

AGESIC

Gerencia de Proyectos

Tutorial para la Solicitud de Certificados para la PGE

Plataforma Microsoft

Historial de Revisiones

Fecha	Versión	Descripción	Autor
30/06/2011	1.0	Versión inicial	Horacio López
11/08/2011	1.1	Mejoras en los ejemplos presentados y ejemplos para la verificación de la correctitud de los pasos ejecutados.	Horacio López
23/07/2012	1.2	Se agregó sección renovación de certificados	Guzmán Llambías

Nombre actual del archivo: Tutorial_Certificados_Microsoft_v1.2.odt

Andes 1365 piso 7°
Montevideo – Uruguay
Tel./Fax: (+598) 2901.2929*
Email: contacto@agesic.gub.uy

www.agesic.gub.uy

Índice de contenido

1.Prerequisitos.....	4
2.Introducción.....	4
3.Herramientas.....	5
4.Emisión de certificado SSL.....	5
4.1. Paso 1: Solicitud de Certificado para Servicio Web	5
4.2. Paso 2: Solicitud de Firma de Certificado e Importación.....	21
4.3. Paso 3: Importar certificado de la CA.....	27
5.Renovación de certificado SSL.....	29
5.1.Paso 1: Solicitud de renovación de certificado.....	29
5.2. Paso 2: Solicitud de firma a la CA.....	36
5.3. Paso 3: Importar certificado solicitado.....	37

1. Prerequisitos

Para el desarrollo de este tutorial es deseable tener conocimiento sobre los siguientes conceptos:

- Criptografía, certificados digitales, SSL.
- Ejecución de herramientas Java sobre Windows/Linux
- RedUy y la PGE

2. Introducción

Una comunicación segura (SSL o TLS) proporciona autenticación, privacidad e integridad de la información entre extremos en una red mediante el uso de criptografía. Entre los pasos que realiza el protocolo SSL para establecer una conexión segura está el intercambio de claves públicas y autenticación basada en certificados digitales. Habitualmente, sobre la PGE el cliente y el servidor son autenticados (es decir se garantiza su identidad) mediante el uso de certificados.

En este documento se presenta una serie de pasos de cómo un organismo debe obtener un certificado SSL para su servidor. Esto implica:

1. crear una clave privada (propiedad del organismo), para luego crear la solicitud de firma de certificado (CSR) a la autoridad certificadora (CA),
2. obtener el certificado de la CA en el cuál se confiará e incluirlo dentro de los certificados de confianza del organismo,
3. y por último a partir del CSR, seguir el procedimiento para obtener el certificado firmado por la CA.

Estos pasos anteriormente mencionados se detallarán en cada sección del documento.

3. Herramientas

En este documento se trabajó con:

- Windows Server 2003
- IIS 6.0

4. Emisión de certificado SSL

En esta sección se describen los pasos para emitir un certificado por primera vez para un IIS. En caso de querer renovar certificados, ver sección ...

4.1. Paso 1: Solicitud de Certificado para Servicio Web

En la plataforma Microsoft la generación de clave privada (private key - PK) y la solicitud de firma de certificado (CSR – Certificate Signed Request) se realizan en conjunto.

Para obtener la solicitud del certificado se deben realizar los siguientes pasos:

1. Ir a “Inicio” → “Todos los programas” → “Herramientas administrativas” → “Administrador de Internet Information Services (IIS)”
2. Seleccionar el servicio web para que se quiere el certificado (ej: ServicioDNPT), click derecho “Propiedades”, Figura 1.
3. Ir a la pestaña “Seguridad de directorios” (Figura 2) y luego click en “Certificado de servidor” (Figura 3).

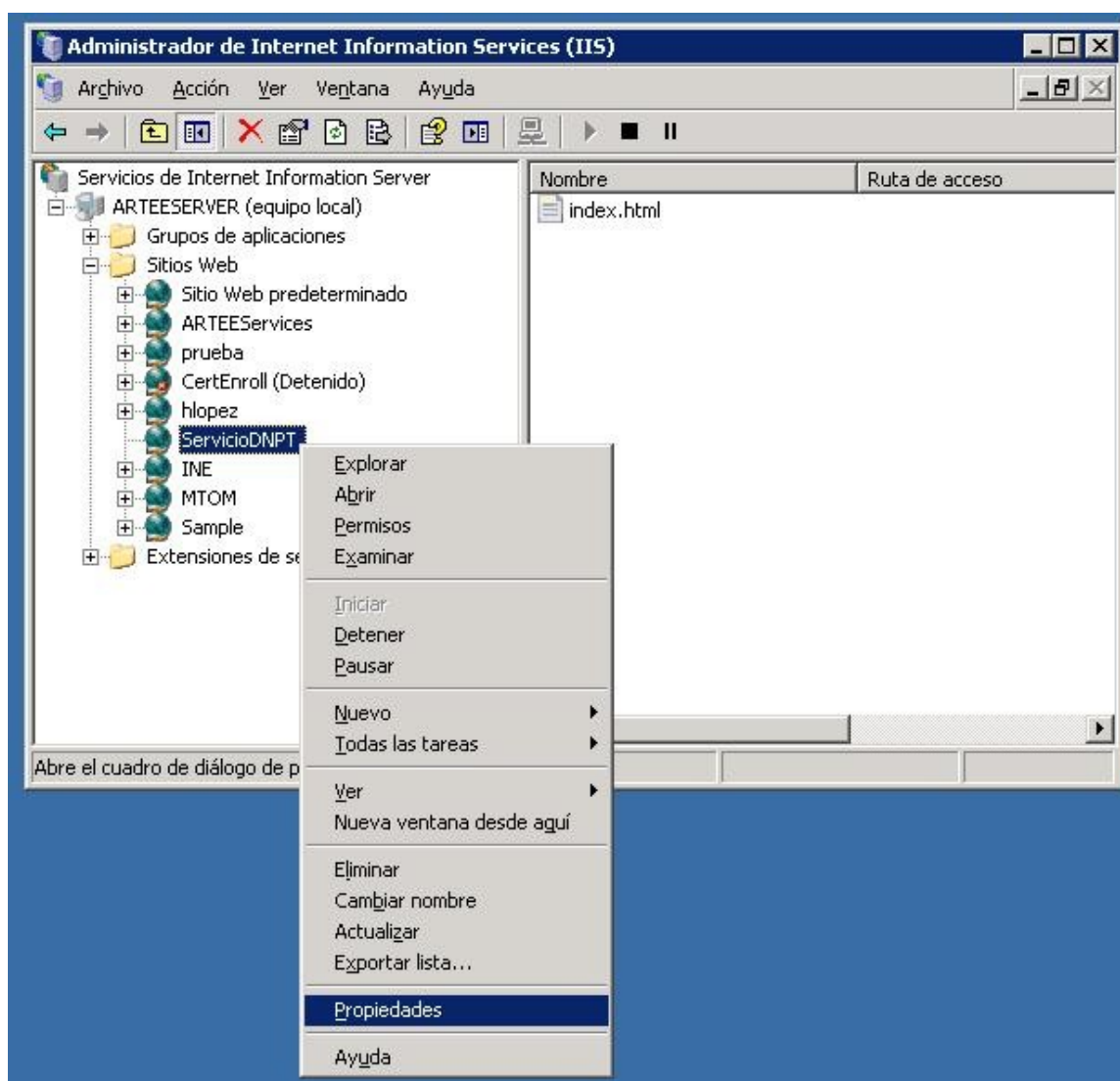


Figura 1: Menú contextual de sitio web IIS

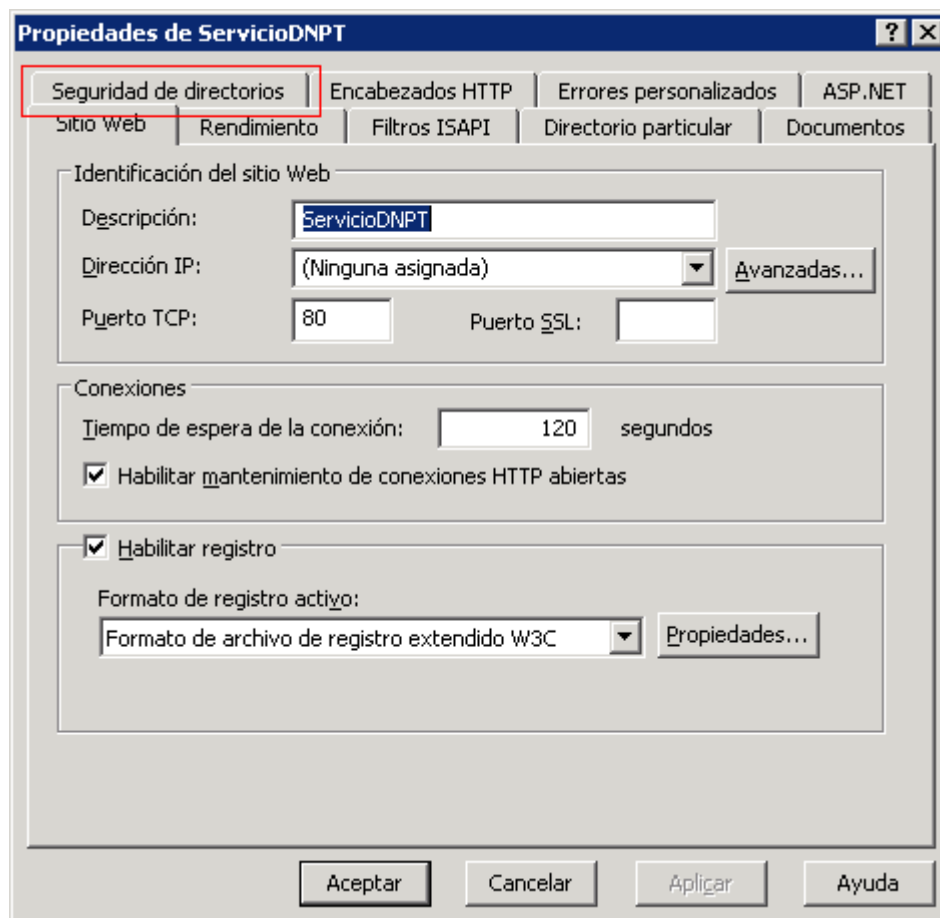


Figura 2: Ventana de propiedades - Pestaña Seguridad

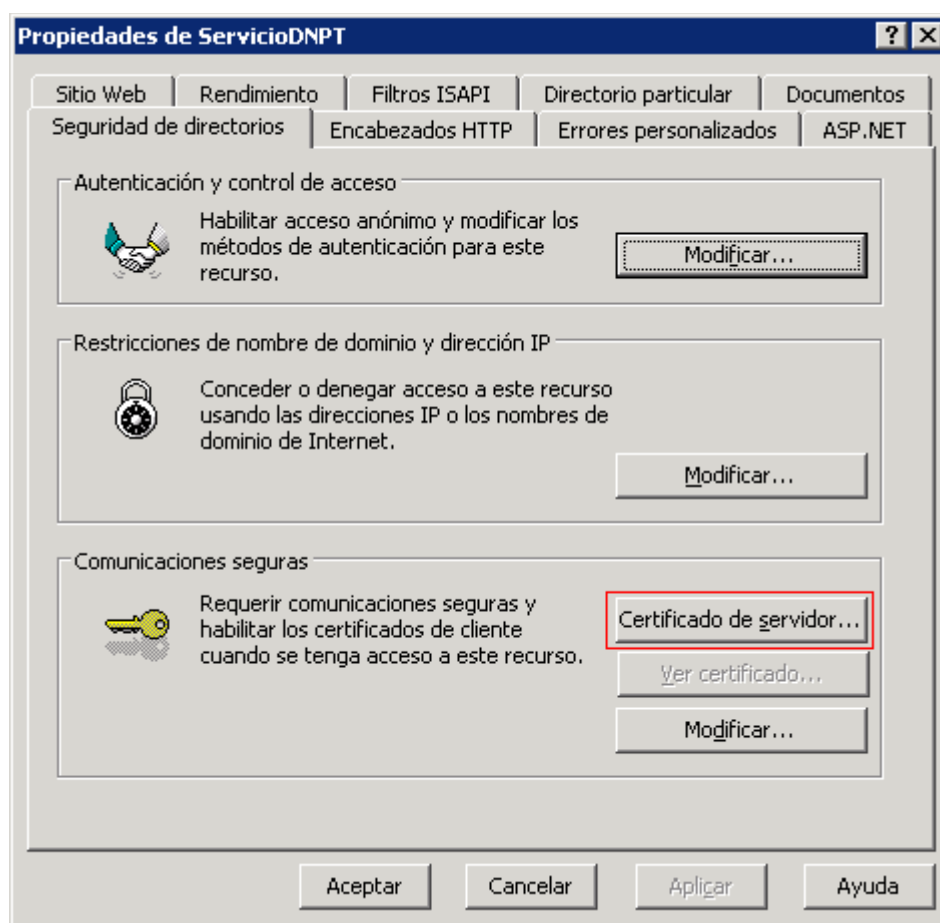


Figura 3: Pestaña "Seguridad de directorios"

4. Se mostrará un wizard para la solicitud, hacer click en "Siguiente". Luego seleccionar "Crear un certificado nuevo" y hacer nuevamente click en "Siguiente", ver Figura 4.

