.

A continuación, se describen los pasos a seguir:

- Abrir cada certificado en un editor de texto plano.
- Crear un nuevo documento en un editor de texto plano.
- Copiar y pegar el contenido de cada certificado en un nuevo archivo.

El orden debe ser:

- myservidorweb.cer
- UNAM_RSA_OV_SSL_CA.pem
- UNAM_Root_R3_raiz.pem

El archivo completo debe estar organizado de esta forma:

```
----- BEGIN CERTIFICATE -----
#Certificado SSL de sitio #
----- END CERTIFICATE -----
----- BEGIN CERTIFICATE -----
#Certificado Intermedio #
----- END CERTIFICATE -----
----- BEGIN CERTIFICATE -----
#Certificado raíz #
----- END CERTIFICATE -----
```

Guardar el paquete de certificados con la extensión bundle.crt

Cargar el paquete de certificados y la clave privada en el directorio del servidor Nginx

Crear host virtual Nginx (opcional).

Si no se tiene configurado el puerto 443 de Nginx se deberá de abrir el archivo de hosts virtual Nginx para configurar el SSL

Si se requiere que el sitio sea accesible a través de conexiones seguras (https) y no seguras (http), necesitará un módulo de servidor para cada tipo de conexión. Es decir, deberá hacer una copia del módulo de servidor no seguro existente y pegarlo debajo del original.

Añadir las siguientes líneas:

```
server {

 listen   443;

 ssl    on;
 ssl_certificate    /etc/ssl/bundle.crt
 ssl_certificate_key    /etc/ssl/myservidorweb.key;

 server_name miservidorweb.unam.mx;
 access_log /var/log/nginx/nginx.vhost.access.log;
 error_log /var/log/nginx/nginx.vhost.error.log;
 location / {
  root   /home/www/public_html/miservidorweb.unam.mx/public/;
  index  index.html;
 }

}
```

Es importante asegurarse de ajustar los nombres de los archivos para que coincidan con sus archivos de certificado:

- ssl_certificate debe ser su certificado primario combinado con el paquete de certificados raíz e intermedio que realizó en el paso anterior bundle.crt
- ssl_certificate_key deberá ser el archivo que contiene la llave privada generado cuando creó el CSR. myservidorweb.key

Reiniciar Nginx:

```
sudo /etc/init.d/nginx restart
```

Fin del proceso.

Instalación de SSL en Tomcat

Se asume que el certificado proporcionado por la DGTIC tiene el nombre de:

- myservidorweb.cer

Los certificados raíz e intermedio vienen comprimidos en un archivo .zip con nombres clave para una correcta identificación:

- UNAM_Root_R3_raiz.zip
- UNAM_RSA_OV_SSL_CA.zip

Archivo de la llave privada, generado cuando creó el CSR:

- myservidorweb.jks

Inicio del proceso

Crear un respaldo del archivo myservidorweb.jks

Nota: /<RUTA>/ hace referencia al directorio donde se encuentran los archivos.

Inyectar los certificados CA root, Intermedio y el certificado SSL del sitio:

- Cargar certificado raíz

```
keytool -importcert -trustcacerts -alias root -file
/<RUTA>/UNAM_Root_R3_raiz.crt -keystore /<RUTA>/myservidorweb.jks
```

- Cargar certificado Intermedio

```
keytool -importcert -trustcacerts -alias intermedio -file
/<RUTA>/UNAM_RSA_OV_SSL_CA.crt -keystore /<RUTA>/myservidorweb.jks
```

- Cargar certificado del sitio

```
keytool -import -trustcacerts -alias aliasmyservidorweb -file
/<RUTA>/myservidorweb.cer -keystore /<RUTA>/myservidorweb.jks
```

Crear conector 443 (opcional).

Si no se tiene configurado el puerto 443 de tomcat se deberá de abrir el archivo ***server.xml*** para configurar el SSL

Abrir el archivo **conf/server.xml** de Tomcat en un editor de texto.

Identificar el conector que se enlazará con el Almacén de certificados, generalmente el archivo ***server.xml*** tiene el conector comentado solo sería cuestión de decomentarlo

```
<Connector port="443" maxHttpHeaderSize="8192" maxThreads="100"
           minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" disableUploadTimeout="true"
           acceptCount="100" scheme="https" secure="true"
           SSLEnabled="true" clientAuth="false"
           sslProtocol="TLS" keyAlias="aliasmyservidorweb"
           keystoreFile="/<RUTA>/myservidorweb.jks "
           keystorePass="passwordmyservidorweb" />
```

Guardar los cambios en el archivo server.xml

Reiniciar Tomcat para que el nuevo certificado se pueda visualizar en el sitio web.

Fin del proceso.

