MANUAL:

Solicitud e Instalación de un Certificado de Servidor Seguro en Windows 2003 Server con IIS 6.0

ÍNDICE.

Título **Página**

1. Objetivos……...3
2. Solicitud……3
3. Instalación……...10
4. Configurar los certificados intermedios……...14
5. Configuración básica y comprobación de funcionamiento……..16

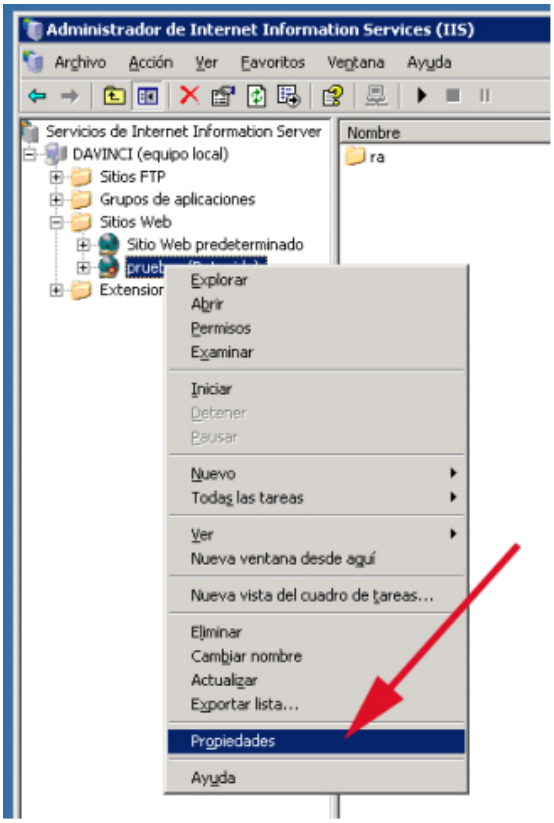
1. OBJETIVOS

El objetivo de este documento, en primer lugar, es informar a los clientes de AC Camerfirma que vayan a solicitar un certificado de servidor seguro, de los requisitos técnicos para realizar dicha solicitud.

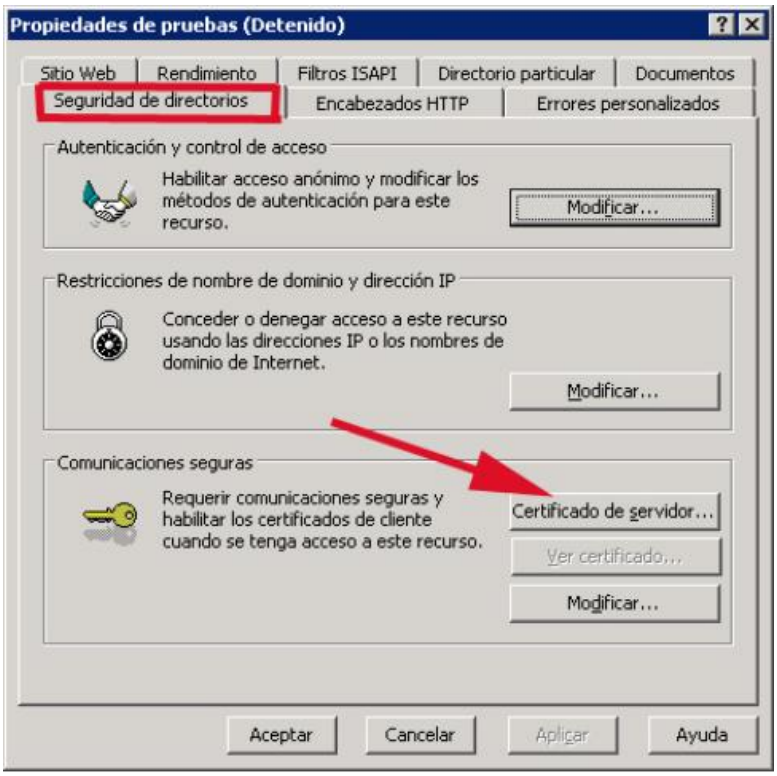
Posteriormente se explicará la instalación del certificado obtenido en un sistema con Windows 2003 Server con IIS 6.0.