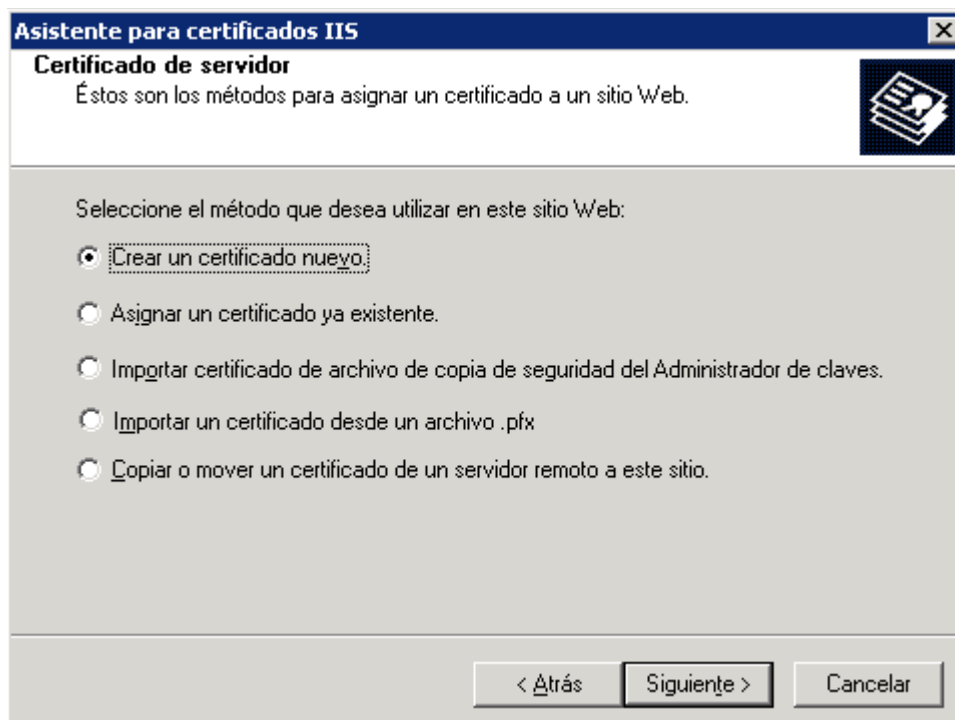


Figura 4: Crear un certificado nuevo

5. Seleccionar “Preparar la petición ahora pero enviarla más tarde”, y hacer click en “Siguiete”, ver Figura 5.

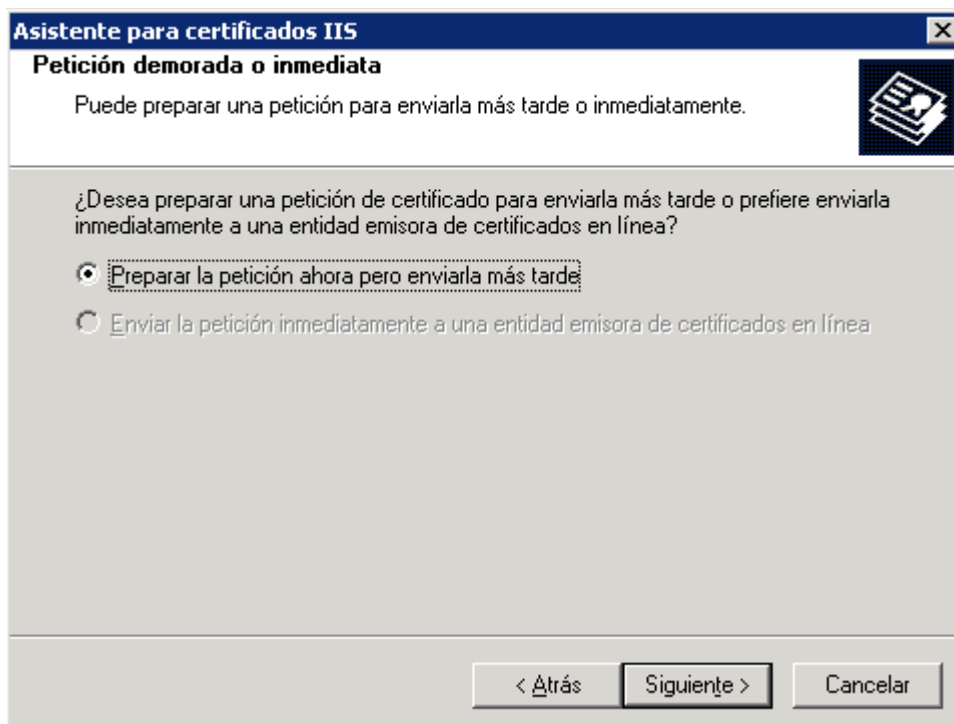
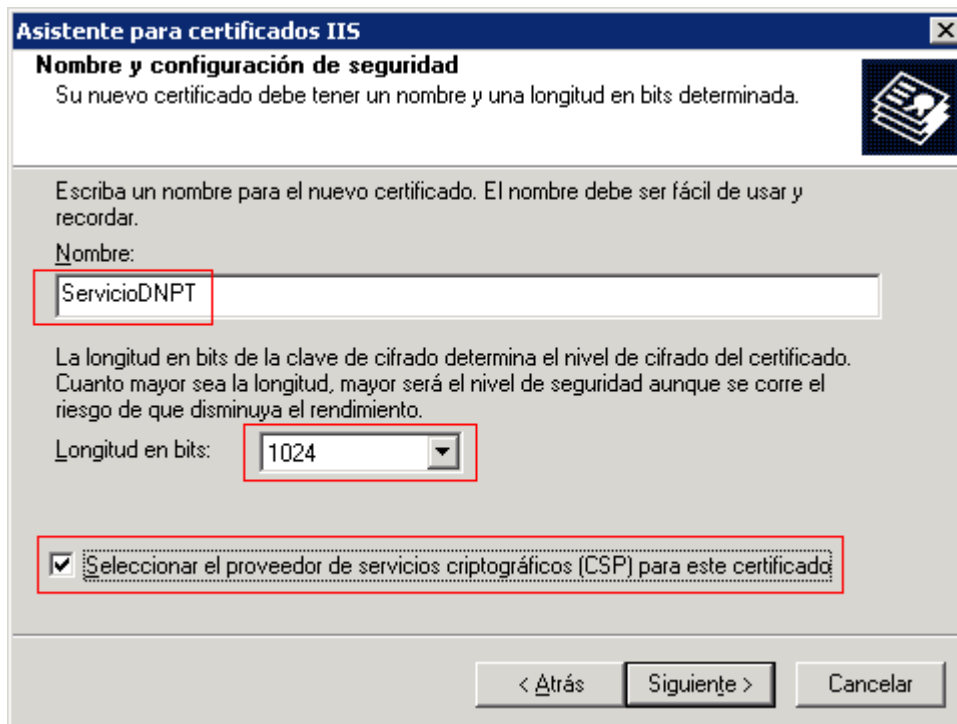


Figura 5: Petición demorada o inmediata

6. Ingresar el nombre del certificado (por defecto el nombre del servicio web, en este caso *ServicioDNPT*) y la longitud que tendrá la clave a crear. Tener en cuenta que el nombre a ingresar no es el CN y que la longitud debe ser 1024. Se debe seleccionar además la opción “Seleccionar el proveedor de servicios criptográficos (CSP) para este certificado” que permitirá elegir el algoritmo de encriptación (ver Figura 6).



Asistente para certificados IIS

Nombre y configuración de seguridad

Su nuevo certificado debe tener un nombre y una longitud en bits determinada.

Escriba un nombre para el nuevo certificado. El nombre debe ser fácil de usar y recordar.

Nombre:

La longitud en bits de la clave de cifrado determina el nivel de cifrado del certificado. Cuanto mayor sea la longitud, mayor será el nivel de seguridad aunque se corre el riesgo de que disminuya el rendimiento.

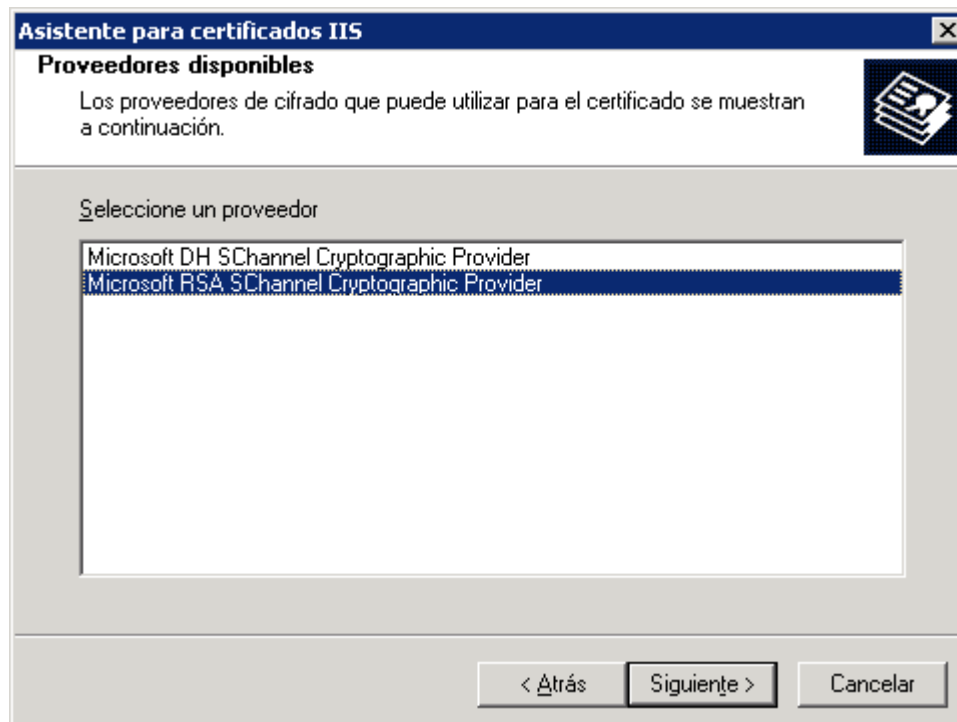
Longitud en bits:

☒ Seleccionar el proveedor de servicios criptográficos (CSP) para este certificado

< Atrás Siguiente > Cancelar

Figura 6: Nombre y configuración de seguridad

7. Seleccionar RSA como algoritmo criptográfico, ver Figura 7.



Asistente para certificados IIS

Proveedores disponibles

Los proveedores de cifrado que puede utilizar para el certificado se muestran a continuación.

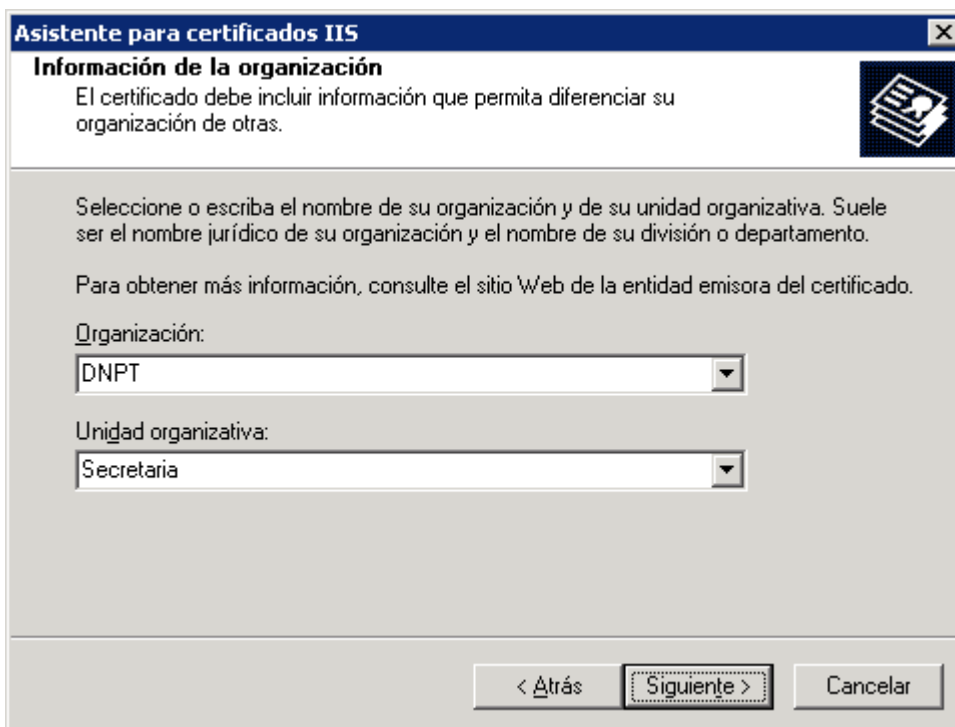
Seleccione un proveedor

- Microsoft DH SChannel Cryptographic Provider
- Microsoft RSA SChannel Cryptographic Provider**

< Atrás Siguiente > Cancelar

Figura 7: Proveedores de cifrado

8. Ingresar “Organización” y “Unidad Organizativa”. En el ejemplo, como organización se muestra “DNPT” y como Unidad Organizativa “Secretaría” (expresandolo en forma simplificada, O=DNPT, OU=Secretaria). Ver Figura 8.



Asistente para certificados IIS

Información de la organización

El certificado debe incluir información que permita diferenciar su organización de otras.

Seleccione o escriba el nombre de su organización y de su unidad organizativa. Suele ser el nombre jurídico de su organización y el nombre de su división o departamento.

