

MS Internet Information Services

Tabla de Contenidos

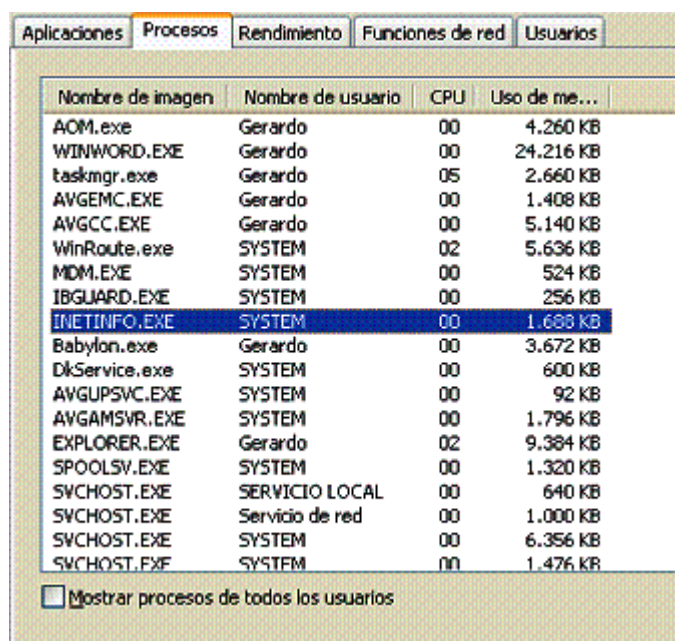
2. MS Internet Information Services.....	2
2.1 Introducción a IIS 5	2
2.2 Configuración	6
2.3 Instalación y Configuración de un Sitio Web.....	11
2.4 Ajuste de la Configuración.....	17
2.5 Sitio Web.....	17
2.6 Operadores.....	18
2.7 Rendimiento.....	19
2.8 Filtros ISAPI.....	20
2.9 Encabezados HTTP.....	20
2.11 Errores Personalizados.....	22
2.12 Extensiones del Servidor.....	23
2.13 Directorio Particular.....	25
2.14 Documentos.....	29
2.15 Seguridad de Directorios.....	30
2.16 Directorios Virtuales.....	33
2.17 Instalando soporte para CGI/PERL.....	37
2.18 Instalando Soporte para ASP.NET.....	38
2.19 Internet Information Services 6.....	39
2.20 Utilización de JSP/Servlets con IIS.....	41
2.21 Soporte de SSL en IIS.....	47



2. MS Internet Information Services

2.1 Introducción A IIS 5

IIS (Internet Information Services) es una plataforma completa capaz de servir *http*, *ftp*, *nntp* y *smtp*. IIS versión 5 se incluye en Windows 2000 Server y se ejecuta como un servicio dentro de Windows 2000 (también viene incluido con Windows XP). Los servicios estándares de Internet se encuentran en un proceso llamado *INETINFO*. En la siguiente figura se muestra el administrador de tareas con el proceso *INETINFO* ejecutándose



Nombre de imagen	Nombre de usuario	CPU	Uso de me...
ACM.exe	Gerardo	00	4.260 KB
WINWORD.EXE	Gerardo	00	24.216 KB
taskmgr.exe	Gerardo	05	2.660 KB
AVGEMC.EXE	Gerardo	00	1.408 KB
AVGCC.EXE	Gerardo	00	5.140 KB
WinRoute.exe	SYSTEM	02	5.636 KB
MDM.EXE	SYSTEM	00	524 KB
IBGUARD.EXE	SYSTEM	00	256 KB
INETINFO.EXE	SYSTEM	00	1.688 KB
Babylon.exe	Gerardo	00	3.672 KB
DkService.exe	SYSTEM	00	600 KB
AVGUPSV.EXE	SYSTEM	00	92 KB
AVGAMSVR.EXE	SYSTEM	00	1.796 KB
EXPLORER.EXE	Gerardo	02	9.384 KB
SPOOLSV.EXE	SYSTEM	00	1.320 KB
SVCHOST.EXE	SERVICIO LOCAL	00	640 KB
SVCHOST.EXE	Servicio de red	00	1.000 KB
SVCHOST.EXE	SYSTEM	00	6.356 KB
SVCHOST.EXE	SYSTEM	00	1.476 KB

☐ Mostrar procesos de todos los usuarios

IIS comparte el mismo modelo de seguridad que Windows 2000, lo que elimina la necesidad de tener una administración particular de cuentas de usuario, a su vez IIS utiliza las herramientas de Windows 2000 para su administración, como ser: MMC, Visor de Sucesos, Monitor del Sistema, etc.

La instalación de IIS 5.0 está integrada en la instalación de Windows 2000 y es instalado por defecto como un

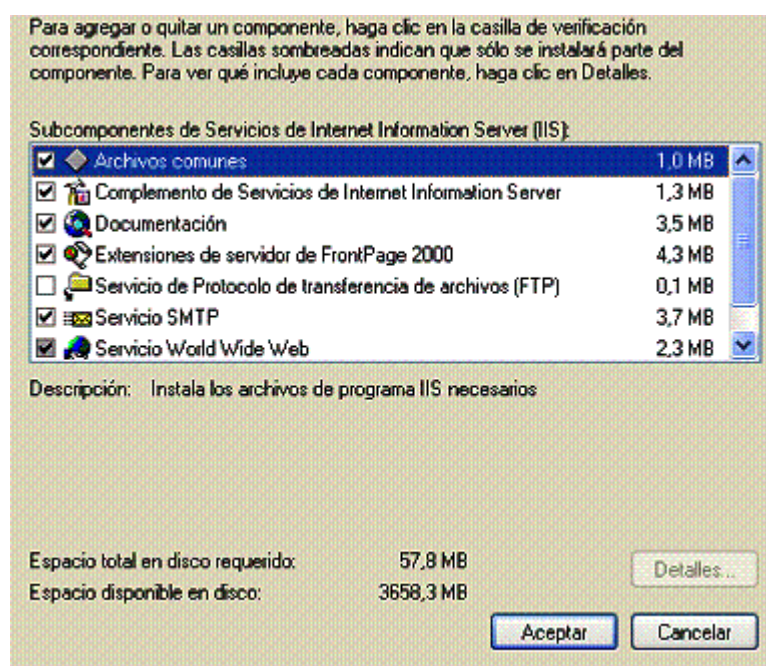
componente de Windows. Es posible, además, desinstalarlo y volverlo a instalar desde *Agregar o quitar programas* del *Panel de Control*. La instalación de IIS crea por defecto:

- Un sitio Web
- Un sitio Web de administración
- Un servidor virtual SMTP

De todas formas, es posible instalar o remover otros componentes auxiliares como ser NNTP (Servicio de noticias). En la siguiente figura se ven los componentes que pueden instalarse con IIS. En este caso no se encuentra instalado el servicio de transferencia de archivos FTP.

Para poder llegar a dicha ventana, hay que seguir los siguientes pasos:

1. Acceder como Administrador
2. Abrir el Panel de Control y Doble-click en *Agregar o quitar Programas*. Aparece la ventana de *Agregar o quitar Programas*.
3. Click en *Agregar o quitar componentes de Windows*. Aparece el asistente de Componentes de Windows.
4. Selecciona en la lista de componentes: *Servicios de Internet Information Server (IIS)* y click en *Detalles*.



La instalación de IIS crea, además, un directorio llamado Inetpub bajo el cual residen un conjunto de subdirectorios para cada servicio instalado. Los subdirectorios son:

AdminScripts	Contiene algunos scripts Visual Basic para uso en la administración.
ftproot	Directorio principal para el servicio FTP.
mailroot	Directorio principal para el servicio SMTP.
nntpfile	Directorio principal para el servicio NNTP.
wwwroot	Directorio principal para el sitio Web por defecto.

IIS puede usarse para hospedar uno o varios sitios Web utilizando múltiples dominios y, mediante la utilización de las extensiones FrontPage del lado servidor, permitir a los usuarios o clientes publicar y administrar sus sitios a través de la herramienta de diseño de Microsoft: FrontPage. El servicio FTP de transferencia de archivos de IIS soporta una característica denominada *resume* que permite que una transferencia que fue interrumpida pueda reiniciarse en el punto de la interrupción sin necesidad de volver a transferir desde el comienzo. Esto permite ahorrar ancho de banda principalmente cuando los usuarios acceden al sitio por conexiones poco confiables o los archivos son muy grandes. El servicio de noticias llamado también *Usenet*: *nntp* (*Network News Transport Protocol*) fue incorporado en la versión 4 de IIS.

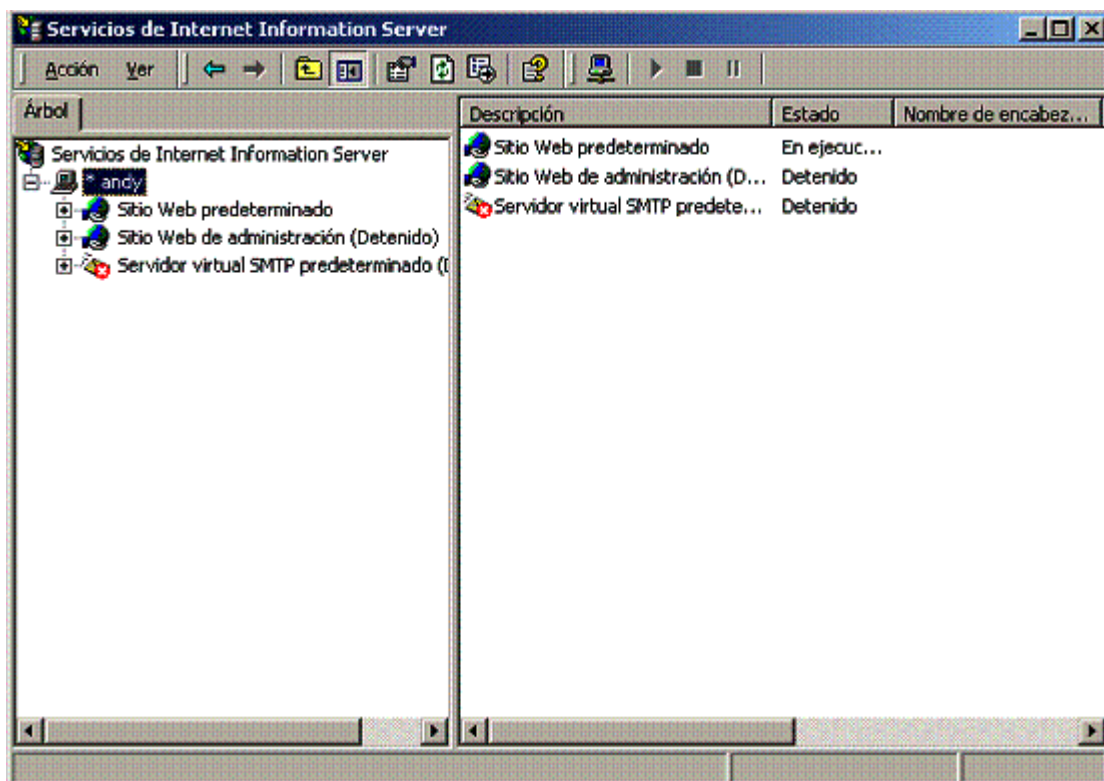
El servicio SMTP (*Single Mail Transfer Protocol*) incorporado en IIS no está pensado para usarse como una plataforma de correo electrónico completa sino como una herramienta de soporte para el resto de los servicios. No cuenta con soporte para los protocolos de recupero de correo POP o IMAP. A pesar de ello, puede usarse para que las aplicaciones Web envíen correo hacia otros destinos (un formulario de registro que envía un mail de confirmación).

Si se realiza una instalación completa (ya sea al instalar el Windows 2000 o posteriormente desde *Agregar o quitar Programas* del *Panel de Control*) se configuran los siguientes *puertos* sobre todas las direcciones IP instaladas:

- Puerto 80: para el servicio *http*.
- Puerto 21. Para el servicio *ftp*.
- Puerto 119: para el servicio *nntp*
- Puerto 25: para el servicio SMTP

El sitio de administración utiliza un puerto aleatorio respondiendo sólo a *localhost* o a la IP 127.0.0.1 (*loop back*).

