



AGESIC Gerencia de Proyectos

Tutorial para la Solicitud de Certificados para la PGE Plataforma Microsoft

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

Historial de Revisiones

Nombre actual del archivo: Tutorial_Certificados_Microsoft_v1.2.odt

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

www.agesic.gub.uy





REPÚBLICA ORIENTAL DEL URUGUAY

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 cerficadora (CA),
- 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 <u>primera</u> <u>vez</u> 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 solucitud de firma de certificado (CSR – Certificate Signed Request) se realizan en conjunto.

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

- 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.
- Ir a la pestaña "Seguridad de directorios" (Figura 2) y luego click en "Certificado de servidor" (Figura 3).





🐚 Administrador de Intern	et Information Services (II	5)	
🕤 Ar <u>c</u> hivo <u>A</u> cción <u>V</u> er	Ve <u>n</u> tana Ay <u>u</u> da		<u>_8×</u>
⇐ ⇒ 🗈 💽 🗙 😭	0 8 2 10 2 >	I	
Servicios de Internet Inform 	nation Server Nombr local) nes eterminado enido)	ex.html	Ruta de acceso
 ServicioDNPT INE INE MTOM Sample Extensiones de se 	Explorar Abrir Permisos Examinar Iniciar		
Abre el cuadro de diálogo de p	<u>N</u> uevo I Todas las tareas I		
	<u>V</u> er Nueva ventana desde aguí		
	Eliminar Cam <u>b</u> iar nombre Actuali <u>z</u> ar E⊻portar lista…		
	Propiedades Ayuda		

Figura 1: Menú contextual de sitio web IIS





Propiedades de ServicioDNPT ? 🗙			
Seguridad de directorios Encabezados HTTP Errores personalizados ASP.NET Sitio Web Rendimiento Filtros ISAPI Directorio particular Documentos			
Identificación del sitio Web			
Descripción: ServicioDNPT			
Dirección IP: (Ninguna asignada) 💽 Avanzadas			
Puerto TCP: 80 Puerto SSL:			
Conexiones <u>T</u> iempo de espera de la conexión: 120 segundos Habilitar mantenimiento de conexiones HITP abiertas			
✓ Habilitar registro Formato de registro activo:			
Formato de archivo de registro extendido W3C			
Aceptar Cancelar Apligar Ayuda			

Figura 2: Ventana de propiedades - Pestaña Seguridad





Propiedades de ServicioDNPT
Sitio Web Rendimiento Filtros ISAPI Directorio particular Documentos
Seguridad de directorios Encabezados HTTP Errores personalizados ASP.NET
Autenticación y control de acceso
Habilitar acceso anónimo y modificar los métodos de autenticación para este recurso.
Restricciones de nombre de dominio y dirección IP
Conceder o denegar acceso a este recurso usando las direcciones IP o los nombres de dominio de Internet.
Modificar
Comunicaciones seguras
Requerir comunicaciones seguras y
habilitar los certificados de cliente
Ver certificado
Modificar
Aceptar Cancelar Apligar Ayuda

Figura 3: Pestaña "Seguridad de directorios"

 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.





Asistente para certificados IIS	×
Certificado de servidor Éstos son los métodos para asignar un ce	ertificado a un sitio Web.
Seleccione el método que desea utilizar e Crear un certificado nue <u>vo</u> Asignar un certificado ya existente. Imp <u>o</u> rtar certificado de archivo de cop Importar un certificado desde un arch	en este sitio Web: pia de seguridad del Administrador de claves. rivo .pfx
C <u>C</u> opiar o mover un certificado de un s	ervidor remoto a este sitio. < <u>A</u> trás Siguien <u>t</u> e > Cancelar

Figura 4: Crear un certificado nuevo

5. Seleccionar "Preparar la petición ahora pero enviarla más tarde", y hacer click en "Siguiente", ver Figura 5.





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		
C Enviar la petición inmediatamente a una entidad emisora de certificados en línea		
< <u>A</u> trás Siguien <u>t</u> e > Cancelar		

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).