Para obtener más información, consulte el sitio Web de la entidad emisora del certificado.

Organización:

DNPT

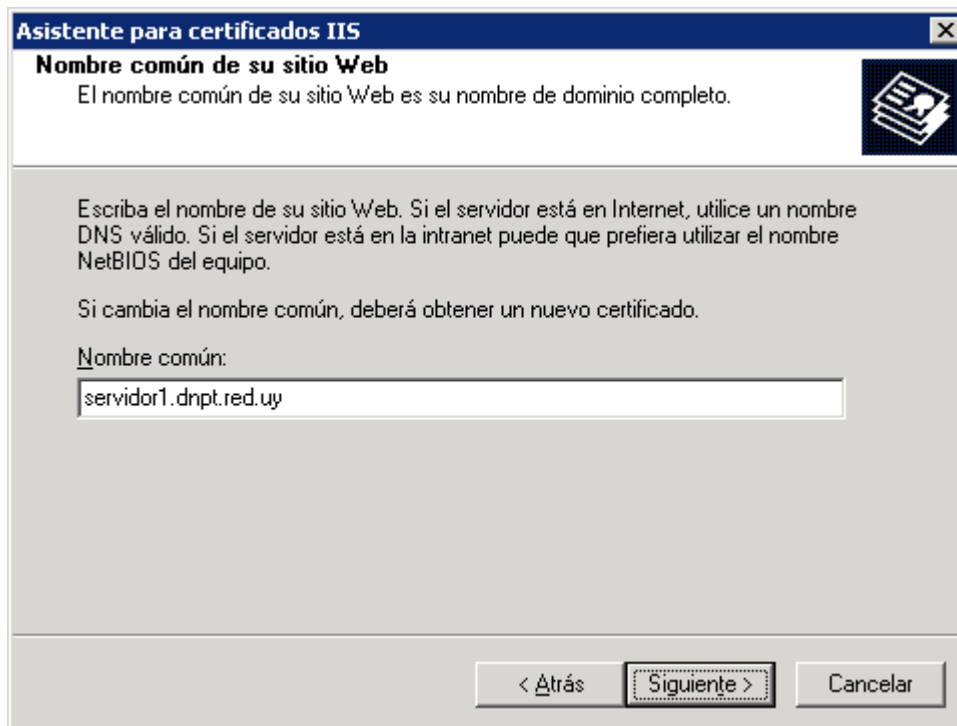
Unidad organizativa:

Secretaria

< Atrás Siguiente > Cancelar

Figura 8: Información de la organización

9. Ingresar el nombre lógico del servidor en el campo “Nombre común”. El formato a seguir debe ser *nombreServidor.nombreOrganismo.red.uy*. En el ejemplo, nombreServidor = servidor1, nombreOrganismo = dnpt, CN = servidor1.dnpt.red.uy. Ver Figura 9.



Asistente para certificados IIS

Nombre común de su sitio Web

El nombre común de su sitio Web es su nombre de dominio completo.

Escriba el nombre de su sitio Web. Si el servidor está en Internet, utilice un nombre DNS válido. Si el servidor está en la intranet puede que prefiera utilizar el nombre NetBIOS del equipo.

Si cambia el nombre común, deberá obtener un nuevo certificado.

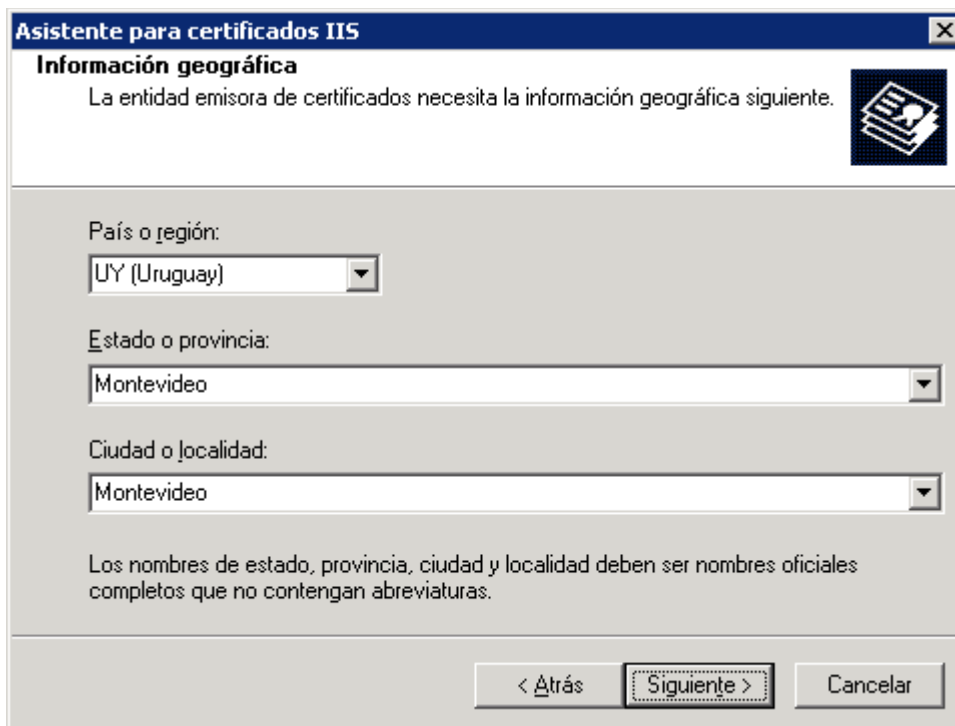
Nombre común:

servidor1.dnpt.red.uy

< Atrás Siguiente > Cancelar

Figura 9: Ingreso del Common Name (CN)

10. Ingresar país, departamento (estado o provincia) y ciudad (o localidad), ver Figura 10.



Asistente para certificados IIS

Información geográfica

La entidad emisora de certificados necesita la información geográfica siguiente.

País o región:
UY (Uruguay)

Estado o provincia:
Montevideo

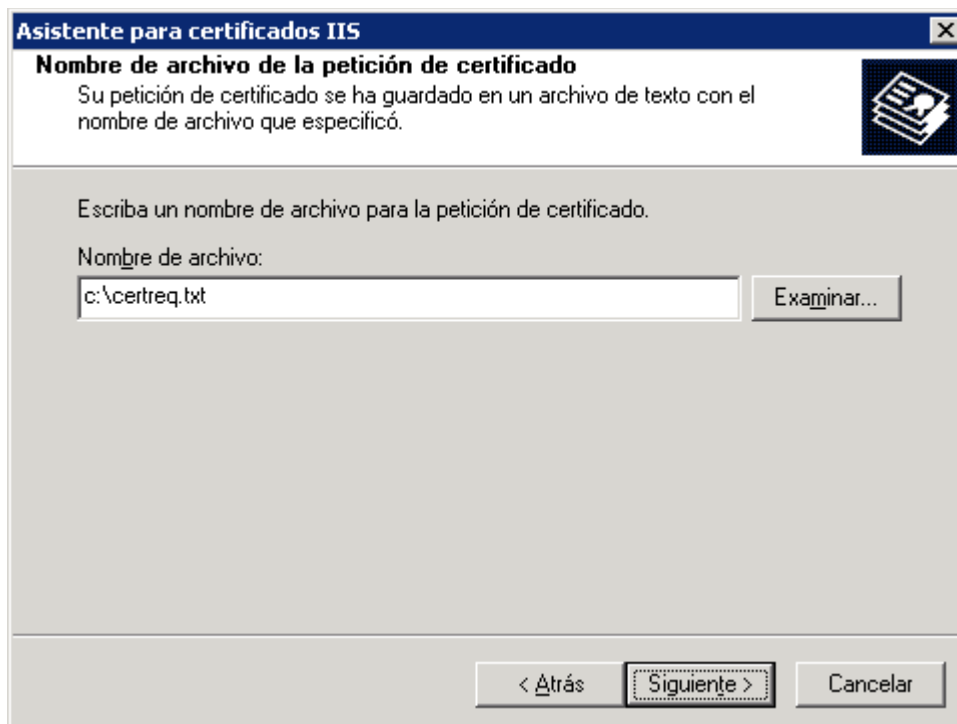
Ciudad o localidad:
Montevideo

Los nombres de estado, provincia, ciudad y localidad deben ser nombres oficiales completos que no contengan abreviaturas.

< Atrás **Siguiente >** Cancelar

Figura 10: Información geográfica

11. Seleccionar el archivo donde se almacenará el archivo CSR (Certificate Signed Request) y hacer click en “Siguiente”, ver Figura 11.



Asistente para certificados IIS

Nombre de archivo de la petición de certificado
Su petición de certificado se ha guardado en un archivo de texto con el nombre de archivo que especificó.

Escriba un nombre de archivo para la petición de certificado.

Nombre de archivo:
c:\certreq.txt

Examinar...

< Atrás Siguiente > Cancelar

Figura 11: Nombre de archivo CSR

12. En este paso se muestra un resumen de todos los datos ingresados anteriormente, si todo está correcto hacer click en “Siguiente” y luego “Finalizar” (Figura 12).

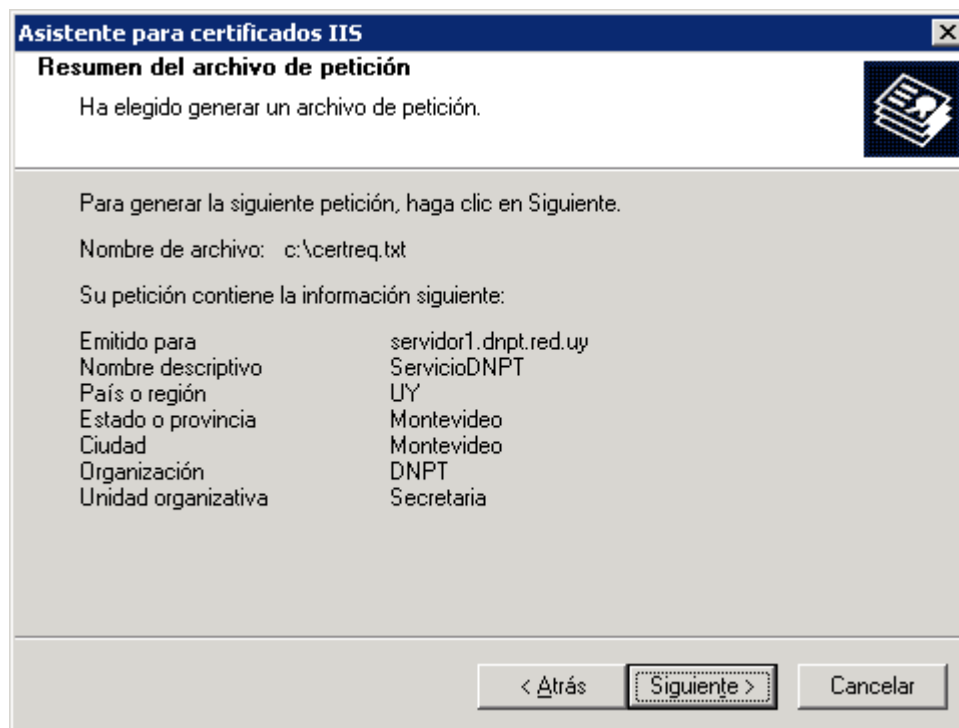


Figura 12: Resumen del archivo de petición (CSR)

Lo que se ha realizado hasta este punto fue crear la solicitud de firma de certificado. Para comprobar la correcta ejecución de todos los pasos se puede realizar lo siguiente:

1. “Inicio” → “Ejecutar” y luego introducir el comando *mmc* como se muestra en la Figura .

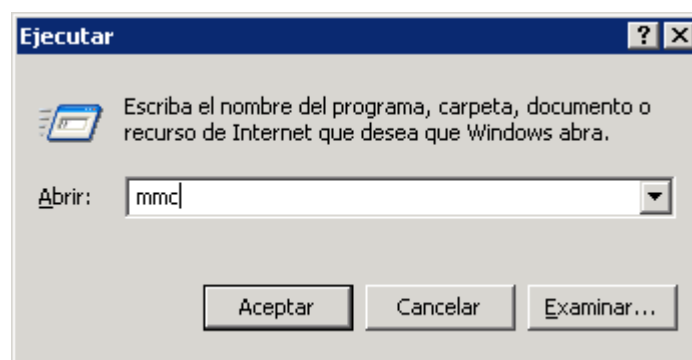


Figura 13: Abrir Microsoft Management Console

2. En la aplicación Certificate Manager seleccionar “Archivo” → “Agregar o quitar complemento”. Se debe obtener un resultado similar al de la Figura 14.