Instalación de SSL en Windows Server 2012

Se asume que el certificado proporcionado por la DGTIC tiene el nombre de:

- myservidorweb.cer

Los certificados raíz e intermedio vienen comprimidos en un archivo .zip con nombres clave para una correcta identificación:

- `UNAM_Root_R3_raiz.zip`
- `UNAM_RSA_OV_SSL_CA.zip`

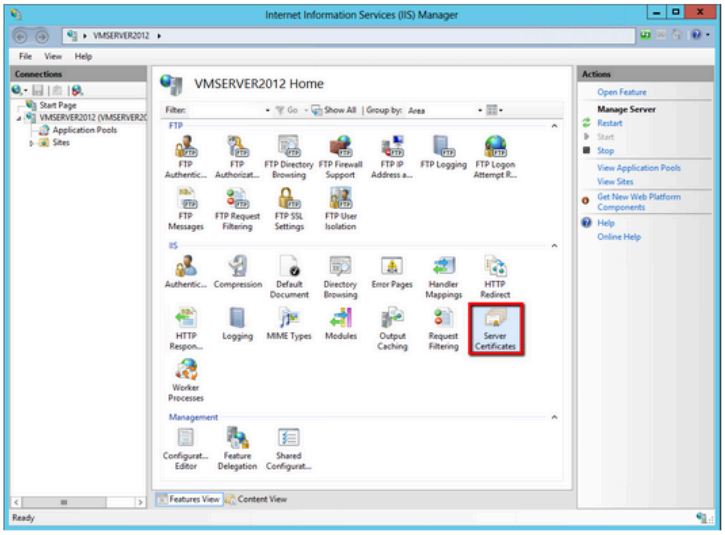
Nota: /<RUTA>/ hace referencia al directorio donde se encuentran los archivos.

Inicio del proceso.

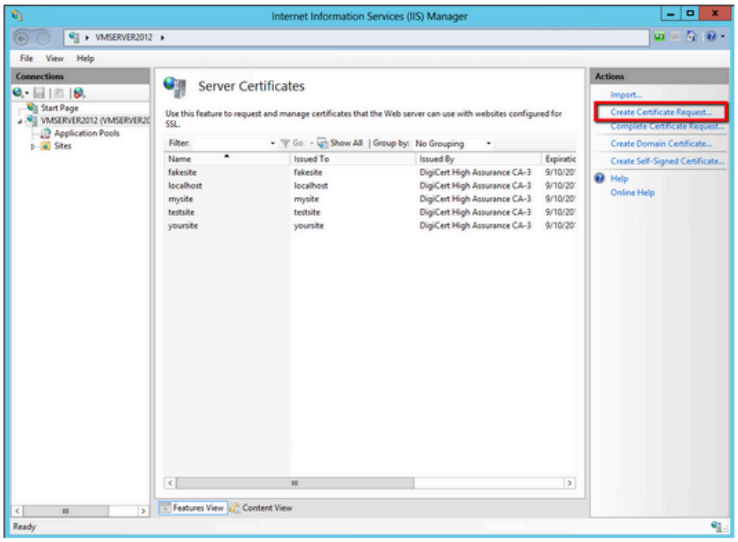
Guardar el archivo del certificado en el servidor IIS donde se generó el *CSR.*

Al ingresar al Administrador de ***Internet Information Services (IIS)***, identificar la opción ***Connections*** y dar clic en el nombre de host del servidor.