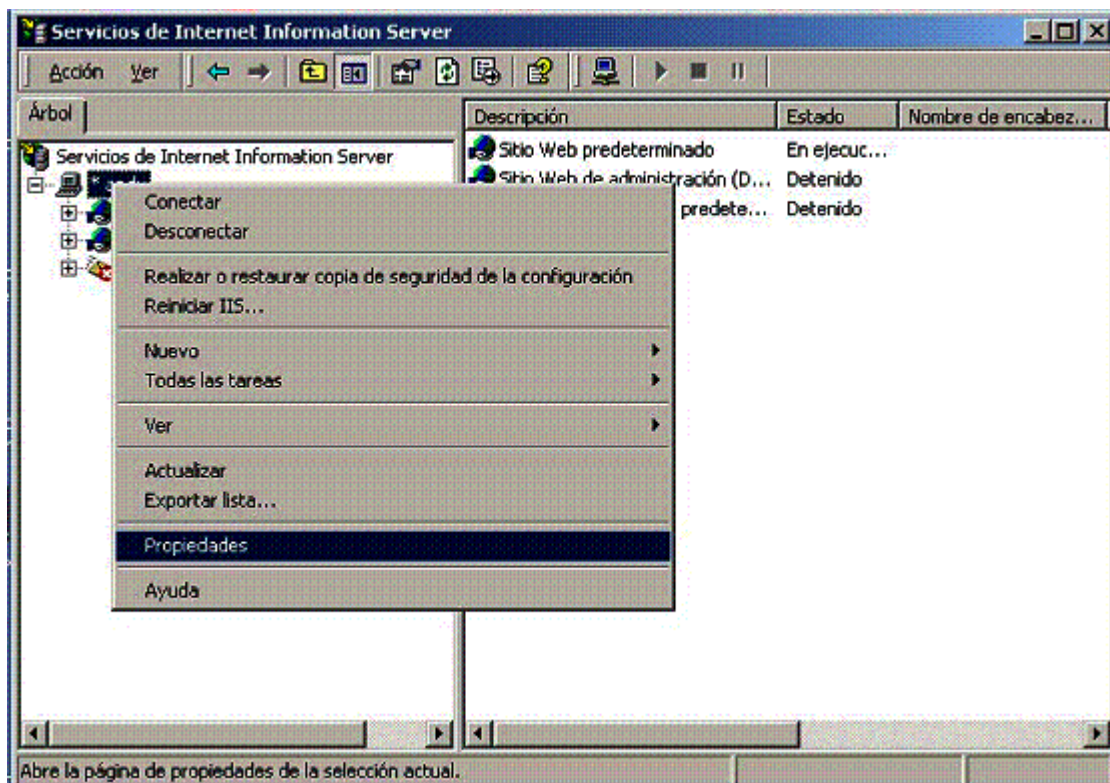
Es importante tener funcionando **solamente** los servicios que se vayan a utilizar, fundamentalmente si la computadora tiene acceso a Internet. Para detener o ejecutar los servicios, se debe acceder a *Servicios de Internet Information Server* desde el menú de *Inicio/Herramientas Administrativas*. En la siguiente figura vemos el Administrador de Servicios de Internet en donde solamente se han instalado los servicios de http y smtp estando este último detenido como lo muestra la cruz en rojo y blanco sobre el nodo.



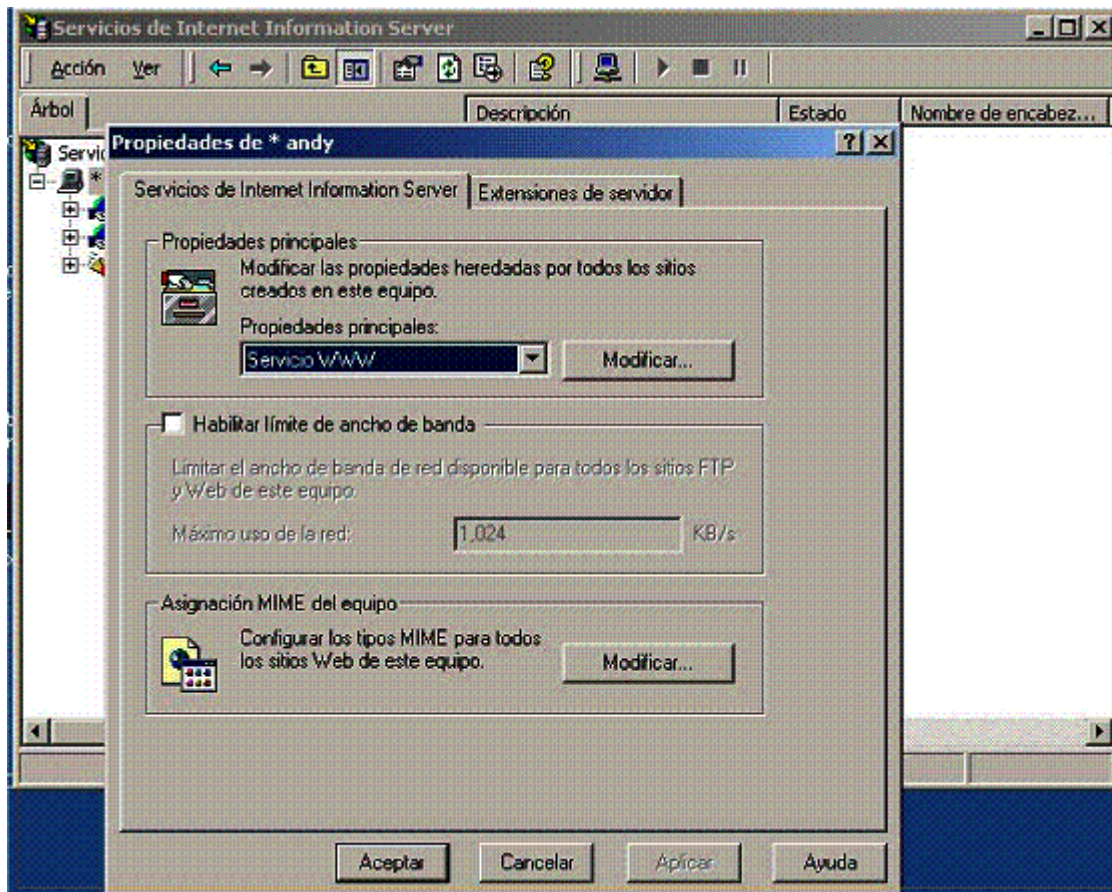
2.2 Configuración

La configuración puede hacerse tanto a nivel servidor como a nivel sitio particular. Es decir, podemos realizar una configuración global y luego sobrescribir algunos de los parámetros en un sitio en particular. Lo indicado es configurar los parámetros generales necesarios a nivel servidor y luego si hace falta ajustar los parámetros de los sitios en particular.

Para acceder a la ventana de configuración desde la consola de *Servicios de Internet Information Server* a nivel servidor es necesario hacer click-derecho en el servidor que estamos configurando y luego en el menú emergente seleccionar *Propiedades*, como se muestra en la siguiente figura:



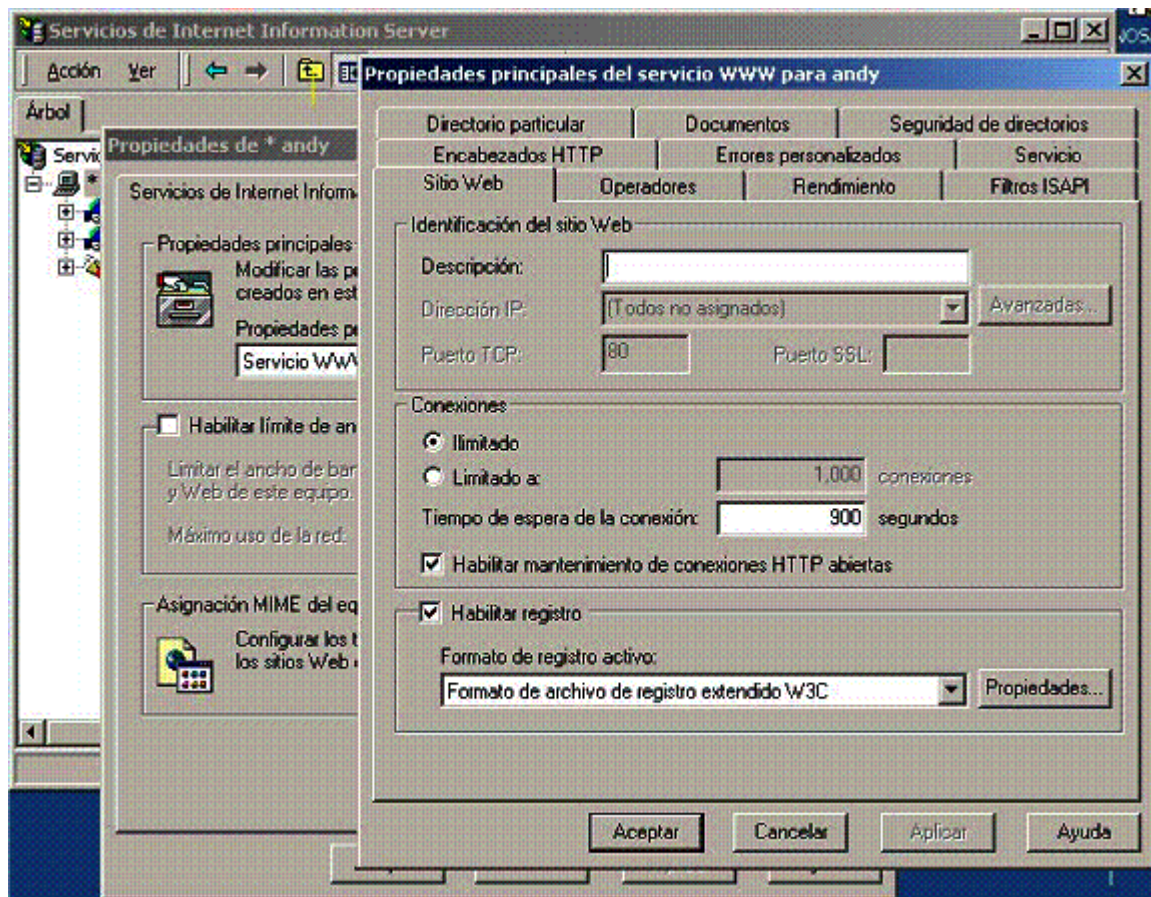
Al seleccionar *Propiedades*, se muestra la ventana de propiedades del servidor en la pestaña de *Servicios de Internet Information Server* como se ve en la figura:



Desde allí, es posible configurar los valores por defecto para todo el servidor y cambiar la configuración existente. En el caso de que ya se tengan sitios configurados ejecutándose en el servidor, Windows 2000 da la opción de aplicar los cambios globalmente o sólo a sitios individuales.

Hay tres aspectos en la pestaña *Servicios de Internet Information Server*: *Propiedades Principales*, *Límite de ancho de Banda* y *Asignación MIME del equipo*.

La opción de *Propiedades Principales* permite modificar las propiedades del servicio. De la lista desplegable se debe elegir el servicio (FTP, WWW) y presionar el botón de modificar. Esto muestra la pantalla *Propiedades Principales del Servicio WWW o FTP*:

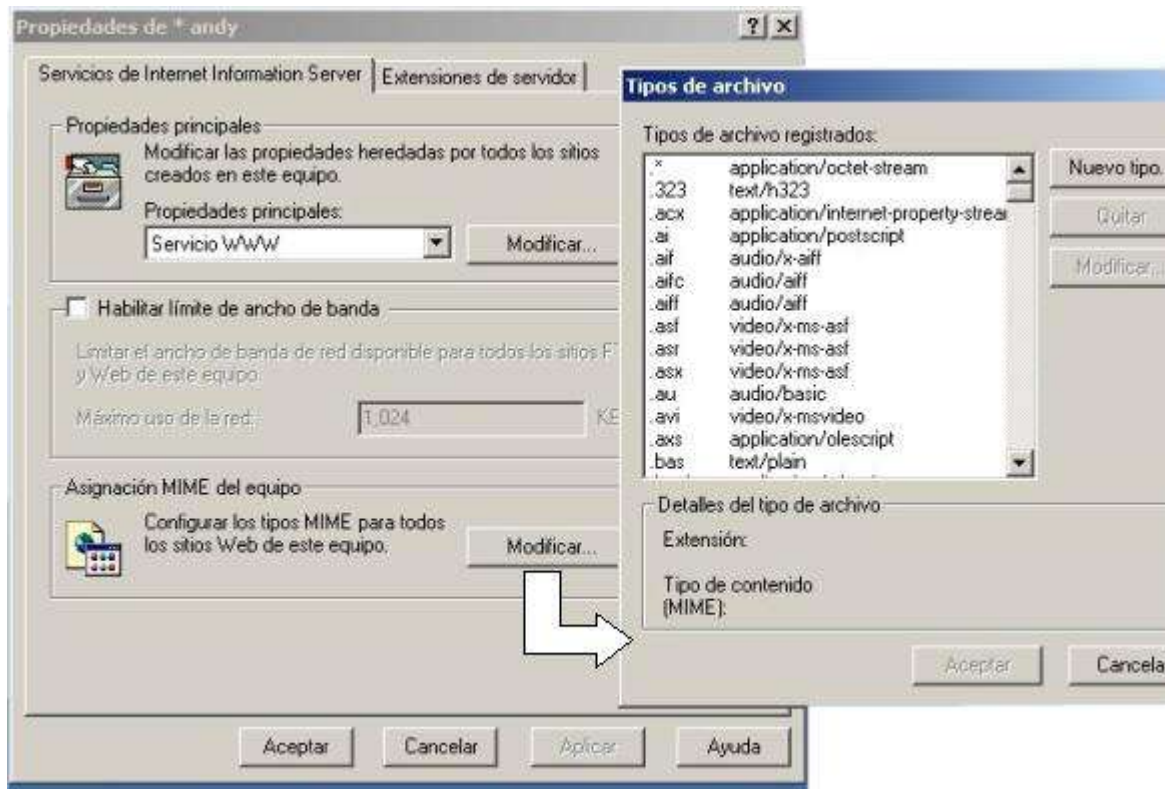


Desde esta ventana es posible configurar detalladamente el servidor, en aspectos como directorios, páginas por defecto, seguridad, errores, etc.

