

# Firma de Scripts

## 1. Las firmas digitales

Una firma digital es un «procedimiento» que permite la identificación del firmante y que garantiza la integridad del documento. Las firmas digitales, también denominadas firmas electrónicas, se utilizan en PowerShell para moderar la ejecución de script según la política de ejecución elegida.

Desde un punto de vista conceptual, una firma digital corresponde generalmente a un cifrado, realizado con la ayuda de una clave privada, de forma abreviada también llamada «huella». La huella de un mensaje es el resultado obtenido después de haber aplicado una función de hash al contenido del documento.

En la otra parte de la cadena, el receptor se asegura de que los datos no han sido modificados durante la transferencia efectuando una comparación entre: la huella que acompaña al documento descifrado gracias a la clave pública, y la huella que él mismo vuelve a calcular. Si las dos huellas son idénticas, significa que los datos son íntegros.

## 2. Los certificados

Un certificado es indisoluble de una clave pública, es este elemento quien permitirá asociar una clave a su propietario. Es decir que cuando se descifra una firma con una clave pública, es más que necesario comprobar que dicha clave es la misma que la del firmante. Al igual que un documento oficial, un certificado contiene información sobre la identidad del propietario. Añadir una firma de un script, significa que usted debe estar en posesión de un certificado electrónico de firma, que permite identificar de forma única a la persona que firma el script. Este certificado puede obtenerse de diversas maneras: puede adquirir un certificado de firma en las autoridades de certificación reconocidas, o puede también crearse usted mismo un certificado (certificado «autofirmado»).

### a. Comprar un certificado

Para comprar un certificado, hay que pasar por un organismo de certificación (*Certificate Authority* o CA) que le expedirá un certificado de clase 1, 2 ó 3, definido según un uso y un nivel de protección determinados. Estos certificados están también asociados a una duración y a una cierta garantía en función del precio que puede ir de algunas decenas a varios centenares de euros. Algunos organismos están incluso reconocidos nativamente por Windows, lo que permite desplegar los scripts firmados sin una manipulación especial.

### b. Crear un certificado autofirmado

Crear un certificado autofirmado es, como se puede esperar, la solución más económica. En realidad es incluso gratuita. Esta solución es por tanto la preferida para aquellos que disponen de un presupuesto reducido.

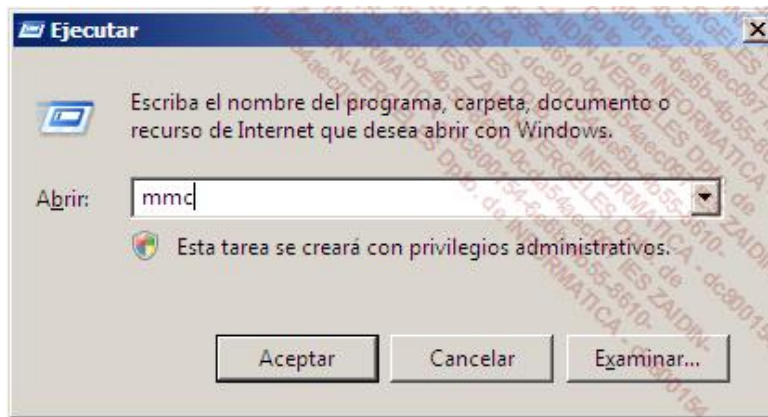
Una de las cosas importantes a saber es que cuando cree usted mismo un certificado, el ordenador en que este certificado ha sido creado, pasa a ser una «autoridad de certificación», y esta autoridad deberá estar aprobada por todos los ordenadores donde se ejecuten los scripts que ha firmado.

Para crear un certificado autofirmado, será necesario en primer lugar descargar e instalar el SDK (*Software Development Kit*) del Framework .NET 3.5 (o 2.0) que está disponible en el sitio de Microsoft.

El SDK contiene numerosas utilidades interesantes, pero ahora la que nos interesa es la utilidad **makecert.exe** que, como su nombre indica, sirve para crear certificados.

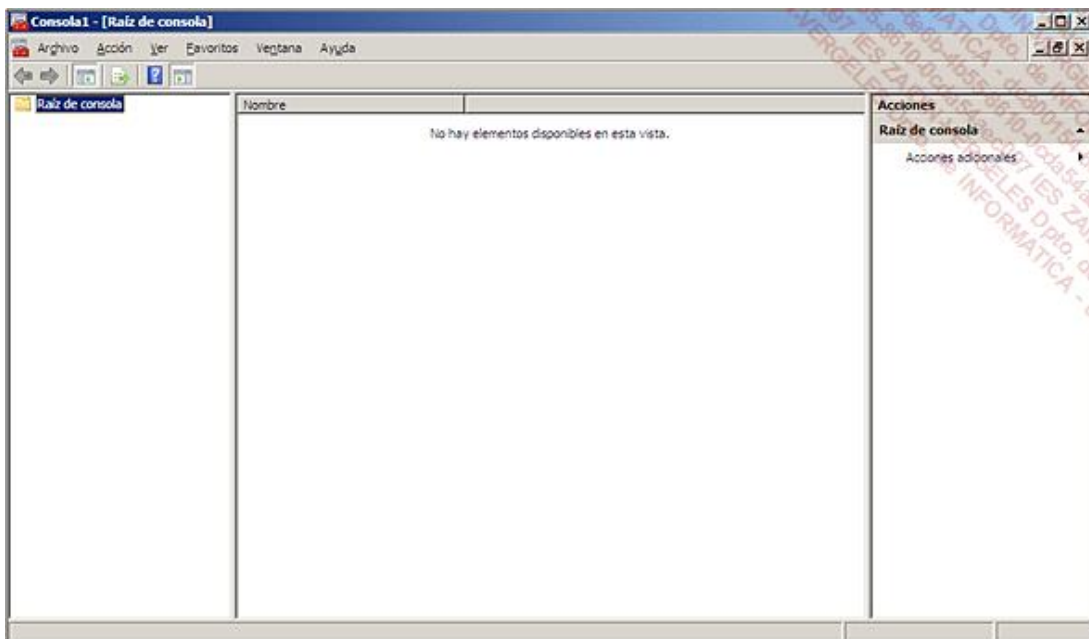
Antes de utilizar el ejecutable **makecert.exe**, le proponemos familiarizarse con la MMC (*Microsoft Management Console*) dando un vistazo a los editores ya aprobados en su ordenador.

Para iniciarla, bastará con teclear **mmc** desde el programa **Ejecutar**.