2. SOLICITUD

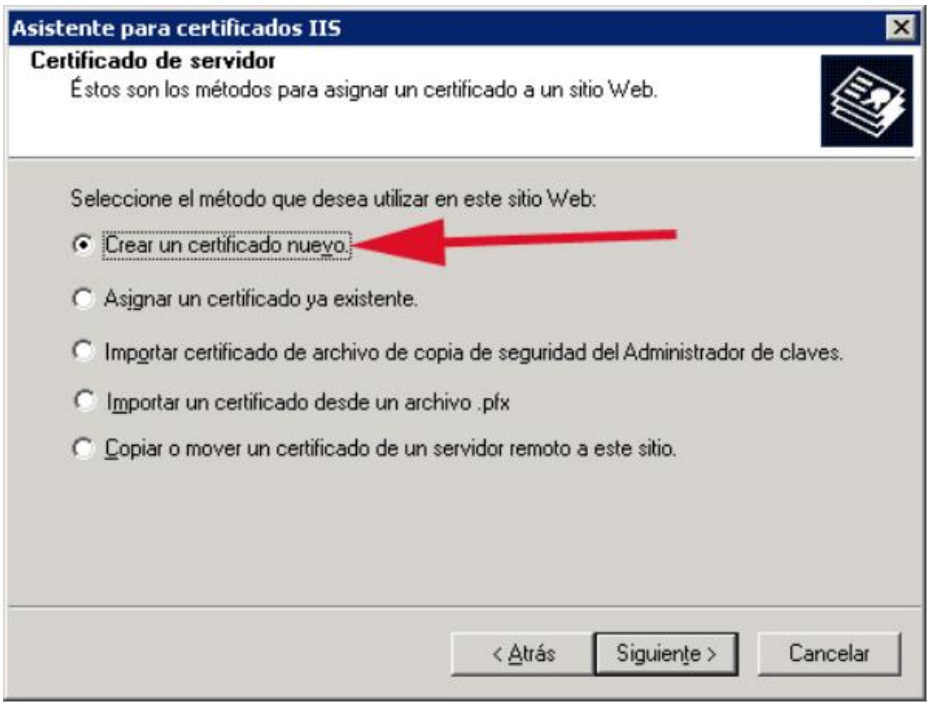
El primer paso es acceder a la administración de Internet Information Server: pulse sobre el botón de *Inicio*, seleccione *Todos los programas*, *Herramientas Administrativas* y después *Administrador de Internet Information Services (IIS)*. Cuando se abra la ventana correspondiente, haga clic en el nombre de su servidor y pulse el botón derecho del ratón para acceder a sus propiedades.



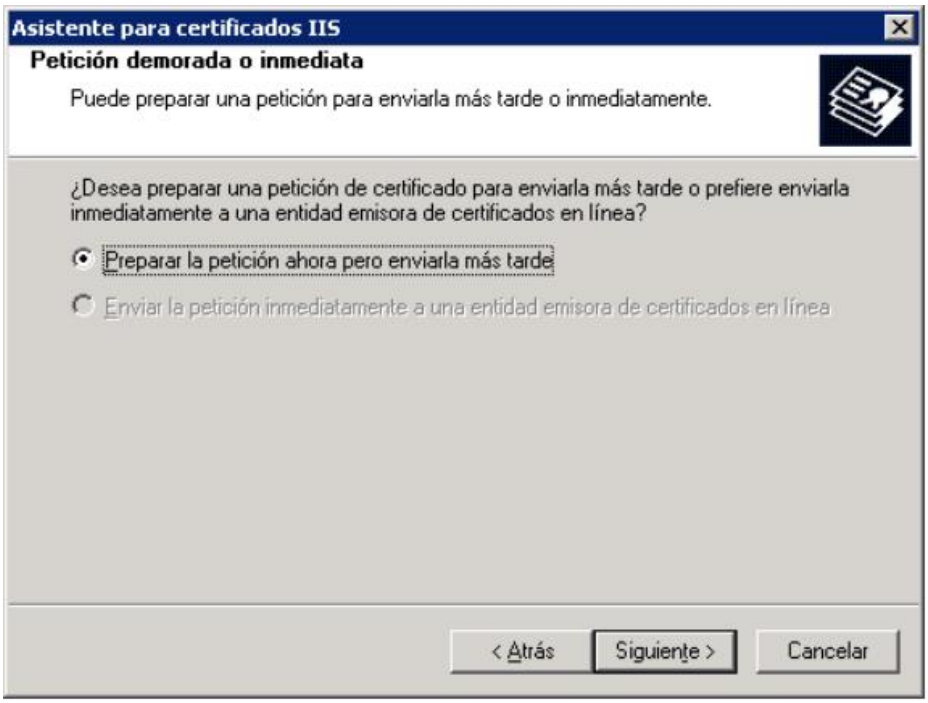
Posteriormente, seleccione la pestaña *Seguridad de directorios* en la parte superior de la ventana. Después, en el apartado *Comunicaciones seguras*, debe seleccionar *Certificado de servidor*, tras lo que se ejecutará el asistente de solicitud de certificado.



Deberemos seleccionar la opción de crear un certificado nuevo y pulsar *Siguiente*:

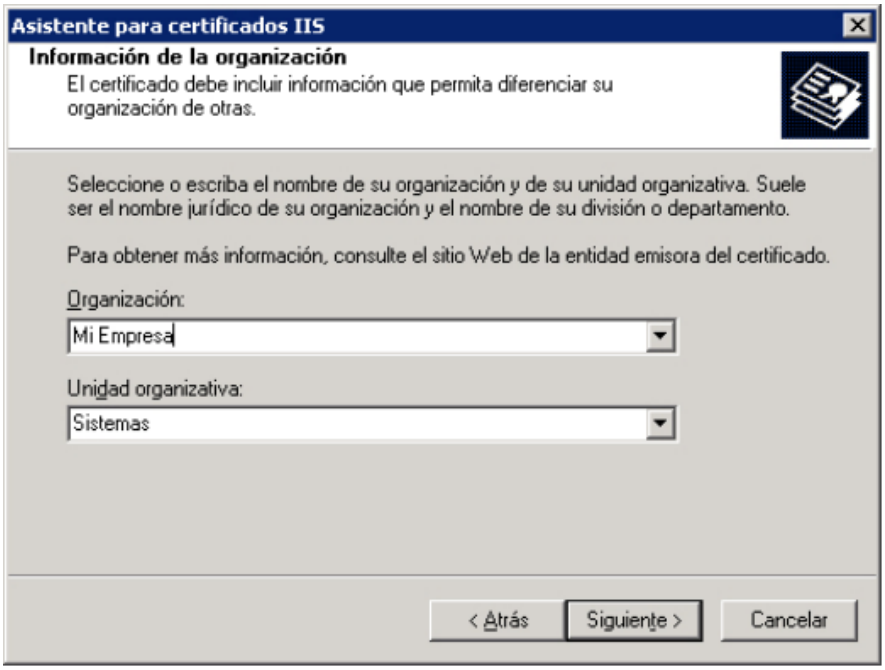


Después, debemos seleccionar *Preparar la petición ahora pero enviarla más tarde*.

