Plataforma de Interoperabilidad

Tutorial de Certificados .NET

Control de Cambios

Fecha	Versión	Descripción	Autor	Aprobado Por
2015	1.0	Versión inicial		
07/07/1905	2.0			

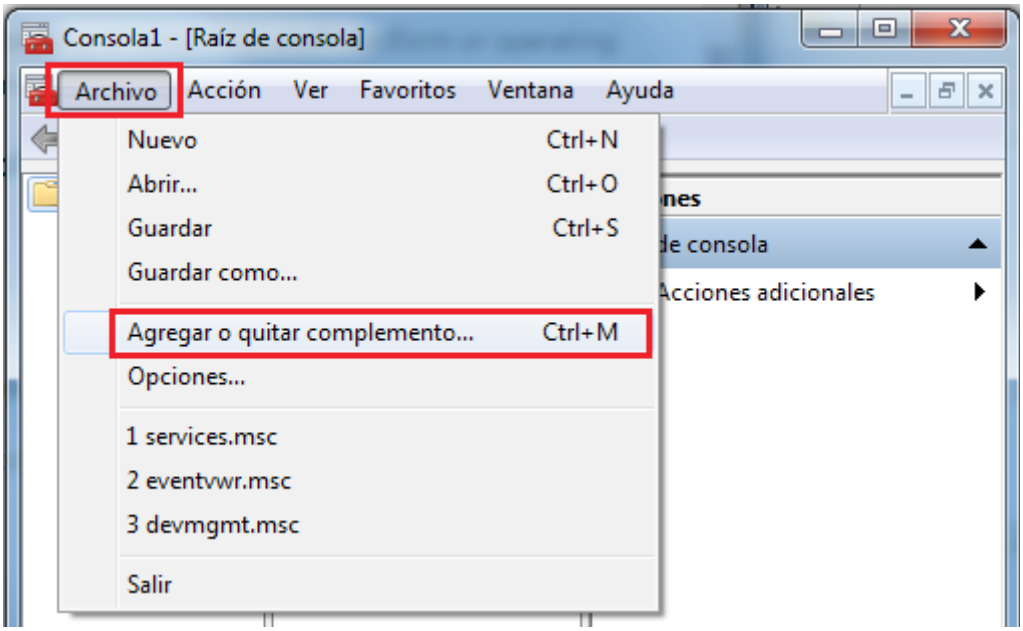
Nombre actual del archivo: Tutorial-Certificados-Microsoft-v02-00.odt

Plataforma de Interoperabilidad

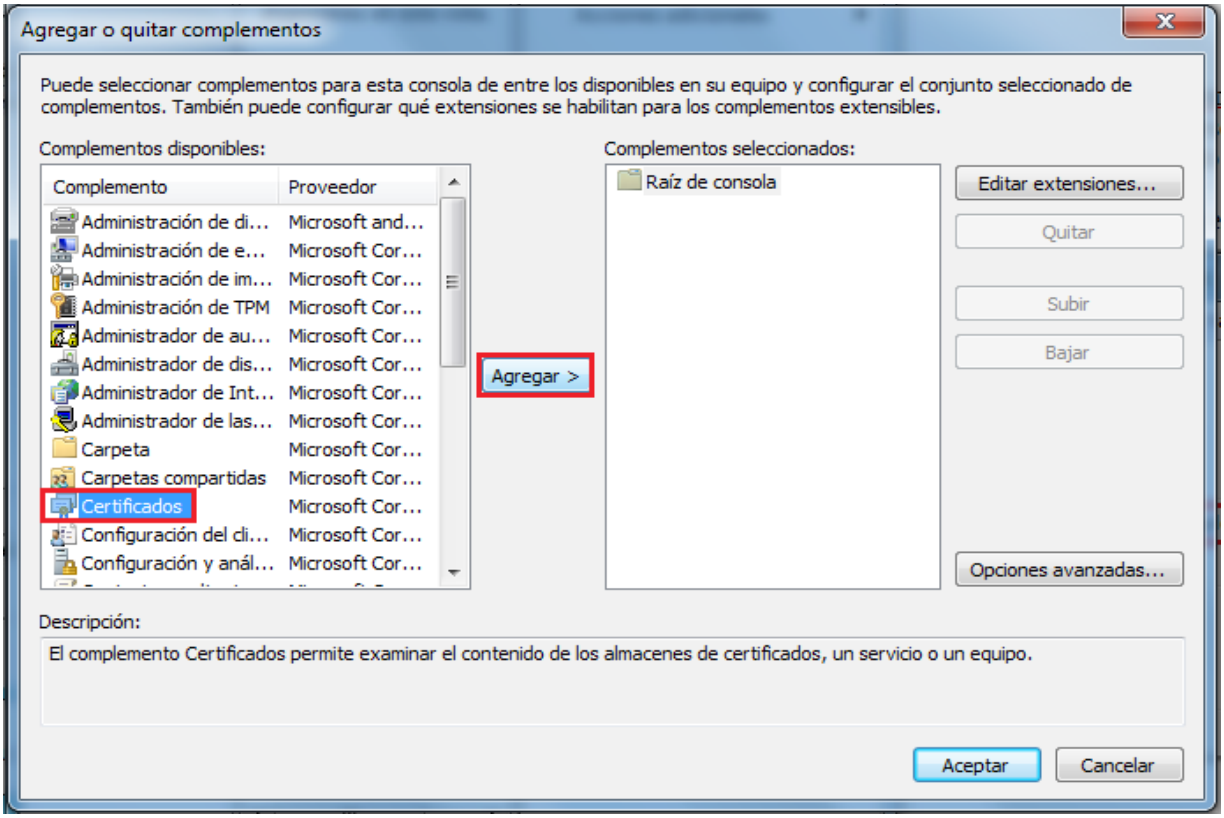
1. Generar la solicitud de certificados

1. Abrir "*Microsoft Management Console*" (mmc)
   - En el menú inicio escriba "mmc"
   - Asegúrese de abrirlo como administrador

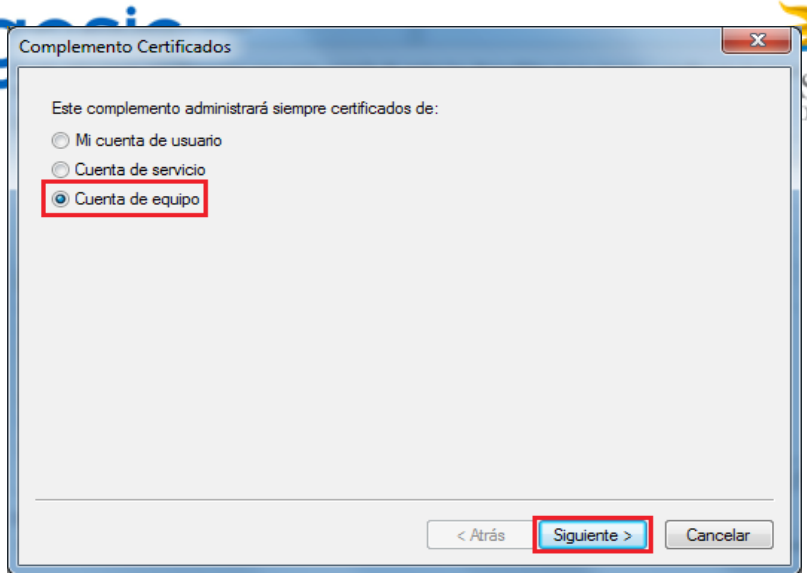
2. En la consola mmc, click en "*Archivo*" y luego en "*Agregar o quitar complemento*"



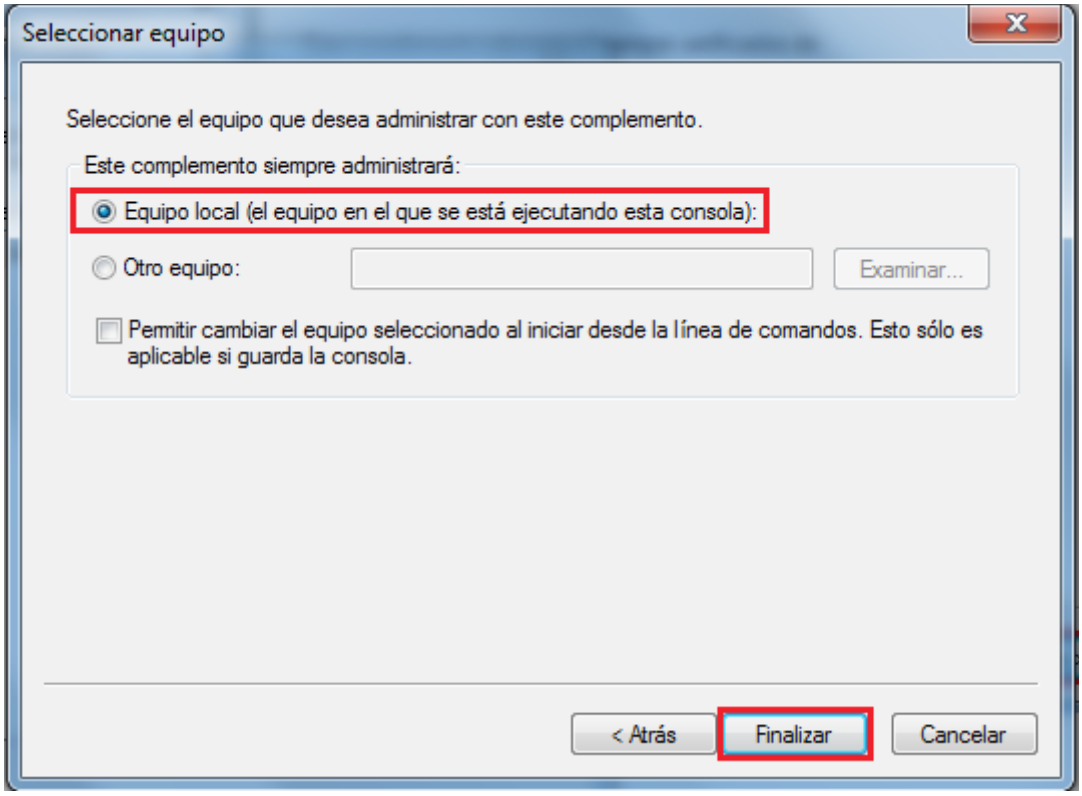
3.En la ventana “*Agregar o quitar complementos*”, bajo complementos disponibles, seleccionar “*Certificados*” y luego, click en “*Agregar*”.