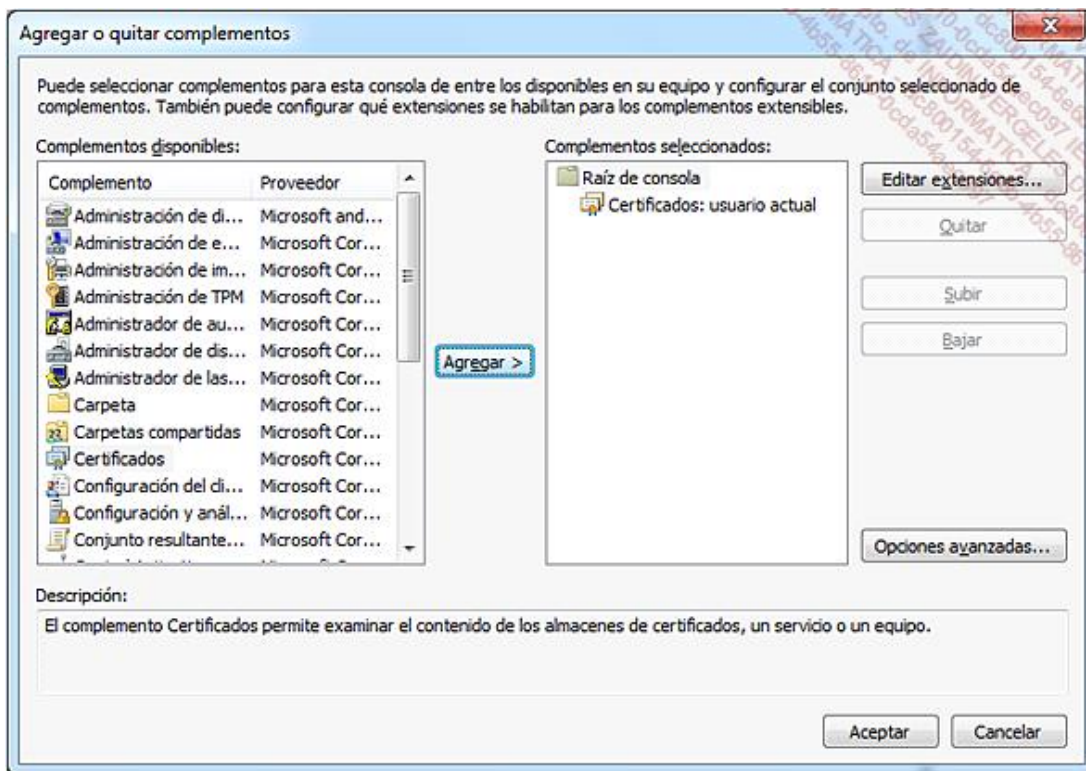


*Interfaz de la aplicación «ejecutar» para iniciar la consola de administración*

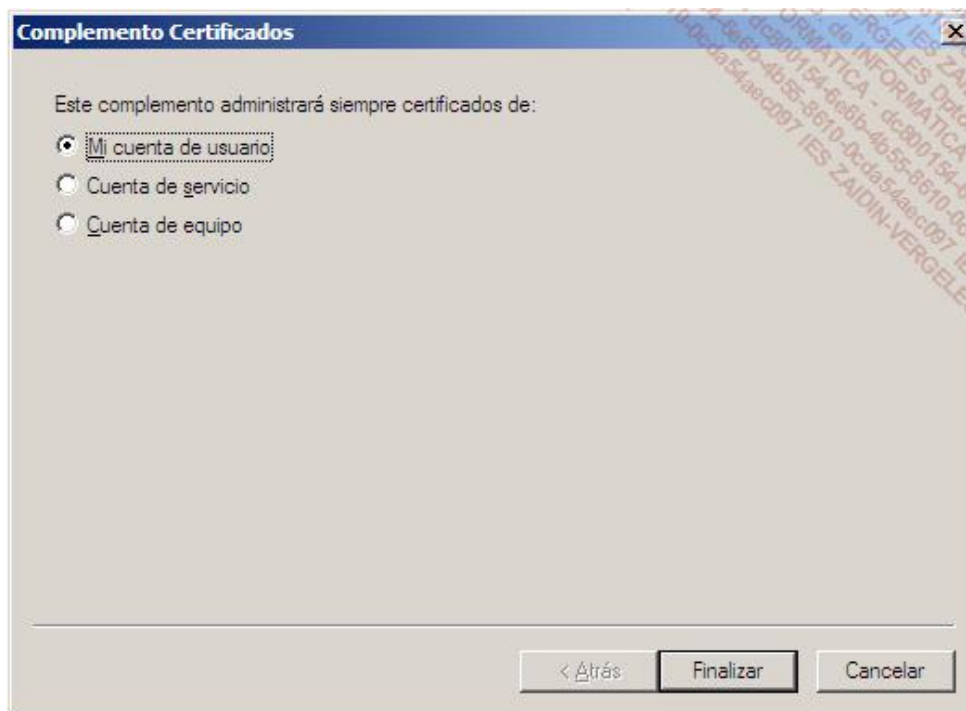
Al abrirla, la consola está vacía y tendrá que añadir lo que llamamos Snap-ins («complementos informáticos conectables»). Para ello, pulse en **Archivo** y **Agregar o quitar complemento ...**.



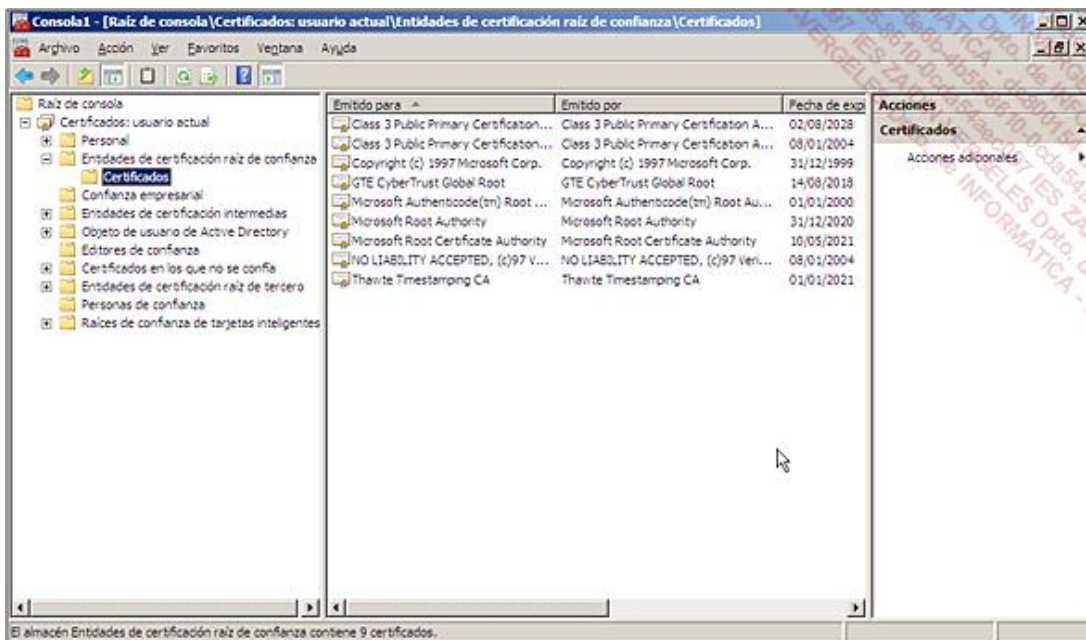
- Seleccionamos el complemento Certificados y pulsamos el botón **Agregar**.



- Finalice la selección marcando **Mi cuenta de usuario** en la pregunta: **Este complemento administrará siempre certificados de:**



Finalmente, con la consola bien configurada, podrá observar sus certificados.



En esta consola, nos referimos principalmente a los certificados personales, a las entidades de certificación raíz de confianza y a los editores de confianza para ver cómo evolucionan a lo largo del tiempo.



No olvide refrescar la consola con el icono apropiado, o la tecla [F5] para ver aparecer las modificaciones que se vayan aportando.

Ahora, después de ver esto, pasemos a cosas más serias.

El primer comando es escribir en modo administrador en el intérprete de comandos del kit de desarrollo:

```
C:\> makecert.exe -n "CN=Certificado Raiz PowerShell" -a sha1 -eku 1.3.6.1.5.5.7.3.3 -r -sv root.pvk root.cer -ss Root -sr localMachine
```

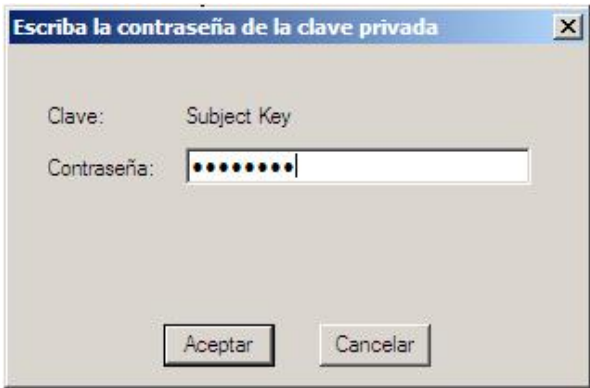
Esta línea de comando llamará a la utilidad **makecert.exe** para crear un certificado de entidad de certificación raíz en su ordenador. Para entender mejor este comando detallaremos las opciones utilizadas:

| Opción | Descripción   |
|--------|---|
| -n     | Especifica el nombre de certificado del sujeto  |
| -a     | Especifica el algoritmo de firma.   |
| -eku   | Inserta en el certificado una lista de identificadores de objetos (OID) para uso mejorado de claves, separados por comas. Por ejemplo, 1.3.6.1.5.5.7.3.3 designa el certificado como utilizable para firmar scripts. Para mayor información, una búsqueda en MSDN con la palabra clave <i>IX509ExtensionMSApplicationPolicies</i> le indicará las diferentes OID que se podrán utilizar en la creación de un certificado. |
| -r     | Indica la creación de un certificado autofirmado.   |
| -sv    | Define el archivo «.pvk» de clave privada asociado al certificado «.cer».   |
| -ss    | Define el nombre del almacén de certificado que va a contener el certificado creado.  |
| -sr    | Define en qué lugar de la base de registro está registrado el almacén de certificado.   |

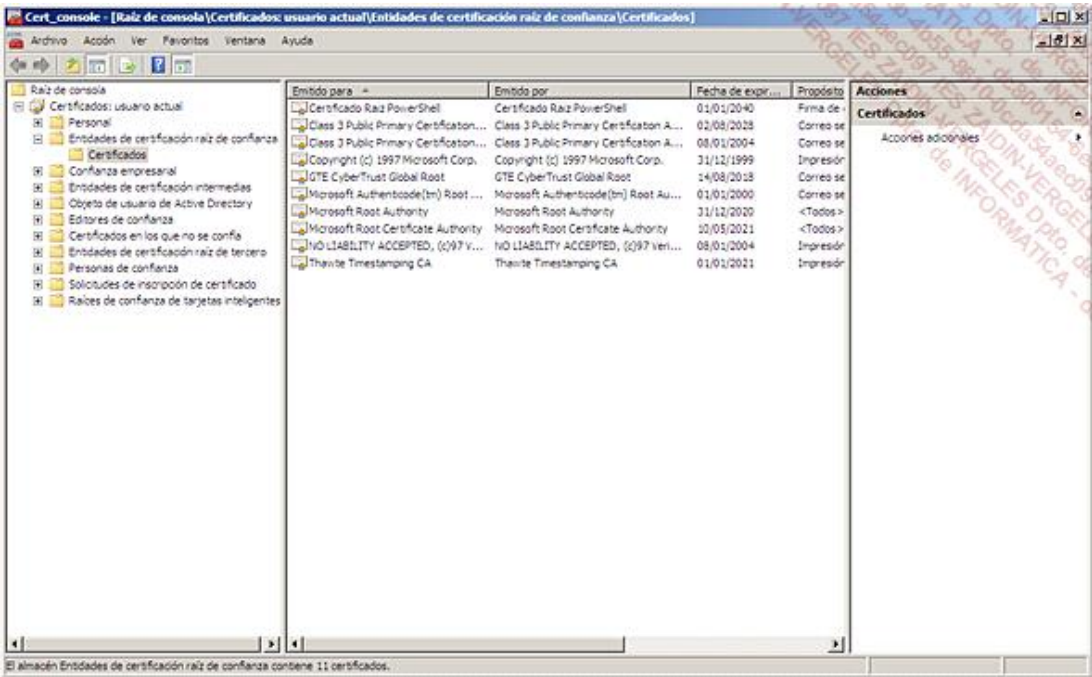
El comando ejecutado, le pedirá introducir la contraseña de su clave privada, clave que será indispensable en la creación del certificado.