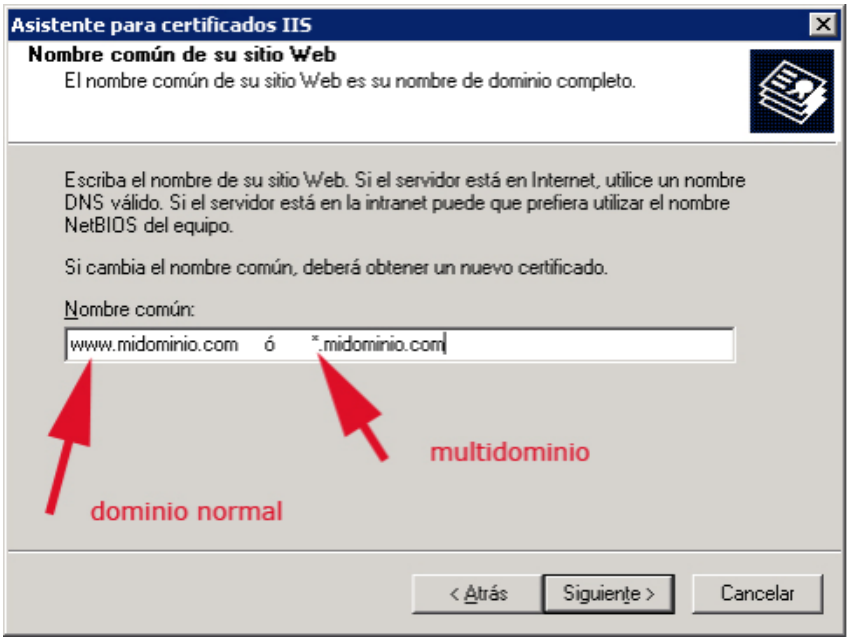


El asistente solicitará un nombre descriptivo para el certificado. Este nombre no estará incluido en el certificado. Únicamente será un alias para facilitar la gestión de los certificados. Debe seleccionar una longitud de clave mayor o igual a 2048 bits.

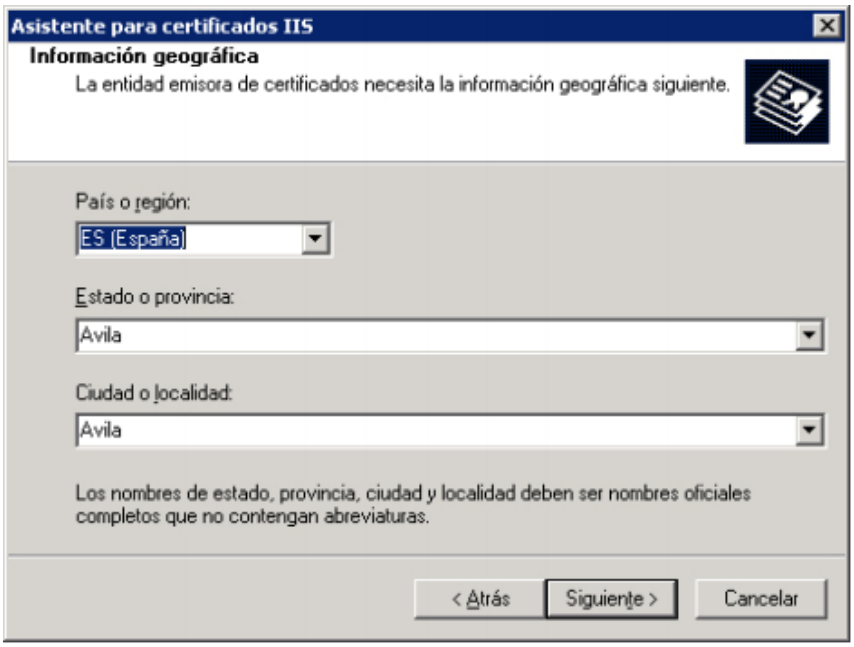
En la siguiente pantalla introduciremos datos como el nombre de la empresa, y el departamento:



