GENERACIÓN DE SOLICITUD DE CERTIFICADO DIGITAL(CSR)

Departamento de Firma Electronica Avanzada UNAM

Emisión de Certificados SSL

Contenido del Documento

Ficha técnica del Documento

Control de Versiones del Documento

Versión	Fecha	Autor	Motivo del Cambio
1.0	15/01/2017	Departamento de Firma Electrónica Avanzada UNAM	Creación del documento Inicial

Dirigido a

El presente documento está dirigido al personal técnico responsable de generar la solicitud de un Certificado Digital SSL (CSR) para cumplimentar el proceso de adquisición de certificados SSL en la UNAM.

Alcance

El documento que a continuación se presenta, establece los pasos a seguir para generar el CSR (Solicitud de Firma de Certificado por sus siglas en inglés) en servidores que requieren brindar el servicio de HTTPS.

Las plataformas comprendidas en el presente manual son: Windows Server, Microsoft Exchange, Apache Server y Tomcat.

Tipografía

Tamaño	Fuente	Cuerpo de texto
11	Courier New	Líneas de comando Ejemplo: `SSLCertificateFile /<RUTA>/my-servidor-web.cer`
12	Arial	Descripción (Texto plano)

Introducción

El Certificate Signing Request o CSR es un archivo que se genera en el servidor donde se va a utilizar el Certificado SSL y consiste en un bloque de texto codificado en base 64 que contiene información de la entidad o dependencia asociada al servidor que habilitará el servicio de HTTPS.

El CSR contiene, el nombre del titular del certificado SSL, dirección, país de residencia, clave pública y el dominio para el que se generará el Certificado SSL, también conocido como *common name*. A continuación se enlista una breve definición de cada campo.

- **Common name:** Es el nombre de dominio o subdominio, de acuerdo a los términos establecidos durante la adquisición del certificado SSL (Wild Card u Organizacional).
- **Organización:** Es el nombre legal de la organización.
- **Sección/Departamento:** Será el departamento, área o división de la empresa que gestionará el certificado.
- **Correo electrónico:** Cuenta de correo electrónico que se usará para contactar al responsable en Entidad o Dependencia.
- **País:** Ubicación de la Entidad o Dependencia.
- **Nombre de Estado o Provincia:** Estado donde encuentra ubicada la Entidad o Dependencia.
- **Localidad:** La localidad donde está ubicada la Entidad o Dependencia.
- **Clave pública:** Será la clave pública que se genera automáticamente y se inserta en el certificado.

Una vez recopilada la información (CSR) solicitada por la DGTIC, se deberá entregar una copia impresa junto con el oficio correspondiente al Departamento de Firma Electrónica Avanzada, asimismo se deberá enviar a firma.tic@unam.mx el archivo CSR correspondiente. La DGTIC validará la información y se pondrá en contacto vía correo para dar continuidad al proceso.

En este manual se proporcionan las instrucciones a seguir para generar el CSR.

Generación de CSR en Windows Server II7

Descripción

Inicio del proceso.

1. Presione (Start) **Inicio**, haga clic en (**Administrative Tools**) **Herramientas Administrativas** y seleccione **Internet Information Services (IIS)**.

2. Seleccione (clic) en el nombre de servidor.

3. En el menú central, haga doble clic en el botón (*Server Certificates*) **Certificados del Servidor** en la sección (*Security*) **Seguridad**.

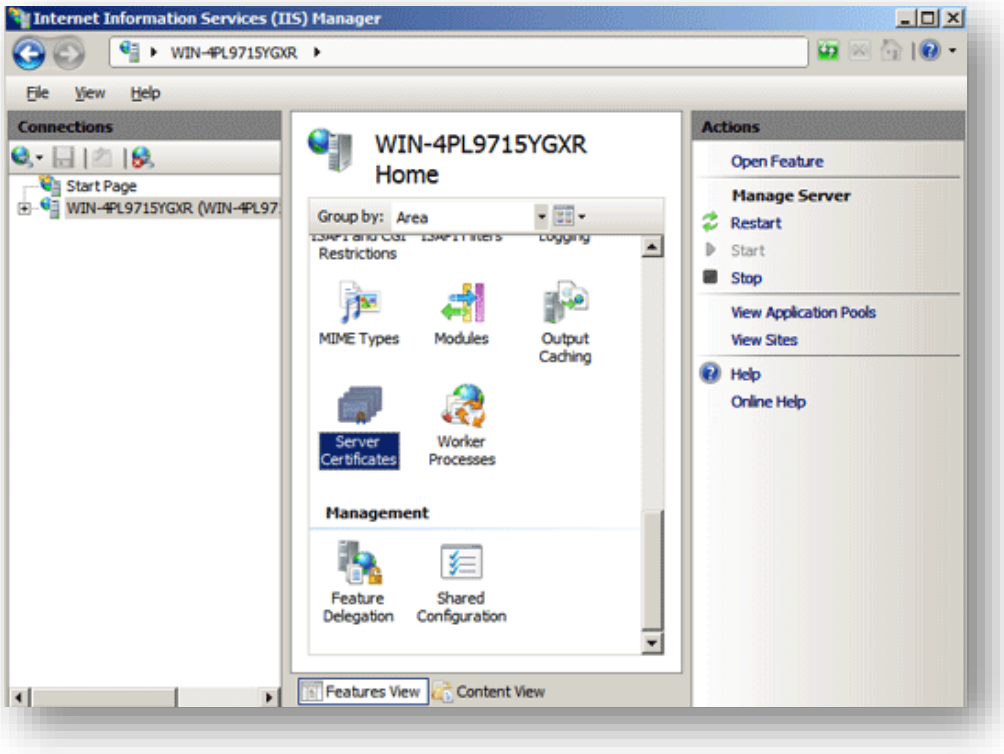

Imagen 1.