La opción *Habilitar el límite de ancho de banda* permite controlar cuanto ancho de banda podrá usar IIS. Esto permite asegurarse que se mantendrá suficiente ancho de banda para otros servicios. De todas formas, es importante tomar en cuenta que la configuración de límite de ancho de banda en sitios individuales *sobrescribirá* la configuración global. La configuración del límite de ancho de banda es también una importante herramienta para medir el comportamiento de sitios Web bajo diversas condiciones de acceso. Un sitio que se comporta correctamente utilizando el ancho de banda completo puede ser muy lento si se utiliza menos ancho de banda (lo que ocurriría si se accede desde una conexión lenta).

Por último, en la pestaña se encuentra la opción de configurar las extensiones MIME (*Multipurpose Internet Mail Extensions*). En general utilizar la configuración por defecto es suficiente, pero si se necesitan tipos MIME particulares hay que hacer *Click* en *Modificar* como se muestra en la siguiente figura:

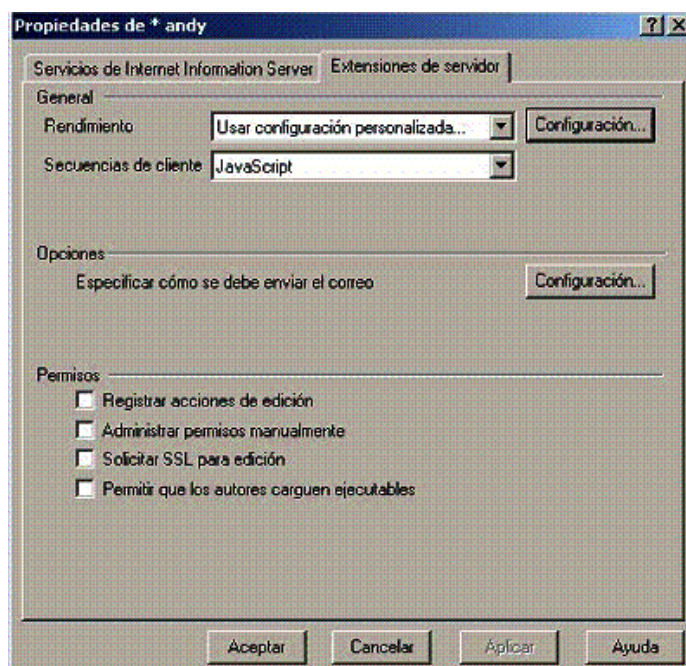




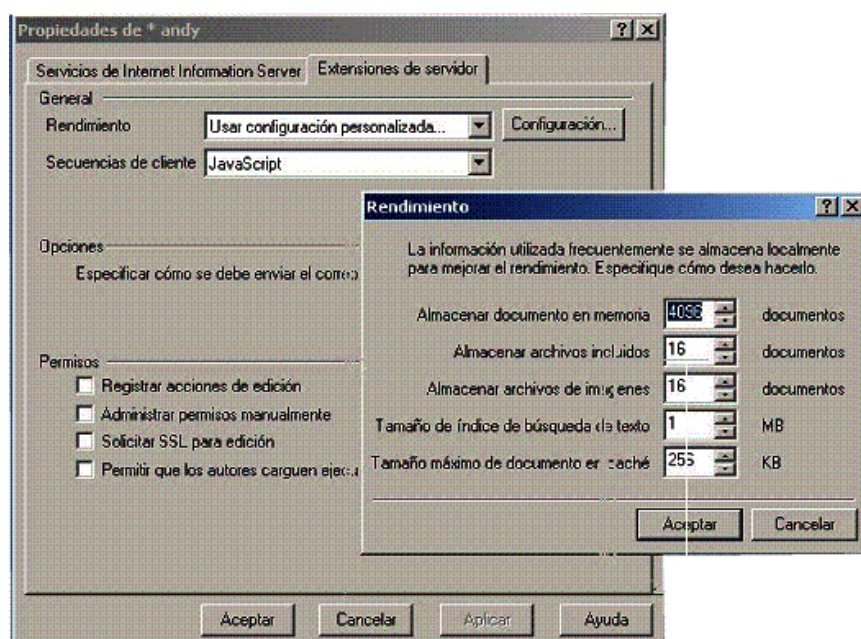
La otra pestaña es la *Extensiones del Servidor*. Bajo ella es posible controlar la configuración de varios aspectos (rendimiento, permisos, correo) de los sitios Web. Mientras que, cuando se realizan *Servicios de Internet Information Server* Windows 2000 avisa si se sobrescribe alguna directiva de un sitio particular permitiendo modificarla o no, en las *Extensiones del Servidor* los cambios en la configuración son aplicados inmediatamente a todos los sitios independientemente de la configuración particular que pudieran tener éstos.



Las opciones disponibles se ven en la siguiente figura:



La configuración rendimiento se modifica desde el botón de configuración mostrando el siguiente dialogo:



Este diálogo permite configurar como se desea que funcione el *cache* para búsqueda y documentos.

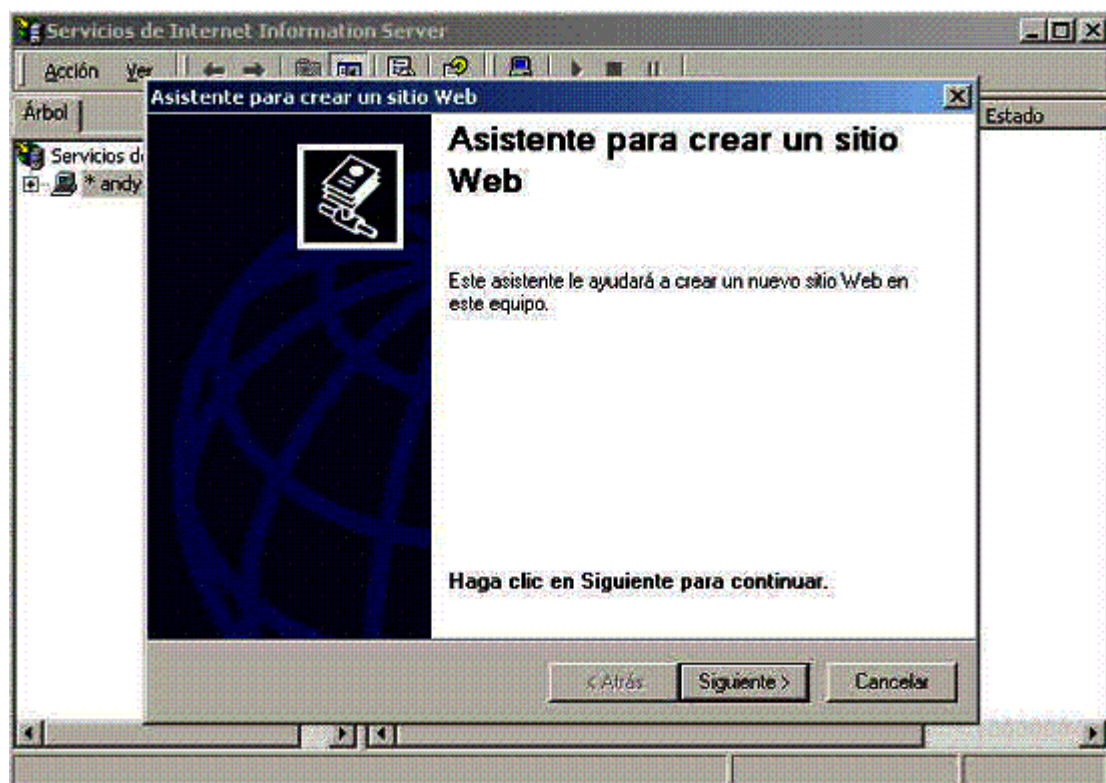
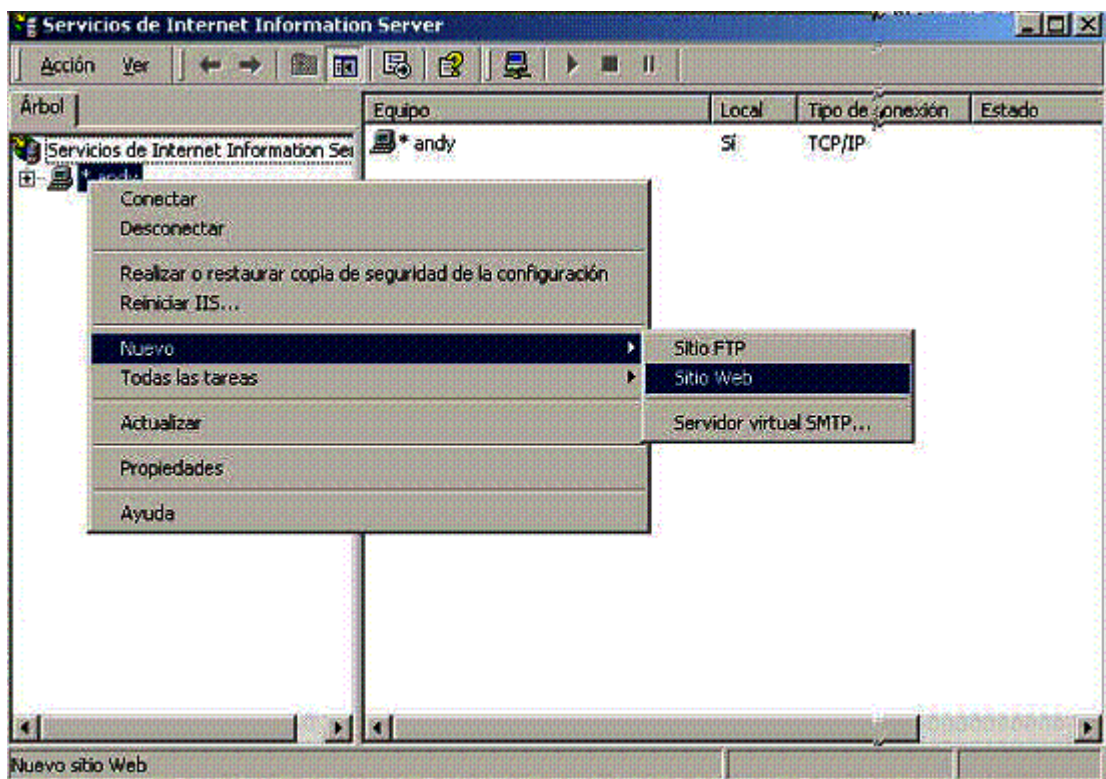
2.3 Instalación Y Configuración De Un Sitio Web

Antes de comenzar la construcción de un sitio Web, hay que decidir algunas cosas para lo cual lo mejor es responder las siguientes preguntas:

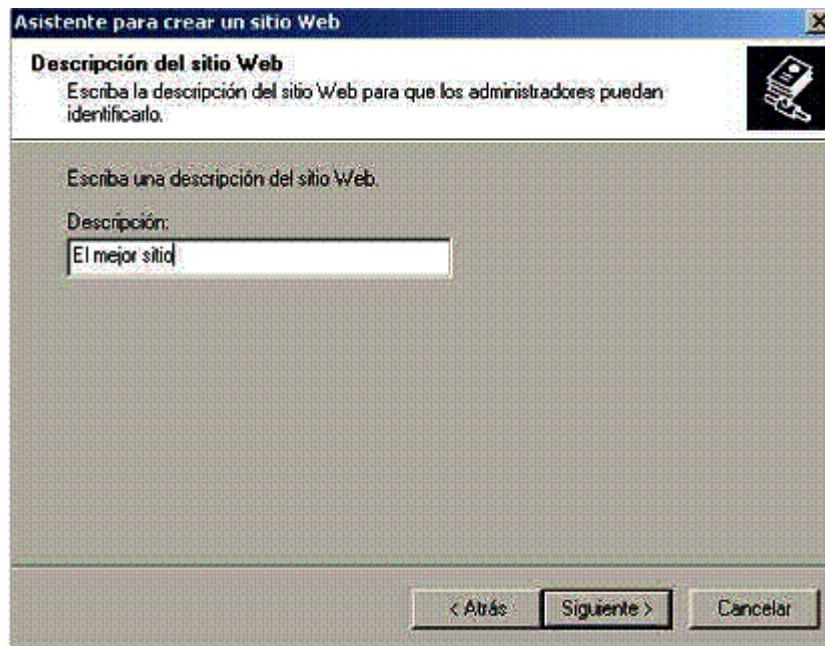
- ¿Qué puertos se usarán para el sitio Web y cuáles para comunicaciones seguras?
- ¿Sobre que dirección IP el servicio estará escuchando?
- ¿A qué nombre responderá el servidor Web?
- ¿Funcionarán múltiples sitios Web sobre el mismo servidor? (www.miempresa.com, www.otraempresa.com, etc.)
- ¿En que directorio se ubicarán los documentos del sitio?