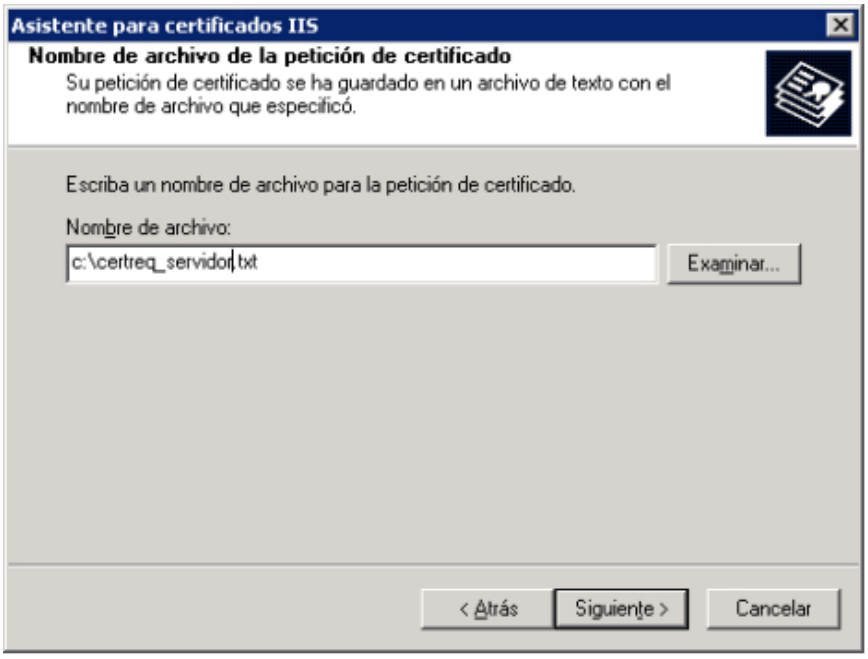
En la siguiente pantalla del asistente, deberá escoger el nombre común del certificado. Esto es, el nombre del dominio para el que vayamos a solicitar el certificado de servidor seguro. Por ejemplo: www.mi-dominio.com o facturacion.mi-dominio.com. Si va a necesitar más de un subdominio quizá deba valorar de solicitar un certificado multidominio, por ejemplo: *.mi-dominio.com.



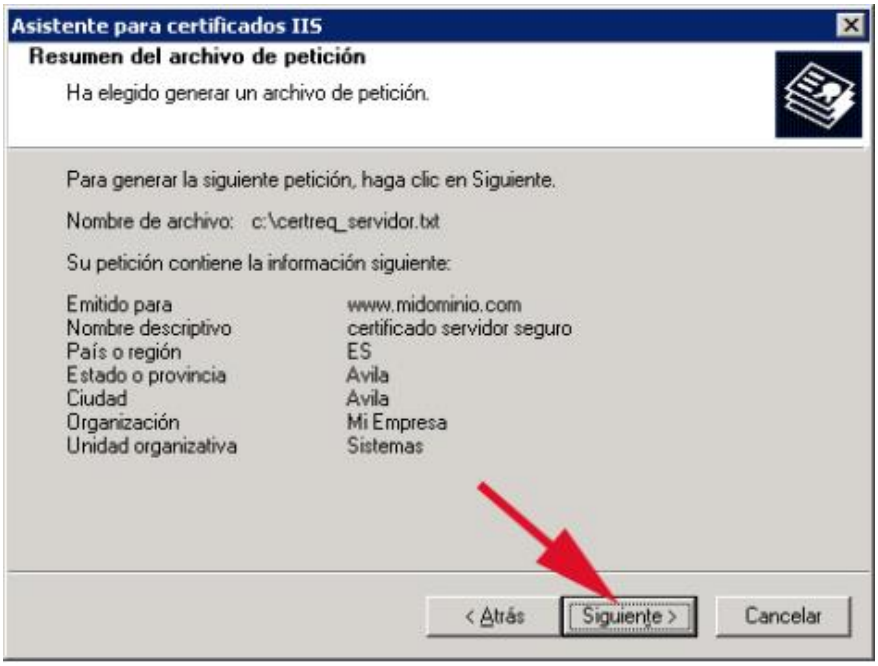
Después, debemos introducir datos relativos a la ubicación de la empresa.



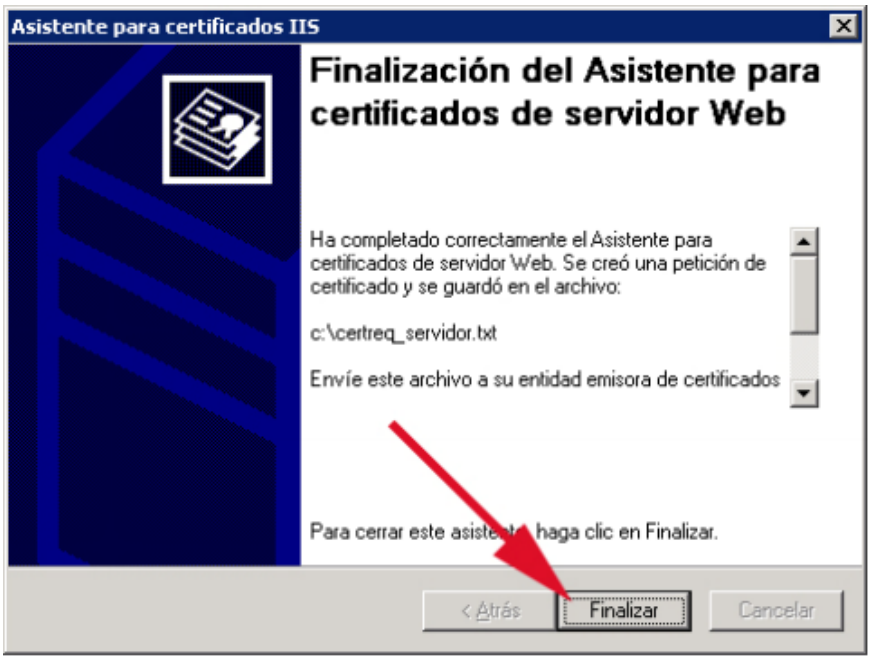
El último dato que solicita el asistente es la ubicación en la que se almacenará la solicitud de certificado de servidor seguro (CSR).