REPÚBLICA ORIENTAL DEL URUGUAY

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:	
ServicioDNPT 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	
< <u>A</u> trás Siguien <u>t</u> e > Can	celar

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 BSA SChannel Cryptographic Provider	
< <u>A</u> trás Siguien <u>t</u> e >	Cancelar

Figura 7: Proveedores de cifrado





 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.

sistente 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
Uni <u>d</u> ad organizativa:
Secretaria 💌
< <u>A</u> trás Siguien <u>te</u> > Cancelar

Figura 8: Información de la organización

 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.



PRESIDENCIA REPUBLICA ORIENTAL DEL URUGUAY

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
< <u>A</u> trás [Siguien <u>t</u> e >] 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)	
<u>E</u> stado o provincia:	
Montevideo	•
Ciudad o localidad:	
Montevideo	•
Los nombres de estado, provincia, ciudad y localidad deben ser nombres oficial completos que no contengan abreviaturas.	es
< <u>A</u> trás <mark>(Siguien<u>t</u>e >)</mark> (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 nara certificados IIS	X
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. Nom <u>b</u> re de archivo:	
c:\certreq.txt	Exa <u>m</u> inar
< <u>A</u> trás Siguien <u>t</u> e >	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).





Asistente para certificados IIS		×
Resumen del archivo de petici Ha elegido generar un archivo c	ión de petición.	
Para generar la siguiente petició	ón, haga clic en Siguiente.	
Nombre de archivo: c:\certreq.	, txt	
Su petición contiene la informac	ción siguiente:	
Emitido para Nombre descriptivo País o región Estado o provincia Ciudad Organización Unidad organizativa	servidor1.dnpt.red.uy ServicioDNPT UY Montevideo Montevideo DNPT Secretaria	
	< <u>A</u> trás Siguien <u>t</u> e > Can	celar

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:

 "Inicio" → "Ejecutar" y luego introducir el comando mmc como se muestra en la Figura .



Figura 13: Abrir Microsoft Managment Console





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

Agregar o quitar cor	nplemento		? ×
Independiente Exte	ensiones		
Use esta página par la consola.	a agregar o quit	ar un complemento indeper:	ndiente de
Complementos agregados a:	aíz de co	nsola	
Descripción			
Agr <u>e</u> gar	Quitar	<u>A</u> cerca de	
		Aceptar	Cancelar

Figura 14: Agregar o quitar complemento

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





Complemento de certificados 🛛 🔀
Este accelerate administrativitation activitation des
Este complemento administrara siempre certificados de:
O <u>M</u> i cuenta de usuario
🔘 Cuenta de <u>s</u> ervicio
Cuenta de equipo
< Atrás Siguiente > Cancelar
Figura 15: Selección de tipo de complemento de certificados

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





normación		
regar o quitar co	mplemento ?	×
independiente Ext	tensiones	
Use esta página pa la consola.	ara agregar o quitar un complemento independiente de	
C <u>o</u> mplementos agregados a:	🔁 Raíz de consola 💌 💼	
Certificados (equipo local)	
Descripcion		
	Outer de	
Agregar	Quitar Acerca de	
	Aceptar Cancela	r

Figura 16: Agregar o quitar complementos

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.





🚡 Consola1 - [Raíz de consola\Certificados (equipo loca)\Solicitudes de inscripción de certi	ficado\Certificados] 💦 🗖 🗙
📸 Archivo Acción Ver Eavoritos Ventana Ayuda		_ & ×
📄 Raíz de consola	Enviado a 🔺	Emitido por
🖻 🗐 Certificados (equipo local)	servidor1.dnpt.red.uy	servidor1.dnpt.red.uy
庄 💼 Personal		
🕀 💼 Entidades emisoras raíz de confianza		
🕀 💼 Confianza empresarial		
🕀 🔲 Entidades emisoras de cert. intermedias		
🕀 🔲 Editores de confianza		
⊡ Certificados en los que no se confía		
Entidades emisoras de certificados raíz de tercero		
🖅 🛄 Personas de contianza		
Him Otras personas		
	1	
	•	Þ
El almacén Solicitudes de inscripción de certificado contiene un cert	ificado.	