4. Ingrese al menú de (*Actions*) **Acciones**, haga clic en (*Create Certificate Request*) **Crear solicitud de certificado**. Esta acción abrirá el Asistente de Solicitud de Certificado.

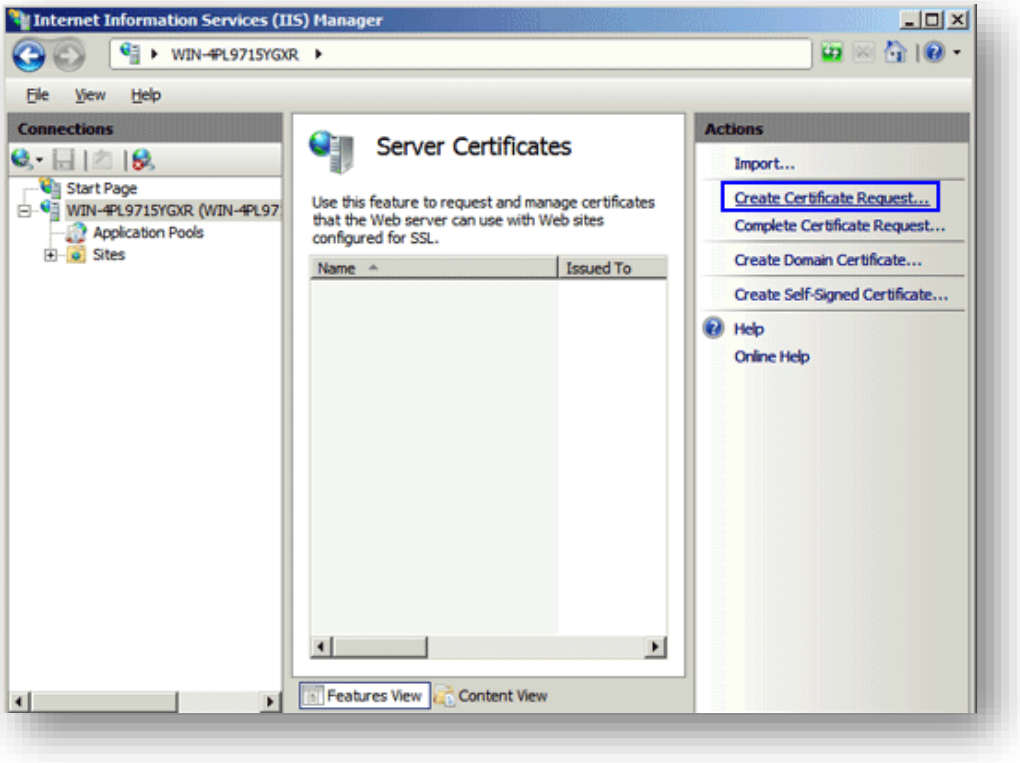

Imagen 2.

5. En la ventana (*Distinguished Name Properties*) **Propiedades de Nombre Distintivo**, introduzca la información listada a continuación:

   - (*Common name*) **Nombre de dominio con www*.**
   - (*Organization*) **Organización.**
   - (*City/locality*) **Ciudad/localidad.**
   - (*State/province*) **Estado/provincia**.
   - (*Country/Region*) **País/Región**.

6. Seleccione (clic) en (*Next*) **Siguiente**.

* se debe incluir si su sitio responderá también a dominio con www.