Una vez introducidos los datos, el asistente muestra un resumen de los datos que hemos introducido, como paso previo a la generación de la solicitud.



Tras lo que la solicitud de certificado habrá sido generada.



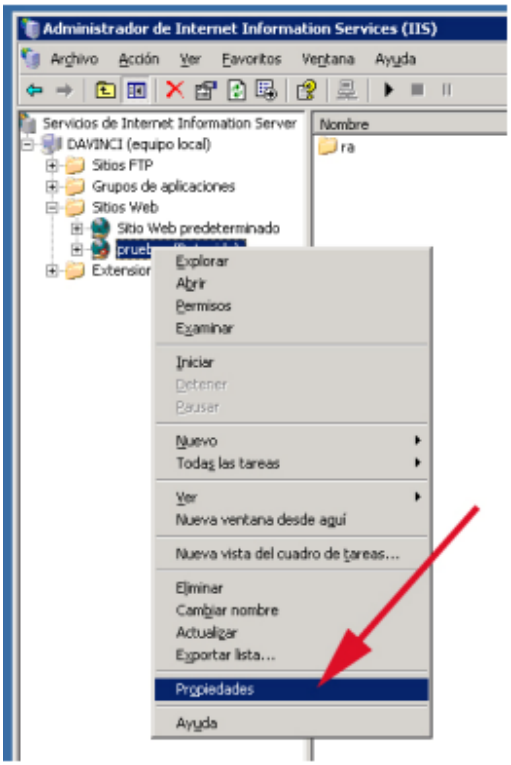
Una vez completado el asistente editamos el fichero de la petición, por ejemplo desde el Bloc de Notas, y copiamos el contenido al campo del formulario de petición de certificado de servidor (www.camerfirma.com) llamado CSR (Certificate Signing Request) y junto con los demás datos, enviamos la solicitud.

La petición tendrá el formato que se puede observar a continuación. Debemos "pegarla" (con las cabeceras) en el formulario.

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVjCCAr8CAQAwezEhMB8GA1UEAxMYbW9ydGFkZWxvLmNhbWVyZmlybWEuY29t
MREwDwYDVQQLEwhTaXN0ZW1hczEWMBQGA1UEChMNQUMgQ2FtZXJmaXJtYTEOMAwG
A1UEBxMFQXZpbGExDjAMBgNVBAgTBUF2aWxhMQswCQYDVQQGEwJFUzCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAtB1yMlqIrXKpaLJYZKjCodIhsGjNKhgnzl3e
SfNEaDncfA6jY5s9X6WTPECUidfSYaU6e6AroG1EiCYX1TOLitgobm6xvlg+vKgQ
wksv/VvV4RiJWAhYuLh3zmm5L1Yz2dZpropqVDazOSI5zgVItfIHV/IrbhajuwPD
vWvuGrECAwEAAaCCAZkwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMHsGCisG
AQQBgjcCAQ4xbTBrMA4GA1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4G
CCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcN
AwcwEwYDVR01BAwwCgYIKwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEe
WgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAA
QwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQBQ
v1G2vDWc9vlizq2Tw35H8AE38oQL76HgPwyKwxqBwK97TtcRyWC8sYKZCsB3E1z+
BwLme8NShpyIuUjh0gBxmH97DiOE2ozuYUR4YI3TpPHZSGBm1ZdcioZomKFZrkpy
JC8jAX02G3DdyKLXJBBHwz6Kx4bGBz5KrnpMc8rxHAAAAAAAAAAAMA0GCSqGSIb3
DQEBBQUAA4GBAHNEwgk1YVf9SIZrntUFVDYYsMs/95iYPo5ApIdP+F6RGUJXdkMC
Hg2SpvBAQK25ysPlbrAmVnMhYmEkYPf0D0t6g3SPfcU//+yIrYuYnTkuprCj7D12
sXKeoUc2XcW8qj/kwbymRdqLXSi5uraavUDrPQb5T6VU0ry1nXm64ZYW
-----END NEW CERTIFICATE REQUEST-----