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 <u>soporte@agesic.gub.uy</u>, con asunto "*Solicitud de PKCS12 – Nombre Organismo* – *Ambiente xxxxx*", 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 xxxxx en el asunto del mail, por "testing" o "producción").

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

 Ir a "Inicio" → "Todos los programas" → "Herramientas administrativas" → "Administrador de Internet Information Services (IIS)"





- Seleccionar el servicio web para el cual se solicitó el certificado (ej: ServicioOrganismo), click derecho "Propiedades", Figura 6.
- 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)

Asistente para certificados IIS	×
Petición de certificado pendiente Una petición de certificado pendiente es una petición a la que la entidad emisora de certificados todavía no ha respondido.	
¿Qué desea hacer con la petición de certificado pendiente?	
Procesar la petición pendiente e instalar el certificado	
O Eliminar la petición pendiente	
< <u>A</u> trás Siguien <u>t</u> e >	Cancelar

Figura 18: Asistente de importación de certificados

 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".





Asiste	ente para certificados IIS	×
Proc	cesar petición pendiente	~
	Procesar una petición de certificado pendiente recuperando el archivo que contiene la respuesta de la entidad emisora de certificados.	
l	Escriba la ruta de acceso y el nombre del archivo que contiene la respu emisora de certificados.	esta de la entidad
<u> </u>	<u>R</u> uta de acceso y nombre de archivo:	
	c:\servidor1.dntp.red.uy.cer	Exa <u>m</u> inar
	< <u>A</u> trás Siguien <u>t</u> e >	Cancelar

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 W	eb.		
Puerto SS <u>L</u> para este sitio Web:			
	< <u>A</u> trás	Siguien <u>t</u> e >	Cancelar

Figura 20: Puerto SSL

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





Asistente para certificado	s IIS	×
Resumen del certificado Ha elegido instalar un ce	ertificado desde un archivo de respuesta.	
Para instalar el siguiente Archivo:	certificado, haga clic en Siguiente. :\servidor1 doto red un cer	
Detalles del certificado: Emitido para Emitido por Fecha de caducidad Propósito planteado Nombre descriptivo País o región Estado o provincia Ciudad Organización Unidad organizativa	servidor1.dnpt.red.uy HGTivoliCA 10/08/2012 Autenticación del servidor ServicioDNPT UY Montevideo DNPT Secretaria	
	< <u>A</u> trás Siguien <u>t</u> e > Canc	elar

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.
- Finalmente observar lo siguiente: En la ventana del almancén 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.





PKESIDEINCIA REPÚBLICA ORIENTAL DEL URUGUAY

🚡 Consola1 - [Raíz de consola\Certificados (equipo local)\Personal\Certificados]	
📸 Archivo Acción Ver Eavoritos Ventana Ayuda		X
← → 🗈 🖬 👗 🖻 🗡 😭 😫 💷		
 Raíz de consola Gertificados (equipo local) Personal Certificados Certificados Certificados Certificados Certificados Certificados Certificados Certificados Certificados Certificados emisoras de cert. intermedias Entidades emisoras de cert. intermedias Certificados en los que no se confía Certificados en los que no se confía Certificados de confianza Certificados de inscripción de certificado Certificados Solicitudes de inscripción de certificado SPC 	Enviado a Agesic Testing HGTivoliCA Proxyts.testagesic.red.uy Proxyts.testagesic.red.uy roxyts.testagesic.red.uy roxyts.testagesic.red.uy servidor1.dnpt.red.uy test_agesic	Emitido por HGTivoliCA HGTivoliCA CA.pge.red.uy HGTivoliCA HGTivoliCA HGTivoliCA HGTivoliCA
l El almacén Personal contiene 7 certificados.		

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.





Certificado ? 🗙
General Detalles Ruta de certificación
Información del certificado
No se puede comprobar este certificado hasta una entidad emisora de certificados en que se confía.
Enviado a: servidor1.dnpt.red.uy
Emitido por HGTivoliCA
Válido desde 10/08/2011 hasta 10/08/2012
🌮 Tiene una clave privada correspondiente a este certificado.
Declaración del emi <u>s</u> or
Aceptar

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

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.