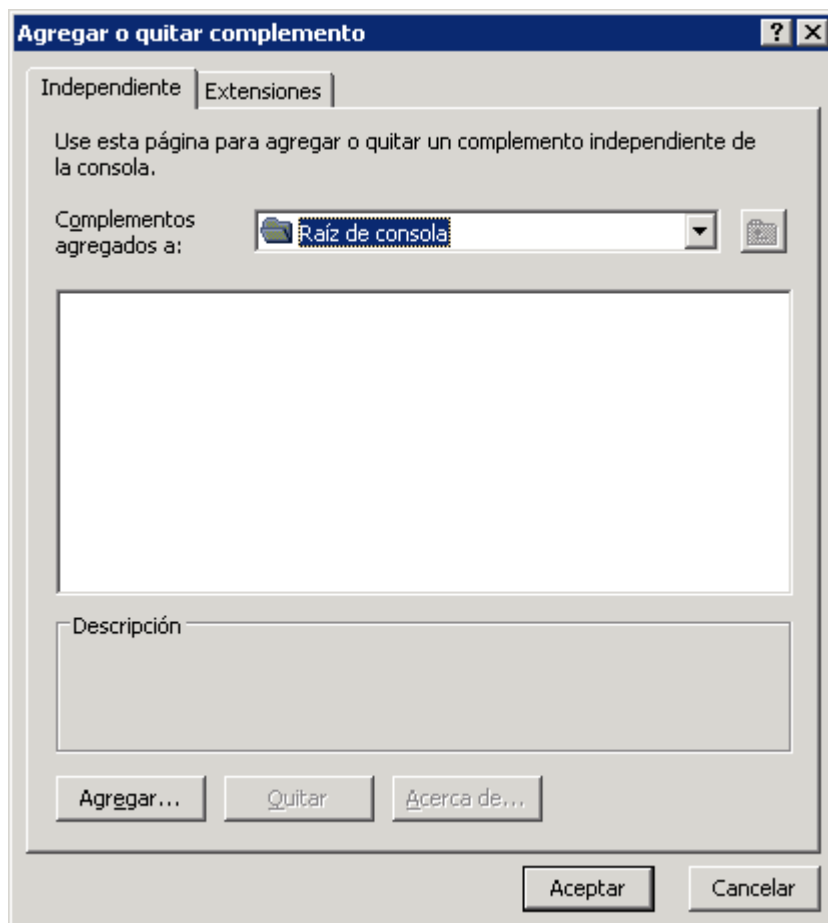
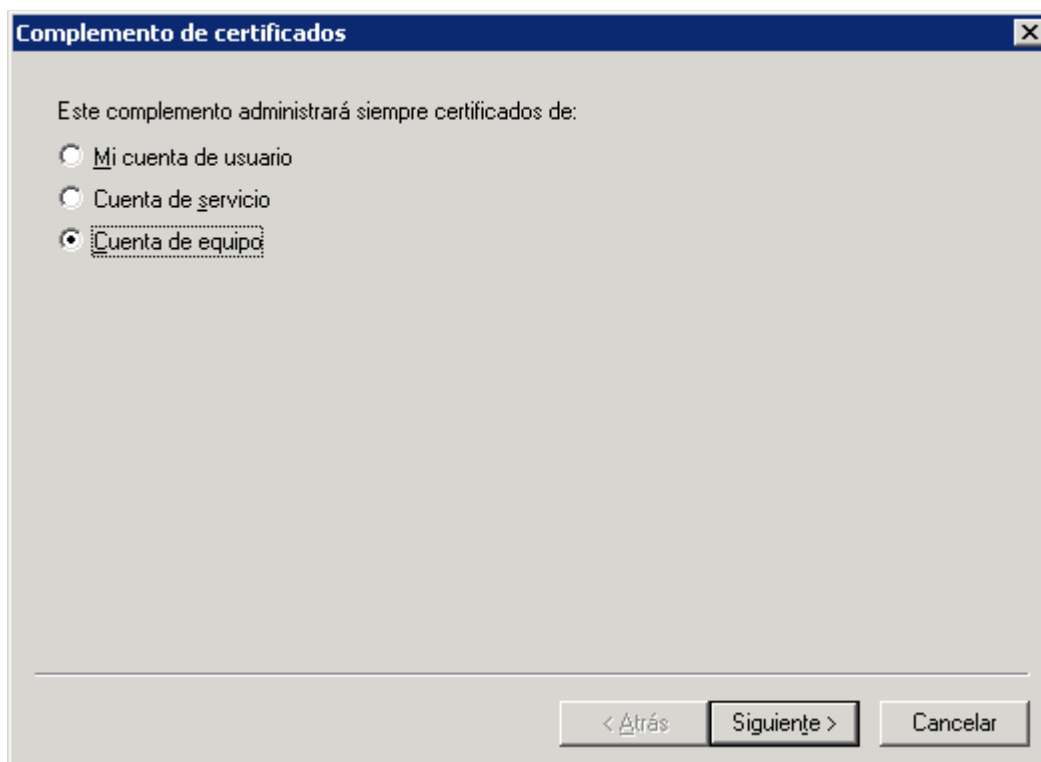


Figura 14: Agregar o quitar complemento

3. Hacer clic en el botón “Agregar” → “Certificados” → “Agregar”. Se debe obtener un resultado similar al de la Figura 15.



Complemento de certificados

Este complemento administrará siempre certificados de:

☐ Mi cuenta de usuario

☐ Cuenta de servicio

☒ Cuenta de equipo

< Atrás Siguiente > Cancelar

Figura 15: Selección de tipo de complemento de certificados

4. Seleccionar la opción “Cuenta de equipo” → “Siguiente” y luego “Finalizar”.
5. Seleccionar el botón Cerrar y obtener un resultado similar al de la Figura 16. Luego, seleccionar el botón “Aceptar” para cerrar la ventana.

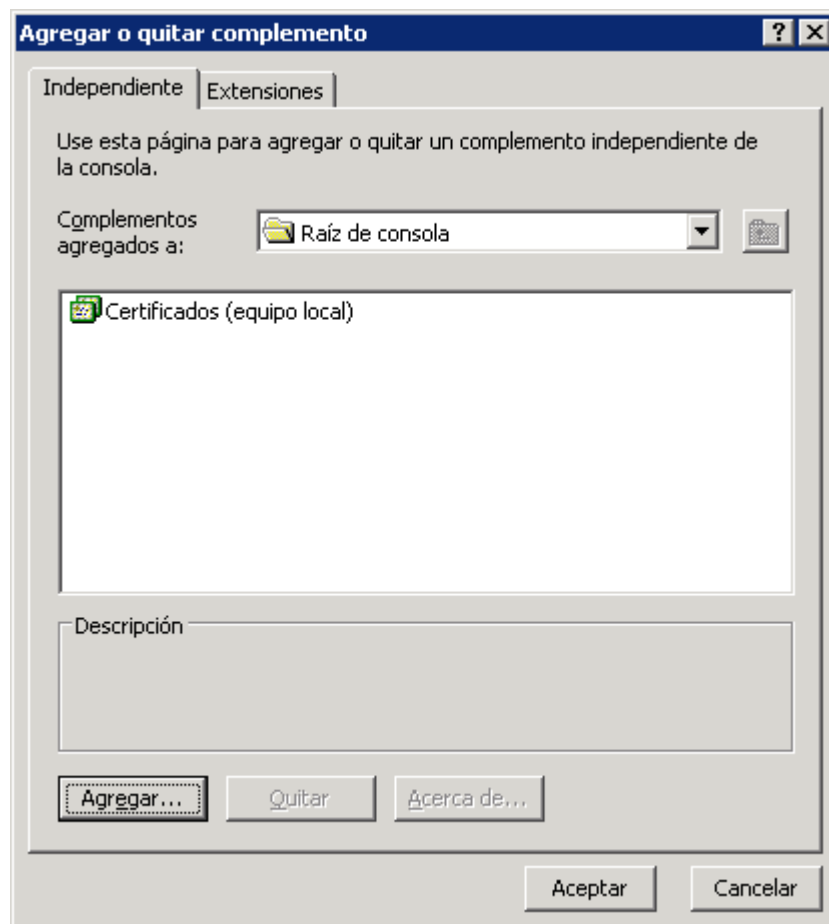


Figura 16: Agregar o quitar complementos

6. Seleccionar “Certificados (equipo local)” → “Solicitud de inscripción de certificado” → “Certificados”. La ventana que se presenta debe ser similar a la Figura 17, donde se puede ver el certificado solicitado.

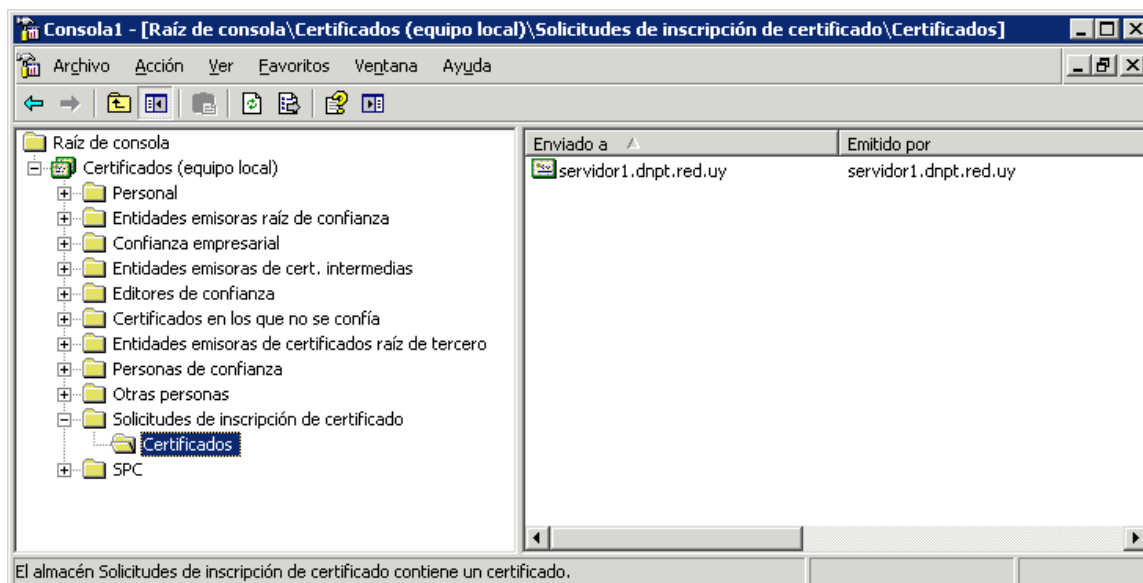


Figura 17: Muestra de solicitud de certificado

4.2. Paso 2: Solicitud de Firma de Certificado e Importación

El segundo paso es solicitar la emisión de un certificado .X509 (con los datos del CSR) firmado por la autoridad certificadora de la Plataforma que garantice que la información es válida y confiable.

Para la solicitud, tomar el archivo CSR creado en el paso 1 y enviar un correo a soporte@agesic.gub.uy, con asunto “*Solicitud de PKCS12 – Nombre Organismo – Ambiente xxxxxx*”, solicitando el certificado .X509 firmado por la CA (PKCS12). No olvidar que es importante aclarar si el certificado solicitado es para el ambiente de producción o el ambiente de testing (substituir xxxxxx en el asunto del mail, por “testing” o “producción”).

Luego de obtenido el certificado enviado por el área de soporte de AGESIC, realizar los siguientes pasos:

1. Ir a “Inicio” → “Todos los programas” → “Herramientas administrativas” → “Administrador de Internet Information Services (IIS)”

2. Seleccionar el servicio web para el cual se solicitó el certificado (ej: ServicioOrganismo), click derecho “Propiedades”, Figura 6.
3. Se desplegará un mensaje de bienvenida al wizard. Hacer click en “Siguiente” y seleccionar la opción “Procesar la petición pendiente e instalar el certificado”, y hacer nuevamente click en “Siguiente” (ver Figura 18)

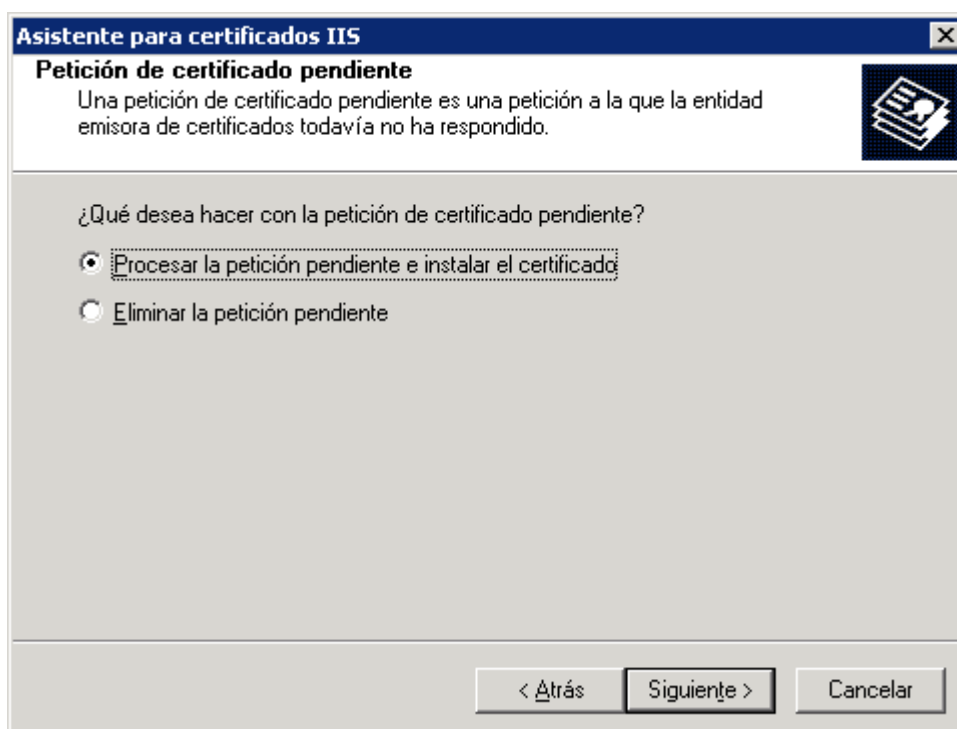


Figura 18: Asistente de importación de certificados

4. Seleccionar la ubicación del archivo correspondiente al certificado enviado por soporte de AGESIC (ej. servidor1.dnpt.red.uy.cer, ver Figura 19) y luego presionar “Siguiente”.