Después de pulsar en **Aceptar**, se le pedirá una vez más volver a introducir la contraseña de su clave privada.



Si usted refresca su consola de administración, verá que la nueva entidad certificadora que acabamos de crear está presente en el almacén *Entidades de certificación raíz de confianza*.



Ahora que su ordenador es una autoridad de certificación, vamos a poder crear un certificado personal expedido por esta misma entidad de certificación. Y para ello, debemos utilizar el comando siguiente:



```
C:\> makecert.exe -pe -n "CN=Mí Empresa" -ss MY -a sha1`  
-eku 1.3.6.1.5.5.7.3.3 -iv root.pvk -ic root.cer
```

Este comando contiene nuevas opciones que mostramos en detalle a continuación:

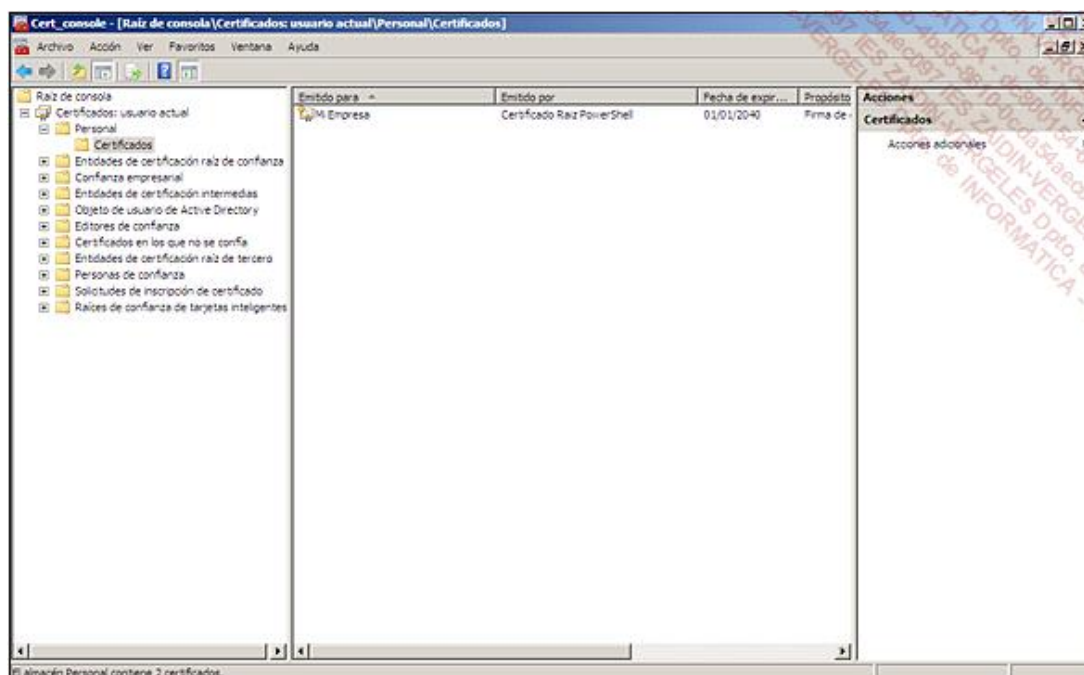
| Opción | Descripción   |
|--------|---|
| -pe    | Permite incluir la clave privada en el certificado. |
| -iv    | Especifica el archivo de clave privada .pvk.        |
| -ic    | Especifica el archivo del certificado «.cer» raíz.  |

- En la interfaz, introduzca la contraseña de su clave privada (la misma que anteriormente) y pulse **Aceptar**.



La operación ha finalizado, usted ha creado un certificado que le permitirá a partir de ahora firmar scripts. Para verificar la creación, vuelva a la consola de administración y actualícela. Seleccione luego en el menú de la izquierda **Personal** y después **Certificados**.

Como podrá constatar, un certificado fue expedido correctamente por la entidad de certificación que hemos creado.



### 3. Firmar su primer script

Para firmar un script, será necesario en primer lugar estar en posesión de un certificado adecuado. Para verificarlo, listaremos todos los certificados contenidos en la unidad «cert:» con el comando: `Get-ChildItem cert: -r -codesign`

Lógicamente, si ha seguido correctamente el desarrollo de «cómo crear un certificado autofirmado», deberá aparecer el certificado siguiente:

```
PS > Get-ChildItem cert: -r -codesign

    Directorio: Microsoft.PowerShell.Security\Certificate ::
CurrentUser\My

Thumbprint                               Subject
-----
63044B1785C5A3ED410E487030A91BD4D99B9800  CN=Mí Empresa
```

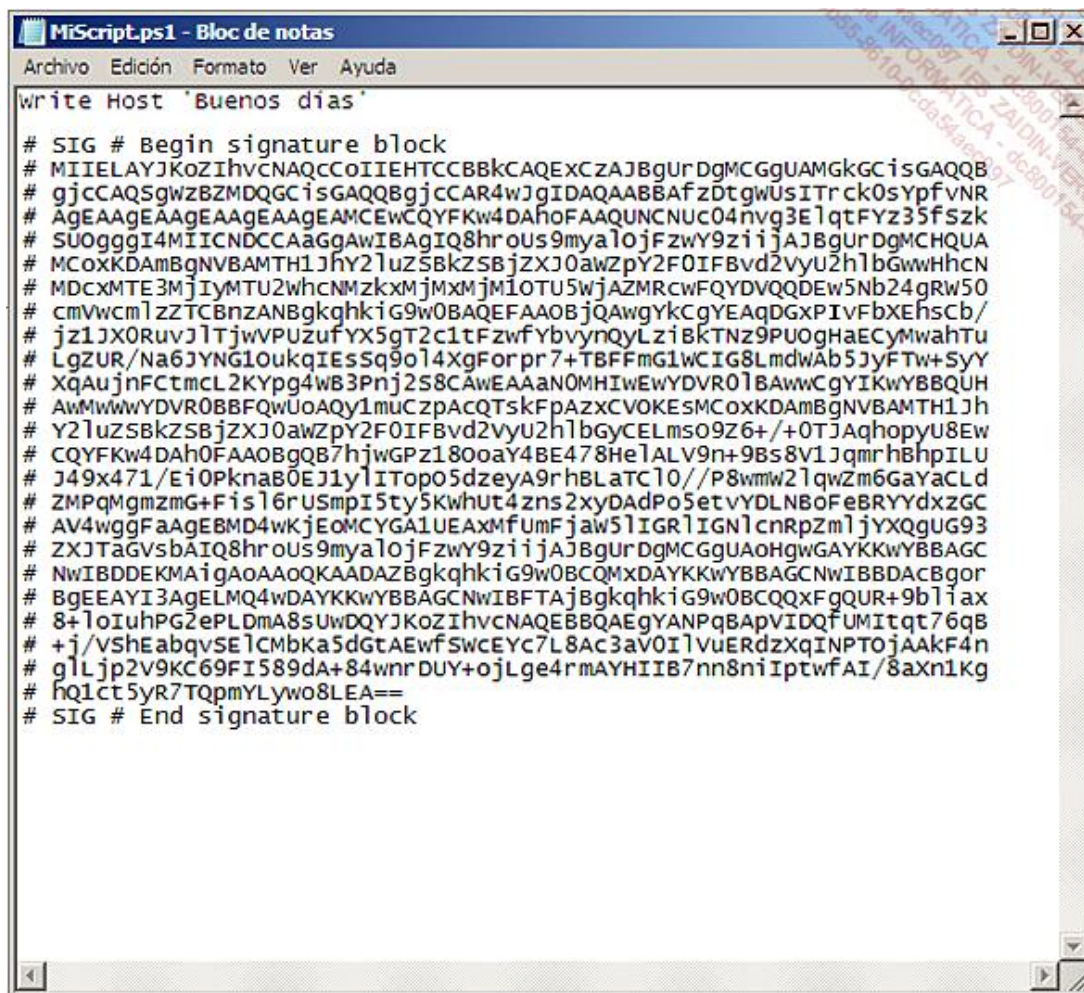
Para la aplicación de una firma digital a un script será necesario utilizar el comando siguiente:

```
PS > $cert = Get-ChildItem cert:\CurrentUser\my -CodeSigningCert

PS > Set-AuthenticodeSignature 'c:\Temp\MiScript.ps1' -cert $cert

Directorio: C:\Temp
SignerCertificate                               Status                               Path
-----
59D92A70DAAEE402A0BDFCFB3C4FD25B7A984C7E  Valid                               MiScript.ps1
```

Después de firmar un script, podrá abrirlo con el Bloc de notas y observar su firma al final del archivo.