PRESIDENCIA

PKESIDEINCIA REPÚBLICA ORIENTAL DEL URUGUAI

🚡 Consola1 - [Raíz de consola\Certificados (equipo local)\Entidades emisoras raíz de confianza\Certificados] 📃 🛛 🗙					
🚡 Archivo Acción Ver Eavoritos Ve <u>n</u> tana Ayuda					
📋 Raíz de consola		Enviado a 🔺	Emitido por	Fecha de caduc 🔺	
📄 🗑 Certificados (equipo	local)	ABA.ECOM Root CA	ABA.ECOM Root CA	09/07/2009	
🗄 📄 Personal		🖼 AddTrust External CA Root	AddTrust External CA Root	30/05/2020	
🖻 📄 Entidades emisor	ras raíz de confianza	🔛 Autoridad Certificadora de la Asoc	Autoridad Certificadora de la Asocia	28/06/2009 🚽	
Certificad	Todas las tareas	▶ Importar bra del Colegi	Autoridad Certificadora del Colegio	29/06/2009	
E Contianza em	<u> </u>	aumore 22 by DST	Baltimore EZ by DST	03/07/2009	
Entidades emi	<u>V</u> er	elgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	21/01/2010	
	Nueva ventana desde aguí	&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	16/10/2009	
	Nueva vista del cuadro de tareas	&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	16/10/2009	
Personas de c			C&W HKT SecureNet CA Root	16/10/2010	
Otras persona	Actualizar	&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	16/10/2009	
E Solicitudes de	Exportar lista	A.pge.red.uy	CA.pge.red.uy	26/07/2015	
E SPC	0vuda	ertisign - Autoridade Certificador	Certisign - Autoridade Certificadora	26/06/2018	
	HY <u>0</u> 00	ertisign - Autoridade Certificador	Certisign - Autoridade Certificadora	26/06/2018	
		🔛 Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	26/06/2018	
		🔛 Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	09/07/2018	
		🖼 Class 1 Primary CA	Class 1 Primary CA	06/07/2020 🚽	
Agregar un certificado en el almacén					

Figura 24: Importar certificado de la CA

- 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."
- 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.





Certificado ?	<
General Detalles Ruta de certificación	
Información del certificado	
Este certificado está destinado a los siguientes propósitos:	
•Asegura la identidad de un equipo remoto	
Enviado a: servidor1.dnpt.red.uy	
Emitido por HGTivoliCA	
Válido desde 10/08/2011 hasta 10/08/2012	
🌮 Tiene una clave privada correspondiente a este certificado.	
Declaración del emi <u>s</u> or	
Aceptar]

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:

- 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.





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

Archivo Acción Ver Ventana Ayuda Image: Archivo Acción Ver Ventana Ayuda Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: Archivo Image: A	🐌 Administrador de Intern	et Information Serv	rices (IIS)		
 ← → È II × P 2 2 2 2 2 1 2 1 1 Servicios de Internet Information Server ARTEESERVER (equipo local) Grupos de aplicaciones Sitios Web Sitio Web predeterminado ARTEEServices prueba CertEnroll (Detenido) hlopez 	🕥 Ar <u>c</u> hivo <u>A</u> cción <u>V</u> er	Ve <u>n</u> tana Ay <u>u</u> da			_8×
Servicios de Internet Information Server ARTEESERVER (equipo local) Grupos de aplicaciones Sitios Web Sitios Web Sitio Web predeterminado ARTEEServices prueba CertEnroll (Detenido) hlopez	← → E X	🖻 🖻 😰 🖬 🛛	是 ▶ ■ Ⅱ		
Abre el cuadro de diálogo de p Ver Nuevo Eliminar Abre el cuadro de diálogo de p Ver Nueva ventana desde aguí Eliminar Cambiar nombre Actualizar Exportar lista	Servicios de Internet Inform ARTEESERVER (equipo Grupos de aplicacio Sitios Web Sitio Web prede ARTEEServices prueba CertEnroll (Dete hlopez ServicioDNPT INE MTOM Sample Extensiones de se	Image:	e aguí	Ruta de acceso	
Ayuda		Ayuda			