Para la creación del sitio se utilizará el *Asistente para crear un sitio Web*. Para acceder al mismo, se debe realizar *click-derecho* en la consola de administración en el servidor correspondiente y luego seleccionar en el menú *Nuevo/Sitio WEB* como se ve en las dos siguientes figuras:





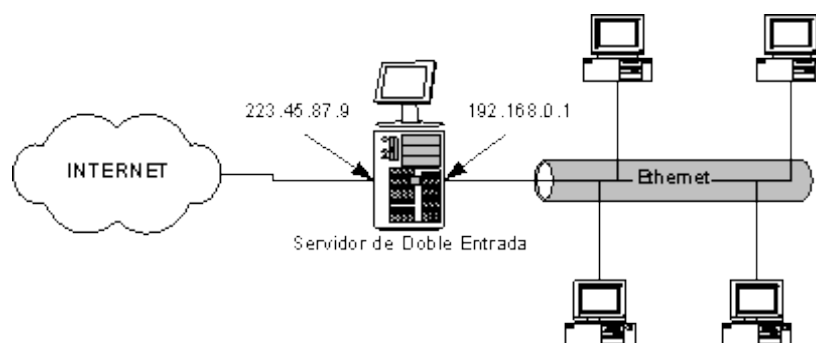
Lo primero que se pide es un nombre descriptivo del sitio:



Y luego la información de configuración donde se debe acceder la dirección IP del sitio (por defecto todas), el puerto y el *Encabezado del host*. En el caso de que solamente se esté alojando un sitio, la configuración por defecto puede ser aceptable pero se debe tener cuidado en el caso de estar alojando múltiples sitios. La dirección IP generalmente indicará el adaptador sobre el cual se recibirán las peticiones. En el caso de una computadora con múltiples adaptadores, cada uno con una dirección IP diferente, es importante asignar la dirección correcta. Por ejemplo, se puede desear que solamente se acceda a este sitio desde la red interna, por lo cual, si la computadora está conectada con dos adaptadores de red, uno será para la red interna (*host* de doble entrada) y otro será para la externa, hay que acceder la dirección IP correspondiente a la red interna.



Por otra parte, es posible que se tenga un adaptador de red con múltiples direcciones IP asignadas a él, en cuyo caso es posible asignar diferentes sitios a diferentes direcciones IP. El siguiente diagrama muestra un host de doble entrada y las direcciones IP correspondiente:

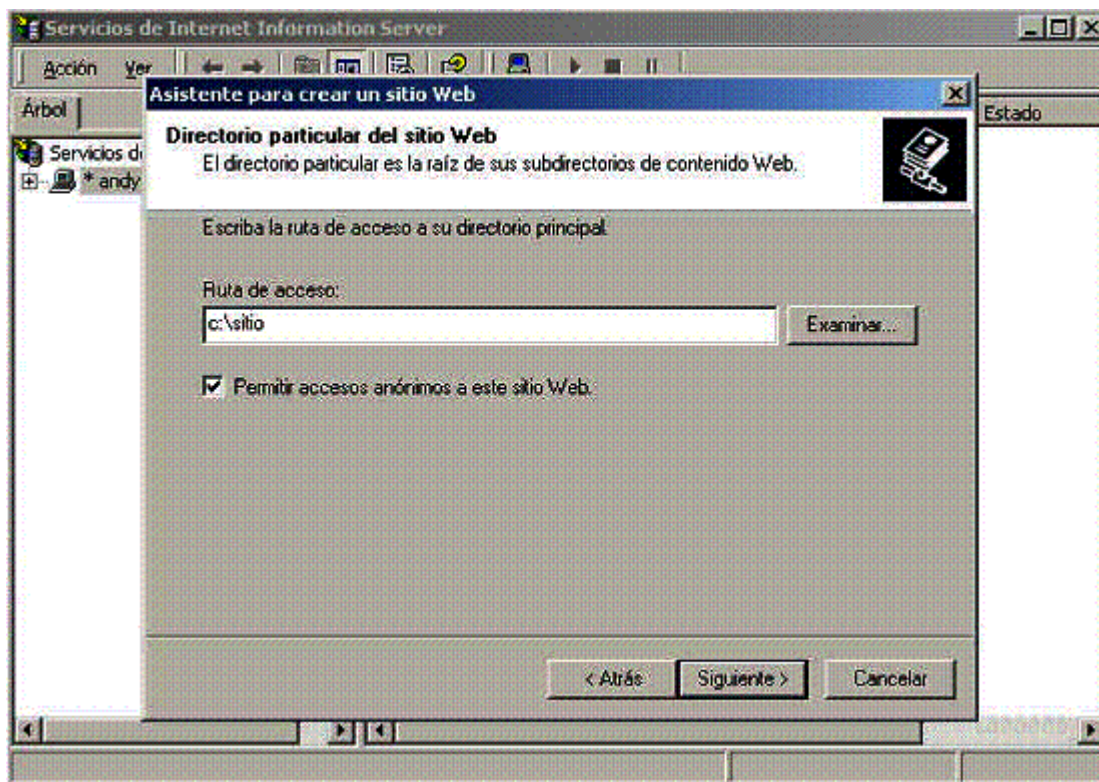


HOST de doble entrada. Si el servidor Web escucha en la dirección 192.168.0.1 sólo los usuarios de la red interna (ethernet) tendrán acceso al sitio

El *encabezado del host* es una herramienta utilizada para asignar múltiples sitios Web a la misma dirección IP. Funciona de la siguiente manera: una vez establecida la conexión TCP entre el navegador cliente y el servidor Web

(generalmente en el puerto 80), el navegador envía un requerimiento para que se transmita una página. En el requerimiento se incluye el *encabezado del host* como ser *www.miempresa.com*. Esto permite que IIS compare el *encabezado del host* con los sitios que tiene alojados respondiendo en consecuencia. Este esquema no funciona con SSL, en cuyo caso se deben usar múltiples direcciones IP. La opción SSL (Secure Socket Layer) aparece deshabilitada dado que se requiere tener un certificado instalado para habilitarla. El puerto por defecto para SSL es el 443.

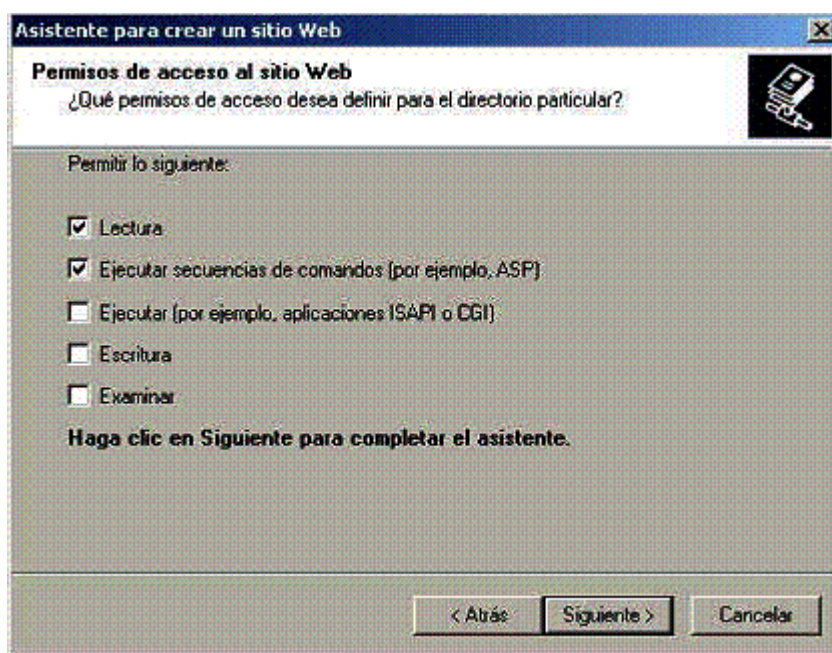
El próximo paso, es decidir la ubicación del sitio en el sistema de archivos, es decir el directorio. El mismo debe estar creado previamente.



Para un sitio público que no requiera autorización para el acceso, se debe dejar marcado el casillero de *Permitir accesos anónimos a este sitio Web*

El último paso es configurar los permisos asignados al directorio raíz del sitio (el seleccionado en el paso anterior) y que son automáticamente heredados por todos los subdirectorios





A continuación se detallan los significados de los diversos permisos:

Lectura: Permite a los usuarios leer archivos desde ese directorio. Esta opción es generalmente habilitada excepto para directorios que contengan programas CGI o ISAPI (luego se detallara el uso de CGI e ISAPI)

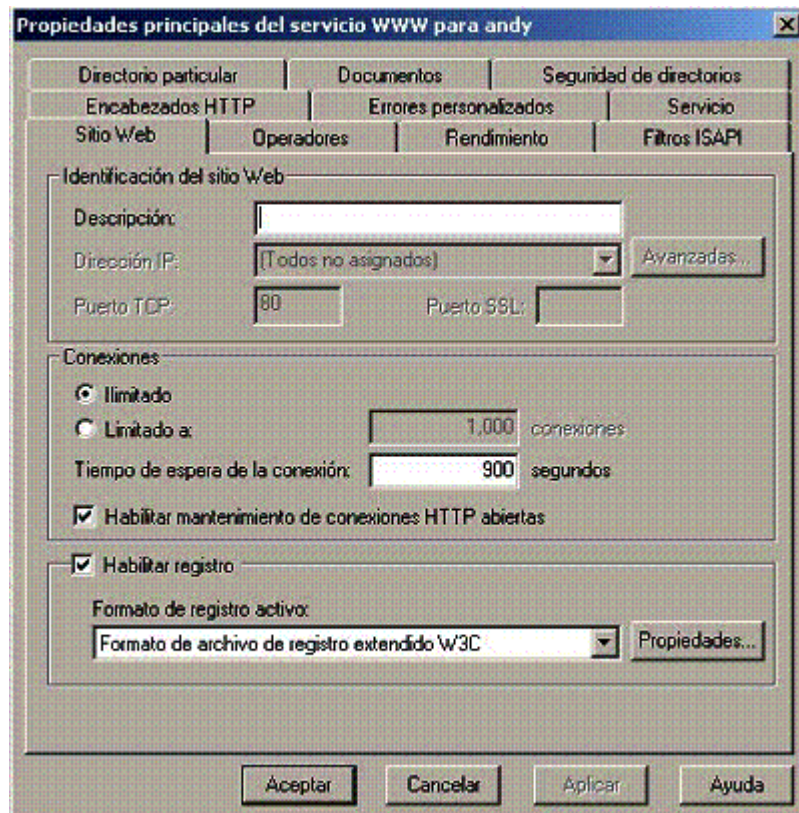
- **Ejecutar secuencias de comandos:** Permite la ejecución de secuencias de comandos como ASP.
- **Ejecutar:** Esta opción se habilita en los directorios donde se ubiquen programas CGI o ISAPI. Además esta opción incluye la anterior.
- **Escritura:** Esta opción es para permitir que el navegador cliente escriba en el mismo. Es peligroso habilitarla salvo para algún directorio particular
- **Examinar:** En caso de no existir una página por defecto y el usuario no requiera ninguna en particular, esta opción permite ver el contenido del directorio. No es recomendado que esta opción esté habilitada.

Salvo las dos primeras opciones *Lectura* y *Ejecutar secuencias de comandos*, el resto no es recomendable habilitarlas en el directorio raíz. Siempre existe la posibilidad de configurar un directorio en forma particular si es necesario.



2.4 Ajuste De La Configuración

Se verá en este apartado como realizar modificaciones a la configuración de un sitio ya instalado. Para acceder a las propiedades del sitio se debe seleccionar el mismo en el Administrador de Servicios de *Internet Information Server* y luego desde el menú *Acción/Propiedades*. La página de propiedades es como se muestra en la siguiente figura:



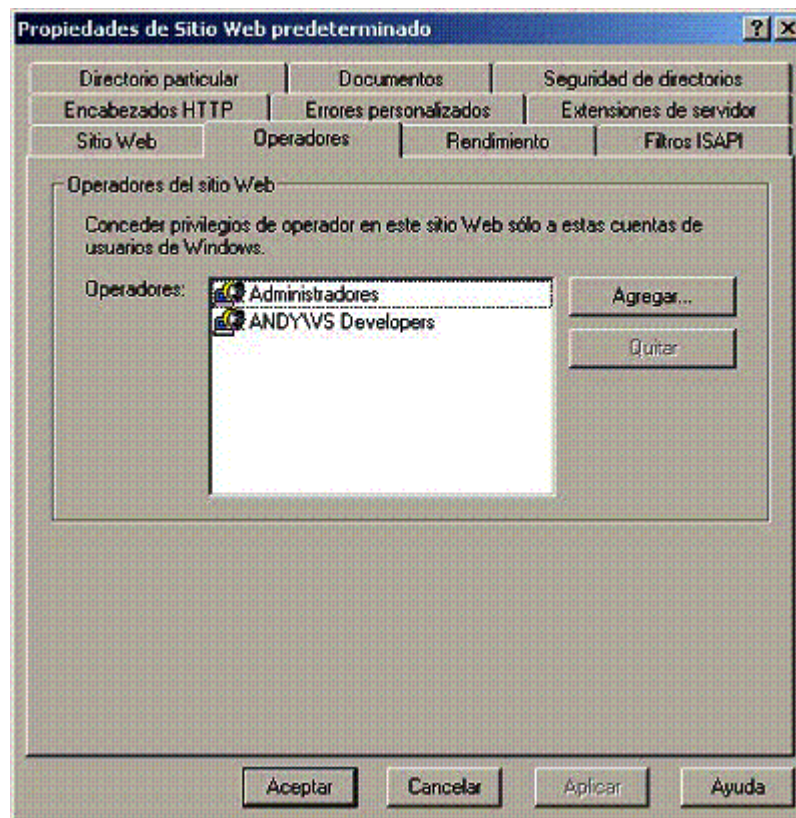
2.5 Sitio Web

Es posible cambiar las opciones de identificación asignadas al sitio al crearlo (lo cual cambiará la forma en que los clientes acceden al sitio). A su vez, se puede establecer el máximo de conexiones permitidas y el tiempo de espera conexión antes de que IIS cierre la misma. La casilla *Habilitar mantenimiento de conexiones http abiertas* permite que el navegador cliente reutilice las conexiones al traer los elementos de una página aumentando el rendimiento. En caso contrario, el cliente debe abrir una conexión por cada elemento de la página. La opción de *Habilitar registro*

permite mantener un registro de las operaciones realizadas. Hay que tener cuidado porque el registro ocupa mucho espacio en disco. Hay varios tipos de formatos disponibles y cada uno con sus propiedades. Los tipos de formato se eligen de la lista desplegable *Formato de registro activo*.