Acaba de firmar su primer script.

#### 4. Ejecutar scripts firmados

Cuando ejecute por primera vez un script firmado en una ubicación distinta a aquella en la que usted ha firmado el script, PowerShell muestra el mensaje de error siguiente:

```
PS > .\MiScript.ps1
No se puede cargar el archivo C:\Temp\MiScript.ps1.
Se ha producido un error interno de encadenado de certificados.
```

Para poder ejecutar un script en modo **AllSigned**, no sólo bastará que el script esté firmado, sino que también estemos en posesión del certificado raíz y que el emisor del script esté aprobado. Si está en posesión o ha importado el certificado raíz (ver cómo importar un certificado en el apartado acerca del despliegue de certificados), entonces faltará aprobar el editor. Ya que de lo contrario PowerShell mostrará esto:

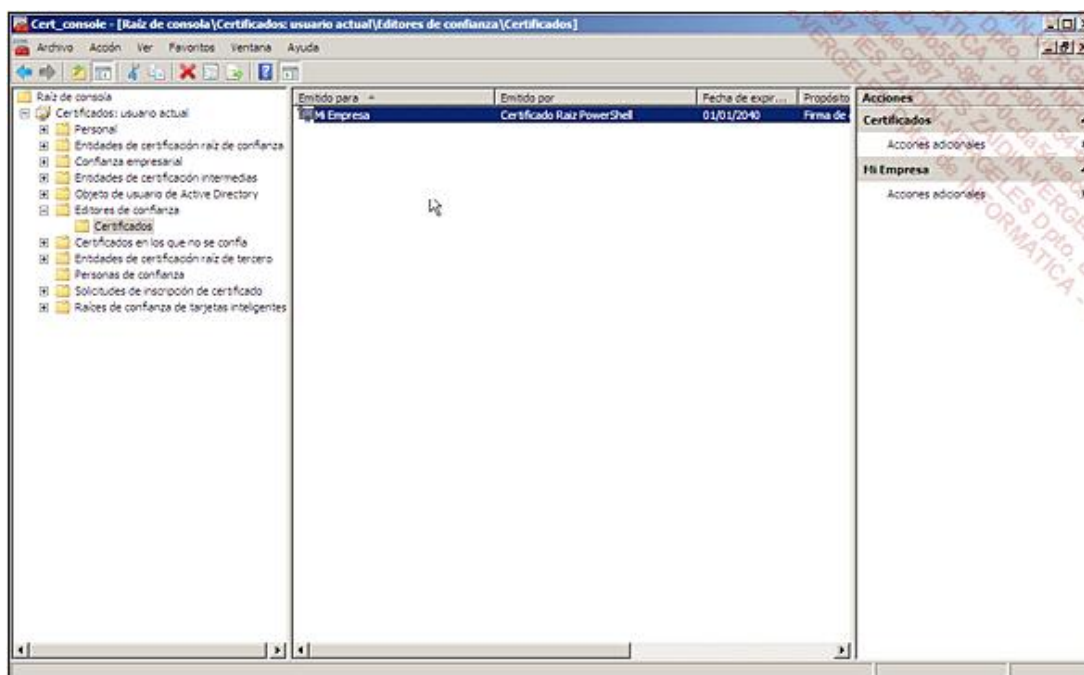
```
PS > .\MiScript.ps1

¿Quiere ejecutar el código de esta entidad no aprobada?
El archivo C:\Temp\MiScript.ps1 está publicado por CN=Mi Empresa y
no está aprobado en su sistema. Únicamente ejecute scripts procedentes
de entidades aprobadas.[O] No ejecutar nunca [N] No ejecutar
[U] Ejecutar una vez [E] Ejecutar siempre [?]
```

Contestando **[E] Ejecutar siempre** a la pregunta anterior, el editor del script pasará a ser un editor aprobado.



- Para consultar la lista de los editores aprobados, seleccione en la consola de administración el almacén **Editores de confianza** y después pulse en **Certificados**.



➤ Atención, asegúrese de estar en modo **AllSigned** para verificar la ejecución de sus scripts firmados.

## 5. Desplegar sus certificados

Como acaba de ver, la ejecución de un script firmado requiere dos cosas:

- Estar en posesión de un certificado de la entidad de certificación raíz.
- Y que su editor esté aprobado.

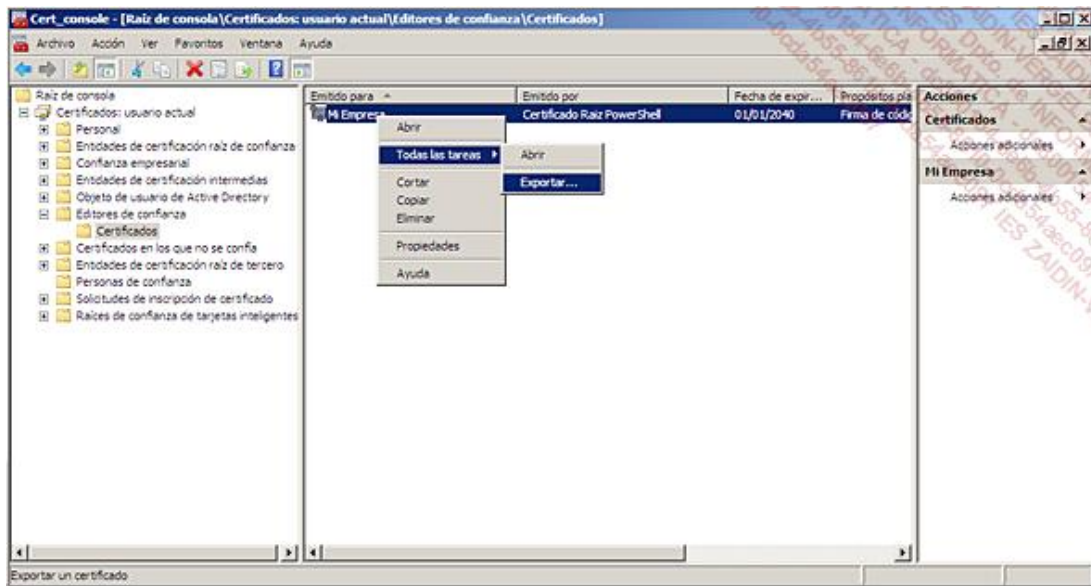
O, si usted ha optado por una política de seguridad que consiste en seleccionar el modo **AllSigned** en todos los puestos informáticos, deberá:

- Desplegar el certificado de la entidad de certificación raíz.
- Aprobar el editor (es decir, usted mismo) de sus scripts vía la consola PowerShell escogiendo la opción **[E] Ejecutar siempre**, o sea, desplegar el certificado que se encuentra en el almacén **Editores de confianza**.

Por supuesto, si dispone de algunas máquinas, esto no planteará un problema excesivo. Pero en el caso de que planea desplegar los scripts PowerShell en un parque informático de mediano o gran tamaño, esto sería diferente.

El despliegue de certificados se hace en dos fases. En primer lugar, la exportación del certificado desde su ordenador, y luego su importación a todos los puestos de trabajo que ejecuten sus scripts firmados.

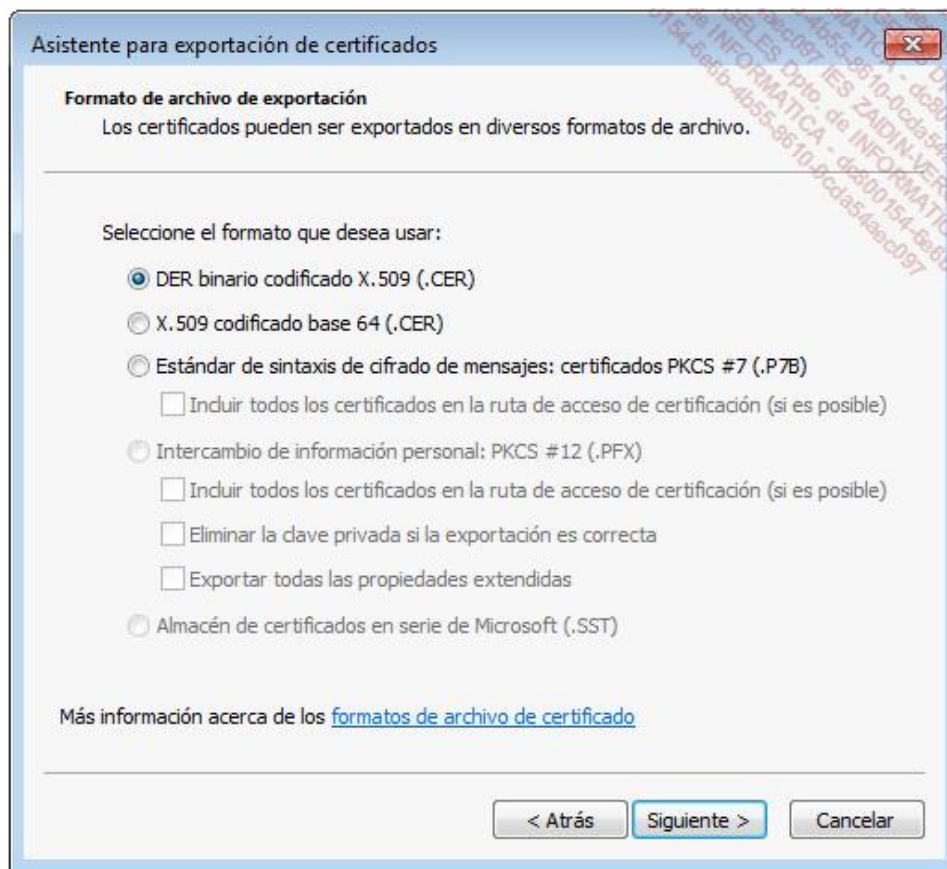
- Para exportar el certificado, selecciónelo y pulse el botón secundario de su ratón, después seleccione **Todas las tareas y Exportar**.