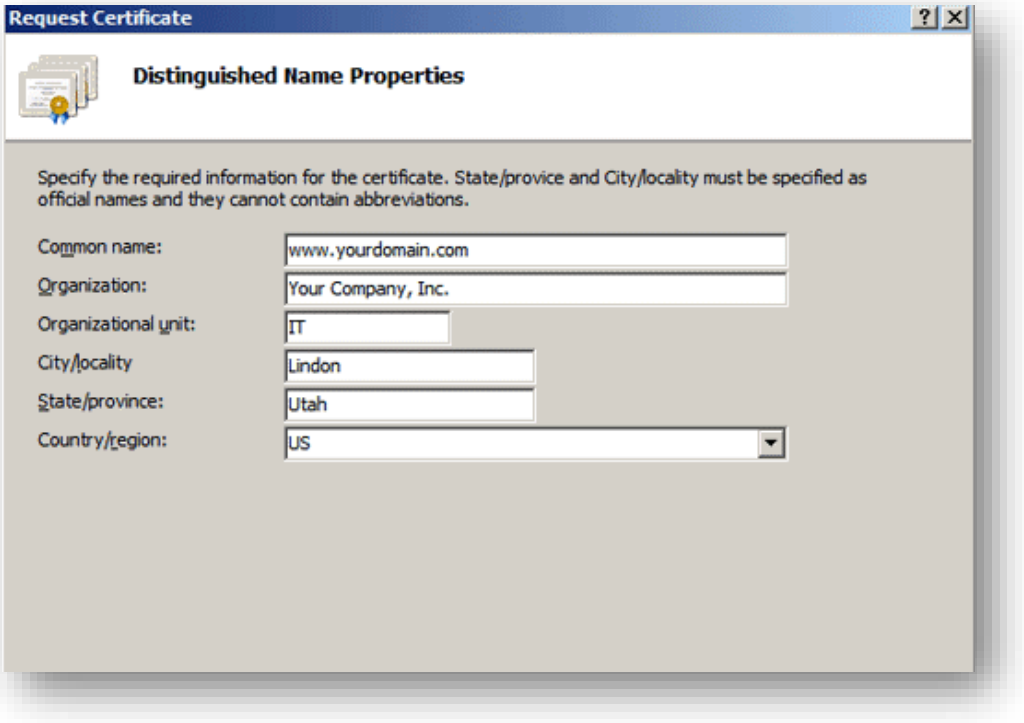

Imagen 3.

7. En la ventana (*Cryptographic Service Provider Properties*) **Propiedades del proveedor de servicios criptográficos**, deje ambos parámetros con sus valores predeterminados (Microsoft RSA SChannel y 2048).

8. Seleccione (clic) en (*Next*) **Siguiente**.

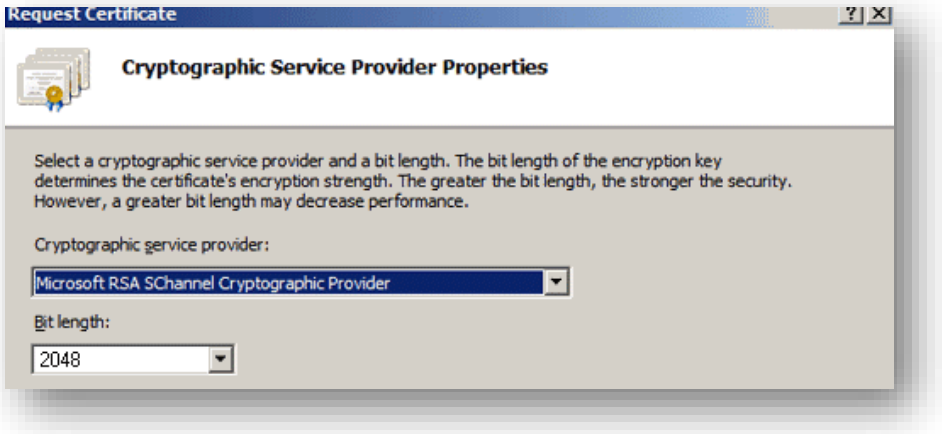

Imagen 4.

9. Introduzca un nombre de archivo para el archivo de Solicitud de Firma de **Certificado (CSR).**

10. Identifique la ruta y guarde el archivo. Será necesario que abra este archivo como un archivo de texto y copie todo el texto completo incluidas las etiquetas `BEGIN CERTIFICATE REQUEST` y `END CERTIFICATE REQUEST`.

Fin de proceso.

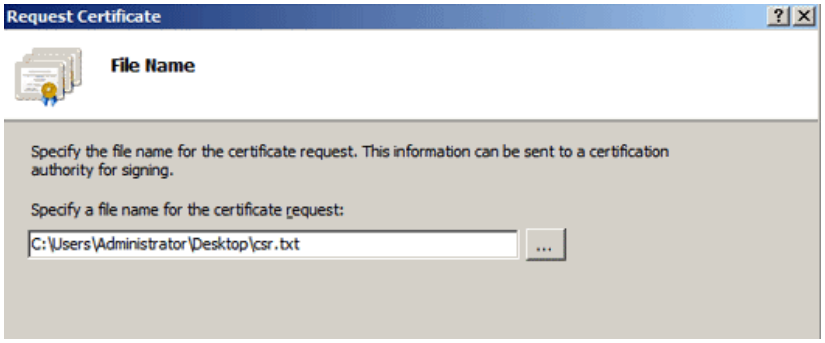

Imagen 5.