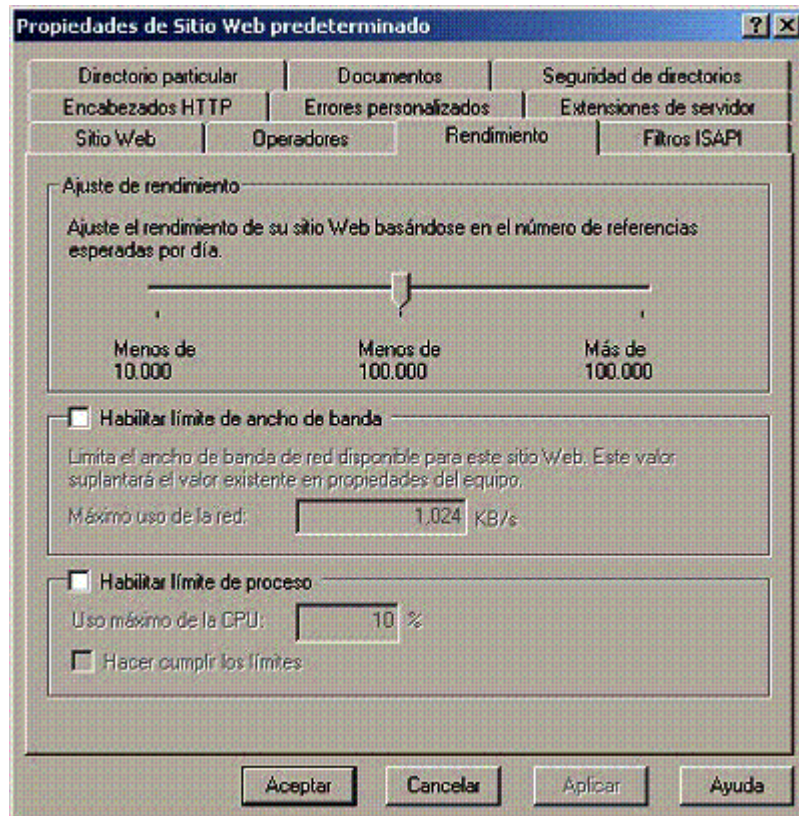
2.6 Operadores

Esta pestaña permite asignar o denegar a cuentas de usuario privilegios de operador para el sitio Web. Para usar los privilegios el usuario debe autenticarse como un usuario Windows 2000. Los operadores pueden: Modificar permisos de acceso, modificar los documentos por defecto del sitio, modificar encabezados http, etc.



2.7 Rendimiento

Esta opción permite ajustar aspectos del rendimiento del sitio. Tres aspectos se configuran en esta pestaña:



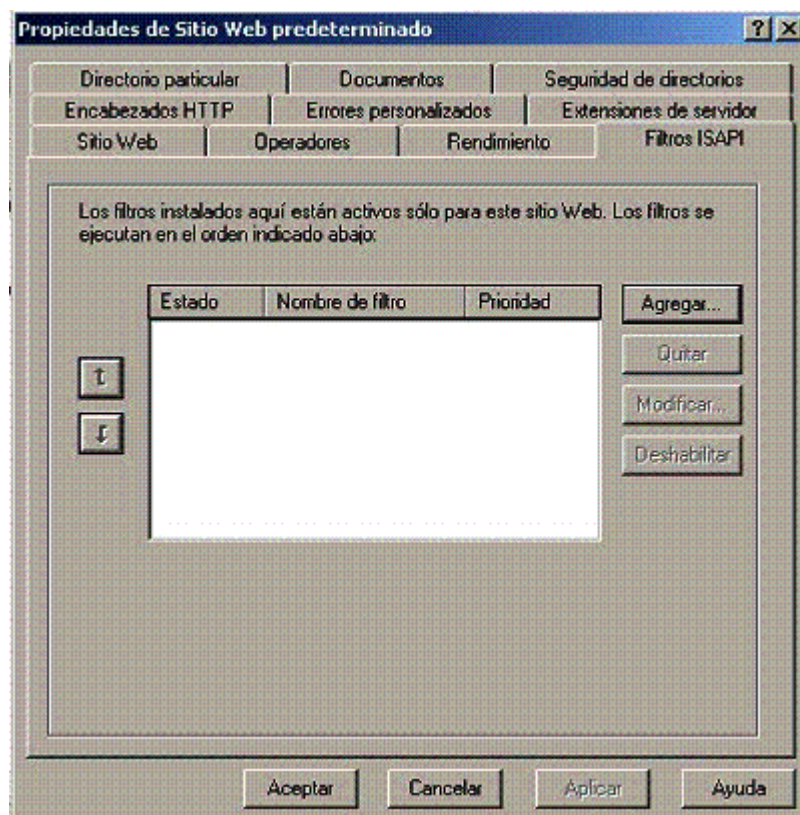
Ajuste de rendimiento: Este ajuste depende del número *hits* diarios esperado. Es conveniente ajustarla a un valor un poco más alto del esperado aunque no mucho.

Habilitar límite de ancho de banda: Esta opción permite establecer el límite para un sitio particular sobrescribiendo la configuración global

Habilitar límite de proceso: Establece un límite al uso de la CPU para atender los requerimientos del sitio. Si se selecciona *hacer cumplir los límites*, entonces el uso de la CPU será limitado al porcentaje establecido, de otra forma se recibirá una notificación en el registro de sucesos.

2.8 Filtros ISAPI

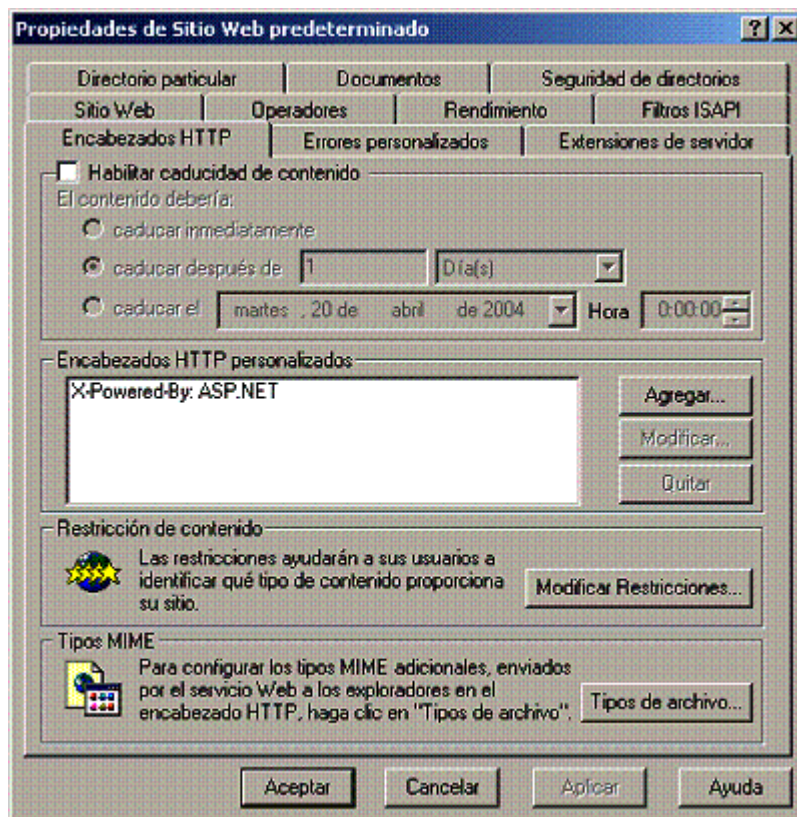
Esta pestaña permite configurar las opciones para los filtros ISAPI. Los filtros ISAPI son programas que responden a eventos que ocurren durante el procesamiento de un requerimiento *http*. Los filtros activos para un sitio Web son la suma de los filtros definidos globalmente más los particulares definidos en el sitio. Es posible agregar nuevos filtros, quitar o deshabilitar filtros existentes o cambiar el orden de prioridad de los mismos (que es el orden en el que se muestran en la lista) usando las flechas de la izquierda.



2.9 Encabezados HTTP

Los *encabezados http* permiten enviar información de control conjuntamente con las páginas html. Entre la información a enviar se encuentran aspectos como tiempo de caducidad, restricciones de contenido, y tipos MIME. Es posible además generar encabezados http personalizados. La opción de *Restricción de contenido* permite configurar

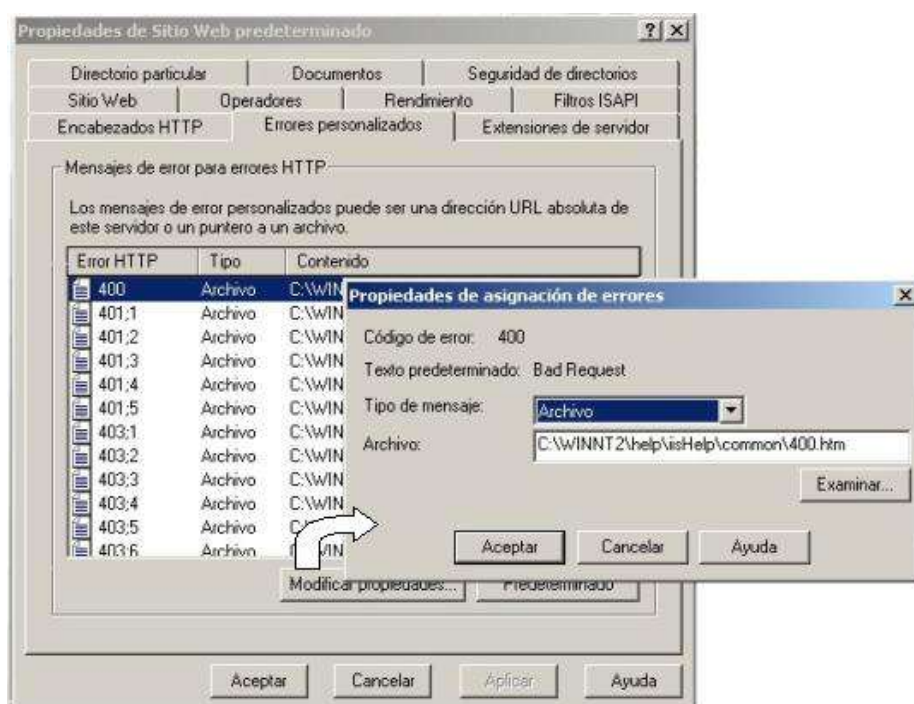
una *categorización* del contenido en temas como violencia, sexo, desnudez y lenguaje. Esta *categorización* está basada en PICS (Platform for Internet Content Selection) del RSAC (Recreational Advisory Council) y permite categorizar cuantitativamente el sitio según el grado de desarrollo de contenidos en los temas anteriores.



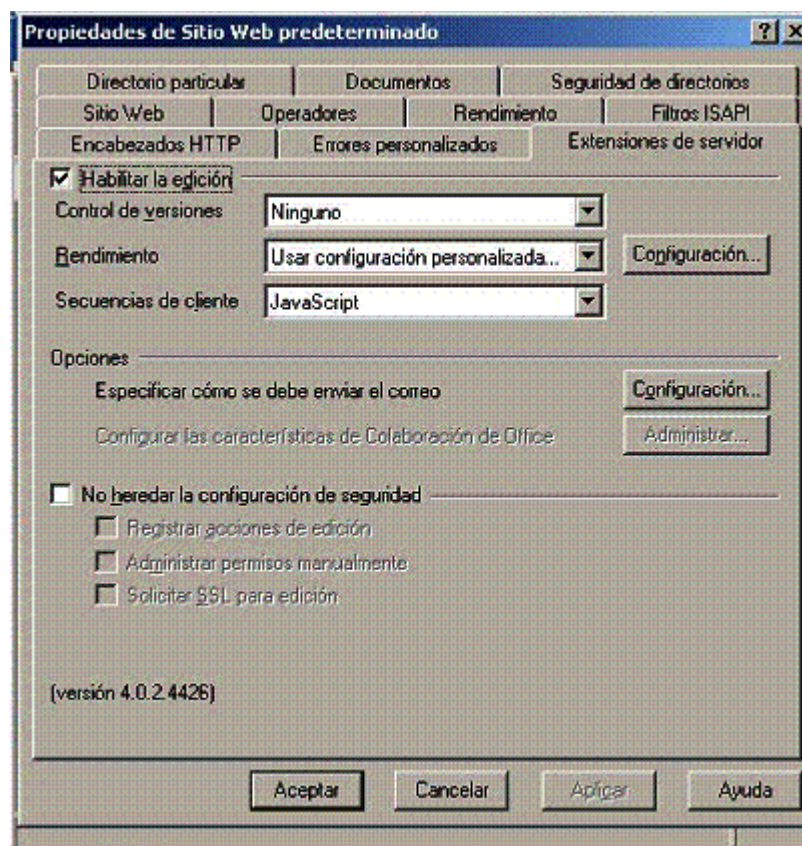
2.10

2.11 Errores Personalizados

Esta pestaña permite configurar el comportamiento en caso de error. Por ejemplo cuando se realiza un requerimiento erróneo se produce un error 400, el cual hace que muestre la página 400.htm. Si se desea cambiar dicho comportamiento puede editarse ese error seleccionándolo y presionando el botón *Modificar propiedades*. Esto permite elegir el tipo de mensaje (en este caso un archivo) y su ubicación si hace falta. Windows 2000 almacena los archivos de mensajes de error en el directorio `%systemroot%\help\iisHelp\common` (%systemroot% es generalmente `c:\winnt`). La siguiente figura muestra la edición del error 400.