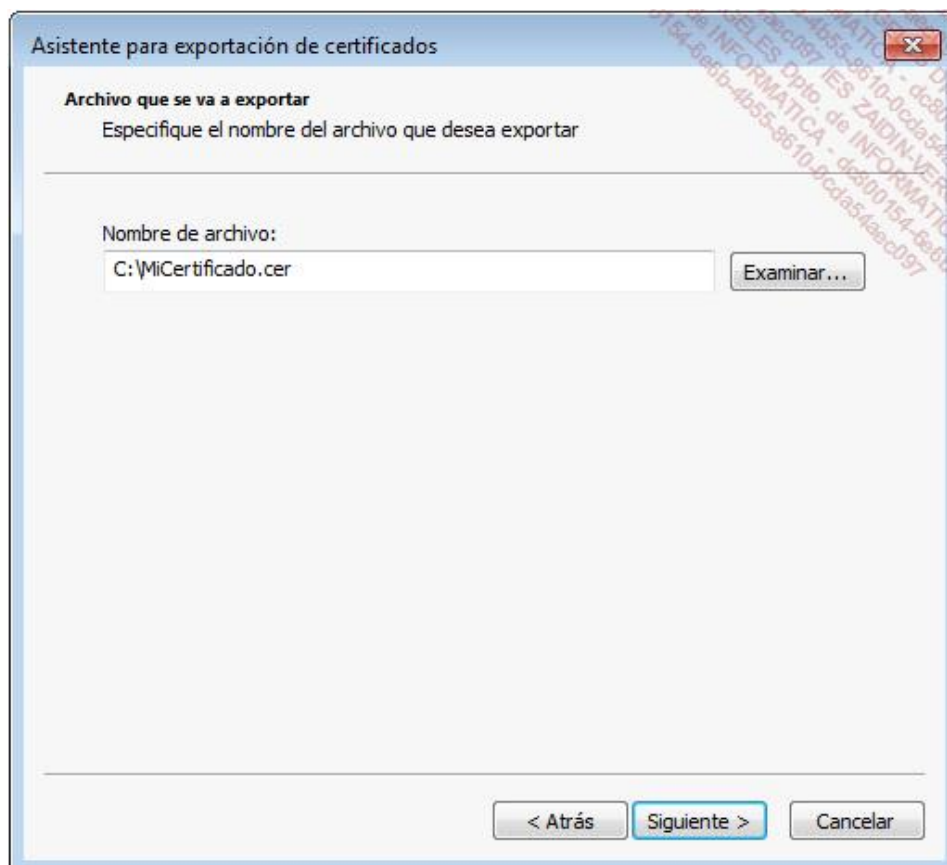
- Se inicia el asistente de exportación, pulse **Siguiente**.



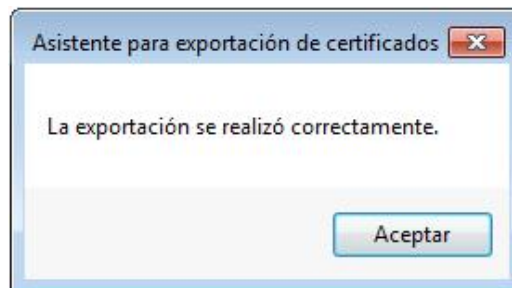
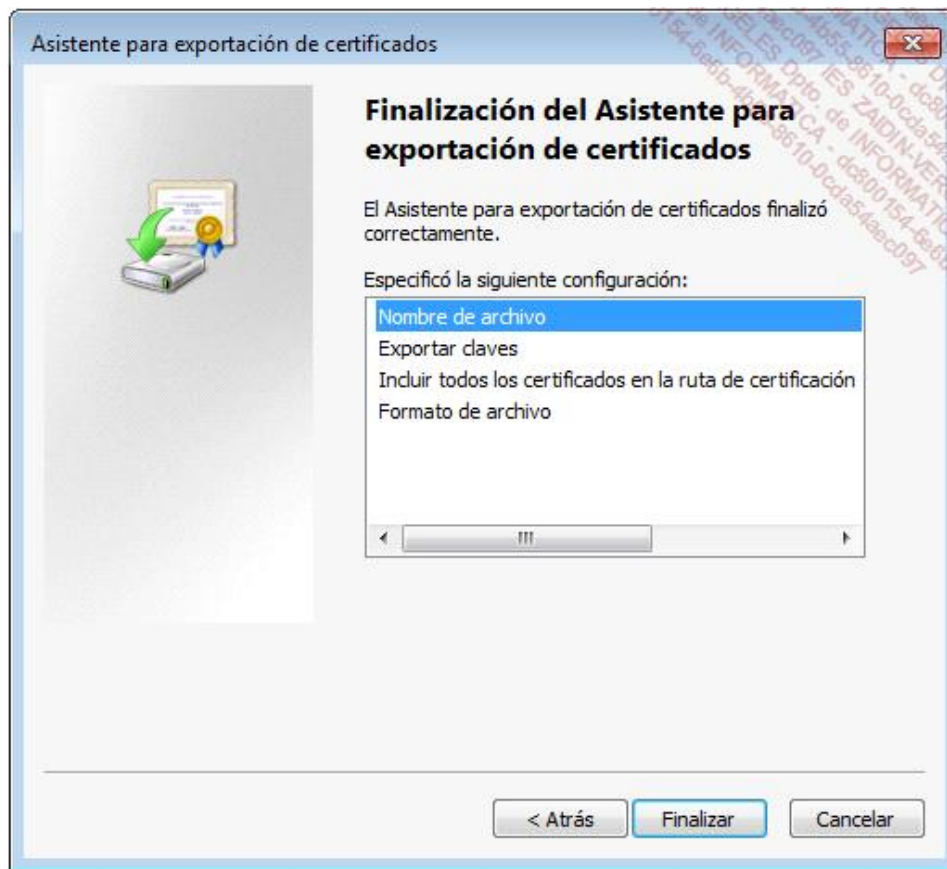
- Seleccione el formato de exportación, y pulse **Siguiente**.



- Asigne un nombre, y pulse **Siguiente**.



- Para finalizar, pulse **Finalizar**.

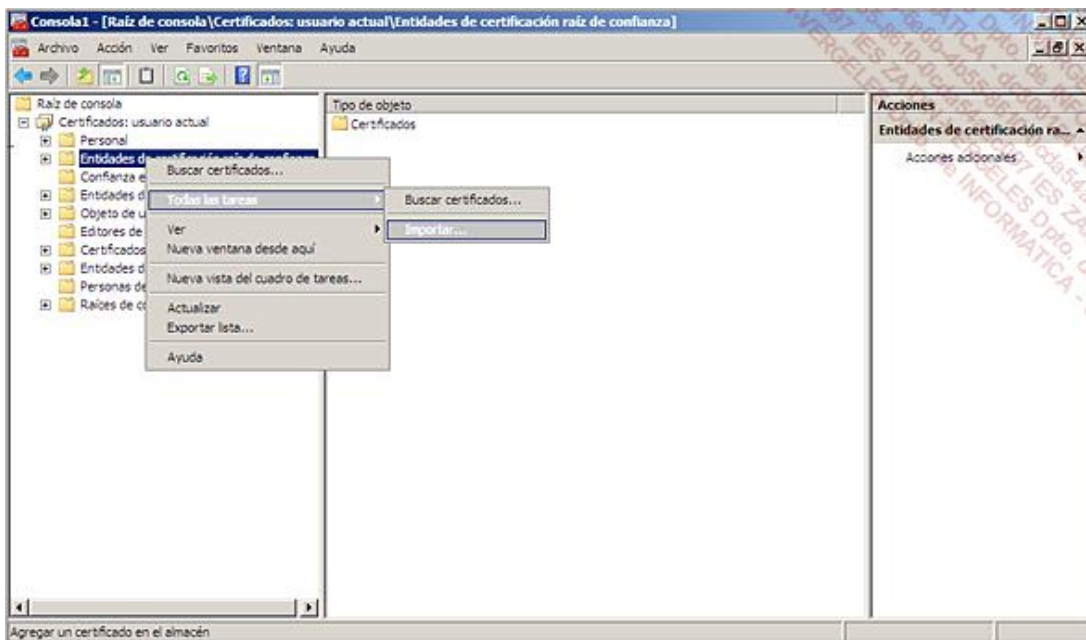


Acabamos de exportar un certificado. Sólo faltará realizar la importación en los puestos de trabajo de destino. Para ello tenemos dos soluciones: importación manual, o la importación con directivas de grupo (GPO) de Active Directory (esta solución requiere que sus puestos de trabajo sean miembros de un dominio).