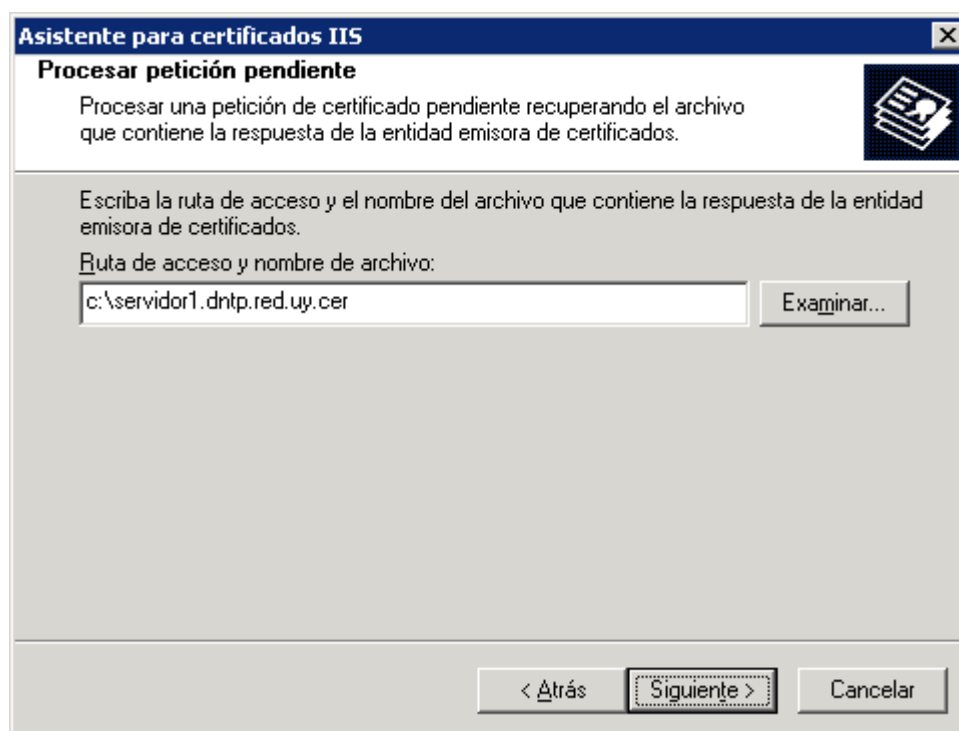
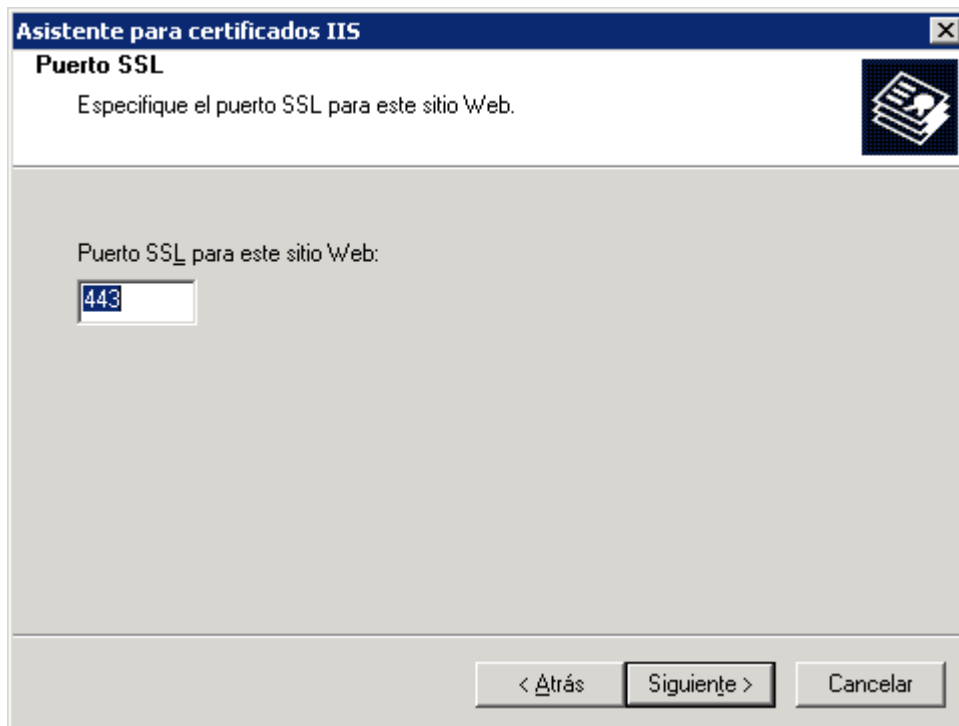


Figura 19: Seleccionar ubicación de certificado

5. Asignar un puerto para la conexión SSL con el servicio (443 es el puerto por defecto, Figura 20).



Asistente para certificados IIS

Puerto SSL

Especifique el puerto SSL para este sitio Web.

Puerto SSL para este sitio Web:

443

< Atrás Siguiete > Cancelar

Figura 20: Puerto SSL

6. Leer el resumen para confirmar que todo esté correcto y hacer click en “Siguiete” (Figura 21). Se mostrará una página de confirmación, luego hacer click en “Siguiete” y luego “Finalizar” y se cerrará el asistente.

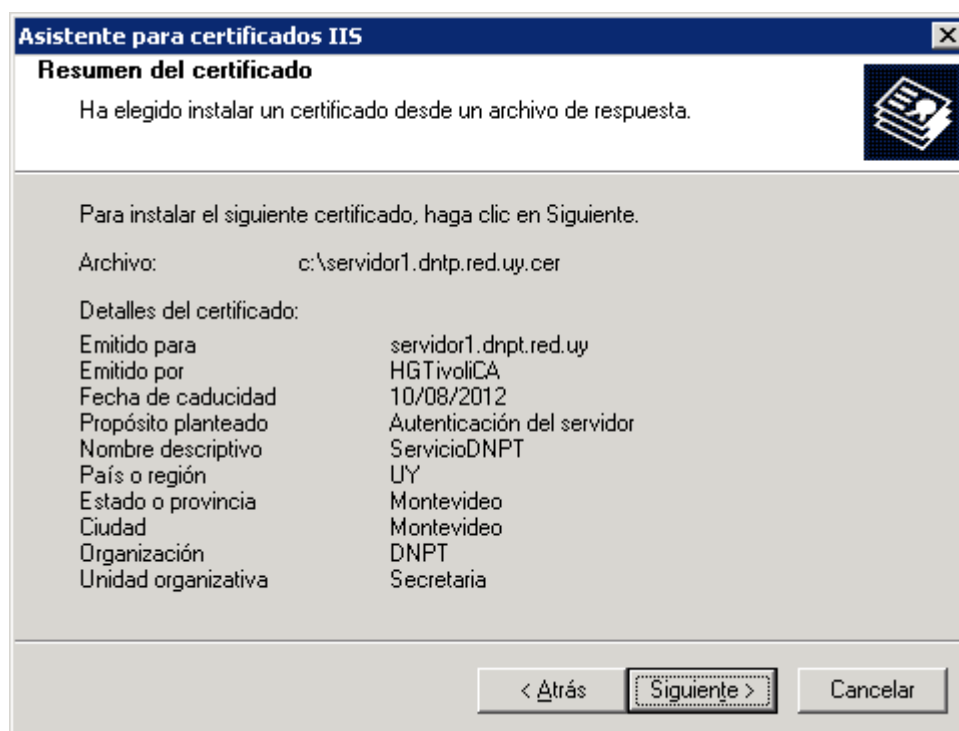


Figura 21: Resumen del certificado

7. Para verificar que la importación haya sido exitosa realizar lo siguiente. En la ventana de la Figura 17, donde antes se listaba la solicitud de certificado (servidor1.dnpt.red.uy), realizar click derecho (en el sector blanco donde se muestran los certificados) y hacer click en “actualizar”. Se observará que el certificado solicitado ha sido eliminado de la de este listado.
8. Finalmente observar lo siguiente: En la ventana del almacén de certificados de windows (misma ventana que en el paso anterior) ir a “Certificados (equipo local)” → “Personal” → “Certificados” y actualizando el listado se puede ver el certificado recientemente importado (servidor1.dnpt.red.uy). Ver Figura 22.

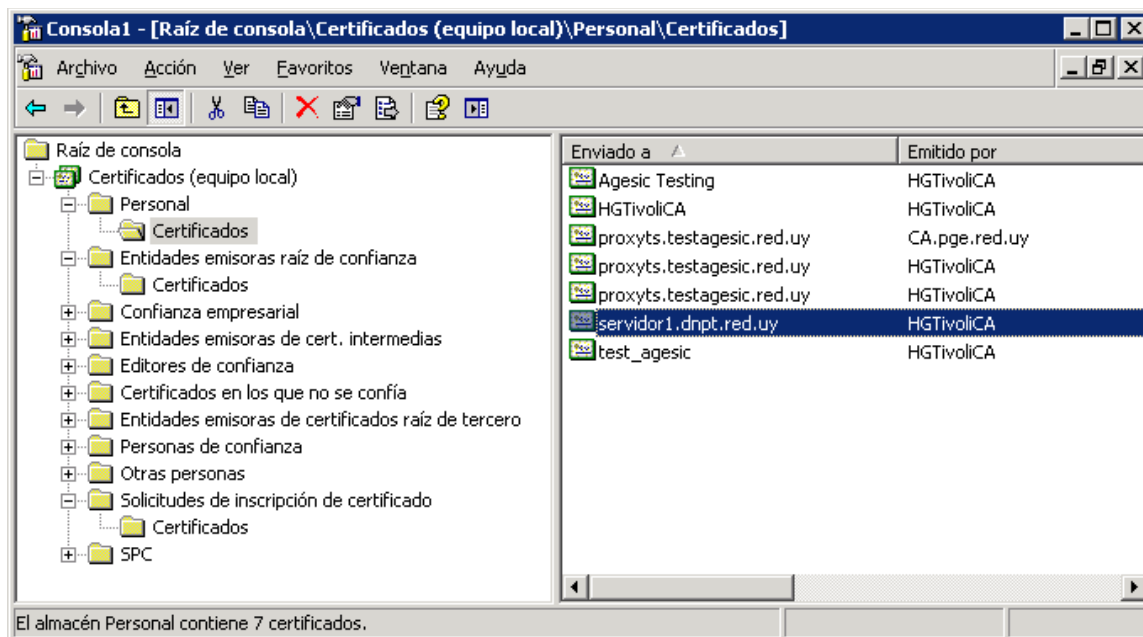


Figura 22: Certificados personales

- En la ventana de la Figura 22, hacer doble click en el certificado importado. En el ejemplo, en “servidor1.dnpt.red.uy” y se presentará una ventana similar a la de la Figura 23.

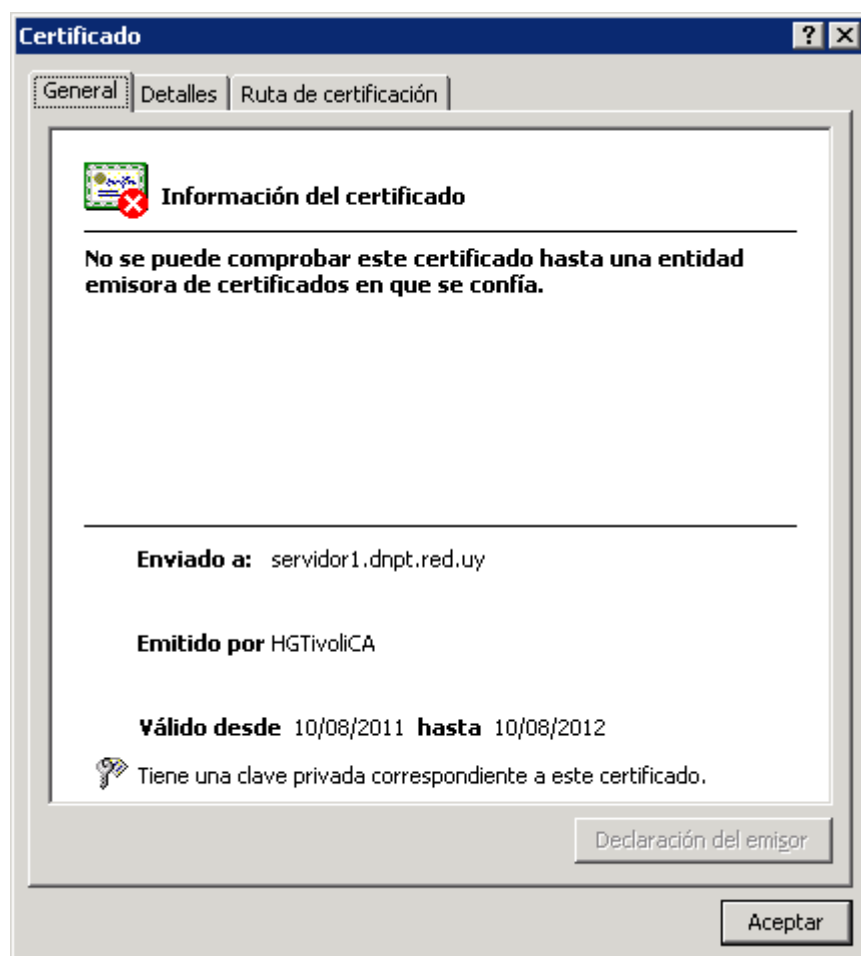


Figura 23: Propiedades de certificado

Notar que en la Figura 23 se presenta un mensaje informando no se puede comprobar la información del certificado, por lo tanto que no aún no se confía en el mismo. Esto significa que falta el último paso que se explicará en la siguiente sección.