Figura 26: Menú contextual de sitio web IIS





Propiedades de ServicioDNPT ? 🗙
Seguridad de directorios Encabezados HTTP Errores personalizados ASP.NET Sitio Web Rendimiento Filtros ISAPI Directorio particular Documentos
Identificación del sitio Web
Descripción: ServicioDNPT
Dirección IP: (Ninguna asignada) 💌 Avanzadas
Puerto TCP: 80 Puerto SSL:
Conexiones <u>T</u> iempo de espera de la conexión: <u>120</u> segundos Habilitar <u>m</u> antenimiento de conexiones HTTP abiertas
☐ Habilitar registro
Formato de registro activo:
Formato de archivo de registro extendido W3C Propiedades
Aceptar Cancelar Apligar Ayuda

Figura 27: Ventana de propiedades - Pestaña Seguridad





Propiedades de ServicioDNPT	? ×			
Sitio Web Rendimiento Filtros ISAPI Direct Seguridad de directorios Encabezados HTTP Erro	rorio particular Documentos res personalizados ASP.NET			
Autenticación y control de acceso Habilitar acceso anónimo y modificar los métodos de autenticación para este	Modi <u>f</u> icar			
Restricciones de nombre de dominio y dirección IP Conceder o denegar acceso a este recurso usando las direcciones IP o los nombres de dominio de Internet. Modificar				
Comunicaciones seguras Requerir comunicaciones seguras y habilitar los certificados de cliente cuando se tenga acceso a este recurso. Ver certificado Ver certificado Modificar				
Aceptar Cancelar	Apligar Ayuda			

Figura 28: Pestaña "Seguridad de directorios"

 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.





Asistente para certificados IIS	×
Modificar la asignación del certificado actual Este sitio Web ya tiene instalado un certificado.	
¿Qué desea hacer con el certificado instalado? Renovar el certificado actual	
Quitar el certificado actual	
Reemplazar el certificado actual	
C Exportar el certificado actual a un archivo .pfx	
Copiar o mover el certificado actual a un sitio de un servidor remoto	
< <u>A</u> trás Siguien <u>t</u> e >	Cancelar

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					
C Enviar la petición inmediatamente a una entidad emisora de certificados en línea					
< <u>A</u> trás Siguien <u>t</u> e > 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	E <u>x</u> aminar
< <u>A</u> trás Siguien <u>t</u> e >	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.

Asistente para certificados IIS 🛛 🛛 🗙
Resumen del archivo de petición Ha elegido generar un archivo de petición.
Para generar la siguiente petición, haga clic en Siguiente. Nombre de archivo: c:\servidor1.dnpt.red.uy Su petición contiene la información siguiente: Emitido para servidor1.dnpt.red.uy Nombre descriptivo ServicioDNPT País o región UY Estado o provincia Montevideo Ciudad Montevideo Organización DNPT Unidad organizativa Secretaria
< <u>A</u> trás Siguien <u>te</u> > Cancelar

Figura 32: Nombre de archivo CSR

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





🎁 certs - [Raíz de consola\Certificados (equipo local)\Solicitudes de inscripción de certificado\Certificados]					
🚡 Archivo Acción Ver Eavoritos Ventana Ayuda					
📄 Raíz de consola	Enviado a 🔺	Emitido por	Fecha de	Propósi	Nombre descripti
🗄 🎯 Certificados (equipo local)	servidor1.dnpt.red.uy	servidor1.dnpt.red.uy	24/07/2013	<todos></todos>	ServicioDNPT
🚊 📲 Personal					
Certificados					
🖻 🛅 Entidades emisoras raíz de confianza					
Certificados					
庄 💼 Confianza empresarial					
吏 💼 Entidades emisoras de cert. intermedias					
🗄 🚞 Editores de confianza					
🕀 🧰 Certificados en los que no se confía					
🕀 💼 Entidades emisoras de certificados raíz de ter					
🔃 💼 Personas de confianza					
🕂 💼 Otras personas					
📄 🧰 Solicitudes de inscripción de certificado					
🗄 💼 SPC					

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.

 enviar un correo a <u>soporte@agesic.gub.uy</u>, 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 xxxxx 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:

- 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".
- Seleccionar la opción "Procesar la petición pendiente e instalar el certificado" y hacer click en "Siguiente", como se muestra en la figura 34.