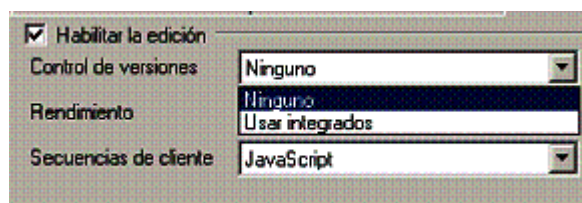


2.12 Extensiones Del Servidor



La pestaña de extensiones del servidor, que se muestra en la figura anterior, nos muestra las propiedades de las extensiones de FrontPage del servidor. Para poder trabajar con esta pestaña primero hay que instalar las extensiones FrontPage, lo cual se logra haciendo click-derecho en el sitio (en el *Administrador de Internet Information Server*) y luego *Todas la tareas/ Configurar extensiones del servidor*. Una vez instalado vemos que la pestaña de Extensiones del Servidor se muestra como la de la figura anterior.

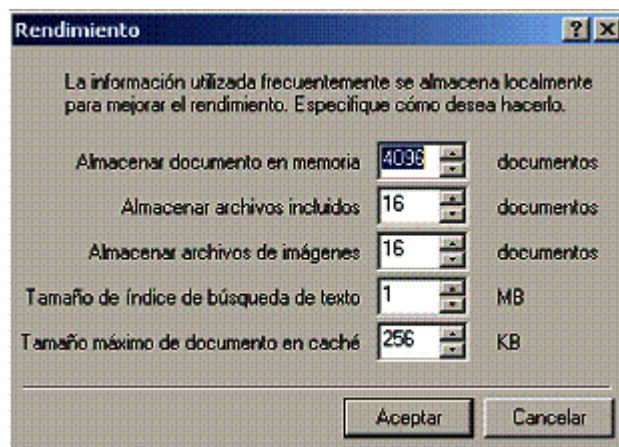
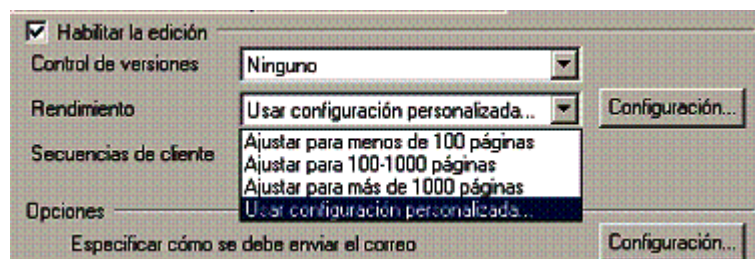
Habilitar la Edición: Permite controlar si los usuarios pueden crear contenido mediante FrontPage. Esta opción habilita también el ajuste de: Control de Versiones, Rendimiento y Secuencias de Cliente.



Control de versiones: Como se ve en la figura es posible utilizar una herramienta de control de versiones integrada que permite llevar un control de quien realiza las modificaciones e impide que se sobrescriban modificaciones entre diferentes autores.

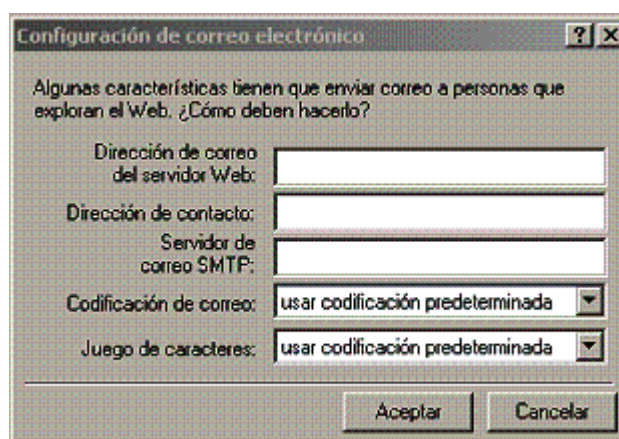
Secuencias de cliente: Permite establecer el lenguaje de *scripting* que se utilizará en el momento que FrontPage genere páginas automáticamente para los usuarios. Puede ser JavaScript o VBScript.

Rendimiento: Como se ve en la siguiente figura, permite ajustar el caché de páginas según la cantidad de páginas que tenga el sitio. Esto logra un balance entre velocidad de respuesta por página en caché y memoria utilizada para el mismo.



Además de las configuraciones de rendimiento preestablecidas, se le agrega la posibilidad de realizar una configuración personalizada. Para ello debe presionarse el botón de *Configuración* a la derecha de la lista desplegable de *Rendimiento*. Como se muestra en la figura anterior, permite un ajuste más fino del caché.

Configuración del correo electrónico: Esta opción permite configurar la utilización del correo electrónico por parte de las extensiones del servidor.



No heredar la configuración de seguridad: Esta opción permite configurar particularmente para el sitio las opciones de seguridad en lugar de heredar las globales. Al marcar la casilla, se habilitan las opciones de: Registrar acciones de edición, Administrar permisos manualmente, Solicitar SSL para edición:

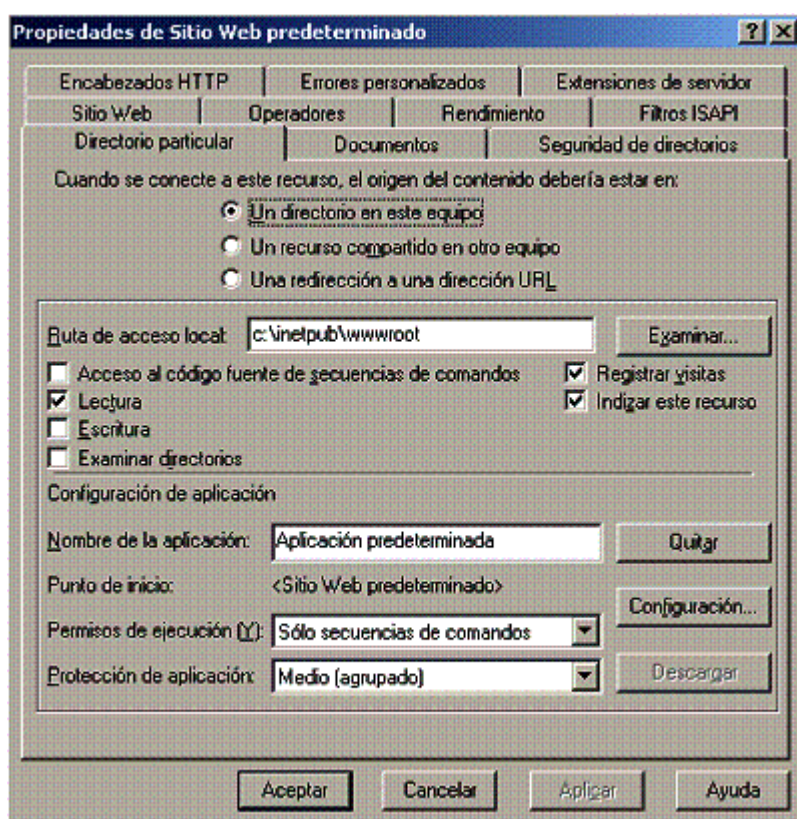
- Registrar acciones de edición: Cada vez que se toma una acción por parte de un autor, como ser modificar el contenido de una página, esta acción se registra en el registro Autor.log ubicada en el directorio _vti_log del sitio. La bitácora contendrá: nombre del autor, nombre del sitio, nombre del host remoto, y datos de la operación.
- Administrar permisos manualmente: Esta opción deshabilita las funciones de configuración de seguridad de las herramientas propias de las extensiones del servidor FrontPage. De esta forma no puede usarse las herramientas como MMC (consola de administración de Microsoft) para modificar la configuración de seguridad.
- Solicitar SSL: Permite que los autores Web utilicen SSL para envío de información. Es útil cuando se utiliza autenticación básica y se quiere evitar que la información sensible como usuario y contraseña puedan ser vista al circular por Internet.

2.13 Directorio Particular

Permite configurar donde se busca el contenido y que permisos se usan para administrar el mismo. Cada sitio Web debe tener un directorio particular. Debe tenerse en cuenta que un sitio Web y un sitio FTP en el mismo equipo no se pueden configurar en el mismo directorio.

Como se ve en la siguiente figura hay tres opciones posibles

- Un directorio ubicado en este equipo.
- Un recurso compartido ubicado en otro equipo.
- Una redirección a una dirección URL.

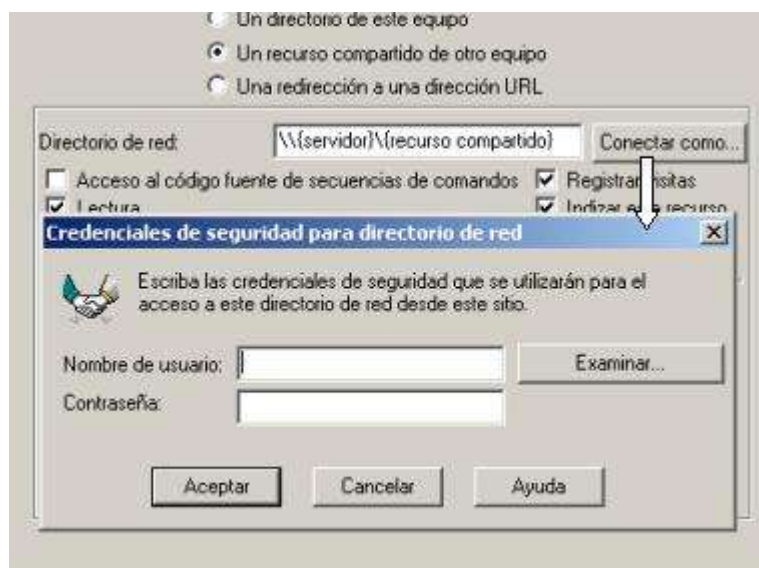


Al seleccionar una de las opciones cambia el resto de la pestaña para adaptar la configuración a la opción seleccionada.

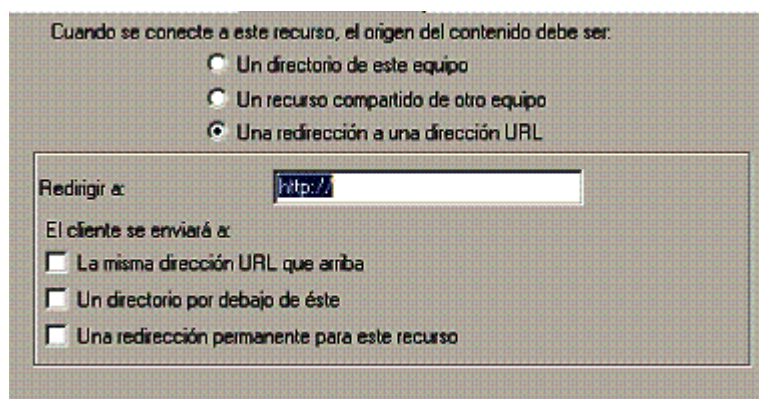
La opción *Un directorio de este equipo* permite elegir un directorio local donde almacenar el contenido del sitio. El directorio es por defecto el especificado al crear el sitio.

La opción *Un recurso compartido en otro equipo* permite distribuir la información en varios servidores. Al seleccionarla la caja de texto *Ruta de acceso local* cambia a *Directorio de red* y muestra el formato UCN `\\{servidor}\{recurso compartido}` para acceder la ubicación. Es posible que IIS deba autenticarse para acceder al servidor donde se encuentran los datos. Para ello se encuentra el botón *Conectar como* que al presionarlo muestra un dialogo donde

se ingresa usuario y password como se ve en la siguiente figura:



La última opción *Una redirección a una dirección URL* permite redirigir al usuario a otra URL específica. Esta alternativa cuenta con tres alternativas de configuración como se ve en la siguiente figura:

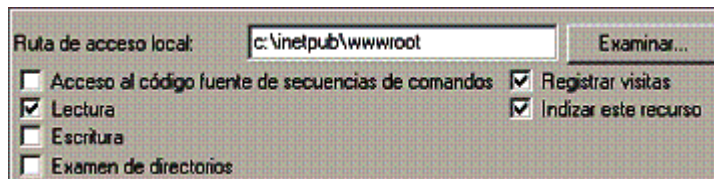


En el cuadro de texto *Redirigir a* se debe acceder la URL a donde se desea redirigir al cliente. La alternativa *La misma dirección URL que arriba* indica que se dirigirá a la dirección exacta que se ingresó. La otra alternativa es que se puede redirigir a un directorio particular.