4.3. Paso 3: Importar certificado de la CA

1. Desde la ventana de la Figura 17, seleccionar “Certificados (equipo local)” → “Entidades emisoras de raíz de confianza” → “Certificados” y luego click derecho y seleccionar “Todas las tareas” → “Importar...”, como se muestra en la Figura 24.

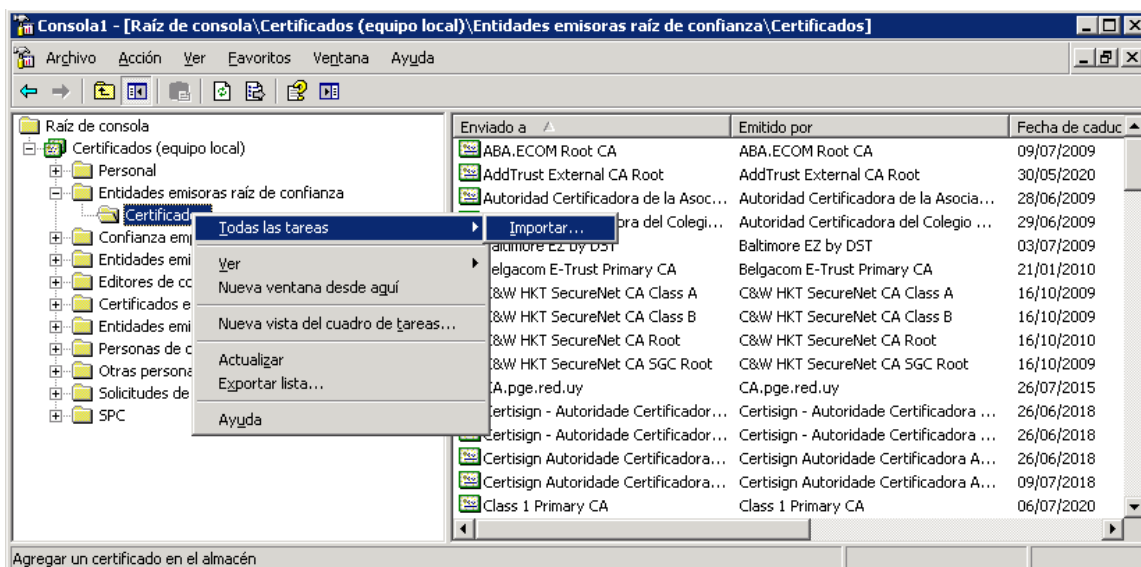


Figura 24: Importar certificado de la CA

2. En el *asistente de importación* seleccionar el botón siguiente y luego indicar la ubicación del archivo (archivo *.cer, certificado de la CA). Luego, presionar el botón “Siguiente” → “Siguiente” → “Finalizar”. Al finalizar se debe presentar el siguiente mensaje: “El certificado se importó correctamente.”
3. Para verificar la importación correcta del certificado de la CA, volver a la ventana de la Figura 23 y notar que ahora es como la de la Figura 25. Ahora la ventana despliega un mensaje identificando los propósitos del certificado.

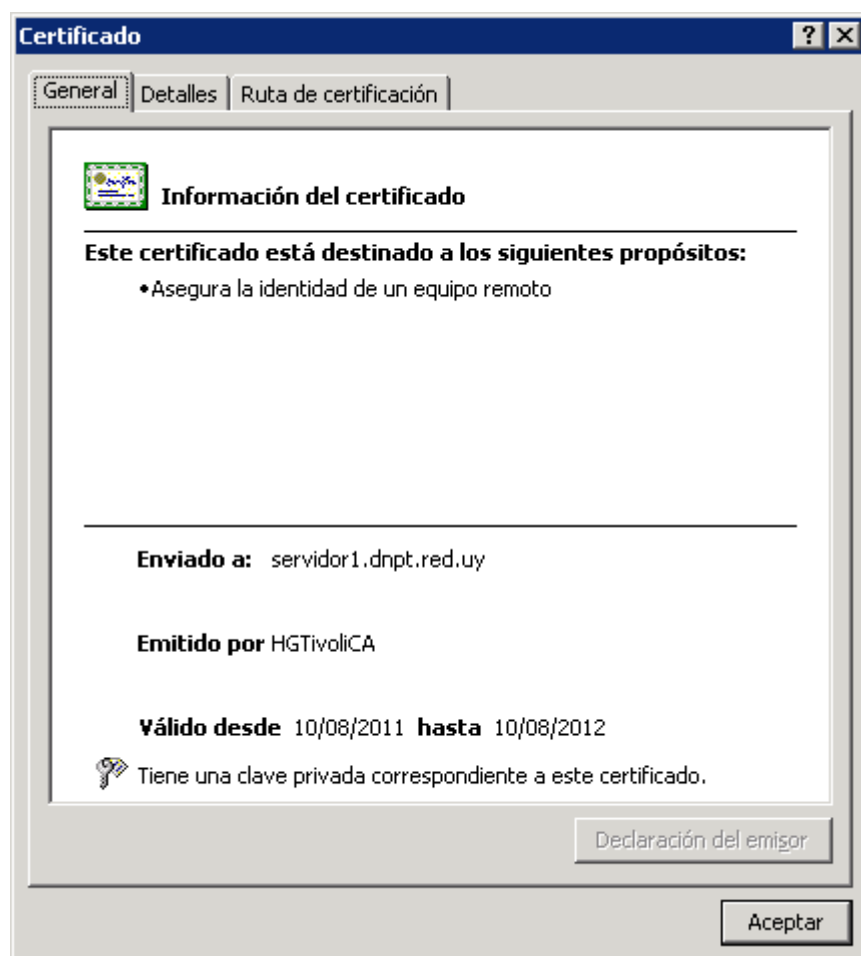


Figura 25: Propiedades de certificado confiable

5. Renovación de certificado SSL

En esta sección se describen los pasos para renovar un certificado SSL en un ISS. En caso de querer emitir un certificado por primera vez, ver sección

5.1.Paso 1: Solicitud de renovación de certificado

Para obtener la solicitud de renovación se deben realizar los siguientes pasos:

1. Ir a “Inicio” → “Todos los programas” → “Herramientas administrativas” → “Administrador de Internet Information Services (IIS)”
2. Seleccionar el servicio web para que se quiere el certificado (ej: ServicioDNPT), click derecho “Propiedades”, Figura 26.