Ejemplo:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDADCCAegCAQAwgaIxCzAJBgNVBAYTAk1YMRkwFwYDVQQIDBBDSVVEQUQgREUg
TUVYSUNPMRkwFwYDVQQHDBBDSVVEQUQgREUgTUVYSUNPMQ0wCwYDVQQKDARVTkFN
MQ4wDAYDVQQLDAVER1RJQzEcMBoGA1UEAwwTY2EudW5hbWdyaWQudW5hbS5teDEg
MB4GCSqGSIb3DQEJARYRY2FtYW5hZ2VyQHVuYW0ubXgwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC8uWZ/+gH622KpIGgckL4T/hx6WAUJ4pDZB0B6hjLL
PipHuhvH933upXWDBRultSeSS77NfbbQ1rq8J3C/GxgoCJ6VwxikTTU/sw2B2mem
PZQ5AkYaOw6S5/wzS/J9po5GlHomZ8YMtfq8wO2UWUSbbUBQ82+t2mcGUd+N0EiO
hM5Sb16zcjKLFf6oapQojNsMfIdV4gcSw11o4gwye03MShtoCiD6ppq/3joES5/s
qQMnonXS/9uQ3swKU0GMxIGunIREO+jCoVK81a396gktyJCv4evsLy/OBvdV9iIK
owzRp46LYo1XZB3r+PhZYYii4+XS0schIx2W8HJ1zXI1AgMBAAGgGDAWBgkqhkiG
9w0BCQcxCQwHMnBiNjltSjANBgkqhkiG9w0BAQsFAAOCAQEAbGKvJ0nP0SAXwuP+
44yO2kLixRTuVumSYeuh9XE0Q58J+ngpEHKV/WXCjY+q8zTI9LpgPQ8cI81yyY2O
1qUHRrlC9I/V3BHGf1Xqx3TmijO3xMUPtewcHHsVG1jcRiklzyLzoQvo791Wzb+u
VpxzAZeqwO2l33ojPyIHdhNsm+pX2MF9RbnA0TKR3Be1rhteZvonKS2aflMOyDzP
V5hkGXS+hzMWrMqQR9rnEKKAOKQkfSzfLCI8KOQuL2Y8WiF+65DOzkvRFC5vjeFI
h8AgOmU7p4UNggpOnQAvia8I5gaJmo7J699nWvZIEZcNp9LwV/ncRLLlUqoIIzb4
jFN/aw==
-----END CERTIFICATE REQUEST-----
```

Generación de CSR en Microsoft Exchange 2013

Descripción

Inicio del proceso.

1. Acceda al Centro de administración de Exchange abriendo en su navegador **https://localhost/ecp**