#### **a. Importación manual**

La importación manual no es ni más ni menos que la operación inversa de la exportación.

- Para importar un certificado, seleccione con el botón secundario del ratón **Certificados** en el almacén escogido, y seguidamente pulse en **Todas las tareas** e **Importar**.

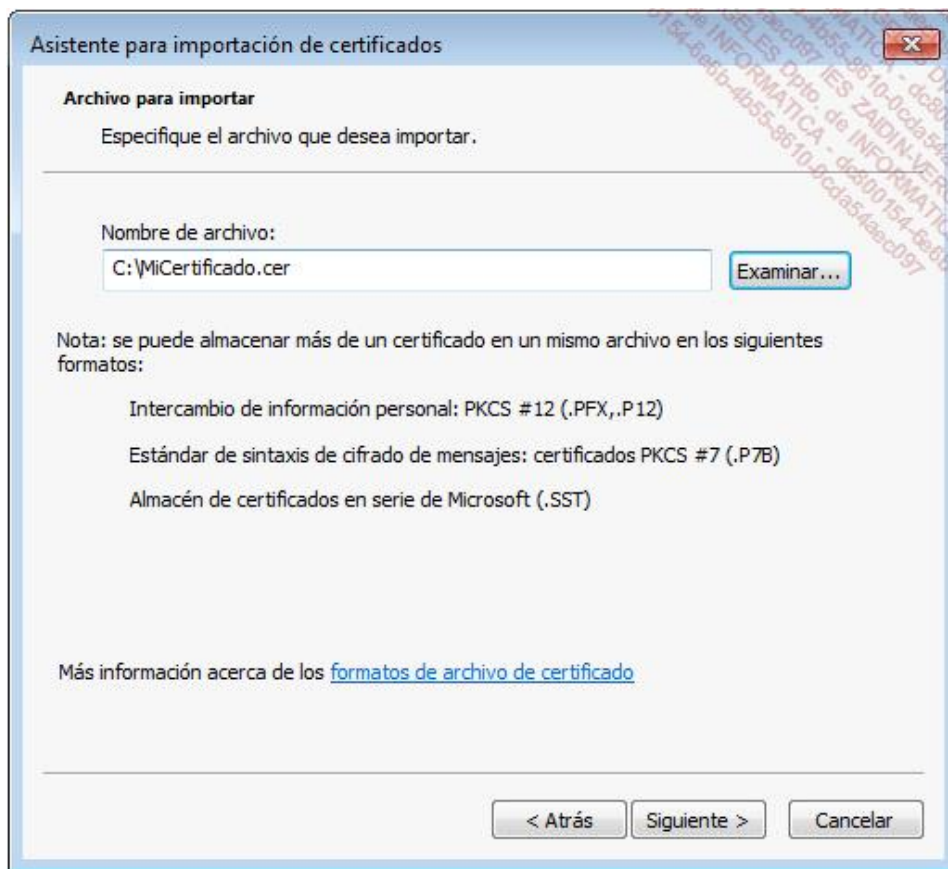


- En esta ocasión se iniciará el asistente de importación, pulse en **Siguiente**.

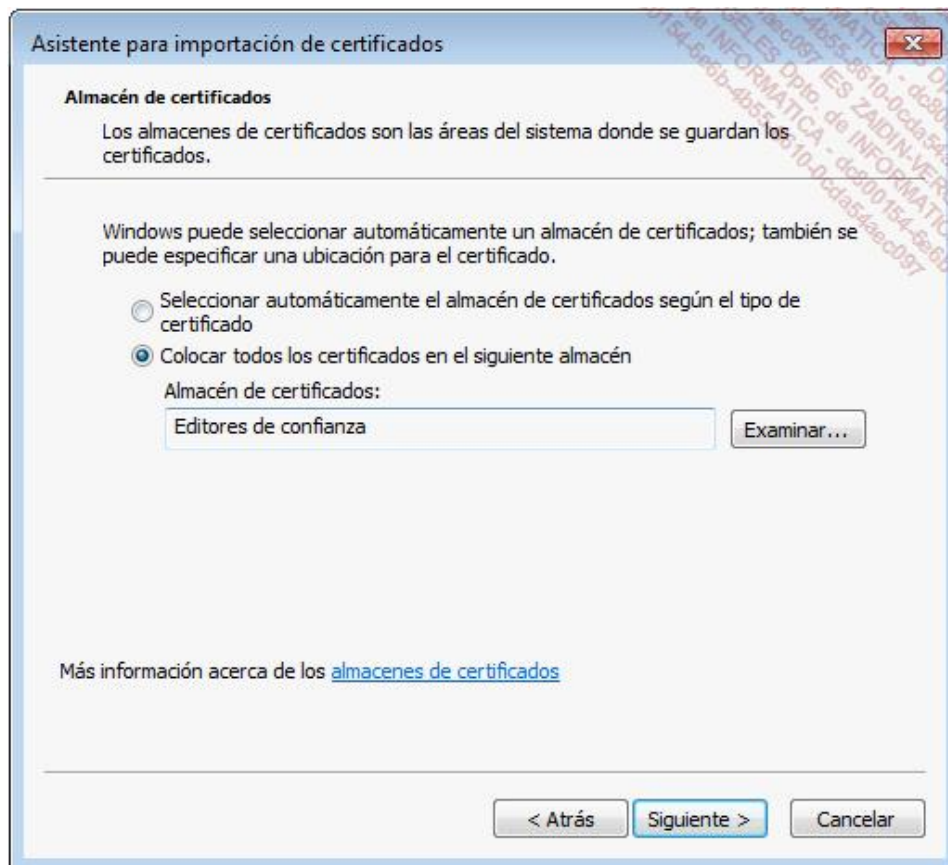


- Pulse **Examinar** para seleccionar su certificado, una vez encontrado y seleccionado, pulse **Siguiente**.

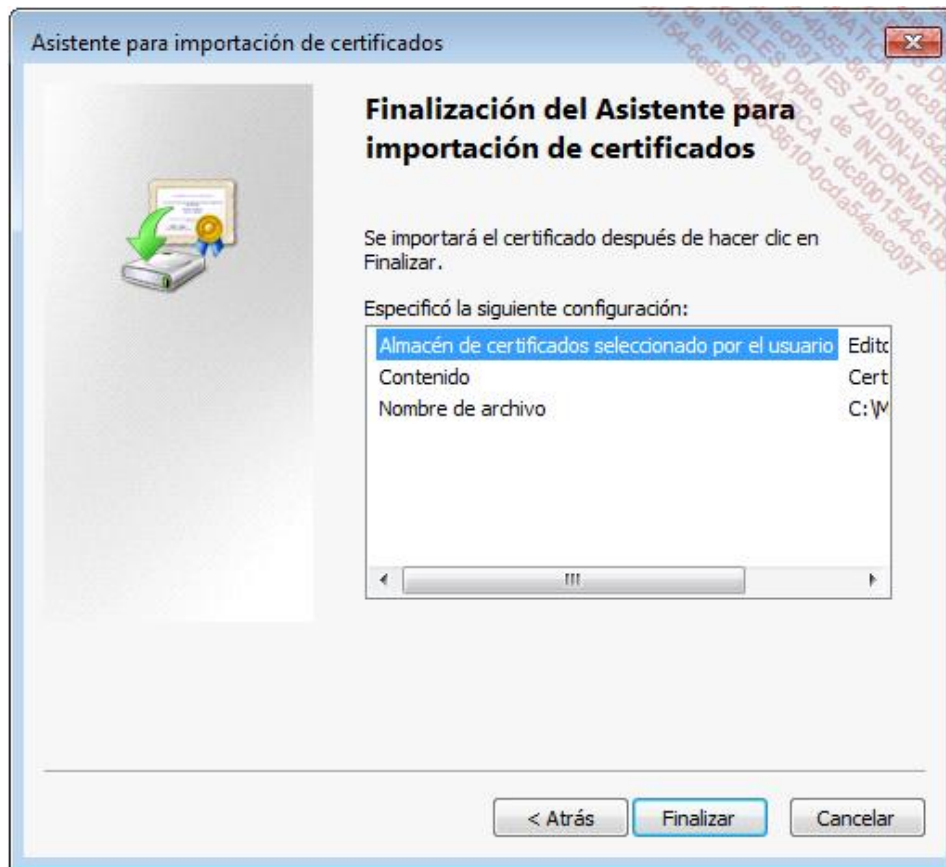




- Asigne el almacén de certificados en el que desea ver su certificado publicado, seleccione el almacén **Editores de confianza** y pulse **Siguiente**.



- Verifique la información en la ventana de fin del asistente, después pulse en **Finalizar**.