3. Ir a la pestaña “Seguridad de directorios” (Figura 27) y luego click en “Certificado de servidor” (Figura 28).

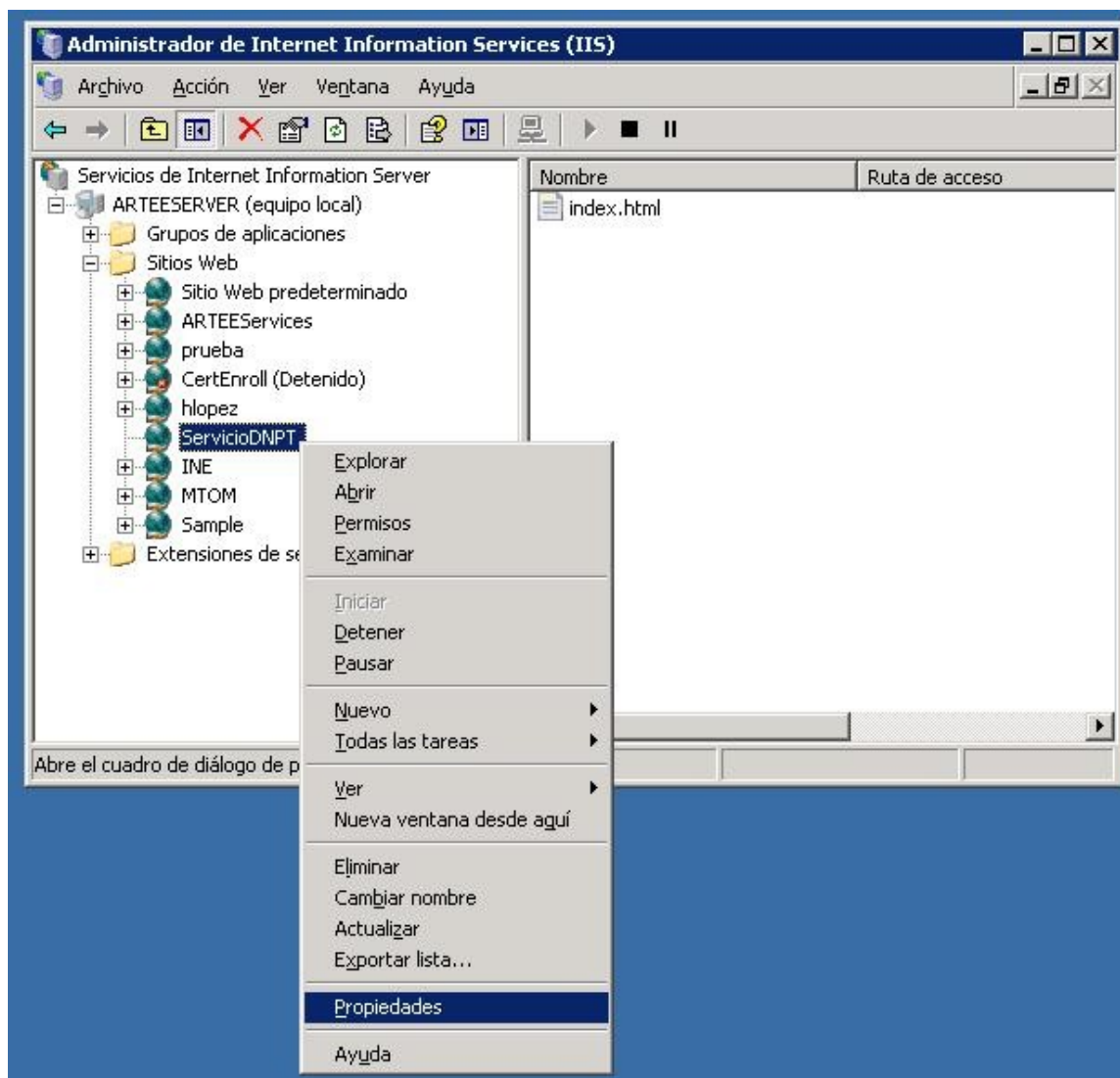


Figura 26: Menú contextual de sitio web IIS

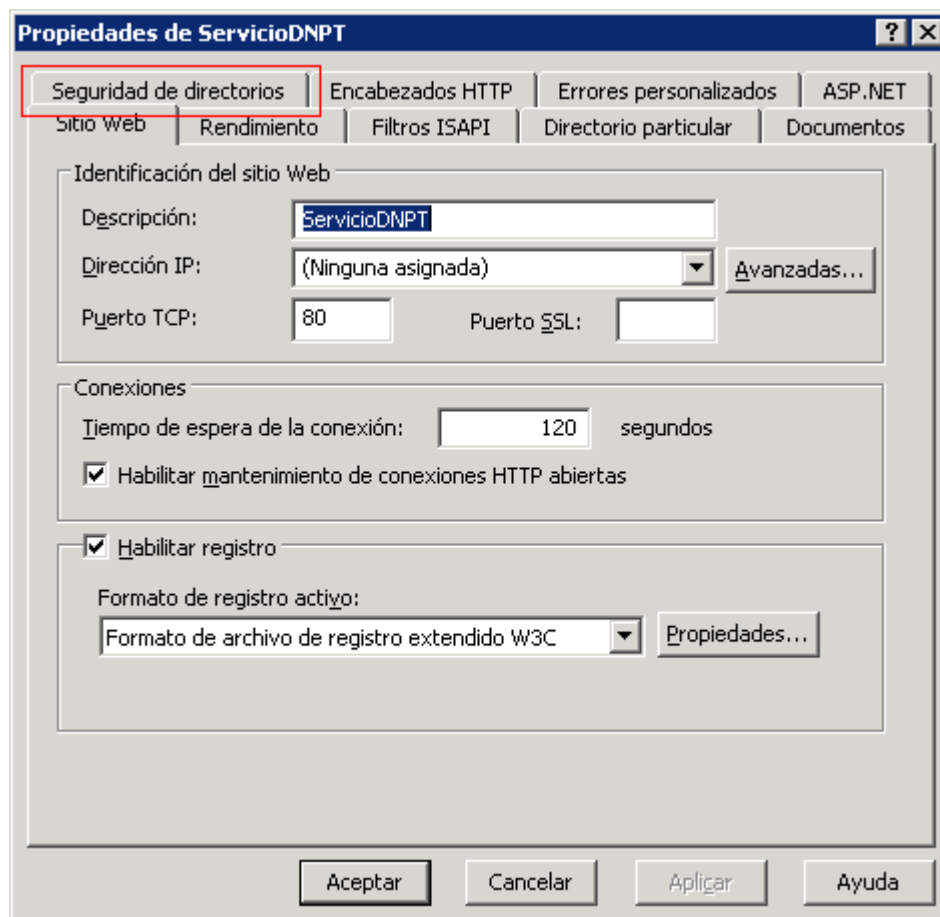


Figura 27: Ventana de propiedades - Pestaña Seguridad

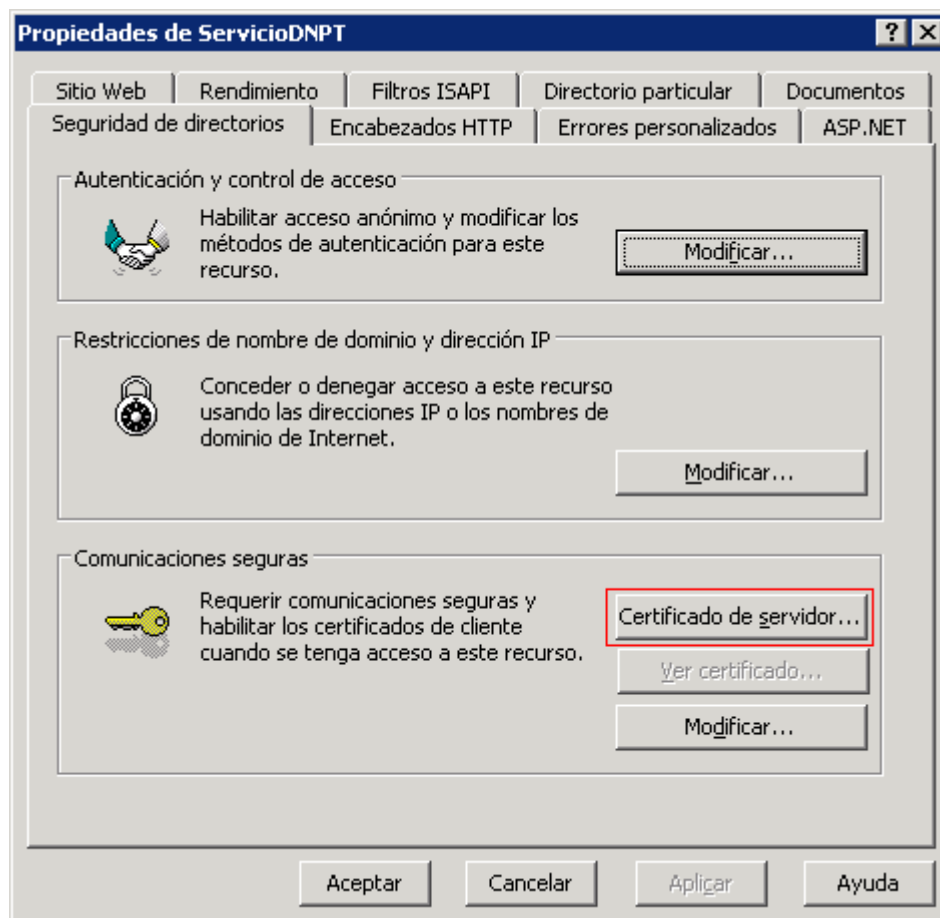


Figura 28: Pestaña "Seguridad de directorios"

4. Se mostrará un wizard para la solicitud, hacer click en "Siguiente". Luego seleccionar "Renovar el certificado actual" y hacer nuevamente click en "Siguiente", ver Figura 29.

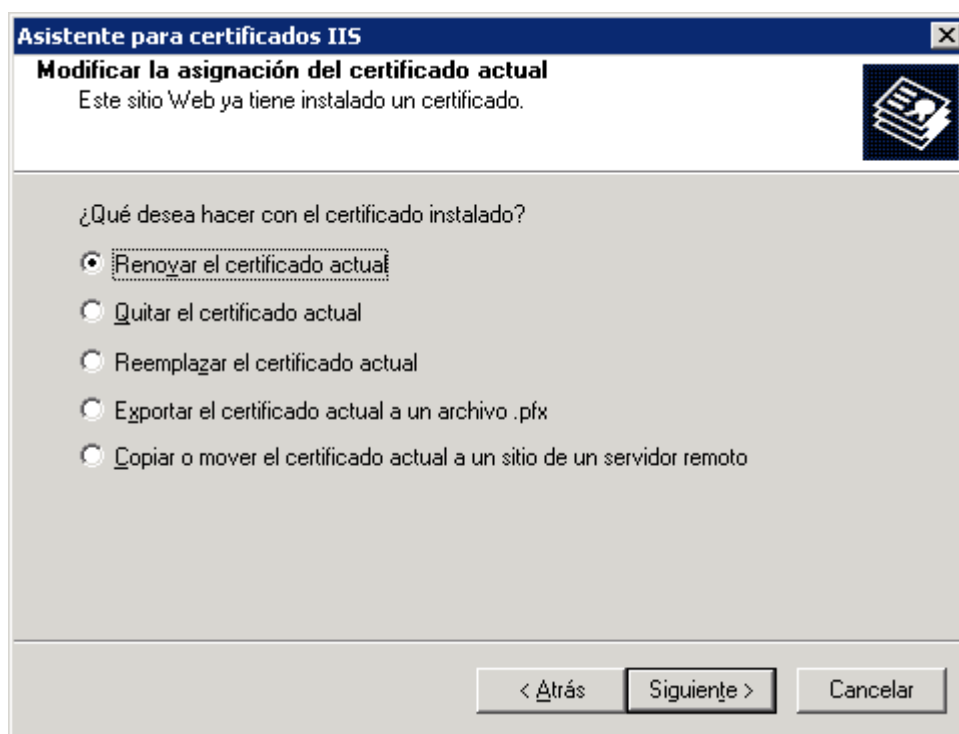
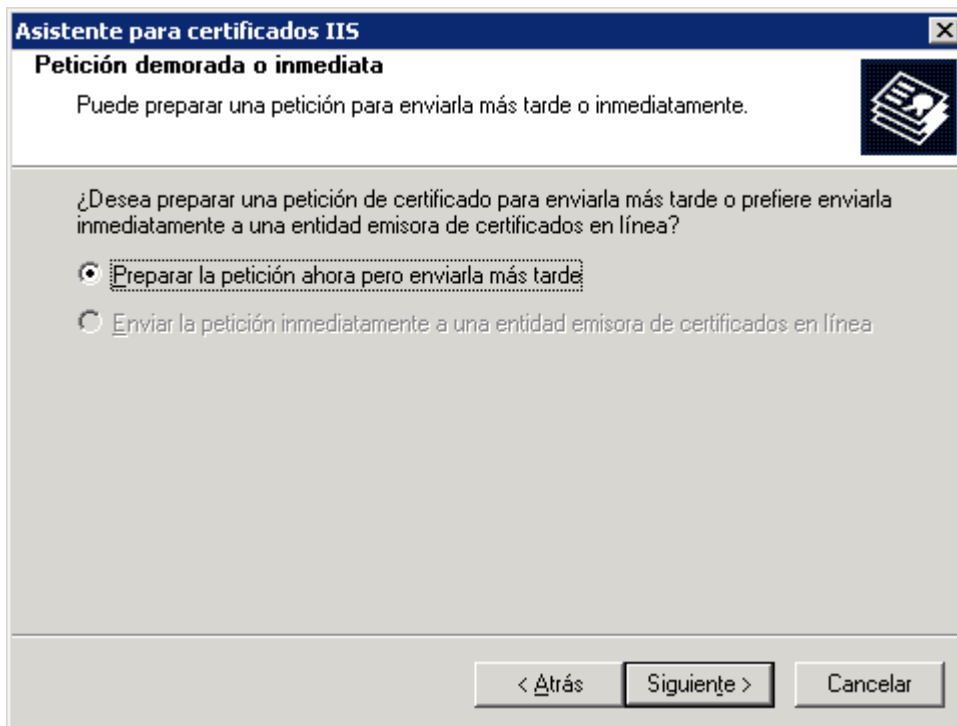


Figura 29: Renovar certificado

5. Seleccionar “Preparar la petición ahora pero enviarla más tarde” y hacer click en “Siguiente”, ver Figura 30.
6. Seleccionar el archivo donde se almacenará el archivo CSR (Certificate Signed Request) y hacer click en “Siguiente”, ver Figura 31.

Nota: Se recomienda que este archivo tenga terminación .csr.



Asistente para certificados IIS

Petición demorada o inmediata

Puede preparar una petición para enviarla más tarde o inmediatamente.

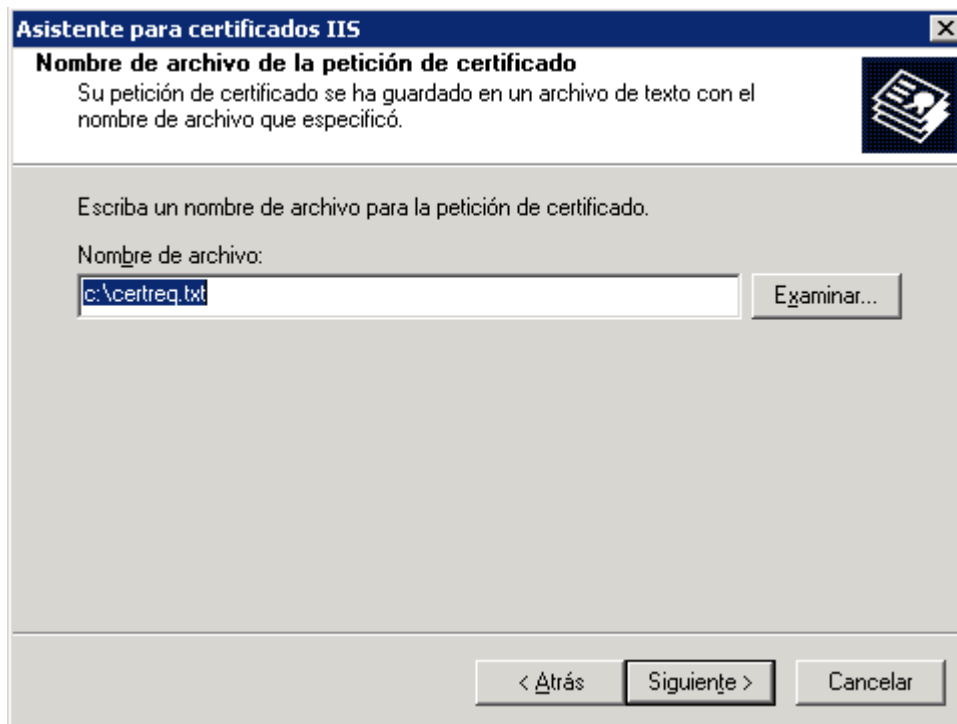
¿Desea preparar una petición de certificado para enviarla más tarde o prefiere enviarla inmediatamente a una entidad emisora de certificados en línea?

☒ Preparar la petición ahora pero enviarla más tarde

☐ Enviar la petición inmediatamente a una entidad emisora de certificados en línea

< Atrás Siguiente > Cancelar

Figura 30: Seleccionar petición demorada



Asistente para certificados IIS

Nombre de archivo de la petición de certificado

Su petición de certificado se ha guardado en un archivo de texto con el nombre de archivo que especificó.

Escriba un nombre de archivo para la petición de certificado.

Nombre de archivo:

c:\certreq.txt Examinar...

< Atrás Siguiente > Cancelar

Figura 31: Nombre de archivo CSR

10. Leer el resumen para confirmar que todo esté correcto y hacer click en “Siguiente” (Figura 32). Se mostrará una página de confirmación, luego hacer click en “Siguiente” y luego “Finalizar” y se cerrará el asistente.

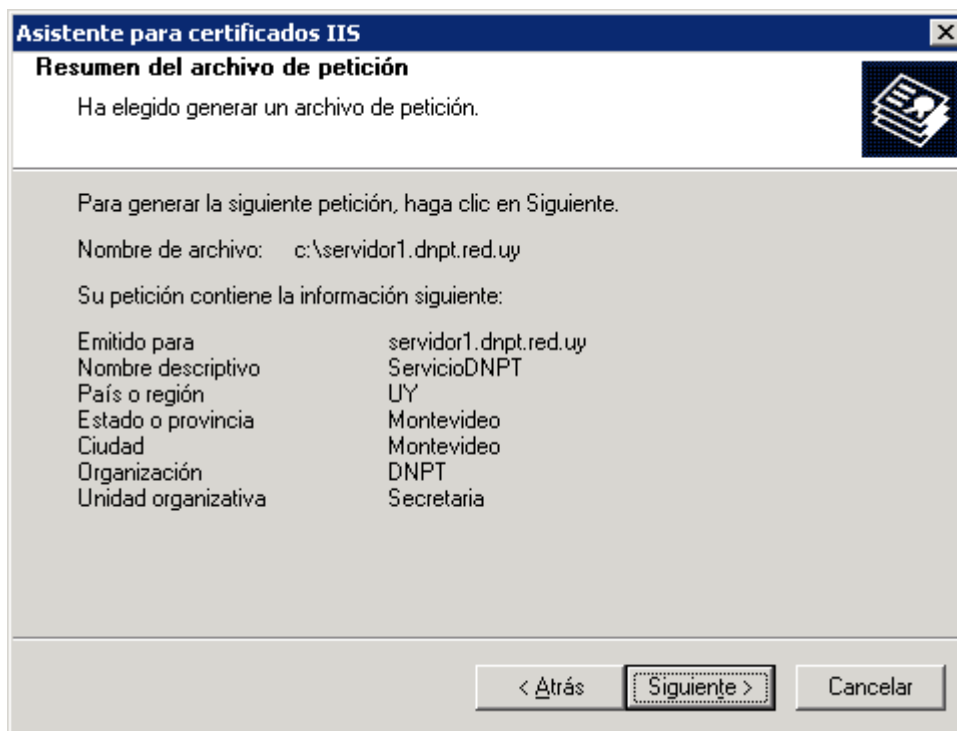


Figura 32: Nombre de archivo CSR

11. Para verificar que la generación del CSR fue exitosa se deberá verificar existe tal petición dentro del almacén de “Solicitudes de inscripción de certificados”. Ver figura 33.