2. Inicie sesión (ingrese nombre de **Usuario** y **Contraseña**).
3. Haga clic en el enlace a Servers/**Servidores**.
4. Seleccione la pestaña superior **Certificates/Certificados.**
5. Enseguida dar clic en el icono **+**.

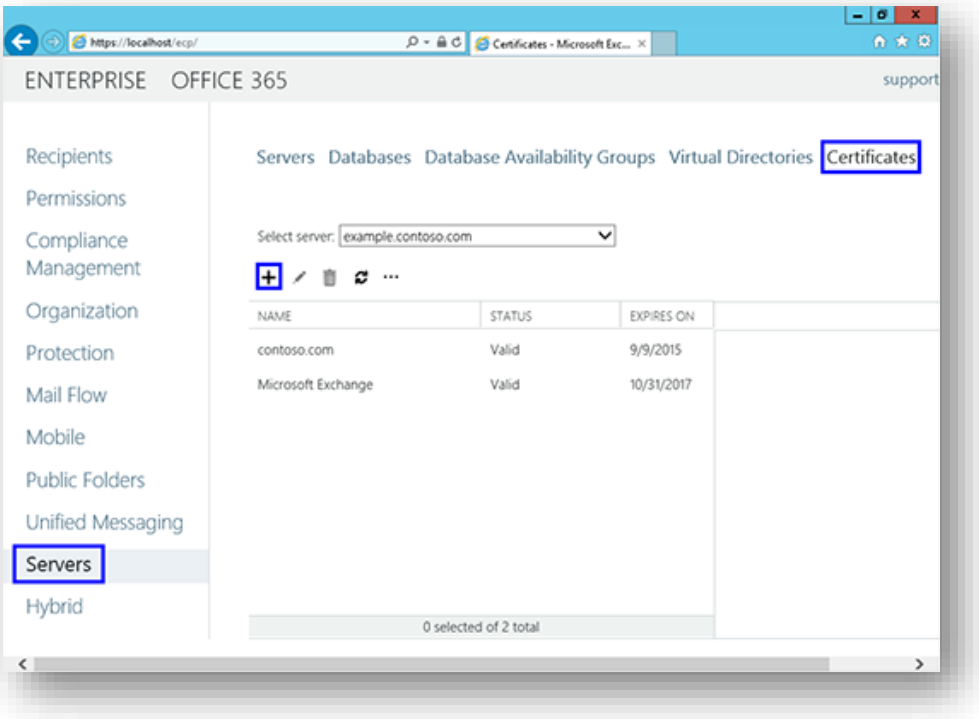

Imagen 6.

6. El asistente **"new exchange certificate"** aparecerá en una ventana emergente.

7. Selecciones **" Create a request for a certificate from a certification authority".**

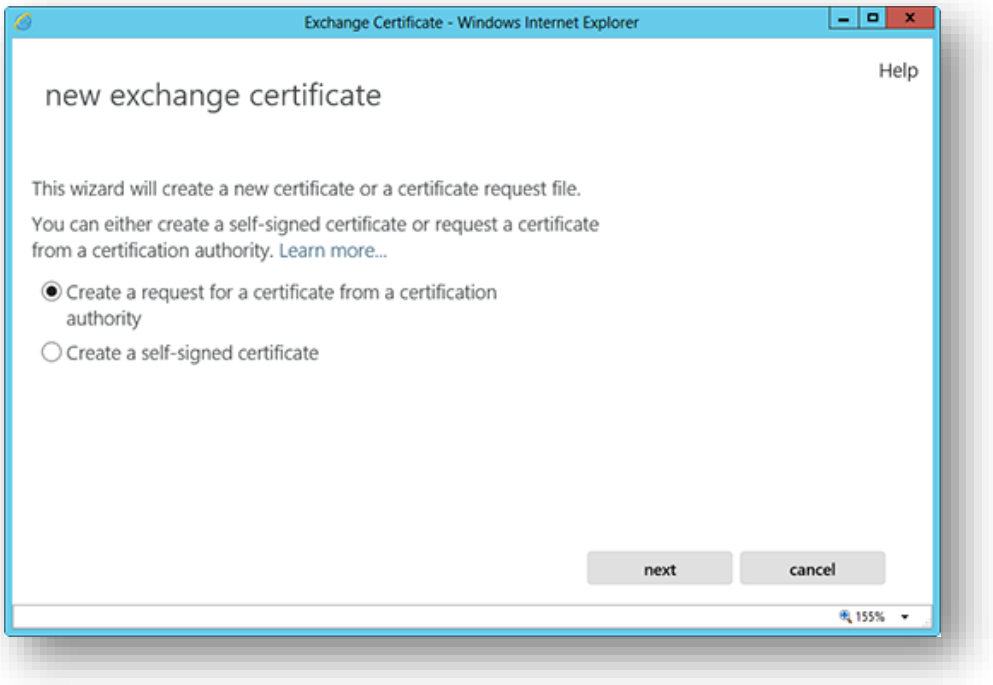

Imagen 7.

8. En el campo del nombre descriptivo, ingrese un nombre para identificar el archivo.

9. Marcar la casilla e ingresar el nombre de dominio raíz (**ingrese www si su sitio responde también a este dominio)** si va a generar el CSR para un **Wildcard cert**. De lo contrario, sólo vaya a la siguiente pantalla y seleccione **Buscar** para elegir en qué servidor desea guardar la solicitud de certificado.

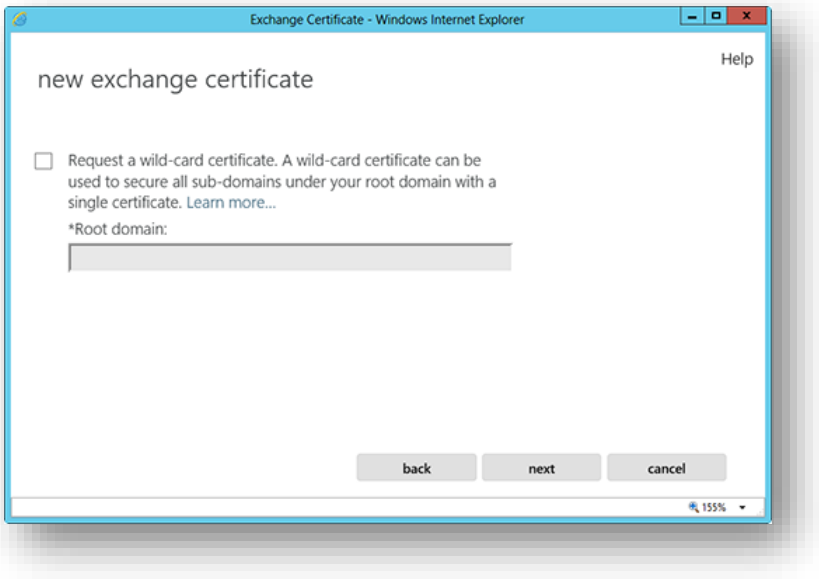

Imagen 8.

10. Si se está realizando un **Wildcard cert**, omitirá este paso. En la lista, seleccione los servicios que planea ejecutar de forma segura utilizando Ctrl + Clic para resaltar los servicios.

11. Ingrese la información correspondiente a su Entidad o Dependencia.

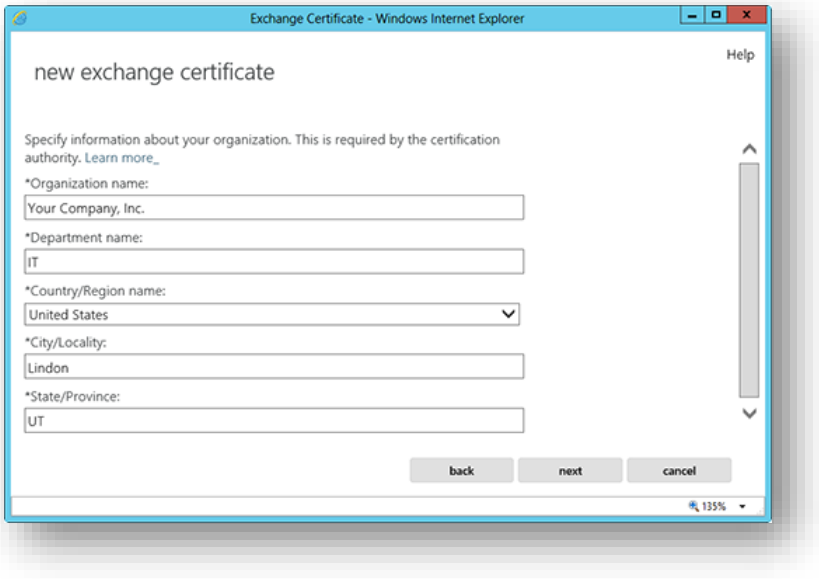

Imagen 9.