4. En la ventana “*Complemento certificados*”, seleccionar “*Cuenta de equipo”* para gestionar los certificados instalados en su equipo.

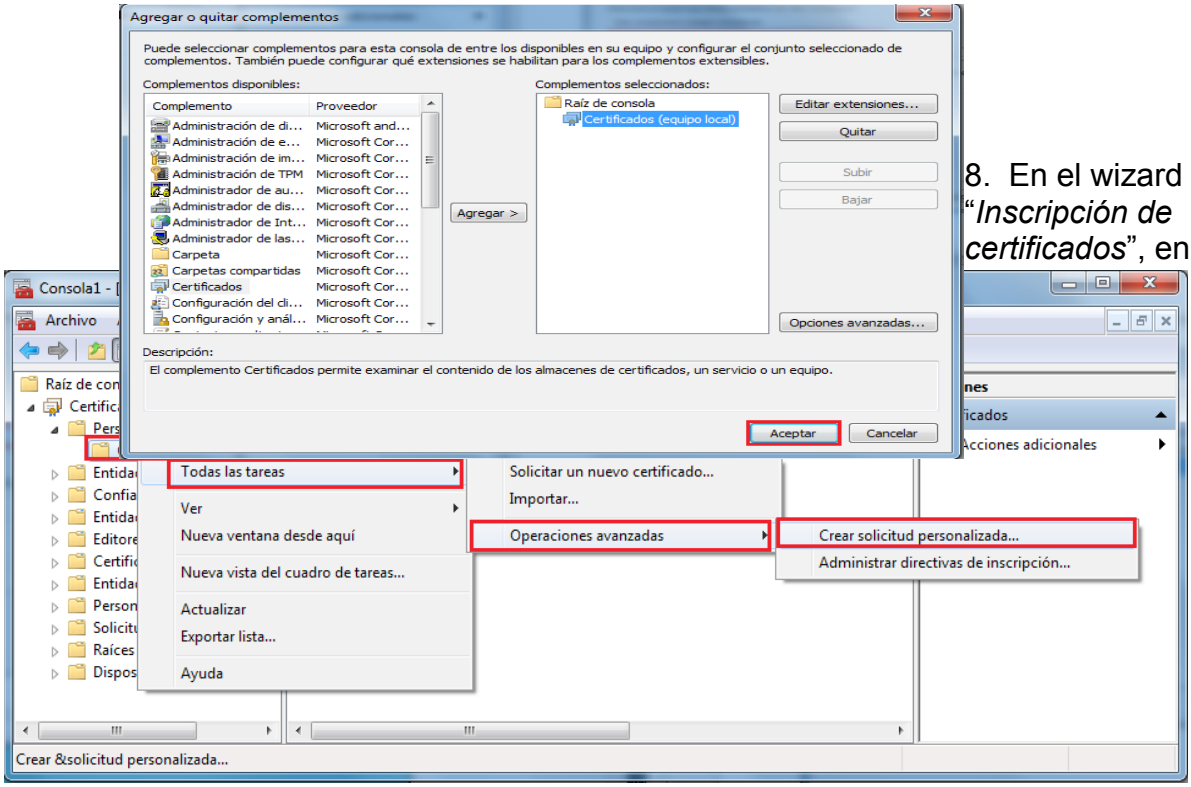


5. En la ventana "*Seleccionar equipo*", seleccionar "*Equipo local (el equipo en el que se está ejecutando esta consola)*", y luego click en "*Finalizar*".

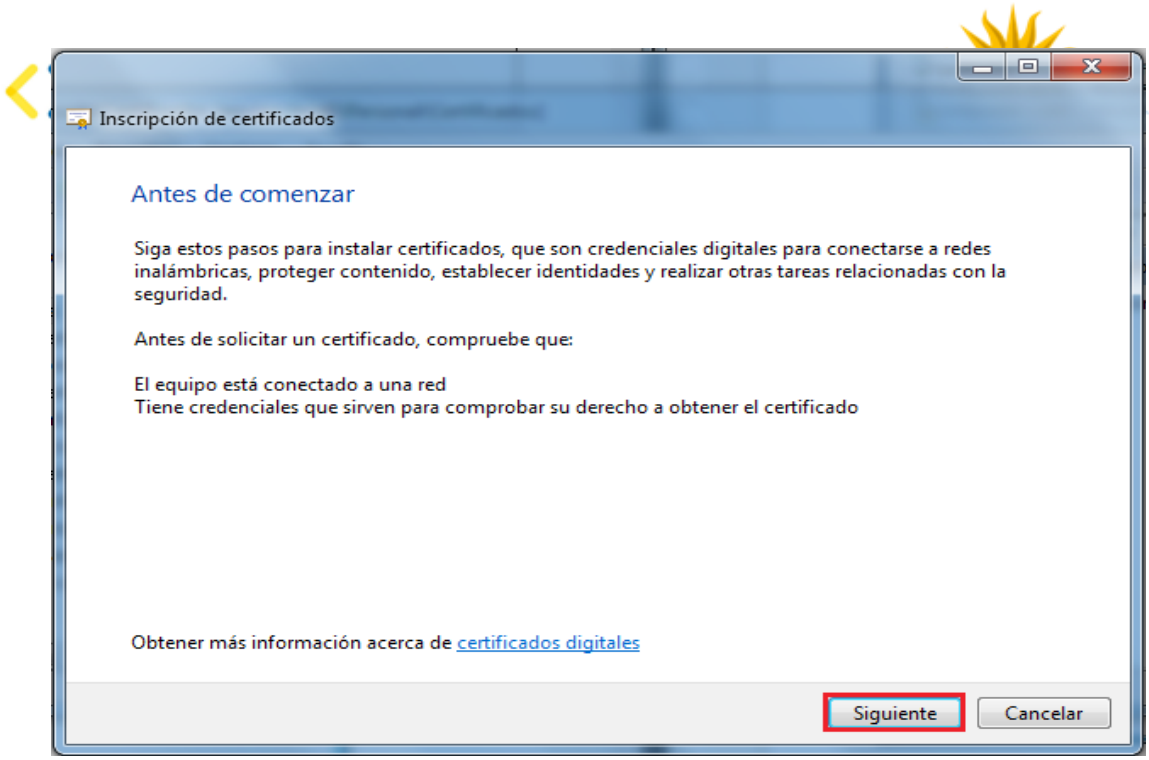


6. En la ventana “*Agregar o quitar complementos*”, apretar “*Aceptar*”.

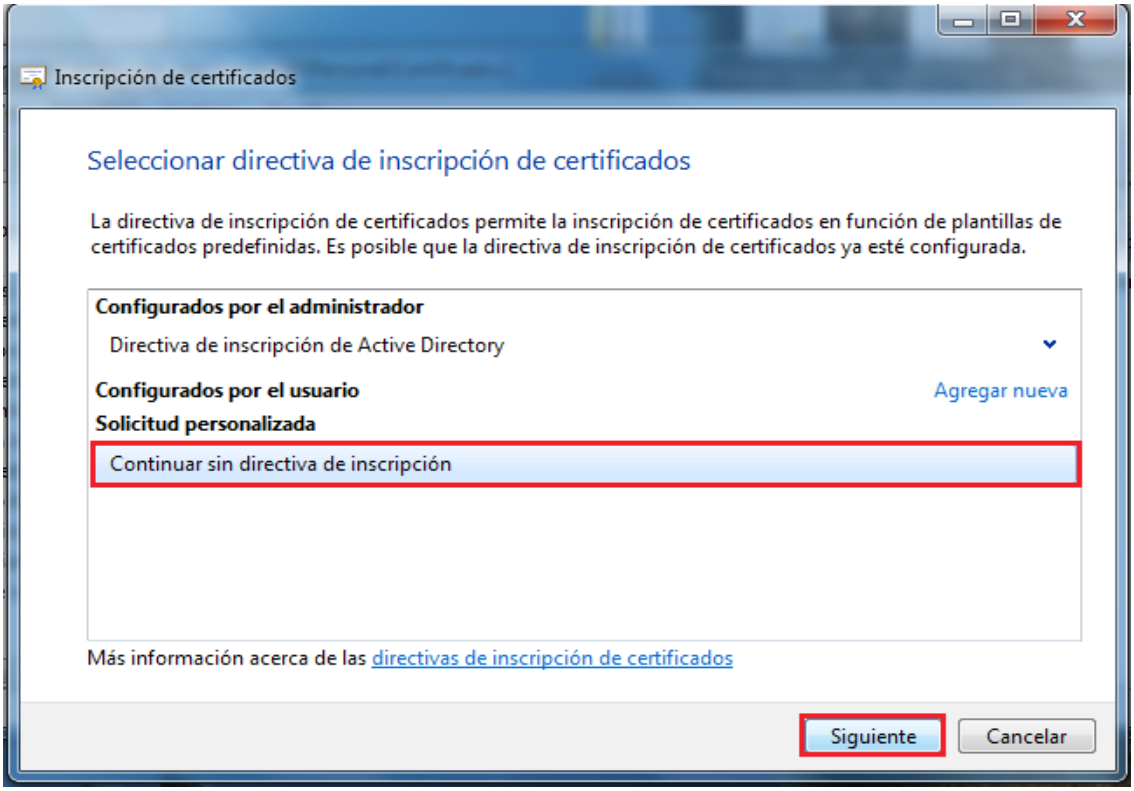
7. En la consola mmc, en el árbol “*Raíz de consola*”, expandir “Certificados > Personal”, click derecho en la carpeta “*Certificados*”, luego click en “*Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada*”