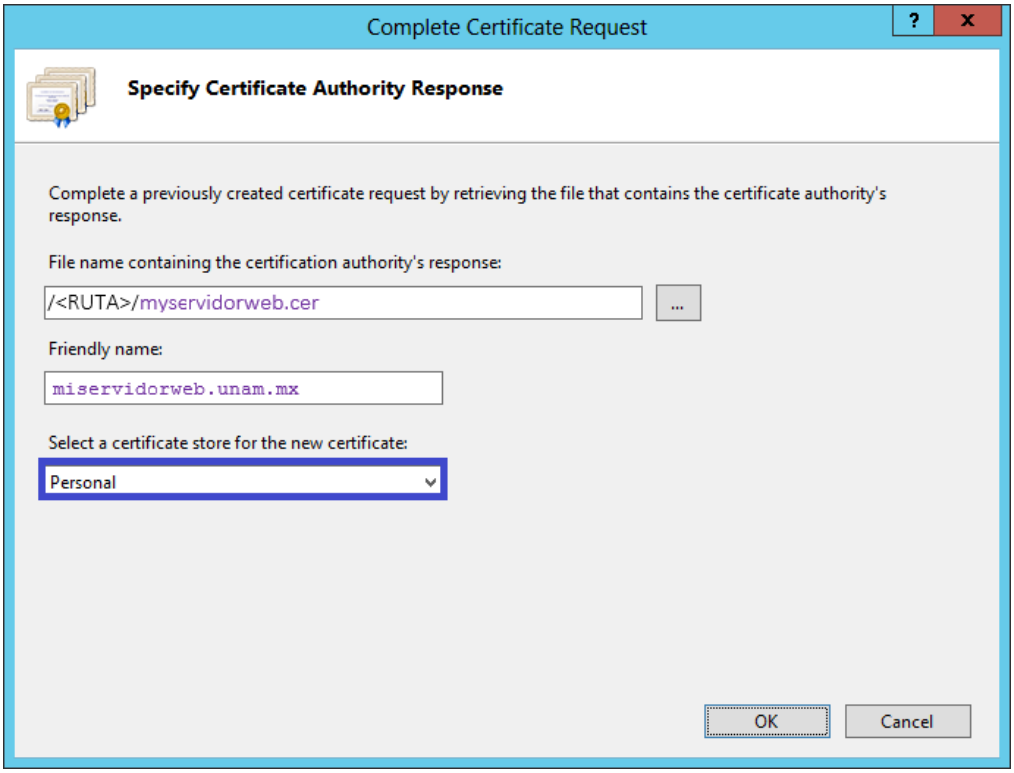
En el menú principal del servidor seleccionado, identificar la sección ***IIS*** y dar doble clic en el icono ***Server Certificates.***



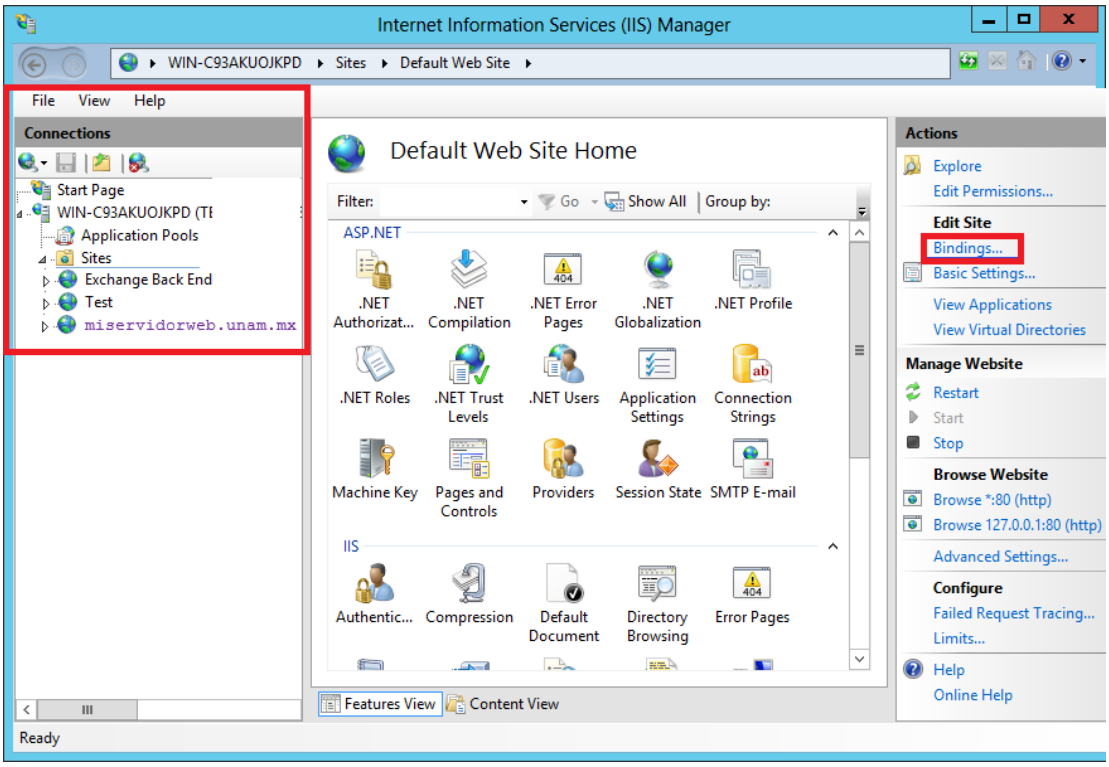
En el menú ***Acciones***, dar clic en ***Completar solicitud de certificado*** para abrir el asistente.