12. Por último Introduzca una ruta de acceso compartido de red para guardar el CSR en su equipo como un archivo **.req** y a continuación dar clic en Finalizar.

Fin de proceso.

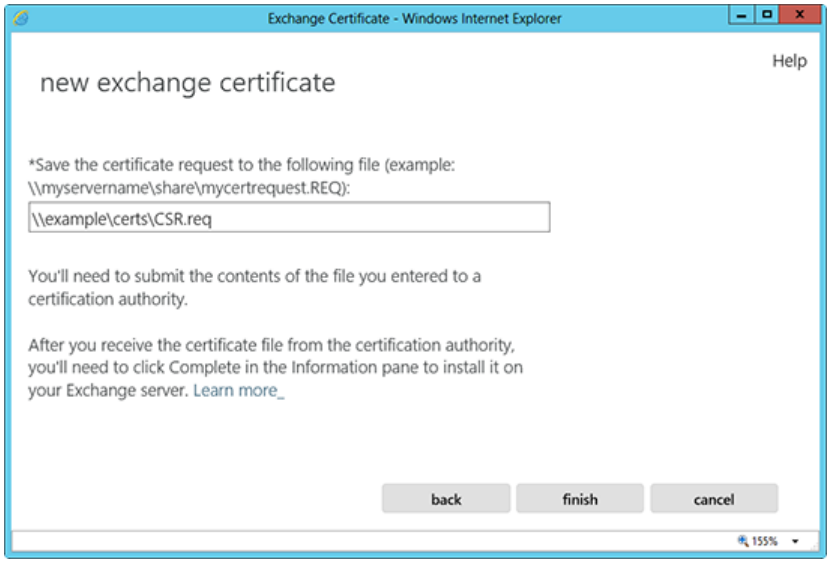

Imagen 10.

Ejemplo:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDADCCAegCAQAwgaIxCzAJBgNVBAYTAk1YMRkwFwYDVQQIDBBDSVVEQUQgREUg
TUVYSUNPMRkwFwYDVQQHDBBDSVVEQUQgREUgTUVYSUNPMQ0wCwYDVQQKDARVTkFN
MQ4wDAYDVQQLDAVER1RJQzEcMBoGA1UEAwwTY2EudW5hbWdyaWQudW5hbS5teDEg
MB4GCSqGSIb3DQEJARYRY2FtYW5hZ2VyQHVuYW0ubXgwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC8uWZ/+gH622KpIGgckL4T/hx6WAUJ4pDZB0B6hjLL
PipHuhvH933upXWDBRultSeSS77NfbbQ1rq8J3C/GxgoCJ6VwxikTTU/sw2B2mem
PZQ5AkYaOw6S5/wzS/J9po5GlHomZ8YMtfq8wO2UWUSbbUBQ82+t2mcGUd+N0EiO
hM5Sb16zcjKLFf6oapQojNsMfIdV4gcSw11o4gwye03MShtoCiD6ppq/3joES5/s
qQMnonXS/9uQ3swKU0GMxIGunIREO+jCoVK8la396gktyJCv4evsLy/OBvdV9iIK
owzRp46LYo1XZB3r+PhZYYii4+XS0schIx2W8HJ1zXI1AgMBAAGgGDAWBgkqhkiG
9w0BCQcxCQwHMnBiNjltSjANBgkqhkiG9w0BAQsFAAOCAQEAbGKvJ0nP0SAXwuP+
44yO2kLixRTuVumSYeuh9XE0Q58J+ngpEHKV/WXCjY+q8zTI9LpgPQ8cI81yyY2O
1qUHRrlC9I/V3BHGf1Xqx3TmijO3xMUPtewcHHsVG1jcRiklzyLzoQvo791Wzb+u
VpxzAZeqwO2l33ojPyIHdhNsm+pX2MF9RbnA0TKR3Be1rhteZvonKS2aflMOyDzP
V5hkGXS+hzMWrMqQR9rnEKKAOKQkfSzfLCI8KOQuL2Y8WiF+65DOzkvRFC5vjeFI
h8AgOmU7p4UNggpOnQAvia8I5gaJmo7J699nWvZIEZcNp9LwV/ncRLLlUqoIIzb4
jFN/aw==
-----END CERTIFICATE REQUEST-----
```