8. En el wizard de “*Inscripción de certificados*”, en la página “*Antes de comenzar*”, click en “*Siguiente*”.



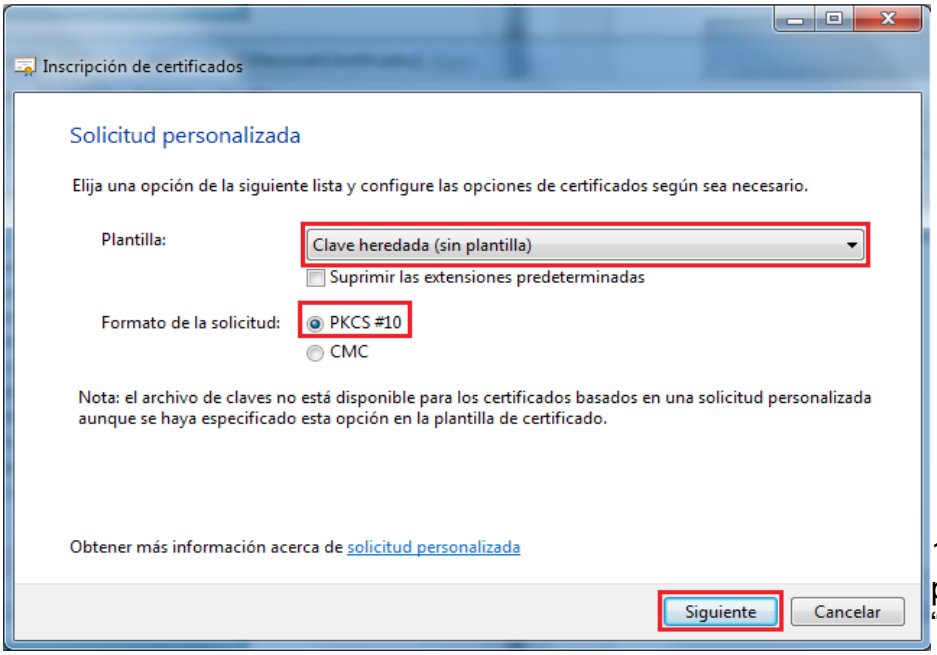
9. En la página "*Seleccionar directiva de inscripción de certificados*", seleccionar "*Continuar sin directiva de inscripción*", y luego, click en "*Siguiente*".



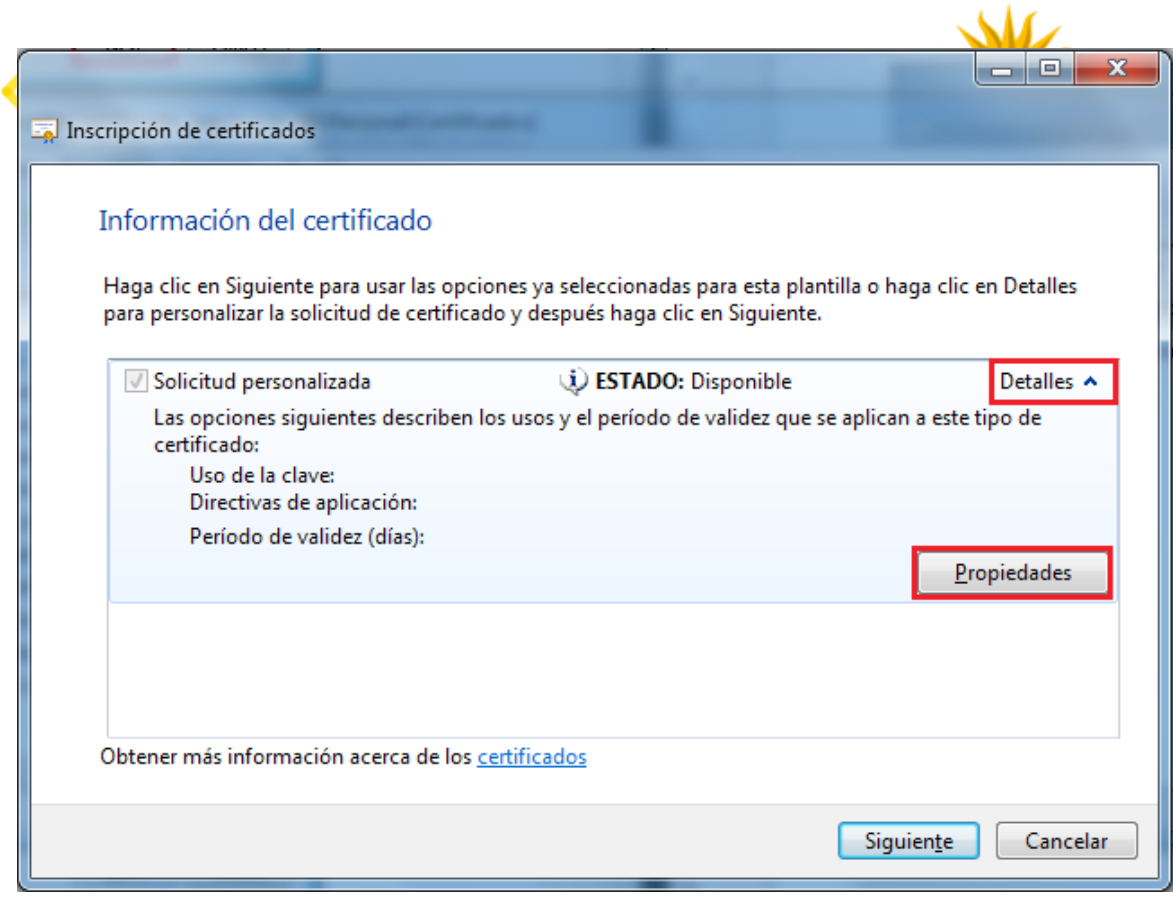
10. En la página “*Solicitud personalizada*”, haga lo siguiente, y luego, click en “S*iguiente*”.

Plantilla: En la lista desplegable, seleccionar “*Clave heredada (sin plantilla)*”

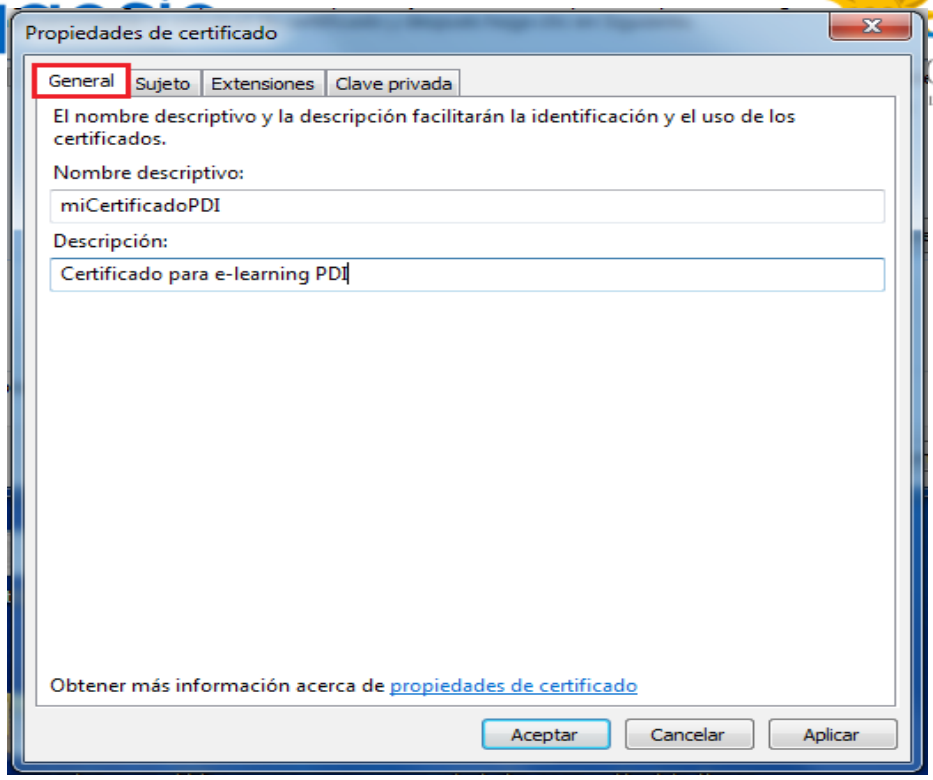
Formato de la solicitud: Seleccionar “*PKCS #10*”