La última, *Una redirección permanente para este recurso* se utiliza si se ha cambiado el sitio de lugar permanentemente y entonces el servidor enviará un mensaje 301 de redirección permanente en lugar de un mensaje redirección temporaria 302. Esto es útil ya que algunos navegadores toman en cuenta estos mensajes para actualizar sus marcas de favoritos.

Si se selecciona la opción *Un directorio en este equipo* o *Un recurso compartido en otro equipo* entonces se presenta la posibilidad de realizar una serie de configuraciones más avanzadas. En la siguiente figura se muestra el

primer grupo de opciones:

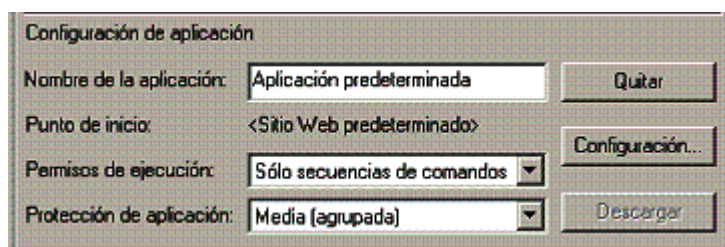


Las opciones de Lectura, Escritura y Examen de directorios son idénticas a las mencionadas anteriormente.

La opción *Acceso al código fuente de secuencias de comandos* permite acceder al código de los scripts incluso los ASP. Sólo se habilita cuando los permisos de Lectura y Escritura están habilitados.

Indexar este recurso que *Microsoft Indexing Service* indexa todo el contenido del sitio acelerando la búsqueda de datos de texto.

El otro grupo de opciones que se muestra en la siguiente figura tiene que ver con la configuración de la aplicación:

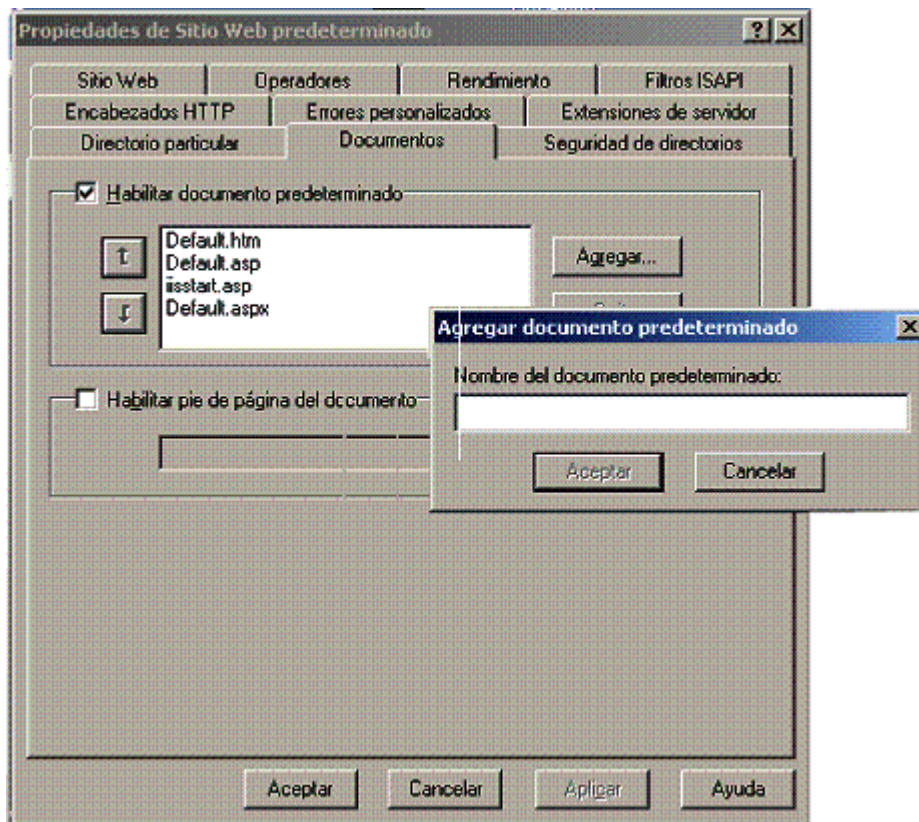


Una aplicación es un archivo que se ejecuta dentro de un conjunto predefinido de directorios del sitio Web. Las opciones de configuración son:

Permisos de ejecución Permite establecer qué se puede ejecutar en el sitio, las alternativas son: sólo secuencia de comandos, secuencia de comandos y ejecutables y ninguno.

Protección de la aplicación: Los niveles de aislamiento de las aplicaciones se configuran seleccionándolos de la lista desplegable. Hay tres niveles posibles: *baja* en el cual las aplicaciones se ejecutan en el mismo espacio de direcciones que IIS, *media* en el cual las aplicaciones se ejecutan en un espacio común para todas, es decir agrupadas, y *alta* donde cada aplicación se ejecuta aislada de las otras.

2.14 Documentos



La figura anterior nos muestra la pestaña de documentos. Aquí es donde se configuran los documentos predeterminados. Si el usuario no ingresa ningún nombre de documento entonces IIS buscará un documento con los nombres de la lista en el orden que está establecido. Si el usuario no ingresa el nombre del archivo y no hay archivo por defecto entonces IIS presentará un mensaje de *Acceso prohibido* (siempre que la opción *Examinar directorios* haya sido deshabilitada).

Si se selecciona *Habilitar pie de página de documento* IIS agregará al pie de cada página enviada el contenido del documento que se especifique como pie de página (por ejemplo el nombre de la empresa, el e-mail de webmaster o información copyright) el documento no debe ser un documento HTML con todos los marcadores completo, sino solamente la parte que se quiere mostrar con los marcadores (tags) necesarios pero como si se estuviera escribiendo dentro de una página (que es lo que en definitiva hace el IIS).

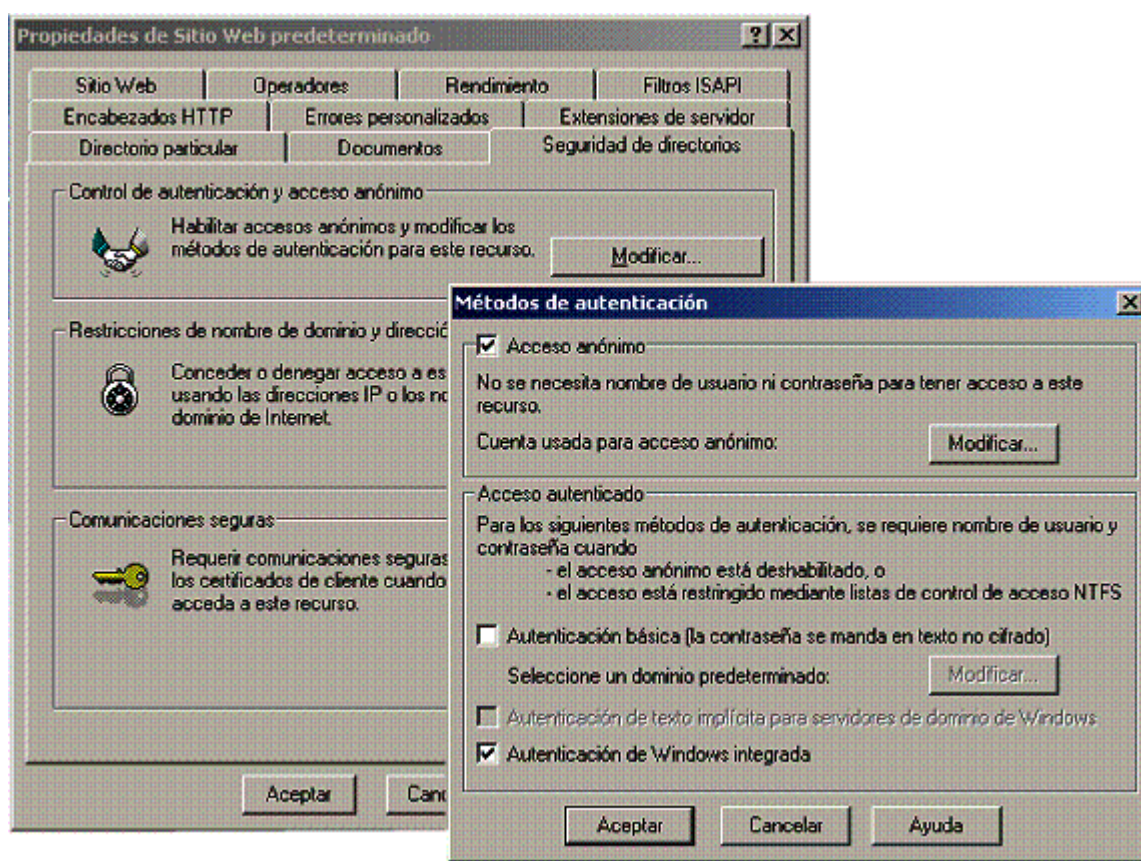
2.15 Seguridad De Directorios

Esta pestaña es la que permite configurar quien y como se accede al sitio Web. Se puede permitir el acceso basado en dirección IP del cliente, autenticación o listas de control de acceso.

La siguiente figura muestra la pantalla con los tres aspectos a configurar: *Control de autenticación y acceso anónimo*, *Restricciones de nombre de dominio y dirección IP* y *Comunicaciones seguras*.



El primer método de seguridad es el control de autenticación, presionando el botón *Modificar* se presenta el siguiente dialogo:



En caso de selección *Acceso Anónimo* no es necesario especificar ni usuario ni contraseña para acceder al sitio. De todas formas, una cuenta debe ser usada para el acceso anónimo. Se utiliza por defecto una cuenta creada por IIS (IUSR_[HOSTNAME]).

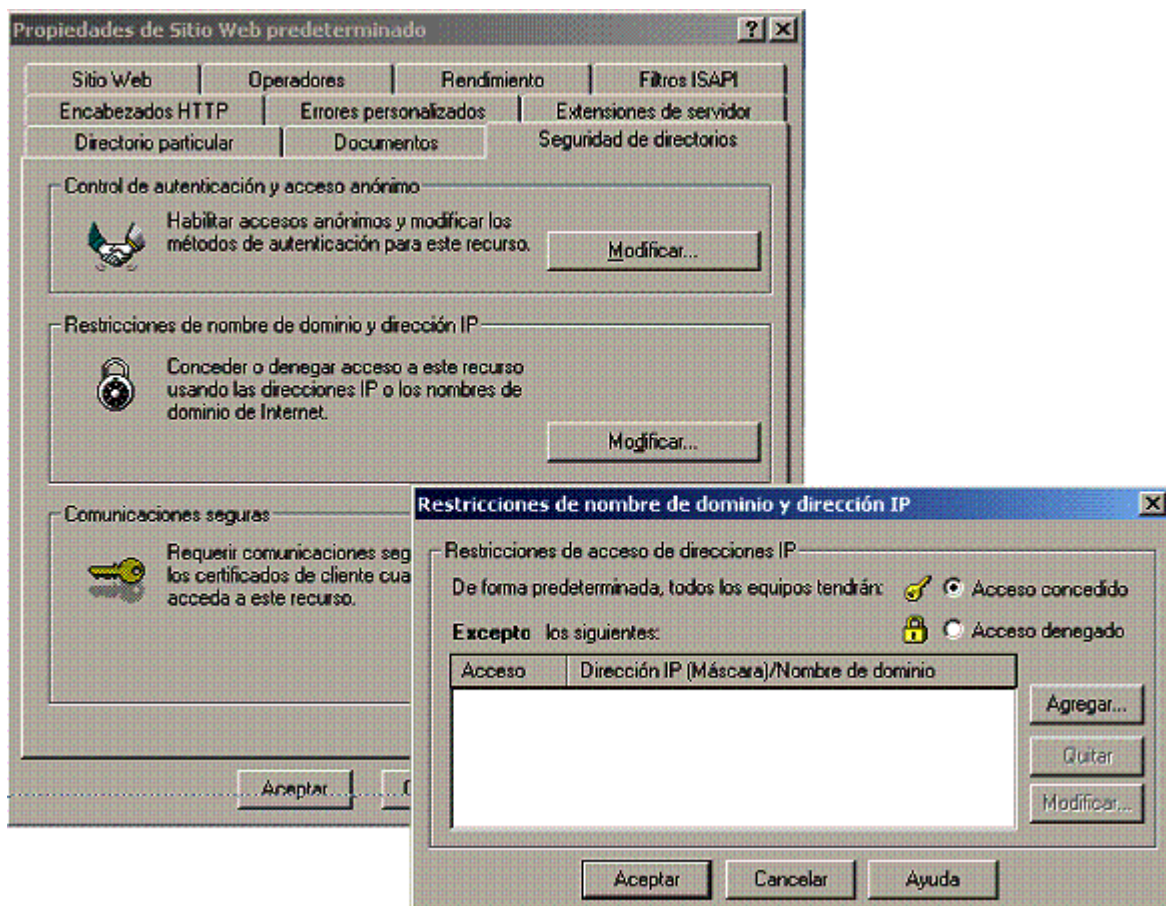
En caso de necesitar proteger o asegurar todo el sitio (o alguna área del mismo) se debe deseleccionar la casilla *Acceso Anónimo*. En este último caso toma importancia el resto de las opciones de los métodos de autenticación que pueden ser *Básica*, *Implícita* o *Windows Integrada*. La primera es la más sencilla y es soportada por la mayor parte de los navegadores. La contraseña y usuario viajan en texto claro por la red por lo cual es también la menos segura.