Generación de CSR en Apache Server (OpenSSL)

Descripción

Inicio del proceso.

1. Inicie sesión en el servidor mediante el terminal **Shell** (ssh). Cuando el sistema se lo solicite, escriba:

```
openssl req -new -newkey rsa:2048 -nodes -keyout servidor.key -out servidor.csr
```

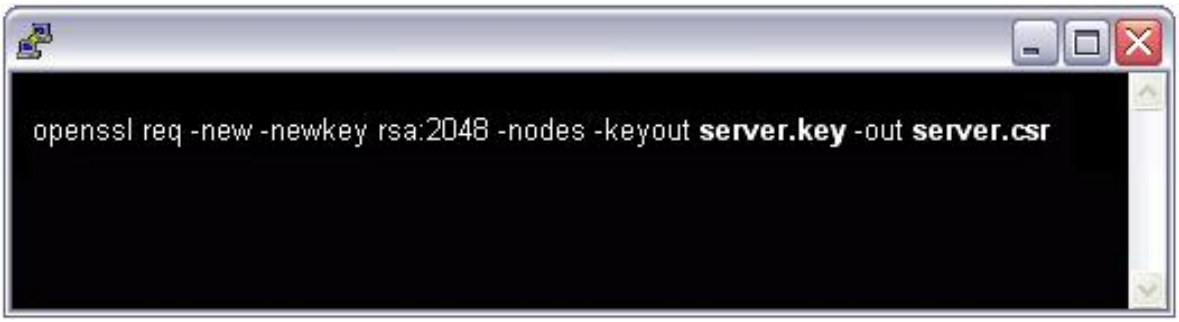

Imagen 11.

IMPORTANTE: Deberá sustituir "**servidor"** por el nombre de su servidor.

2. Al ingresar el comando se inicia el proceso de generación de dos archivos: el archivo de la **llave privada** y un archivo de Solicitud de Firma de Certificado (**.csr**).

3. Cuando el sistema le solicite el **nombre común** (nombre de dominio), introduzca el nombre de dominio completo correspondiente al sitio que desea proteger, **incluyendo www si su sitio responderá también a este.**

IMPORTANTE: Si genera un archivo de Solicitud de Firma de Certificado en Apache para un Certificado Wildcard SSL, el nombre común debe comenzar con un asterisco (**`*.ejemplo.com`**).

4. Enseguida se le solicitará que especifique la información de su organización. Es posible que ya exista información establecida de forma predeterminada.

Esta acción creará su archivo **`openssl .csr.`**

5. Abra el archivo de **Solicitud de Firma de Certificado (CSR)** con un editor de texto.

6. Guarde una copia de seguridad del archivo **.KEY** en un lugar seguro ya que, posteriormente, se requerirá para la instalación del certificado SSL.

Fin de proceso.

Ejemplo:


```
-----BEGIN CERTIFICATE REQUEST-----
MIIDADCCAegCAQAwgaIxCzAJBgNVBAYTAk1YMRkwFwYDVQQIDBBDSVVEQUQgREUg
TUVYSUNPMRkwFwYDVQQHDBBDSVVEQUQgREUgTUVYSUNPMQ0wCwYDVQQKDARVTkFN
MQ4wDAYDVQQLDAVER1RJQzEcMBoGA1UEAwwTY2EudW5hbWdyaWQudW5hbS5teDEg
MB4GCSqGSIb3DQEJARYRY2FtYW5hZ2VyQHVuYW0ubXgwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC8uWZ/+gH622KpIGgckL4T/hx6WAUJ4pDZB0B6hjLL
PipHuhvH933upXWDBRultSeSS77NfbbQ1rq8J3C/GxgoCJ6VwxikTTU/sw2B2mem
PZQ5AkYaOw6S5/wzS/J9po5GlHomZ8YMtfq8wO2UWUSbbUBQ82+t2mcGUd+N0EiO
hM5Sb16zcjKLFf6oapQojNsMfIdV4gcSw11o4gwye03MShtoCiD6ppq/3joES5/s
qQMnonXS/9uQ3swKU0GMxIGunIREO+jCoVK8la396gktyJCv4evsLy/OBvdV9iIK
owzRp46LYo1XZB3r+PhZYYii4+XS0schIx2W8HJ1zXI1AgMBAAGgGDAWBgkqhkiG
9w0BCQcxCQwHMnBiNjltSjANBgkqhkiG9w0BAQsFAAOCAQEAbGKvJ0nP0SAXwuP+
44yO2kLixRTuVumSYeuh9XE0Q58J+ngpEHKV/WXCjY+q8zTI9LpgPQ8cI81yyY2O
1qUHRrlC9I/V3BHGf1Xqx3TmijO3xMUPtewcHHsVG1jcRiklzyLzoQvo791Wzb+u
VpxzAZeqwO2l33ojPyIHdhNsm+pX2MF9RbnA0TKR3Be1rhteZvonKS2aflMOyDzP
V5hkGXS+hzMWrMqQR9rnEKKAOKQkfSzfLCI8KOQuL2Y8WiF+65DOzkvRFC5vjeFI
h8AgOmU7p4UNggpOnQAvia8I5gaJmo7J699nWvZIEZcNp9LwV/ncRLLlUqoIIzb4
jFN/aw==
-----END CERTIFICATE REQUEST-----
```


Generación Tomcat Server (Keytool)

Descripción

Inicio del proceso.

1. Se debe generar un almacén de claves nuevo, ingrese el comando de **keytool** para crear y administrar el nuevo archivo de almacén de llaves. Es posible que tenga que agregar el directorio **java** o **bin** a su variable de ambiente **PATH** (opcional) antes de que se reconozca el comando **keytool**. Después de

confirmar el almacén de claves, identifique el directorio en donde se planea administrar el almacén de claves y los certificados.

2. Introduzca el siguiente comando:

```
keytool -genkey -alias servidor -keyalg RSA -keysize 2048 -
keystore servidor.jks
```

IMPORTANTE: Deberá sustituir "**servidor"** por el nombre de su servidor.