11. En la página “*Información del certificado*”, expandir “*Detalles*”, y luego click en “*Propiedades*”.

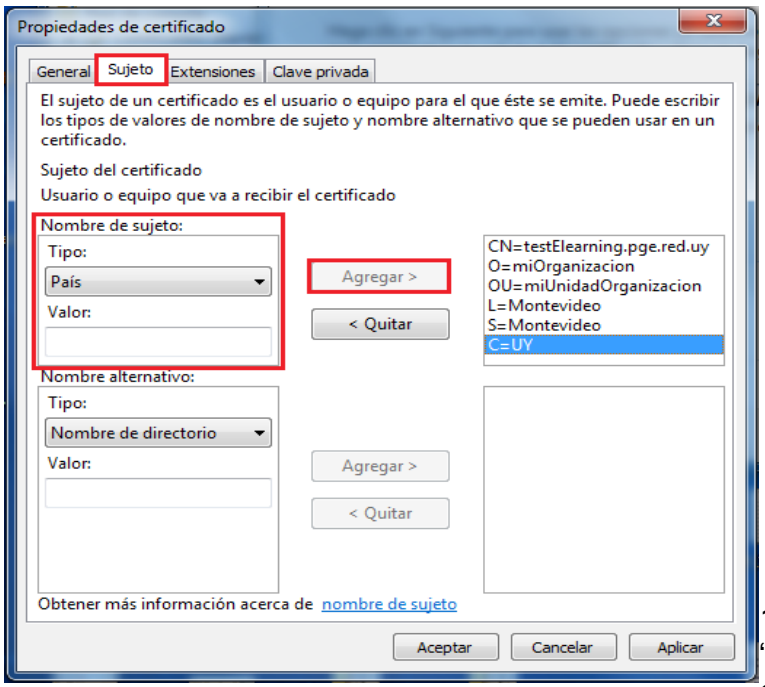


12. En la ventana "*Propiedades de certificados*", en la pestaña "*General*", hacer lo siguiente:

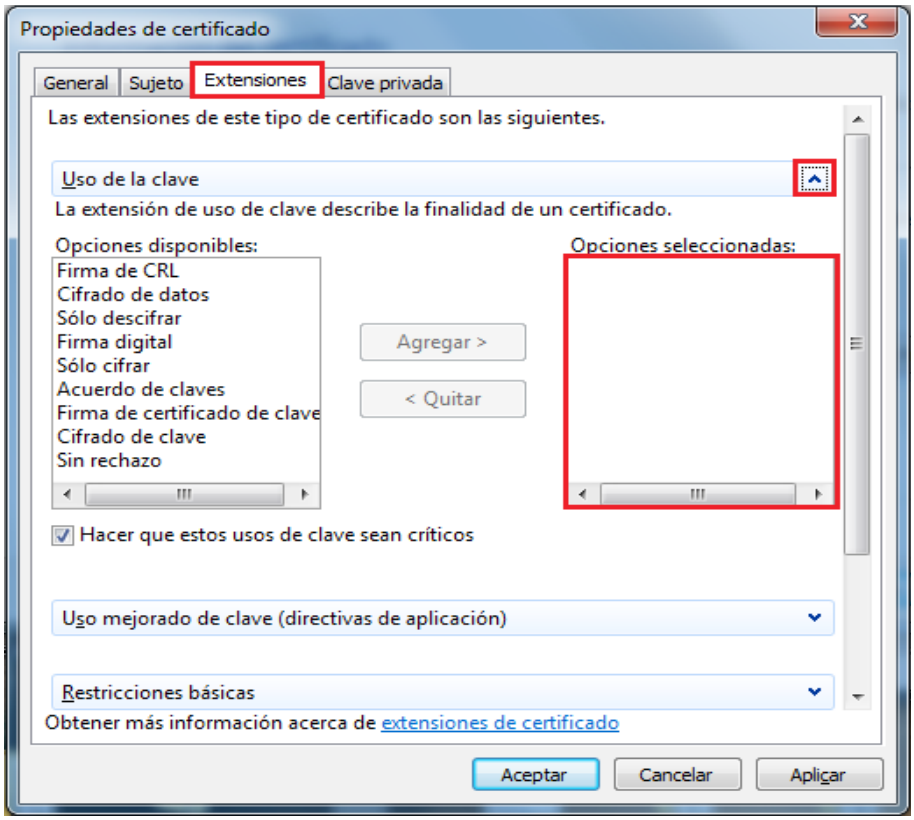


13. En la pestaña “*Sujeto*”, en la sección “*Nombre de sujeto*”, seleccionar el tipo correspondiente, el valor correspondiente, y seleccionar agregar:

Tipo	**Valor**
Nombre común	Para este tutorial utilize el siguiente formato: incial nombre, apellido, y luego agregue “.pge.red.uy”. Por ejemplo: “jperez.pge.red.uy”
Organización	Ingrese el nombre de su organización
Unidad de organización	Ingrese el nombre su unidad dentro de la organización.
Localidad	Ingrese el nombre de su localidad
Estado o provincia	Ingrese el nombre de su estado o provincia
País	Para este tutorial usaremos: UY

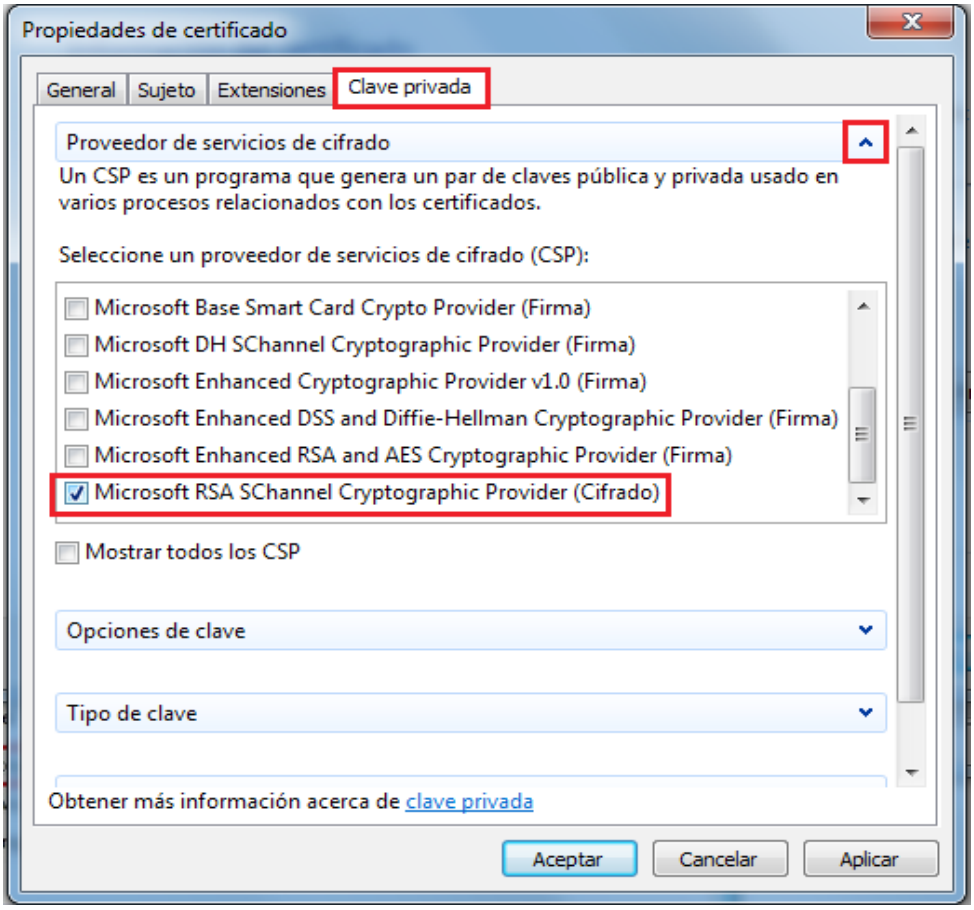


14. En la pestaña "*Extensiones*", expandir "*Uso de la clave*". Es importante que la sección "*Opciones seleccionadas*" esté vacía



15. En la pestaña "*Clave privada*", expandir "*Proveedor de servicios de cifrado*", y en la sección "*Seleccione un proveedor de servicios de cifrado (CSP)*":

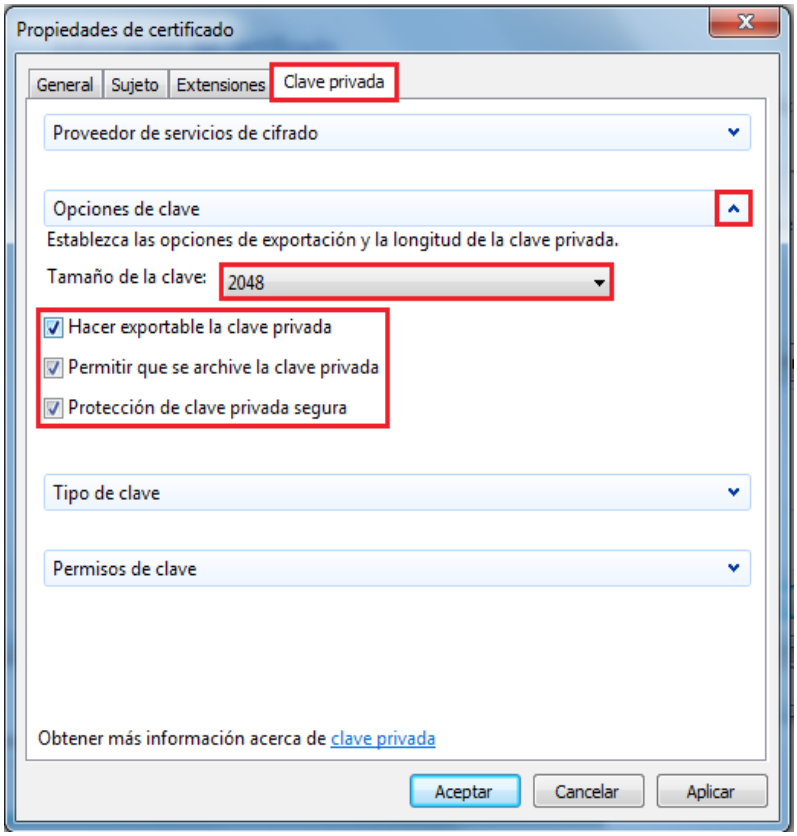
- Des-seleccionar la opción que viene por defecto
- Seleccionar "*Microsoft RSA Schannel Cryptographic Provider (Cifrado)*"



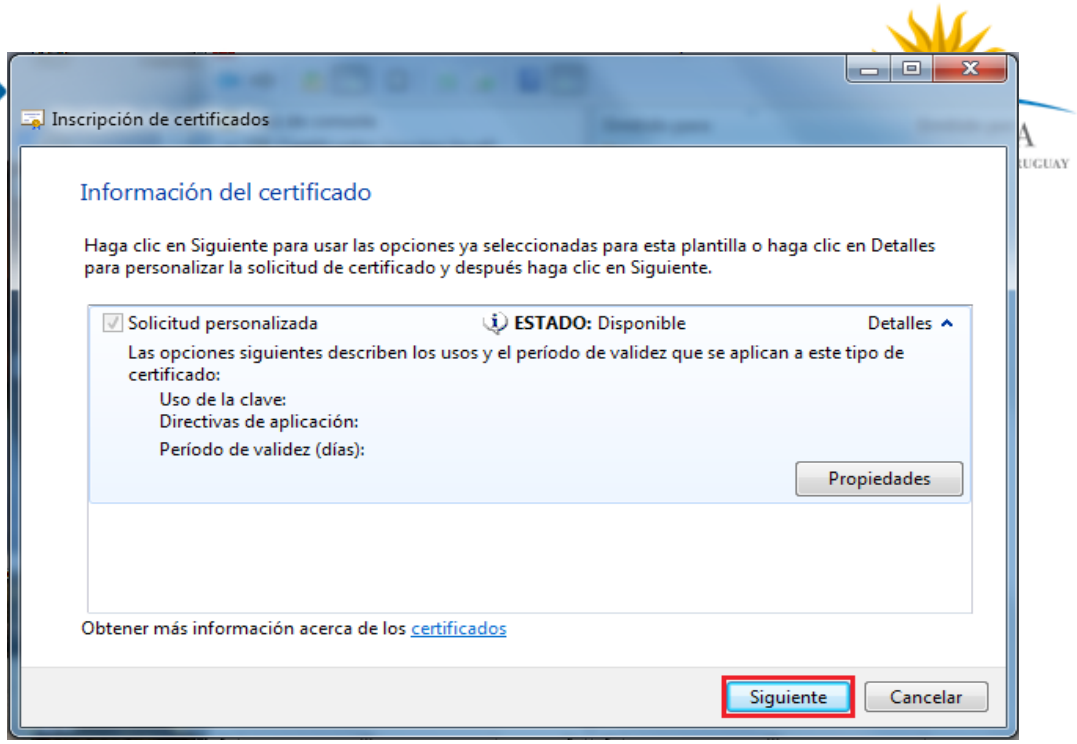
16. Luego, en la misma pestaña, expandir "*Opciones de clave*":