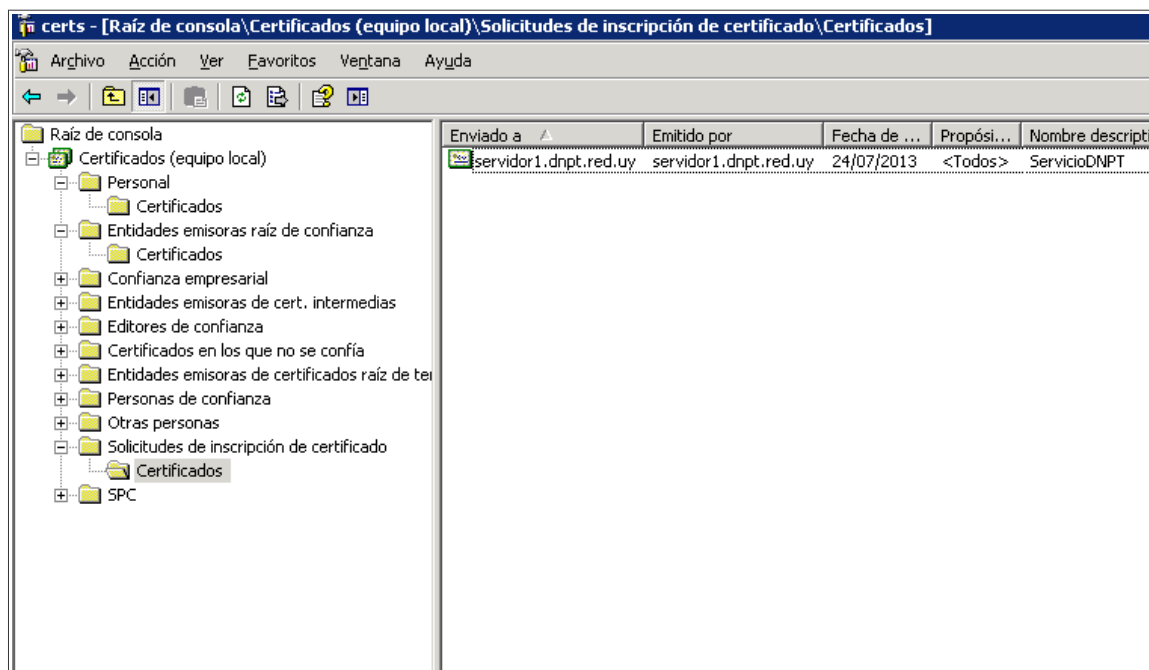


Figura 33: Ver solicitudes de inscripción de certificados pendientes

5.2. Paso 2: Solicitud de firma a la CA

El siguiente paso es solicitar la emisión de un certificado .X509 (con los datos del CSR) firmado por la autoridad certificadora de la Plataforma que garantice que la información es válida y confiable.

1. enviar un correo a soporte@agesic.gub.uy, con asunto “*Solicitud de PKCS12 – Nombre Organismo – Ambiente xxxxxx*”, solicitando el certificado .X509 firmado por la CA (PKCS12).

Importante: No olvidar indicar si el certificado solicitado es para ambiente de testing o producción (substituir xxxxxx en el asunto del mail, por “testing” o “producción”).

5.3. Paso 3: Importar certificado solicitado

Por último, se deberá importar el certificado enviado por Agesic. Este proceso involucra los siguientes pasos:

1. Dentro del IIS, seleccionar el sitio Web e ir a Seguridad de Directorios.
Por detalles para ejecutar este paso, ver sección 4.1.
2. Seleccionar “Certificado de servidor”. Se mostrará un wizard para la solicitud, hacer click en “Siguiente”.
3. Seleccionar la opción “Procesar la petición pendiente e instalar el certificado” y hacer click en “Siguiente”, como se muestra en la figura 34.

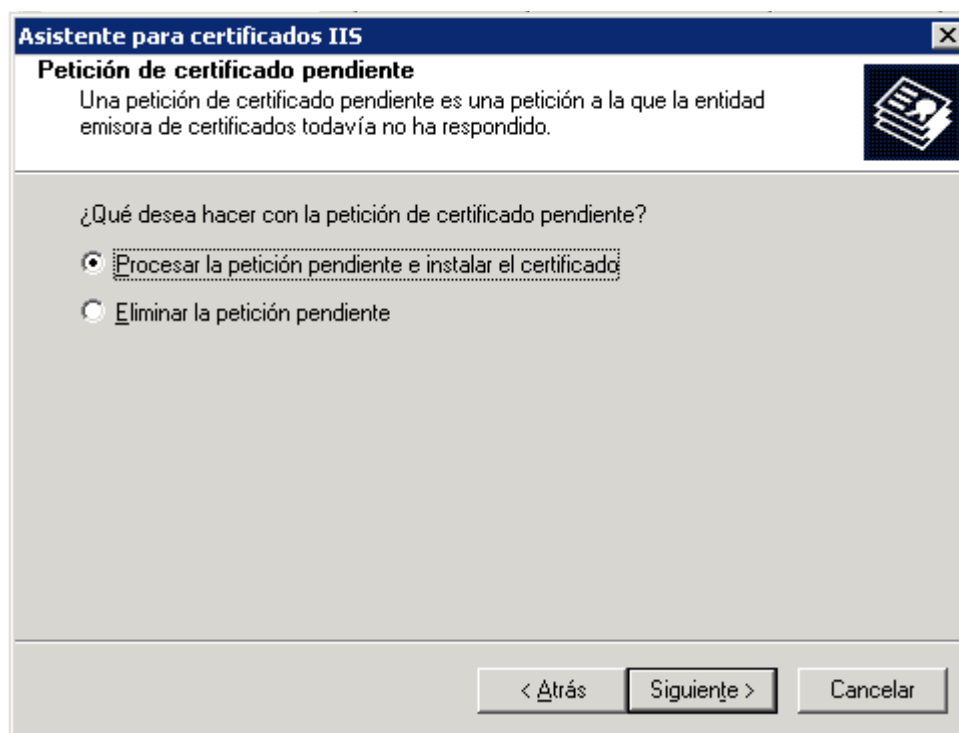


Figura 34: Procesar petición pendiente e instalar certificado

4. Seleccionar la ubicación del archivo correspondiente al certificado y luego presionar “Siguiente”, como se muestra en la figura 35.
5. Seleccionar el puerto SSL (443 es el puerto por defecto, figura 35).
6. Confirmar la información del certificado a importar y hacer click en “Siguiente” y luego en “Finalizar”. Ver figura 36

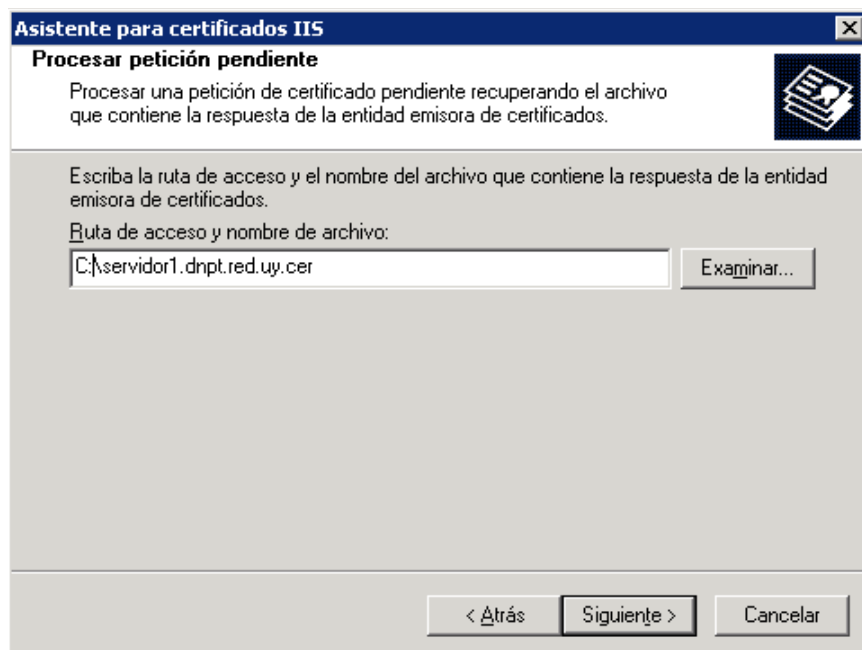


Figura 35: Seleccionar ubicación del certificado

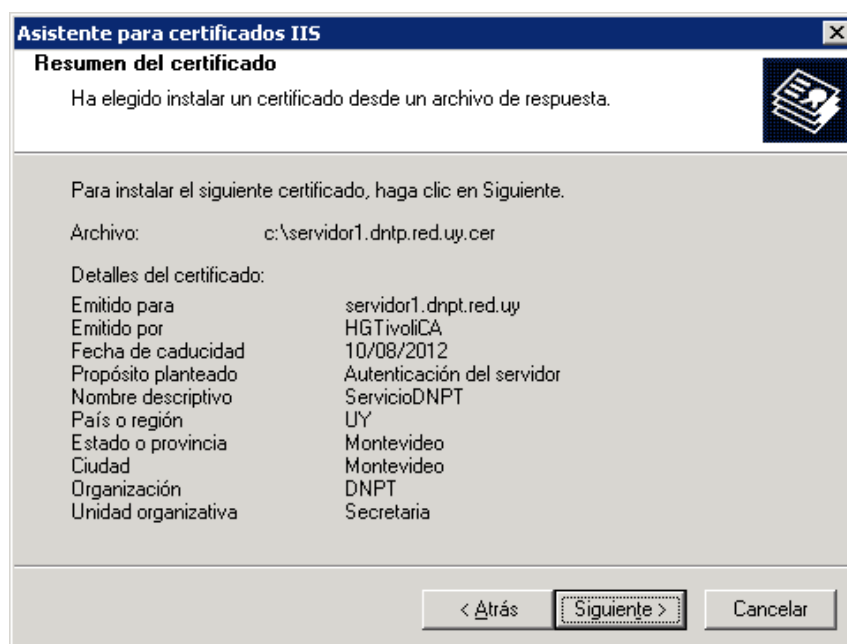


Figura 36: Resumen del certificado

7. Para verificar la importación se debe realizar lo siguiente:

- verificar no hay solicitudes pendientes: entrar en el almacén de “solicitudes de inscripción del certificado” y verificar no existe más la solicitud generada.
- verificar existe el certificado importado: entrar en el almacén “Personal” y verificar la existencia del certificado. Ver figura 37.

Nota: en el almacén “Personal” deberán aparecer dos certificados: el “viejo” y el “nuevo” correspondiente a la renovación.

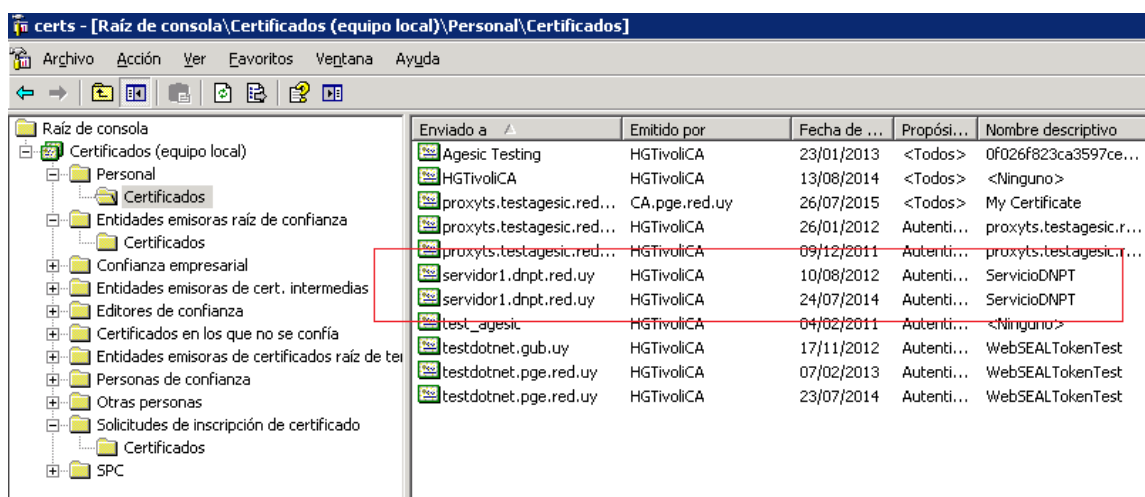


Figura 37: Almacén Personal con el certificado importado