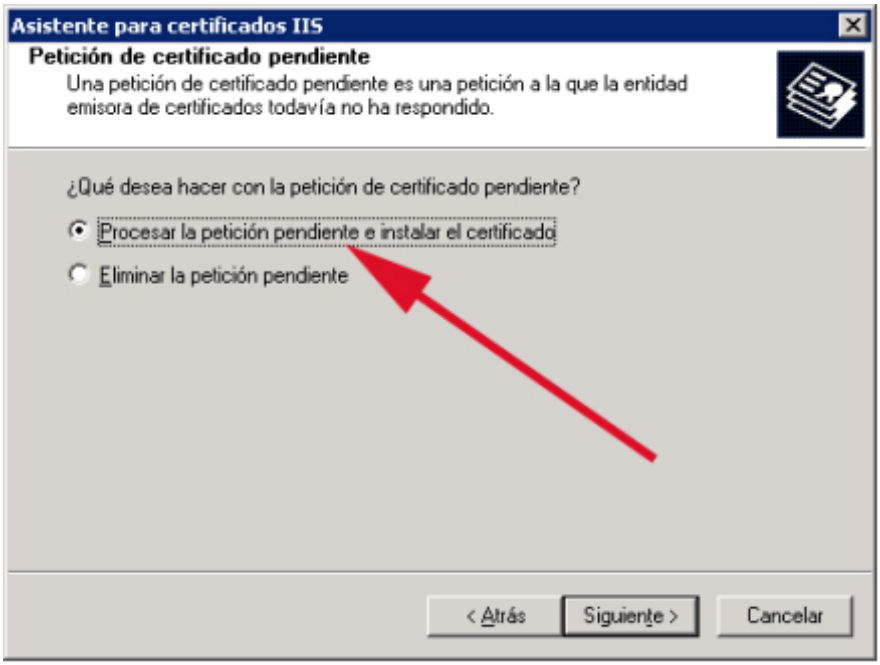
3. INSTALACIÓN

Una vez Camerfirma le haya enviado su certificado, vuelva a acceder a la administración de Internet Information Server: pulse sobre el botón de *Inicio*, seleccione *Todos los programas*, *Herramientas Administrativas* y después *Administrador de Internet Information Services (IIS)*. Cuando se abra la ventana correspondiente, haga clic en el nombre de su servidor y pulse el botón derecho del ratón para acceder a sus propiedades.

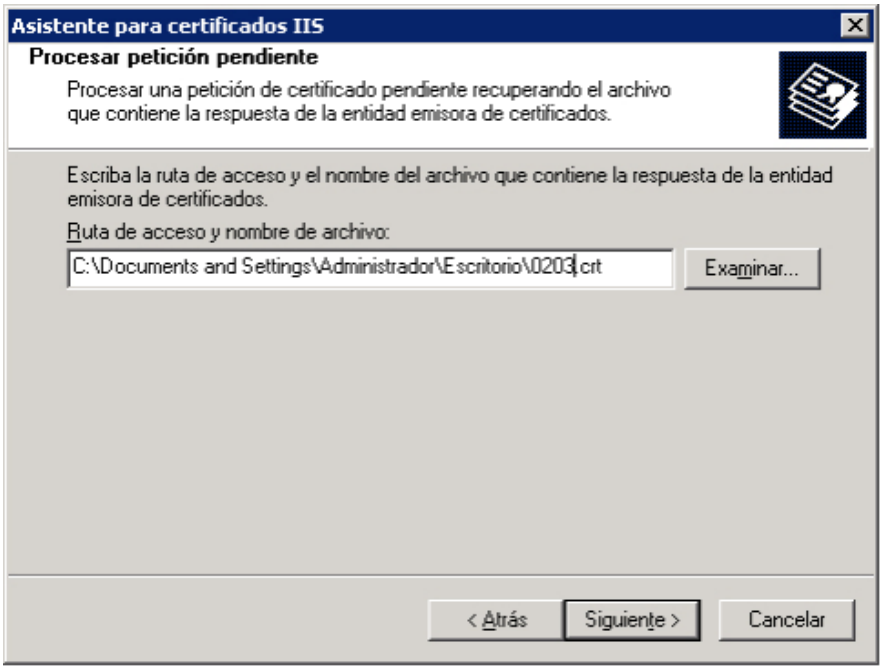


Acceda de nuevo a la pestaña *Seguridad de directorios* y seleccione *Certificado de servidor*.

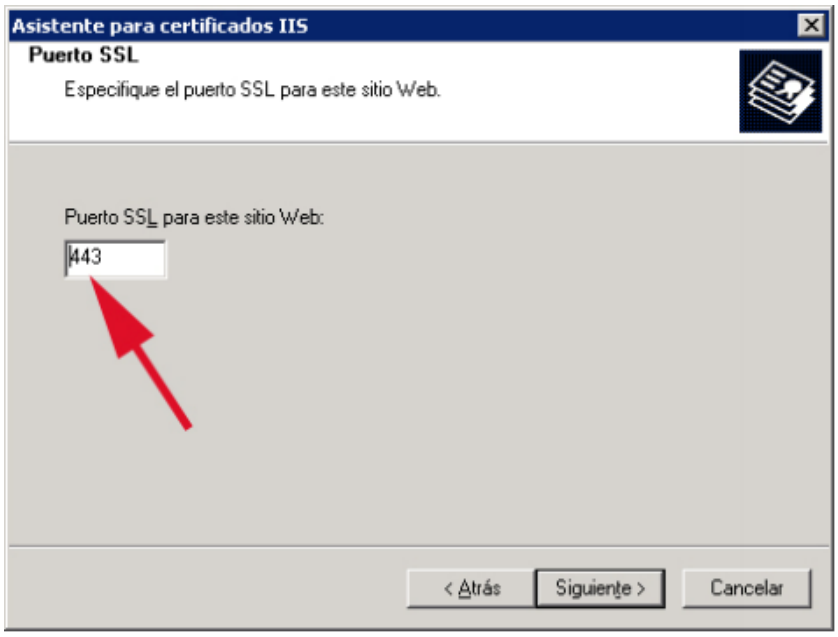
Se volverá a iniciar el asistente, y seleccionaremos *Procesar la petición pendiente e instalar el certificado*.