- En "*Tamaño de la clave*" seleccionar "*2048*"
- Seleccionar los tres checkbox:
  - "*Hacer exportable la clave privada*"
  - "*Permitir que se archive la clave privada*"
  - "*Protección de clave privada segura*"

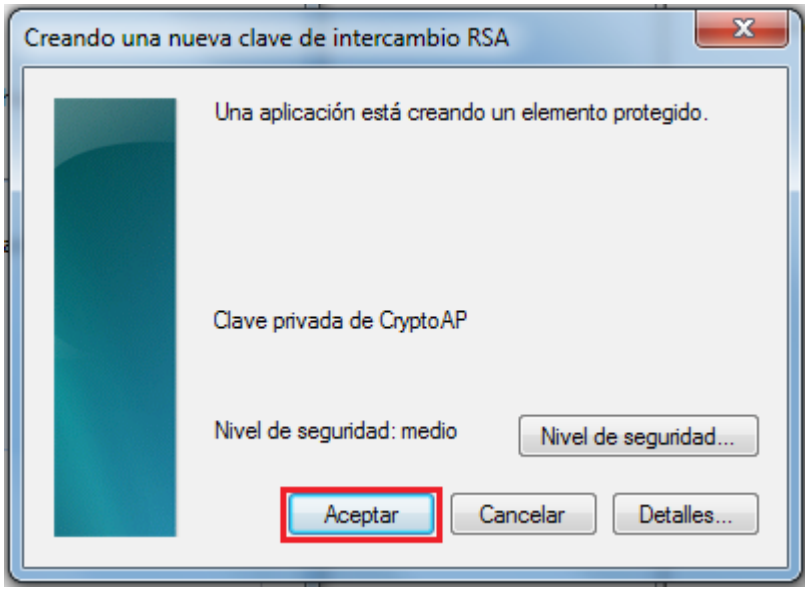
Luego click en "*Aceptar*".



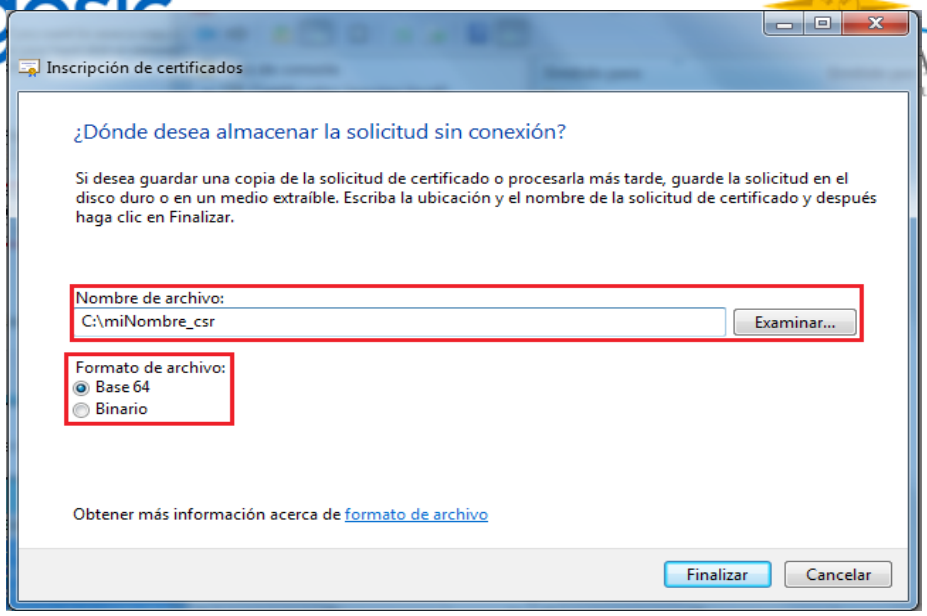
17. De vuelta en la ventana "*Inscripción de certificados*" hacer click en siguiente.



18. Veremos una ventana "*Creando una nueva clave de intercambio RSA*", hace click en "*Aceptar*".



19. En la ventana "*Inscripción de certificados*", elija la ruta donde se guardará el archivo a generar. Para facilitar la tramitación de la firma de los certificados, favor utilizar el siguiente formato para el nombre del archivo: inicial nombre, apellido, y luego anexar al final "_csr". Por ejemplo: "jperez_csr"



Es importante que en "F*ormato del archivo*" esté seleccionado "*Base64*"

20. Luego, seleccionar "*Finalizar*". A esta altura hemos generado

el archivo CSR (en formato PKCS10) se debe adjuntarlo como tarea en el módulo II del moodle.

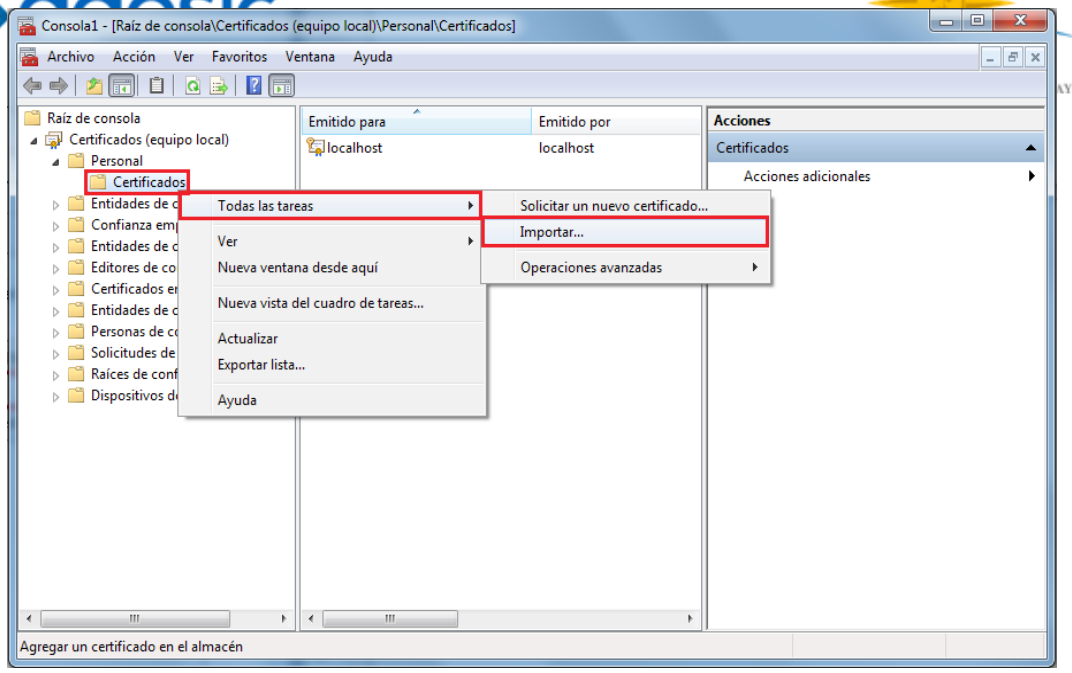
El formato del archivo deberá ser *inicialNombreApellido.elearning.red.uy*

Luego se adjuntará a través del mismo medio la respuesta de AGESIC conteniendo la firma de los datos; cuando se reciba la respuesta,

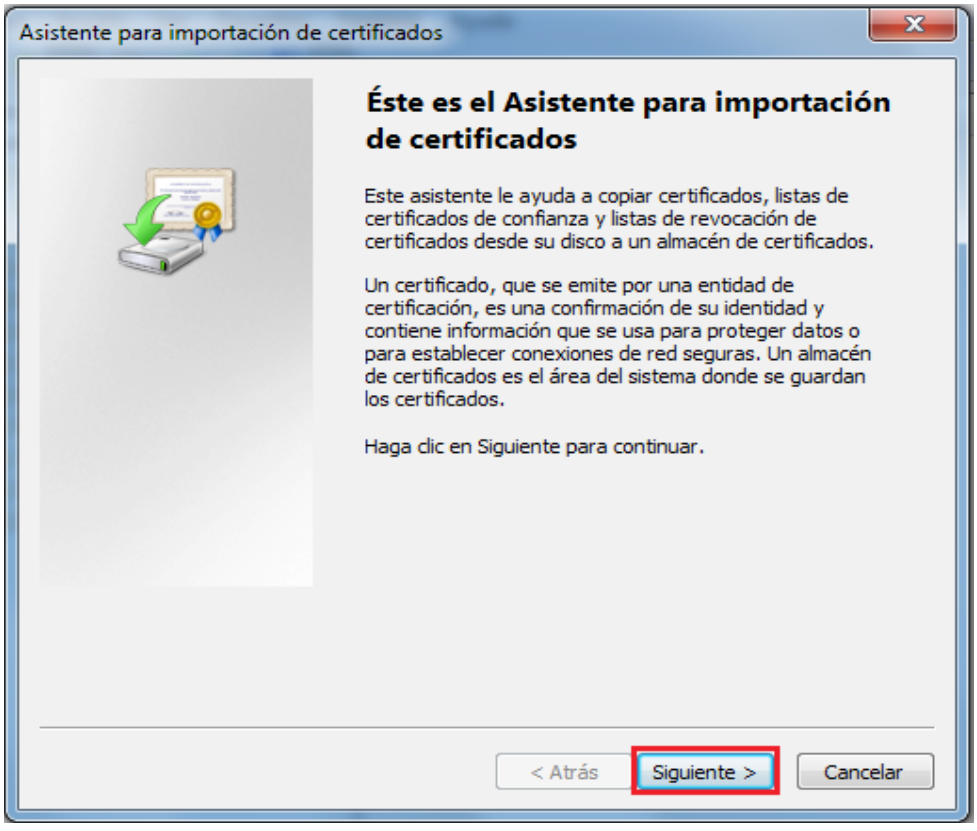
2. Importar el certificado emitido por AGESIC