3. Enseguida se solicitará una contraseña para el almacén de claves. Si el almacén especificado no existía previamente, este proceso asignará la contraseña ingresada.

4. A continuación tendrá que ingresar la información requerida de su organización para la generación del CSR.

   - Dominio completo para el sitio que desea proteger.
   - Si solicita un certificado **Wildcard,** no olvide ingresar el **carácter *. (ejemplo: *.sudominio.com).**

5. Al finalizar de ingresar la información, verifique que los datos sean correctos y presione la tecla **`'y'`** o escriba la palabra **`'yes'`**(sin comillas).

6. Enseguida el servidor solicitará que confirme la contraseña previamente creada. Asegúrese de recordar la contraseña.

7. A continuación el archivo de almacén de datos con el nombre **`servidor.jks`** se creará en el directorio de trabajo actual

8. Para generar el CSR del nuevo almacén de claves , se utilizará la herramienta **Keytool;** introduzca el siguiente comando:

```
keytool -certreq -alias servidor -file csr.txt –keystore
servidor.jks
```

9. Escriba la contraseña del almacén de claves que definió anteriormente y presione **ENTER**.

10. El archivo de Solicitud de Firma de Certificado denominado **csr.txt** se generará en el directorio actual. Abra el archivo **CSR** con un editor de texto.

Fin de proceso.

EJEMPLO TIPO DE DOCUMENTO CSR PARA ADJUNTO

Los datos referidos en el siguiente ejemplo en color azul, deberán ser los mismos en la emisión del CSR, los amarillos corresponden a los datos del solicitante.

```
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:CIUDAD DE MEXICO
Locality Name (eg, city) []:CIUDAD DE MEXICO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNAM
Organizational Unit Name (eg, section) []:UNAM
Common Name (e.g. server FQDN or YOUR name) []:www.dominio.unam.mx
Email Address []:correo del contacto técnico

-----BEGIN CERTIFICATE REQUEST-----
MIIDADCCAegCAQAwgaIxCzAJBgNVBAYTAk1YMRkwFwYDVQQIDBBDSVVEQUQgREUg
TUVYSUNPMRkwFwYDVQQHDBBDSVVEQUQgREUgTUVYSUNPMQ0wCwYDVQQKDARVTkFN
MQ4wDAYDVQQLDAVER1RJQzEcMBoGA1UEAwwTY2EudW5hbWdyaWQudW5hbS5teDEg
MB4GCSqGSIb3DQEJARYRY2FtYW5hZ2VyQHVuYW0ubXgwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC8uWZ/+gH622KpIGgckL4T/hx6WAUJ4pDZB0B6hjLL
PipHuhvH933upXWDBRultSeSS77NfbbQ1rq8J3C/GxgoCJ6VwxikTTU/sw2B2mem
PZQ5AkYaOw6S5/wzS/J9po5GlHomZ8YMtfq8wO2UWUSbbUBQ82+t2mcGUd+N0EiO
hM5Sb16zcjKLFf6oapQojNsMfIdV4gcSw11o4gwye03MShtoCiD6ppq/3joES5/s
qQMnonXS/9uQ3swKU0GMxIGunIREO+jCoVK8la396gktyJCv4evsLy/OBvdV9iIK
owzRp46LYo1XZB3r+PhZYYii4+XS0schIx2W8HJ1zXI1AgMBAAGgGDAWBgkqhkiG
9w0BCQcxCQwHMnBiNjltSjANBgkqhkiG9w0BAQsFAAOCAQEAbGKvJ0nP0SAXwuP+
44yO2kLixRTuVumSYeuh9XE0Q58J+ngpEHKV/WXCjY+q8zTI9LpgPQ8cI81yyY2O
1qUHRrlC9I/V3BHGf1Xqx3TmijO3xMUPtewcHHsVG1jcRiklzyLzoQvo791Wzb+u
VpxzAZeqwO2l33ojPyIHdhNsm+pX2MF9RbnA0TKR3Be1rhteZvonKS2aflMOyDzP
V5hkGXS+hzMWrMqQR9rnEKKAOKQkfSzfLCI8KOQuL2Y8WiF+65DOzkvRFC5vjeFI
h8AgOmU7p4UNggpOnQAvia8I5gaJmo7J699nWvZIEZcNp9LwV/ncRLLlUqoIIzb4
jFN/aw==
-----END CERTIFICATE REQUEST-----
```

IMPORTANTE: Esta impresión deberá acompañar al oficio, se generará un CSR por cada certificado solicitado.

IMPORTANTE: El archivo CSR deberá ser enviado al correo firma.tic@unam.mx, acompañado del digital del oficio.

IMPORTANTE: No se deben usar acentos

Anexo I

Apoyo y Soporte Técnico

Mtra. Lizbeth Angélica Barreto Zúñiga

Jefa del Departamento de Firma Electrónica Avanzada

Correo electrónico: bazuli@unam.mx

Teléfono: 56223875

Implementación y procesos:

Ing. Jhonatan Rafael Pontaza López

Jefe de Administración de aplicaciones

Correo electrónico: jr.pontaza@unam.mx

Teléfono: 56223875

DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA

2017