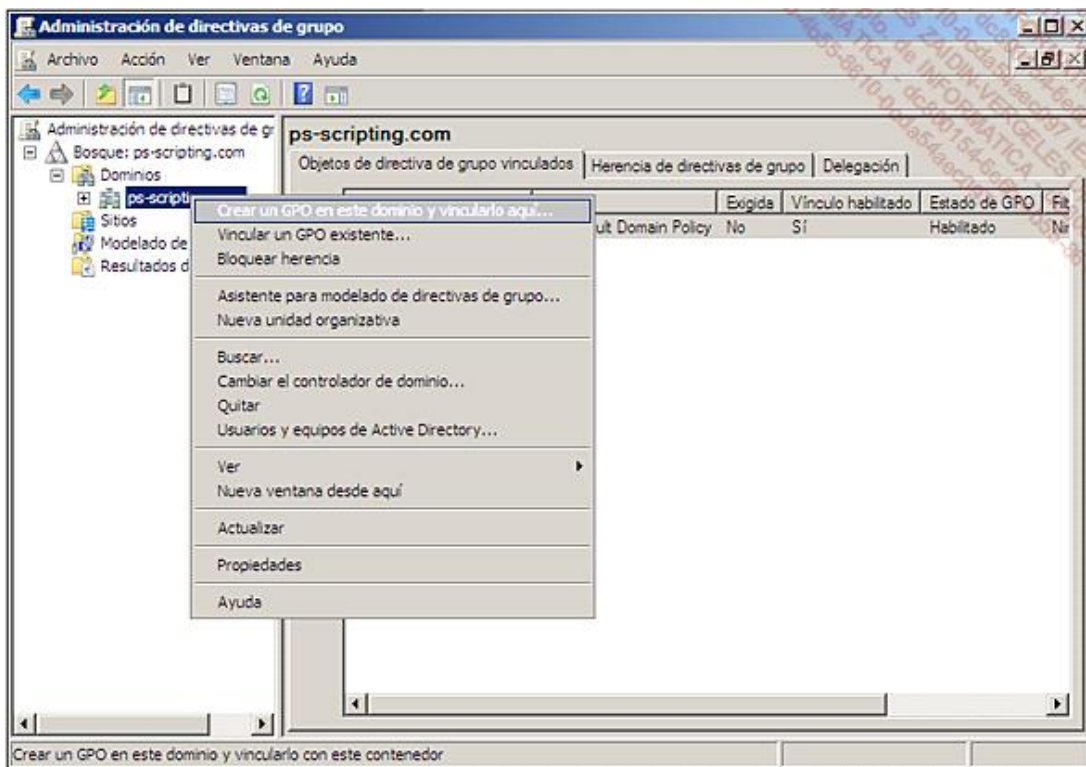


Su certificado está ahora disponible en el almacén correspondiente.

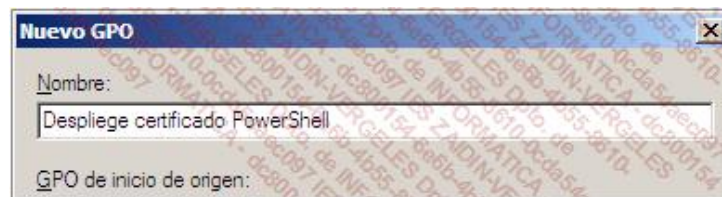
## b. Importación por GPO

La importación por GPO es la solución menos restrictiva cuando se dispone de un parque de máquinas considerable, o geográficamente distribuidas. Sin embargo, la importación por GPO requiere que cada máquina sea miembro de un dominio perteneciente al mismo dominio Active Directory.

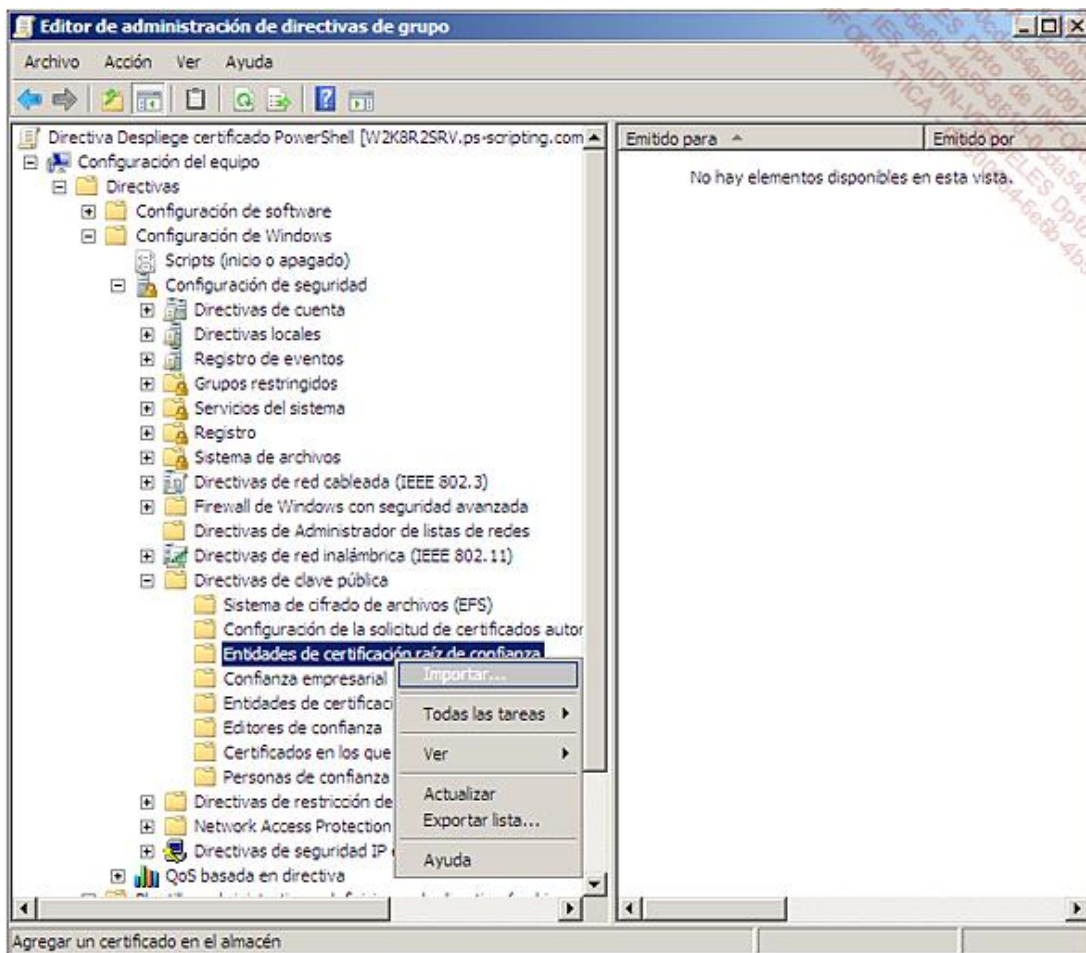
- Para importar un certificado por GPO en Windows Server 2008, abra la consola de **Administración de directivas de grupo**. Después, en la consola, seleccione el dominio y pulsando el botón secundario del ratón seleccione **Crear un GPO en este dominio y vincularlo aquí...**



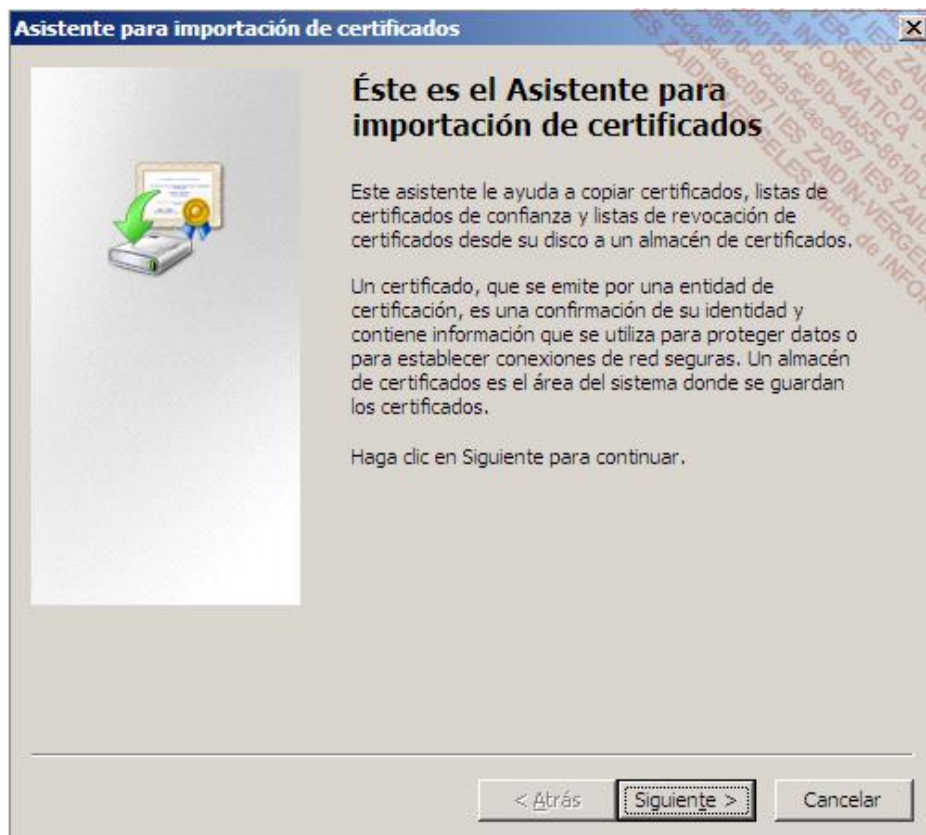
- De un nombre a la directiva de grupo, por ejemplo **Despliegue certificado PowerShell**.