1. Abrir "*Microsoft Management Console*" (mmc)
    - En el menú inicio escriba "mmc"
    - Asegúrese de abrirlo como administrador

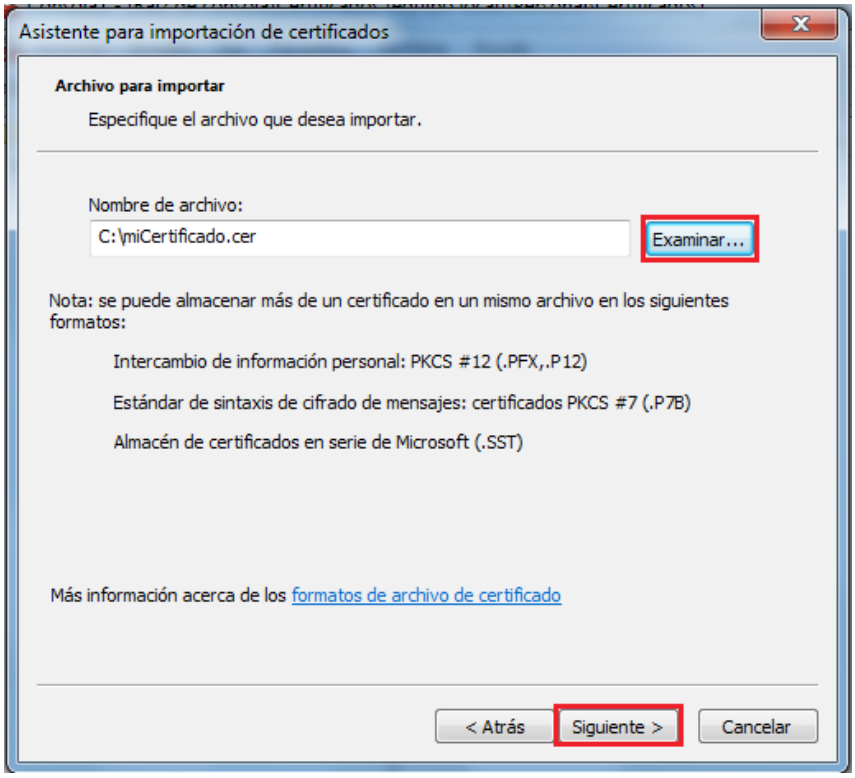
2. En la consola mmc, en el árbol "*Raíz de consola*", expandir "*Certificados* > *Personal*", click derecho en la carpeta "*Certificados*", y luego seleccionar "*Todas las tareas* > *Importar*".



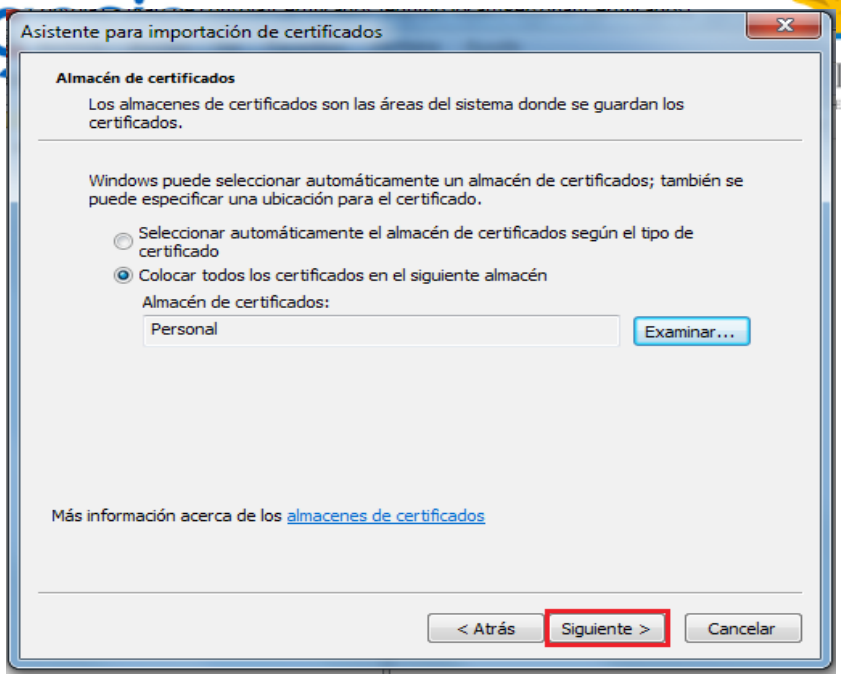
3. Se abrirá el "*Asistente para importación de certificados".* Click en siguiente.



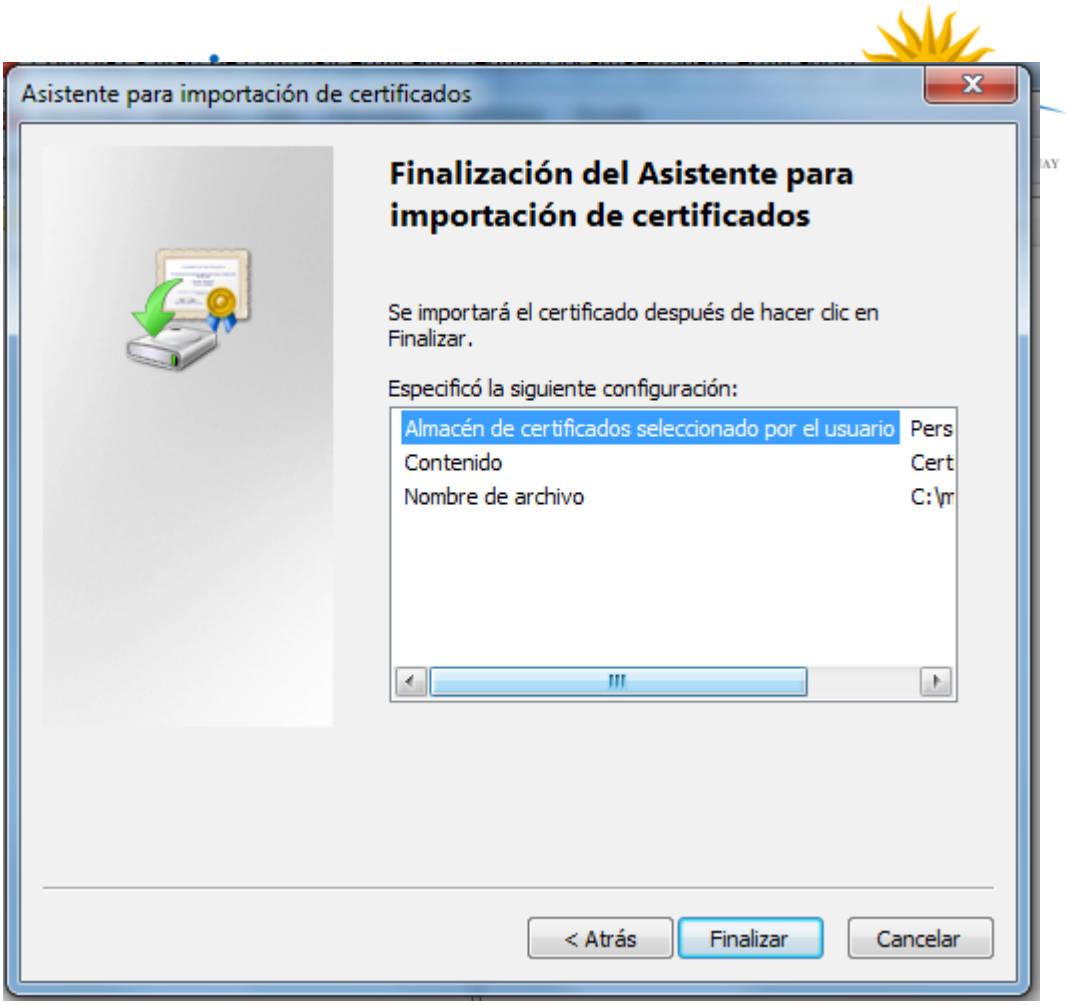
4. En la página "*Archivo para importar*", click en "*Examinar*" y seleccionar la ruta al certificado emitido por AGESIC. Luego, click en siguiente.



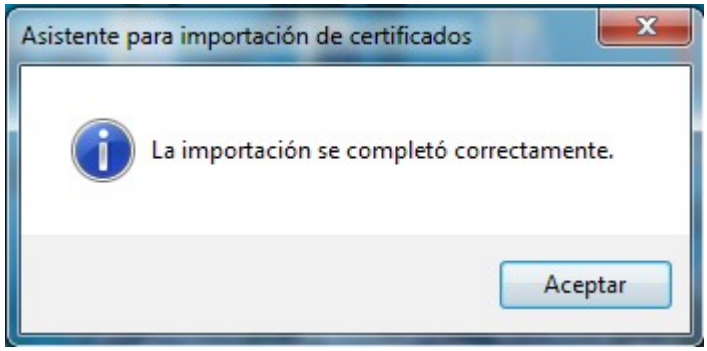
5. En la página "*Almacén de certificados*", dejar seleccionada la opción "*Colocar todos los certificados en el siguienre almacén*", y en "*Almacen de certificados*" elegir "*Personal*". Luego, click en "*Siguiente*"



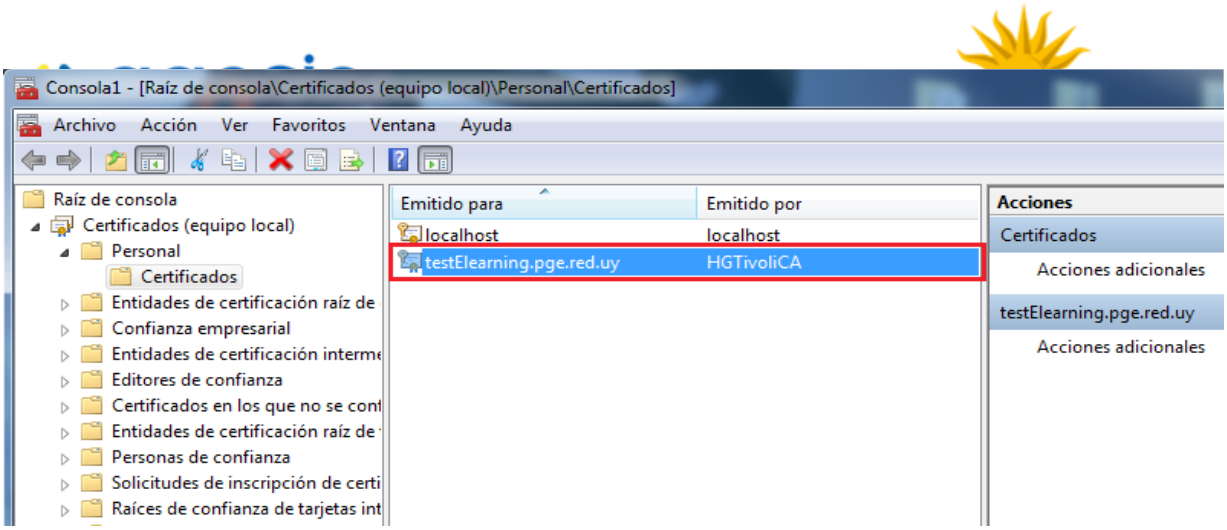
6. Luego en la página "*Finalización del asistente para importación de certificados*", click en "*Siguiente*".