Asistente para certificados IIS 🛛 🛛 🔀
Petición de certificado pendiente Una petición de certificado pendiente es una petición a la que la entidad emisora de certificados todavía no ha respondido.
¿Qué desea hacer con la petición de certificado pendiente?
Procesar la petición pendiente e instalar el certificado
O Eliminar la petición pendiente
< <u>A</u> trás Siguien <u>t</u> e > Cancelar

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).
- Confirmar la información del certificado a importar y hacer click en "Siguiente" y luego en "Finalizar". Ver figura 36



PRESIDENCIA

REPÚBLICA ORIENTAL DEL URUGUAY

Asistente para certificados IIS	×
Procesar petición pendiente	
Procesar una petición de certificado pendiente recuperando el archivo que contiene la respuesta de la entidad emisora de certificados.	
Escriba la ruta de acceso y el nombre del archivo que contiene la respu emisora de certificados.	iesta de la entidad
<u>R</u> uta de acceso y nombre de archivo:	
C:\servidor1.dnpt.red.uy.cer	Exa <u>m</u> inar
< <u>A</u> trás Siguien <u>t</u> e >	Cancelar

Figura 35: Seleccionar ubicación del certificado

Asistente para certificados IIS Resumen del certificado Ha elegido instalar un certificado desde un archivo de respuesta.							
Para instalar el siguient Archivo:	e certificado, haga clic en Siguiente. c:\servidor1.dntp.red.uy.cer						
Detalles del certificado: Emitido para Emitido por Fecha de caducidad Propósito planteado Nombre descriptivo País o región Estado o provincia Ciudad Organización Unidad organizativa	servidor1.dnpt.red.uy HGTivoliCA 10/08/2012 Autenticación del servidor ServicioDNPT UY Montevideo DNPT Secretaria						
	< <u>A</u> trás Siguien <u>te</u> > Cancelar						

Figura 36: Resumen del certificado

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





- a) verificar no hay solicitudes pendientes: entrar en el almacén de "solicitudes de inscripción del certificado" y verificar no existe más la solicitud generada.
- b) 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.

📅 certs - [Raíz de consola\Certificados (equipo local)\Personal\Certificados]							
🚡 Archivo Acción Ver Eavoritos Ventana Ayuda							
📄 Raíz de consola	Enviado a 🛛 🛆	Emitido por	Fecha de	Propósi	Nombre descriptivo		
🖻 👹 Certificados (equipo local)	🔛 Agesic Testing	HGTivoliCA	23/01/2013	<todos></todos>	0f026f823ca3597ce		
Personal Certificados Certificados Certificados Certificados Certificados Certificados Confianza empresarial Confianza empresarial	🔛 HGTivoliCA	HGTivoliCA	13/08/2014	<todos></todos>	<ninguno></ninguno>		
	🔤 proxyts.testagesic.red	CA.pge.red.uy	26/07/2015	<todos></todos>	My Certificate		
	🔤 proxyts.testagesic.red	HGTivoliCA	26/01/2012	Autenti	proxyts.testagesic.r		
	Broxyts.testagesic.red	HGTivoliCA	09/12/2011	Autenti	proxyts.testagesic.r		
	🔤 servidor1.dnpt.red.uy	HGTivoliCA	10/08/2012	Autenti	ServicioDNPT		
	🔤 servidor1.dnpt.red.uy	HGTivoliCA	24/07/2014	Autenti	ServicioDNPT		
	📇 test_agesic	HGTivoliCA	04/02/2011	Autenti	<ningano></ningano>		
Entidados en los que no se conna	🔛 testdotnet.gub.uy	HGTivoliCA	17/11/2012	Autenti	WebSEALTokenTest		
Personas de confianza	🔛 testdotnet.pge.red.uy	HGTivoliCA	07/02/2013	Autenti	WebSEALTokenTest		
Otras personas	🔤 testdotnet.pge.red.uy	HGTivoliCA	23/07/2014	Autenti	WebSEALTokenTest		
Solicitudes de inscripción de certificado							
Certificados							

Figura 37: Almacén Personal con el certificado importado