- Seleccione la directiva creada, pulse el botón secundario del ratón y seleccione **Modificar**.
- Se mostrará la consola de administración de Directivas de grupo. Pulse el botón secundario del ratón en **Configuración del equipo** - **Configuración de Windows** - **Configuración de seguridad** - **Directivas de clave pública** - **Entidades de certificación raíz de confianza**. Seleccione **Importar...**

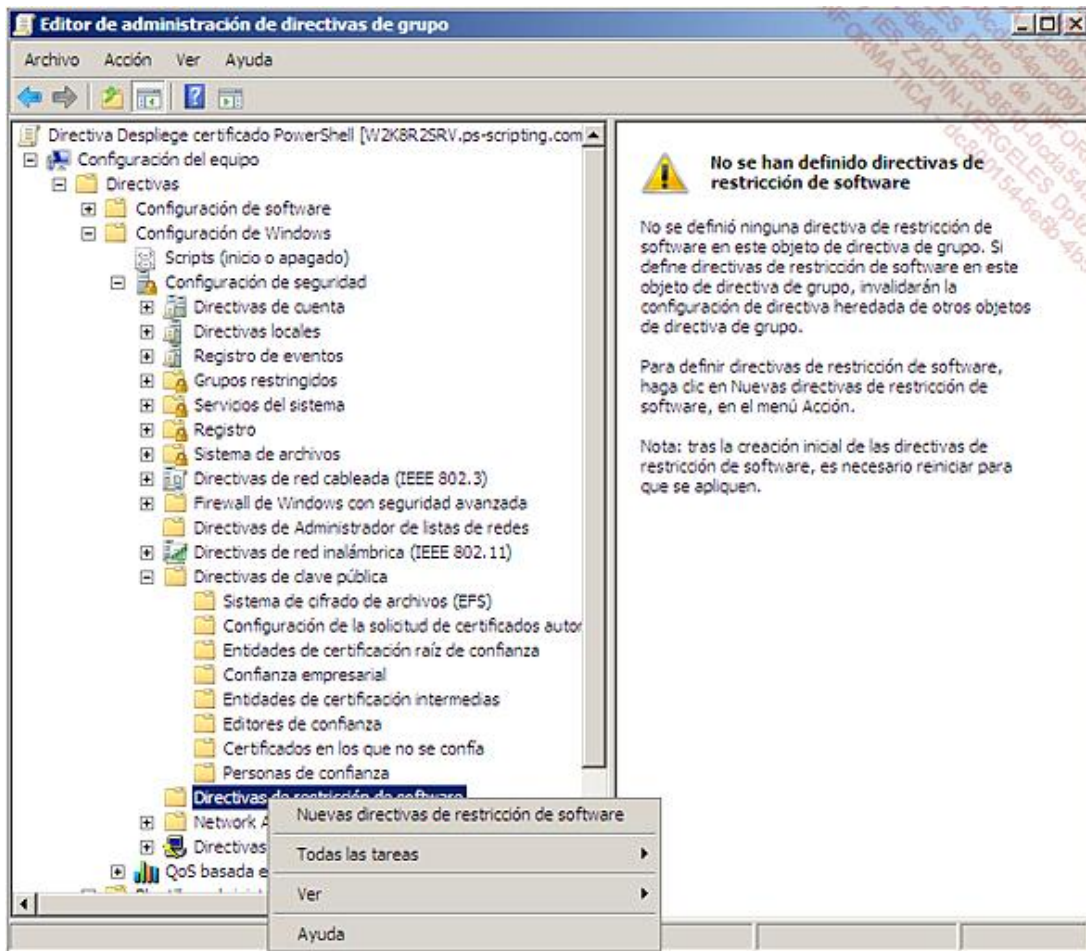


- El asistente de importación le guiará para importar el certificado de entidad de certificación raíz.



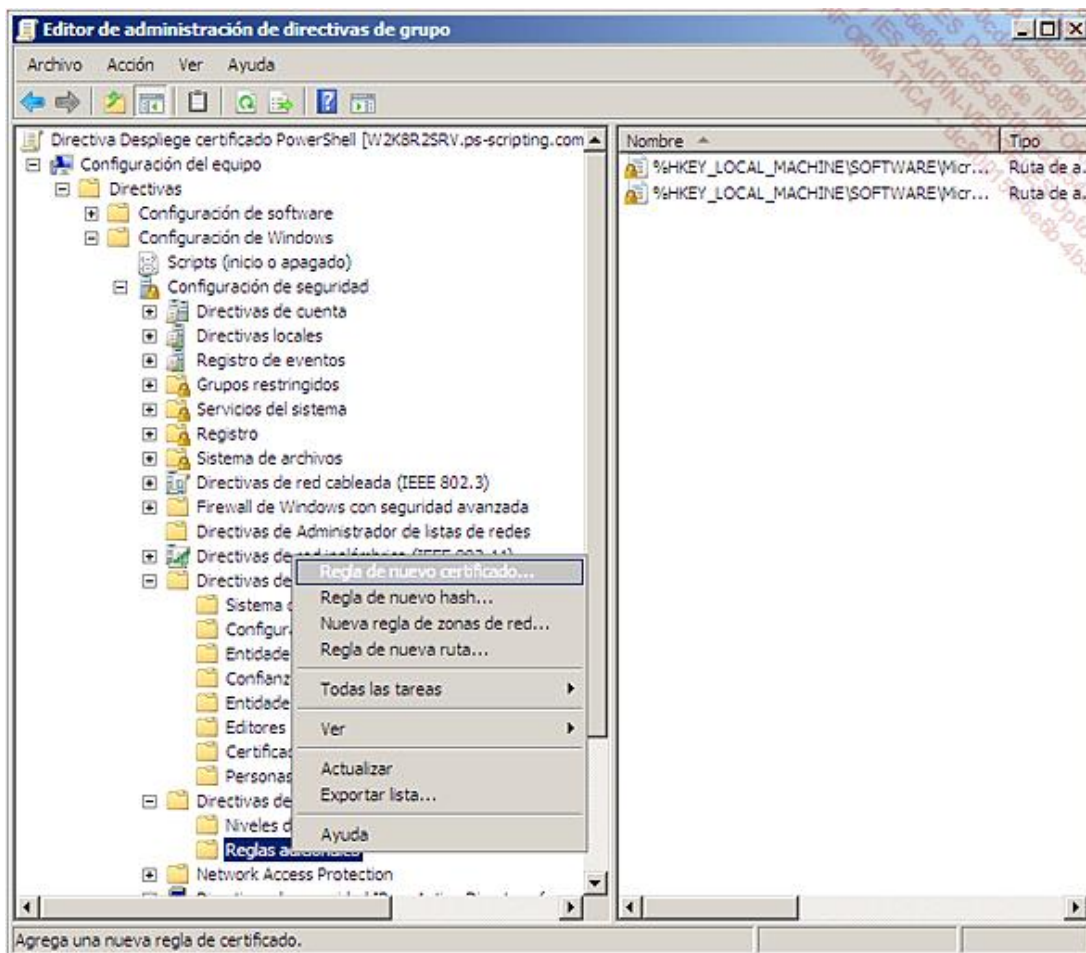


- Una vez se ha importado el certificado raíz, se debe permitir también a todos los puestos de trabajo para aprobar automáticamente el editor de la firma. Y para ello, haga clic en el botón secundario del ratón en **Configuración del equipo - Configuración de Windows - Configuración de seguridad - Directivas de restricción de software**. Después seleccione **Nuevas directivas de restricción de software**.



Aparecerán dos nuevos subdirectorios. Haga clic en el botón secundario del ratón en **Reglas adicionales** y seleccione **Regla de nuevo certificado**.






- En el editor de la nueva regla, seleccione **Examinar** para buscar su certificado. Después escoja el nivel de seguridad **No permitido**. Pulse en **Aplicar** seguido de **Aceptar**.

La aplicación del nivel **No permitido** tendrá por efecto determinar los permisos de acceso al software en función de los permisos de acceso del usuario.

**Regla de nuevo certificado**

General


 Use reglas para invalidar el nivel de seguridad predeterminado.  
Haga clic en Examinar para seleccionar un certificado y después seleccione un nivel de seguridad.

Nombre de sujeto del certificado:

Para ver los detalles del certificado seleccionado, haga clic en Detalles.

Nivel de seguridad:

Descripción:

 Nota: las reglas de certificado tendrán un efecto negativo en el rendimiento del equipo.

Obtener más información acerca de las [directivas de restricción de software](#)

- Responda **Sí** a la pregunta que se le plantea con el fin de activar las reglas de certificados.

Sus certificados se han desplegado correctamente sin tener que realizar ninguna operación en los puestos de trabajo, únicamente será necesario reiniciarlos para que tengan en cuenta la nueva directiva de grupo.