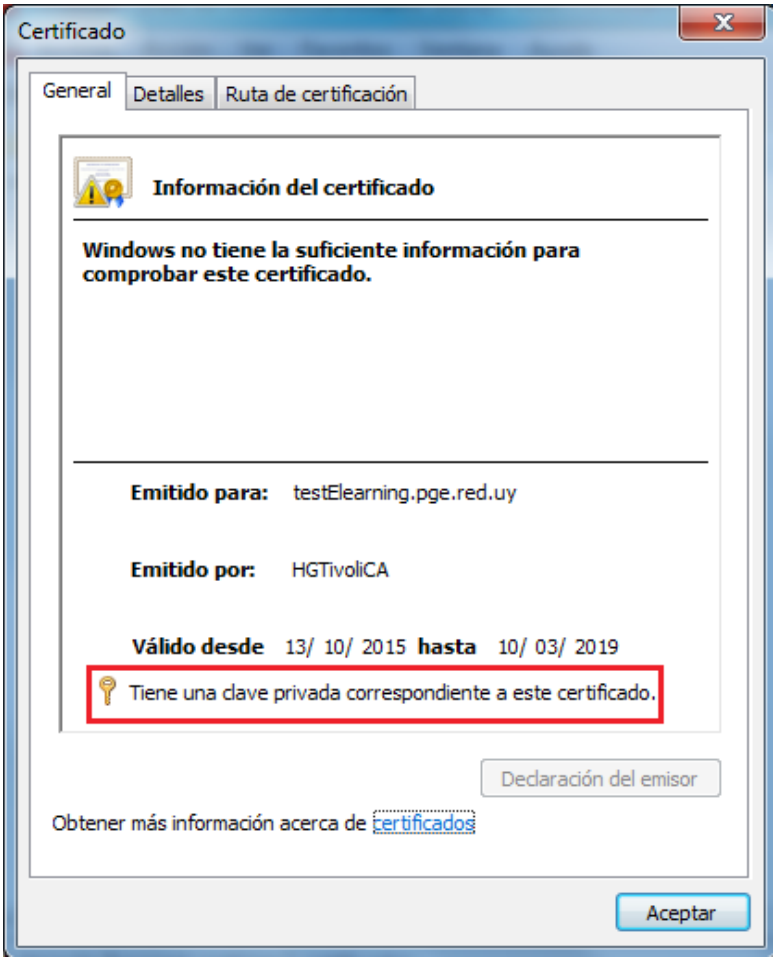
Luego de unos segundos deberíamos ver una ventana que confirma que el certificado se importó correctamente:



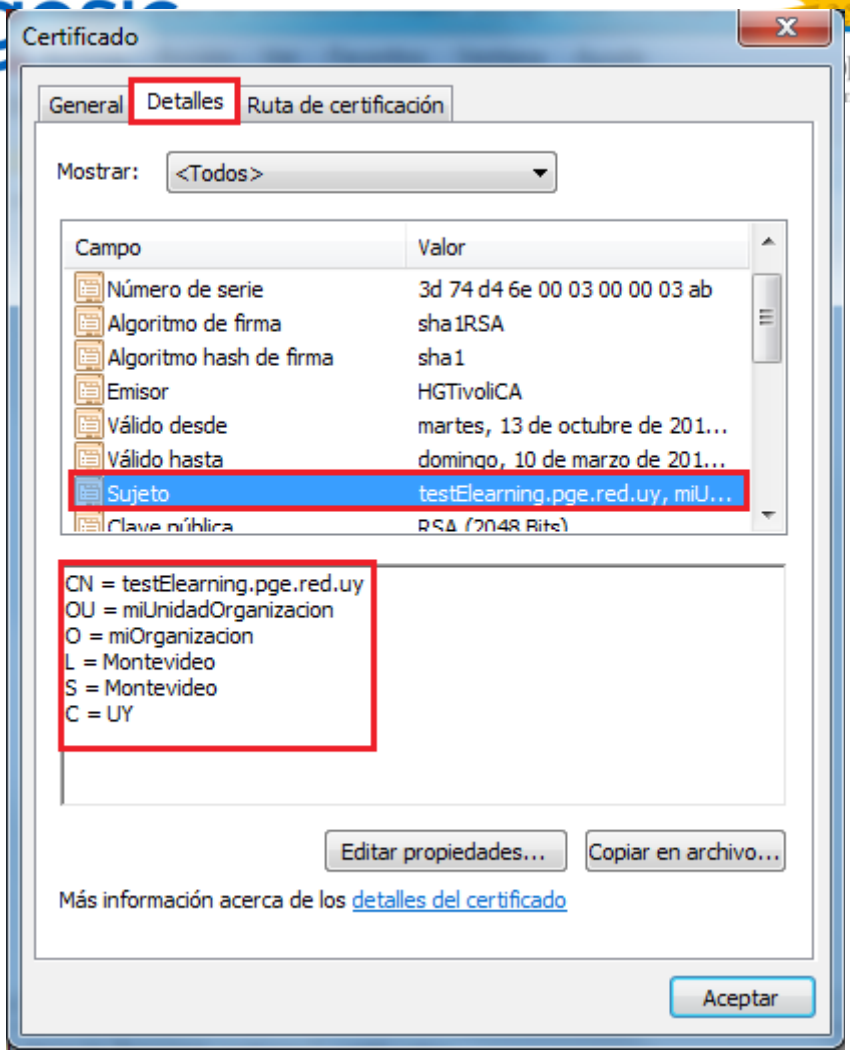
7. Verificar que en el almacén de certificados "*Personal*", aparece el certificado que emitimos.



8. Hacer doble click en el mismo. Se abrirá una ventana "*Certificado*"
9. En la pestaña "*General*" asegurarse que tiene una clave privada.

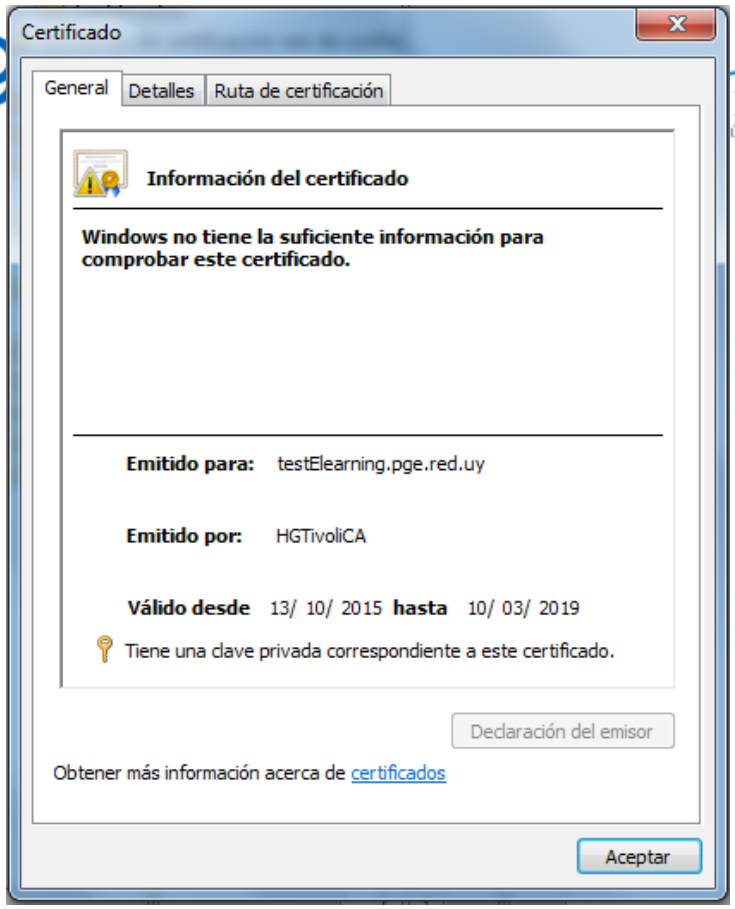


9. En la pestaña "*Detalles*", en el campo "S*ujeto*", corroborar que la información coincide con los datos que ud ingresó antes, cuando hizo la solicitud.