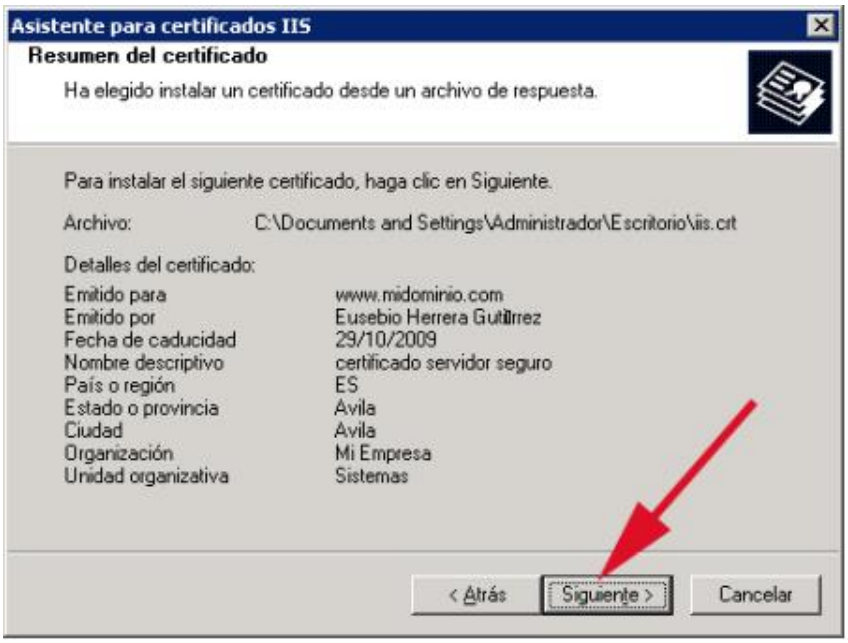
Tras pulsar siguiente, debemos especificar la ubicación del certificado que hemos recibido de AC Camerfirma.



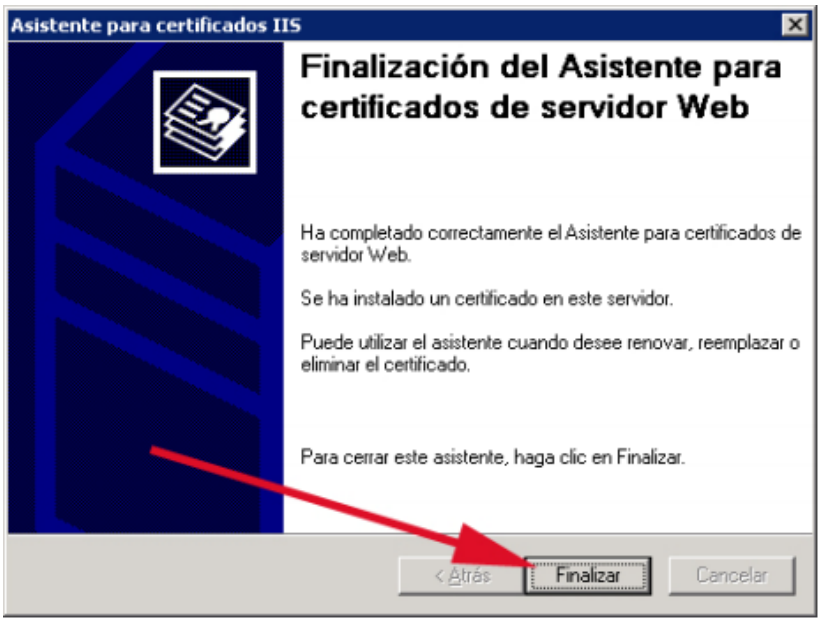
En la siguiente pantalla, el asistente nos solicitará el puerto al que va a estar asociado el sitio web para el que hemos solicitado el certificado. El puerto por defecto para las conexiones seguras es el 443.



El asistente nos mostrará una nueva pantalla previa a la instalación del certificado de servidor, únicamente a modo de resumen.



Al pulsar *Siguiente* el certificado quedará instalado en el servidor.



4. CONFIGURAR LOS CERTIFICADOS INTERMEDIOS

Para configurar los certificados intermedios para que el certificado de Servidor Seguro funcione correctamente se deben seguir los siguientes pasos:

1. Abrir el complemento certificados de Microsoft Management Console (MMC):
    - En *Inicio*, ejecutar *Símbolo del Sistema*, y escribir Mmc.exe.
    - Si se está ejecutando el programa como Administrador integrado, pedirá permiso para ejecutar el programa. En el cuadro de diálogo *Seguridad de Windows*, hacer clic en *Permitir*.
    - En el menú *Archivo*, hacer clic en *Agregar o quitar complemento*.
    - En el cuadro de diálogo *Agregar o quitar complementos*, hacer clic en el complemento *Certificados* en la lista complementos disponibles, hacer clic en *Agregar* y, a continuación, hacer clic en *Aceptar*.
    - En el cuadro de diálogo *Complemento de certificados*, hacer clic en *Cuenta de equipo* y, a continuación, hacer clic en *Siguiente*.
    - En el cuadro de diálogo *Seleccionar equipo*, haz clic en *Finalizar*.
    - En el cuadro de diálogo *Agregar o quitar complementos*, haz clic en *Aceptar*.