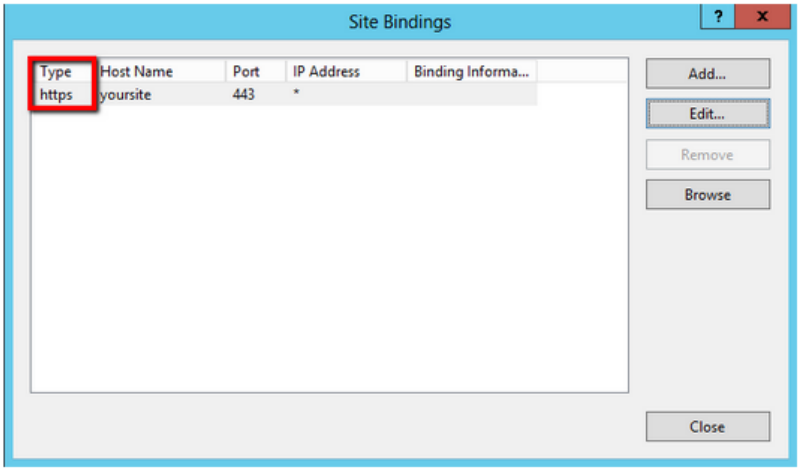
En la opción ***Specify Certificate Authority Response***, seleccionar el archvo .cer del certificado SSL adquirido. A continuación, ingrese un nombre descriptivo para identificar el certificado



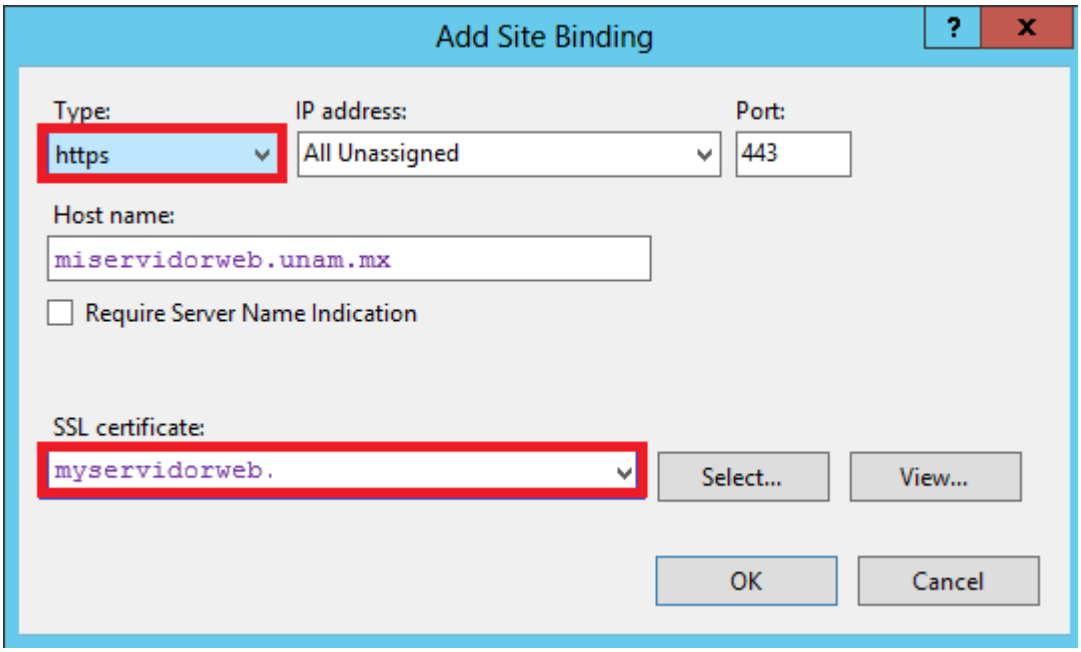
En el panel de administración de ***(IIS)***, Seleccionar el sitio en el que desea habilitar el certificado SSL.



En el menú ***Acciones***, identificar la opción ***Editar sitio***, dar clic en ***Enlaces***. A continuación seleccionar el enlace para ***https*** y dar clic en ***Editar***.



En la ventana ***Editar enlace del sitio***, seleccionar en la lista desplegable el Certificado SSL y dar clic en ok.



Fin del Proceso.

Renovación de certificado SSL.

El proceso de renovación de Certificados SSL consiste en reemplazar el archivo del Certificado SSL del sitio que ha expirado, así como los certificados raíz e intermedio que corresponden al nuevo certificado.

El procedimiento a seguir para su reemplazo será el definido para cada plataforma.

Si tiene dudas puede enviar correo a firma.tic@unam.mx

Datos de contacto

Departamento de Firma Electrónica Avanzada
DGTIC UNAM
firma.tic@unam.mx
55562-23599

Responsable
Mtra. Lizbeth Angélica Barreto Zúñiga
Jefa del Departamento de Firma Electrónica Avanzada
bazuli@unam.mx
55562-23975

Asesoría y soporte para instalación de SSL:
Ing. Jhonatan Rafael Pontaza López
Jefe de Administración de aplicaciones
jr.pontaza@unam.mx
55562-23982

DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA

2020