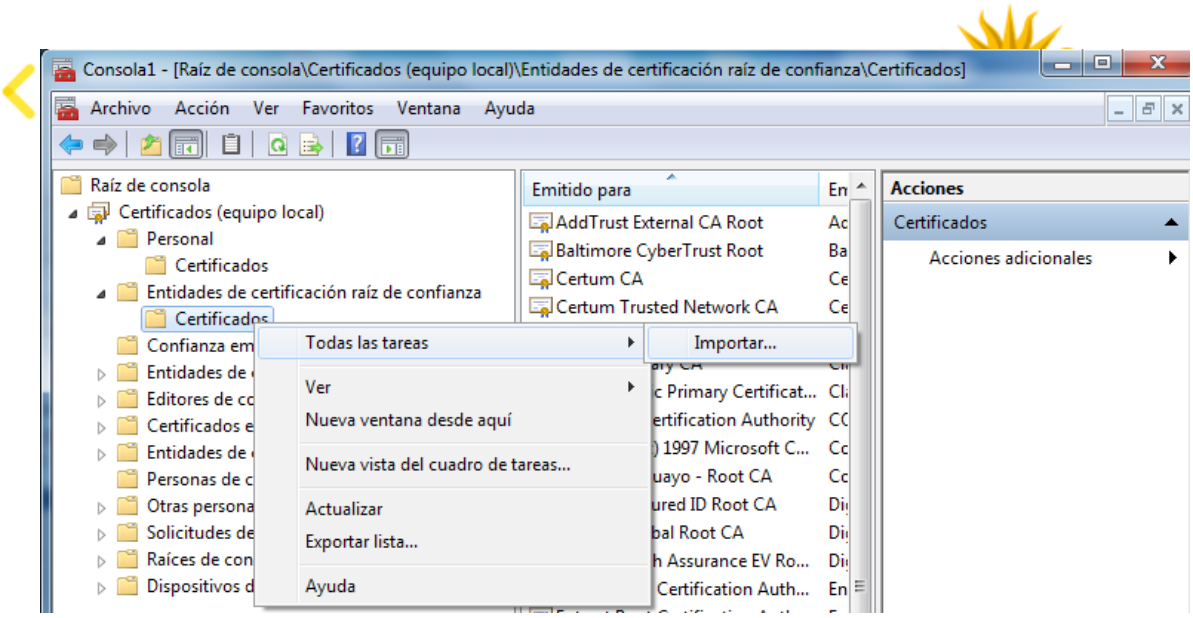


Instalar certificado de la CA

Para completar la instalación del certificado se debe instalar el certificado de la CA que firmó *test_agesic* (HGTivoliCA) en el almacén de *Entidades emisoras raíz de confianza*. De lo contrario, al hacer doble clic en el certificado *test_agesic*, se obtendrá un resultado similar al de la siguiente figura:

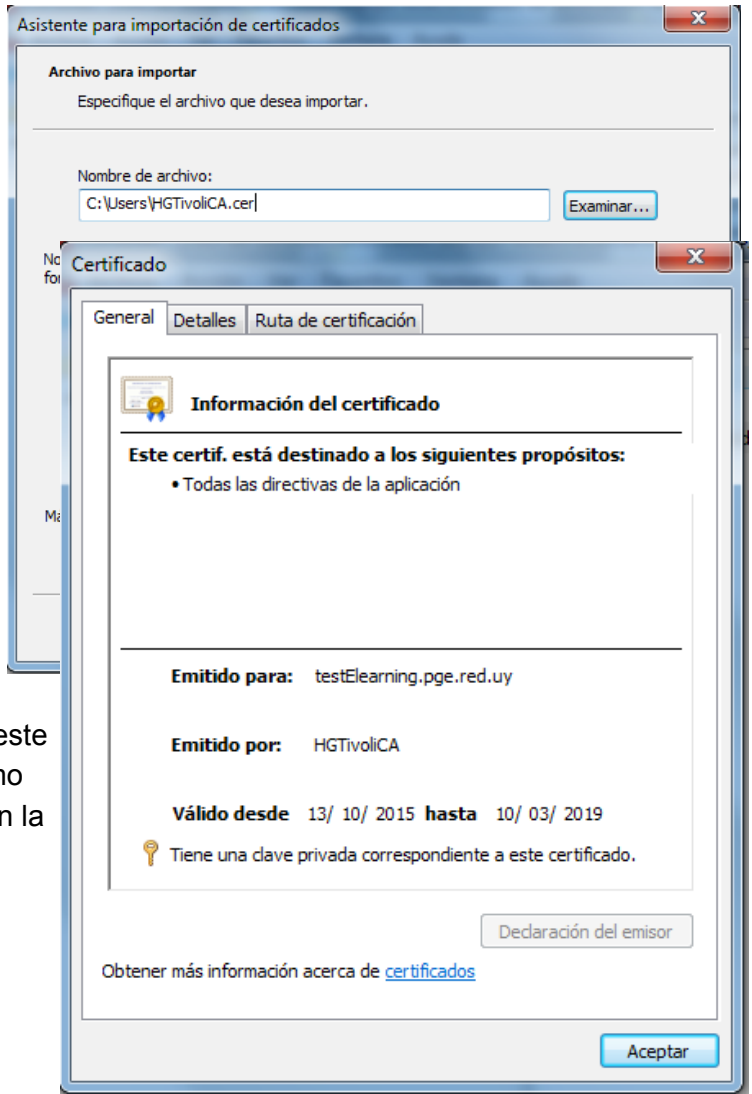


1. Seleccionar *Certificados (equipo local) → Entidades emisoras de raíz de confianza → Certificados y luego clic derecho y seleccionar Todas las tareas → Importar...*



2. En el *asistente de importación* seleccionar el botón siguiente y luego indicar la ubicación del archivo como HGTivoliCA.cer (disponible en el FTP) similar a como se presenta en la figura Error: no se encontró el origen de la referencia.

   Luego, presionar el botón *Siguiente* → *Siguiente* → *Finalizar*. Se debe presentar el siguiente mensaje: “El certificado se importó correctamente.”

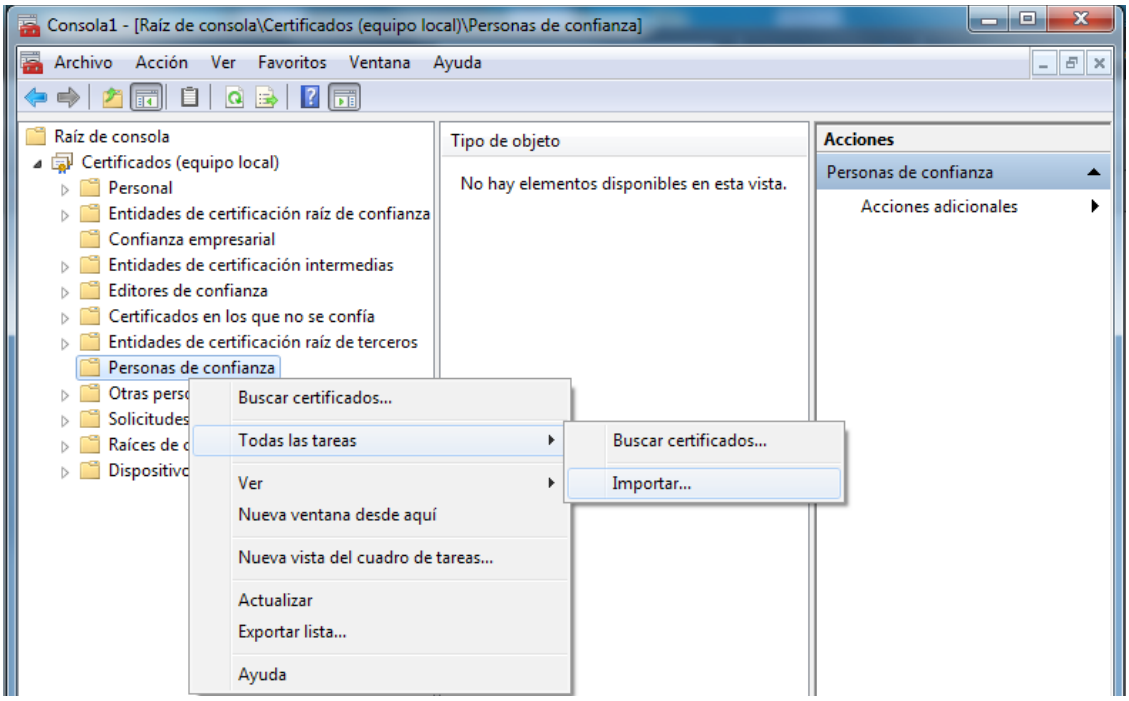


Al abrir nuevamente el certificado test_agesic, este es válido como se muestra en la siguiente:

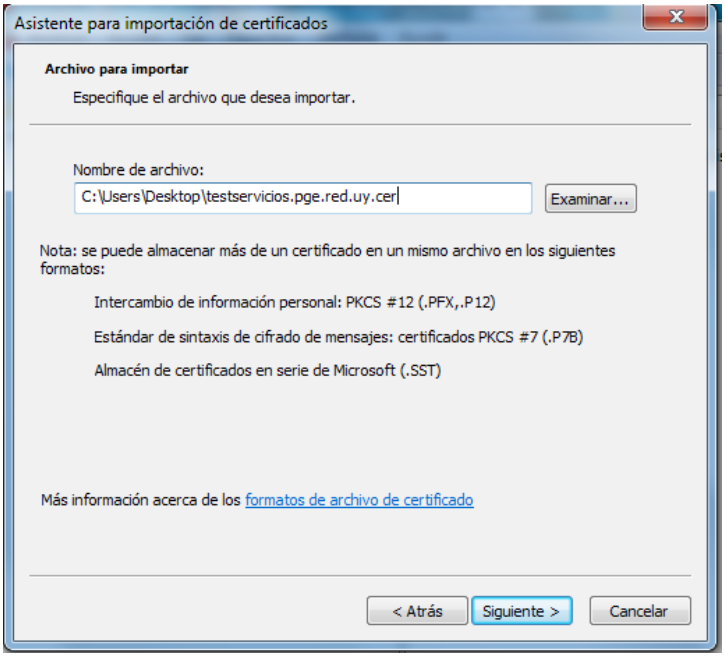
Instalar certificado del servidor (PGE)

En una comunicación SSL el certificado de servidor permite entre otras cosas, autenticar al servidor con el cual se está comunicando.

1. Seleccionar *Certificados (equipo local) → Personas de confianza → Certificados y luego clic derecho y seleccionar Todas las tareas → Importar..., como se muestra en la figura Error: no se encontró el origen de la referencia.*



2. Presionar el botón siguiente y luego indicar la ubicación del certificado, por ejemplo: testservicios.pge.red.uy.cer como se muestra en la siguiente figura. Luego, seleccionar *Siguiente → Siguiente → Finalizar.*



3. Como resultado se debe presentar un mensaje indicando que el certificado se importó de forma correcta.

Instalar certificado del cliente

En este tutorial se utiliza el mismo certificado para firmar el token SAML que para llevar a cabo la comunicación SSL. Por lo que no es necesario realizar ningún paso extra para completar esta sección.