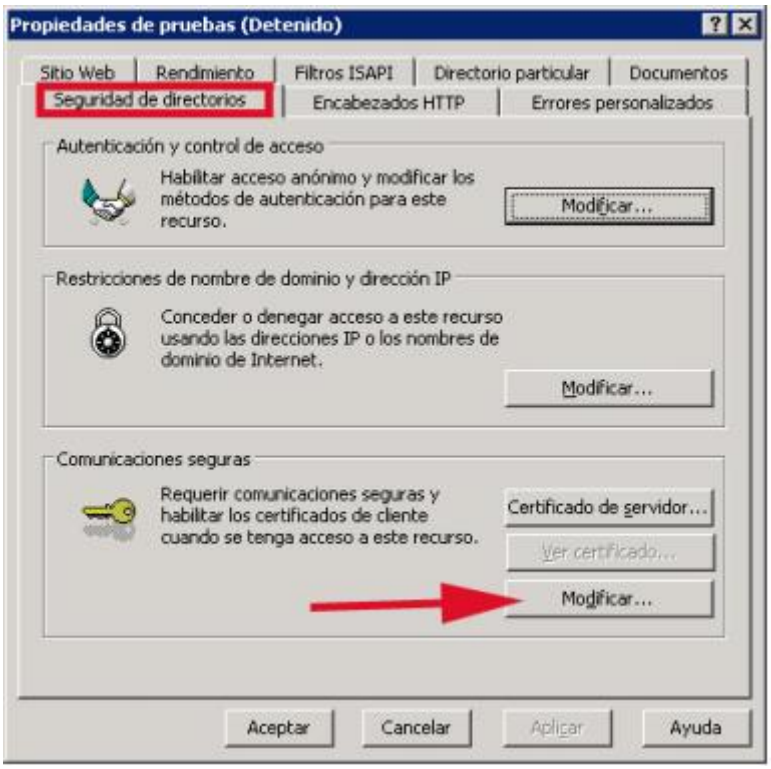
2. Para agregar un certificado intermedio, hay que seguir estos pasos:
    - Primeramente, se deben descargar las claves públicas de los certificados intermedios de la web https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/ en el apartado *Políticas de Certificación (2003 y 2008 CCR).* Primero hay que descargar *CHAMBERS OF COMMERCE ROOT* (el archivo descargado tendrá el nombre *camerfirma_tsa-2009.cer*):

Después, hay que descargar *Corporate Server* de la misma web que antes (el archivo descargado se llama *camerfirma_cserverii-2015.cer*):

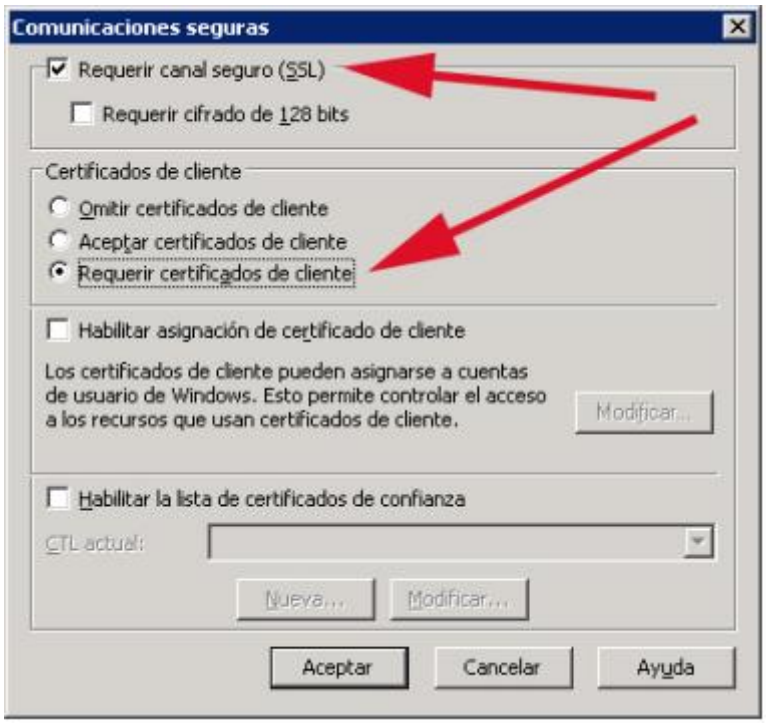
- En el complemento MMC certificados, expande certificados, hacer clic en *Entidades emisoras de certificados intermedias*, seleccionar *Todas las tareas* y, a continuación, hacer clic en *Importar*.
- En el Asistente para *Importación de certificados*, hacer clic en *Siguiente*.
- En la página archivo para importar, escribir el nombre de archivo del certificado que deseamos importar en el cuadro nombre de archivo y, a continuación, hacer clic en *Siguiente*. Primero hay que importar *camerfirma_tsa-2009.cer* y luego *camerfirma_cserverii-2015.cer*.
- Hacer clic en *Siguiente* y, a continuación, completar el Asistente para importación de ambos certificados intermedios.

5. CONFIGURACIÓN BÁSICA Y COMPROBACIÓN DE FUNCIONAMIENTO

Una vez instalado, podemos realizar la configuración del sitio seguro. Para ello, volveremos a acceder a la pestaña *Seguridad de directorios* de nuestro servidor web, pero esta vez, pulsaremos sobre el botón *Modificar*.



Debemos activar la opción de *Requerir canal seguro (SSL)*. Si además deseamos que los clientes se conecten al servidor a través de sus certificados personales, debemos marcar la opción *Requerir certificados de cliente*.



Para comprobar que está correctamente instalado, podemos hacer lo siguiente:

- Acceder al sitio utilizando HTTP. Poner en un navegador "http://localhost/". Recibiremos un mensaje que diga "HTTP 403.4 - Forbidden: SSL required.".
- Acceder a la misma página Web mediante una conexión segura (HTTPS) escribiendo https://localhost/ en el navegador. Si aparece la página, significa que has instalado correctamente el certificado.