La segunda es nueva en IIS 5 y Windows 2000. En lugar de transmitirse la contraseña en texto claro se envía un código de *hashing*. Como contra, tiene una serie de exigencias para su uso como ser tener un navegador Internet Explorer 5 o superior y que la contraseña se almacene en *Active Directory* en forma de texto claro.

La última (que es marcada por defecto) requiere Internet Explorer (desde la versión 2 ya funciona) y se envía un código de hash (en lugar de la contraseña) luego se controla contra el dominio de IIS.

Como alternativa es posible mantener el Acceso Anónimo y utilizar los permisos de NTFS para controlar el acceso a los directorios. Cuando el acceso falla porque la cuenta del usuario anónimo no tiene suficientes permisos, IIS utiliza alguno de los otros métodos de autenticación establecidos (integrado por defecto).

El segundo método de seguridad es restringir el acceso por dirección IP o nombre de dominio. De esta forma sólo usuarios conectados desde determinados dominios o desde determinada dirección IP, tendrán acceso al sitio. Es posible conceder o denegar acceso al sitio a determinadas direcciones IP (siempre es mejor que usar nombres de dominio porque se evita una búsqueda). Como se ve en la siguiente figura es posible conceder acceso a todos excepto a algunas direcciones, seleccionando *Acceso concedido* y agregando las direcciones IP a las que se les quiera denegar el acceso. También es posible denegar el acceso a todos y permitir sólo a algunas; esto se logra seleccionado *Acceso denegado* y luego agregando las direcciones IP a las que se les quiera conceder el acceso. Este tipo de seguridad puede combinarse con la anterior para tener un ambiente aún más seguro.



La última opción es requerir el uso de Comunicaciones Seguras mediante SSL para lo cual es necesario tener instalado un certificado. Al usar SSL el tráfico entre el cliente y el servidor viaja cifrado.



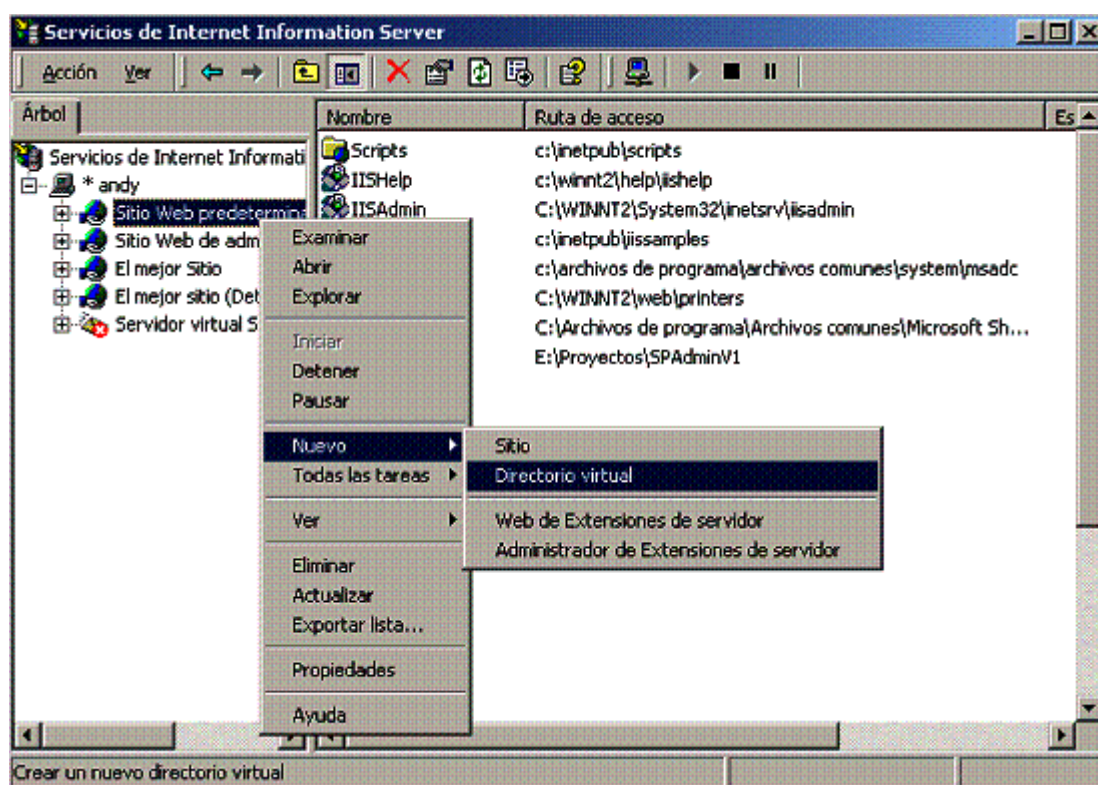
2.16 Directorios Virtuales

Hasta aquí se han organizado los sitios en un directorio raíz, con la posibilidad de agregarle subdirectorios a éste para organizar el contenido. Esta forma de organización está limitada al disco y computadora donde reside el directorio raíz. Existe otra forma de organizar la estructura de los sitios utilizando directorios en otros discos de la misma máquina o diferentes equipos. Se trata de los *directorios virtuales*.

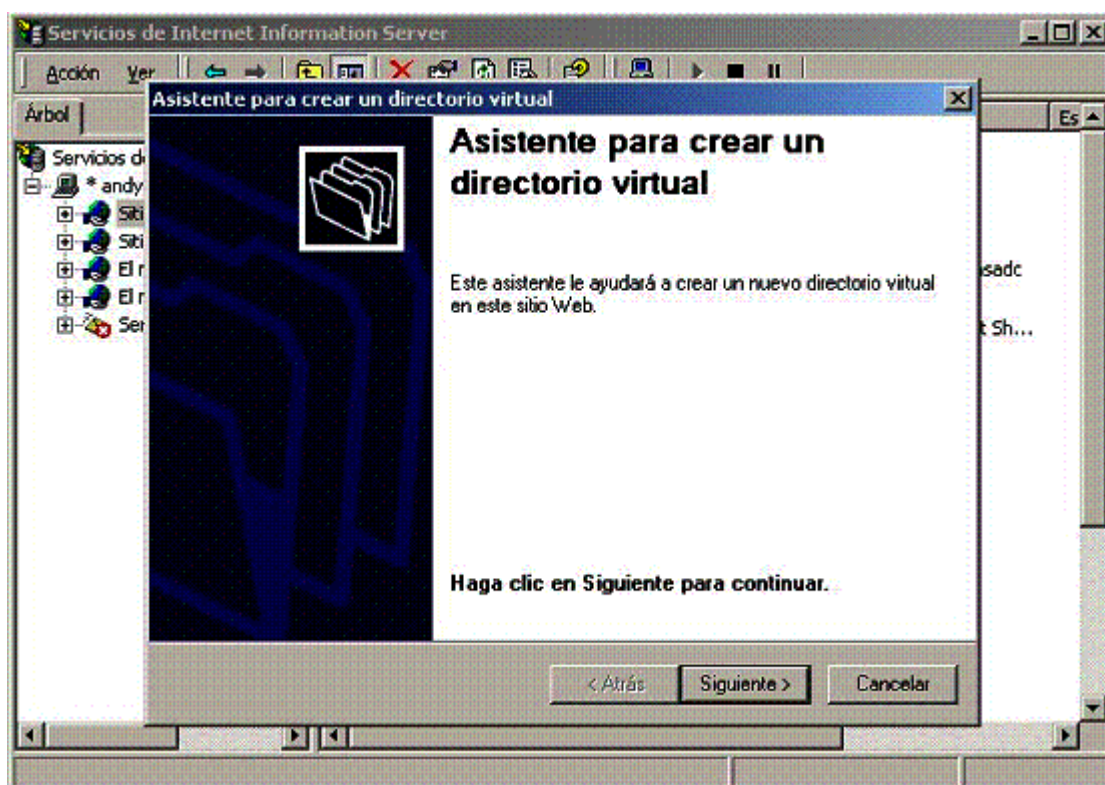
Para crear un directorio virtual es necesario definir un *alias* para él. Por ejemplo si el sitio Web tiene como nombre *www.miempresa.com* es posible definir un alias *virtual1*, de tal forma que el acceso al directorio virtual sea de la siguiente forma: *www.miempresa.com/virtual1*.

Los pasos a seguir para crear un directorio virtual son los siguientes:

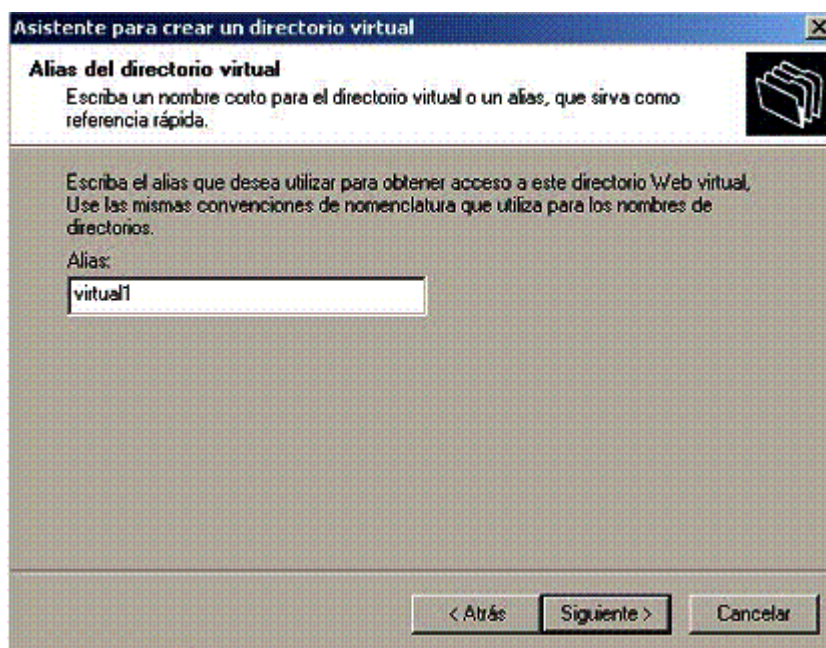
1) En la consola de administración de Servicios de *Internet Information Server* se debe seleccionar el sitio bajo el cual se desea crear el directorio virtual y hacer *click-derecho/Nuevo/Directorio virtual* como se ve en la figura siguiente:



2) Se mostrará el *Asistente para crear un directorio virtual*. Se presiona *Siguiente*

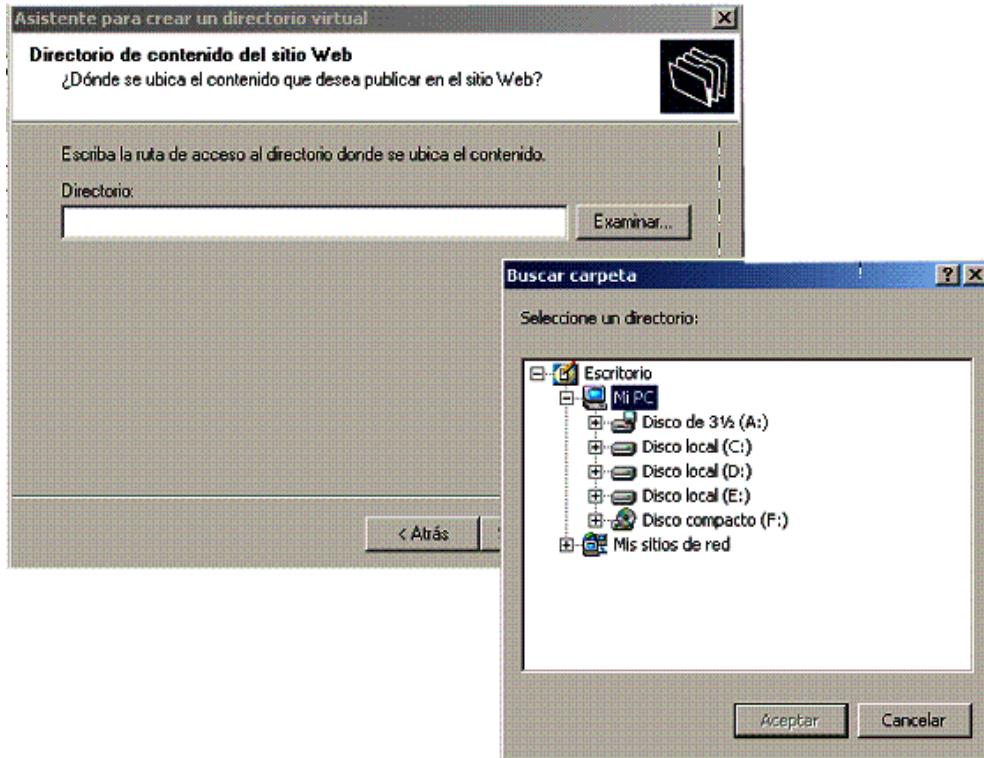


- 3) Lo primero que se debe acceder es el alias, bajo el cual se accederá al *directorio virtual*.



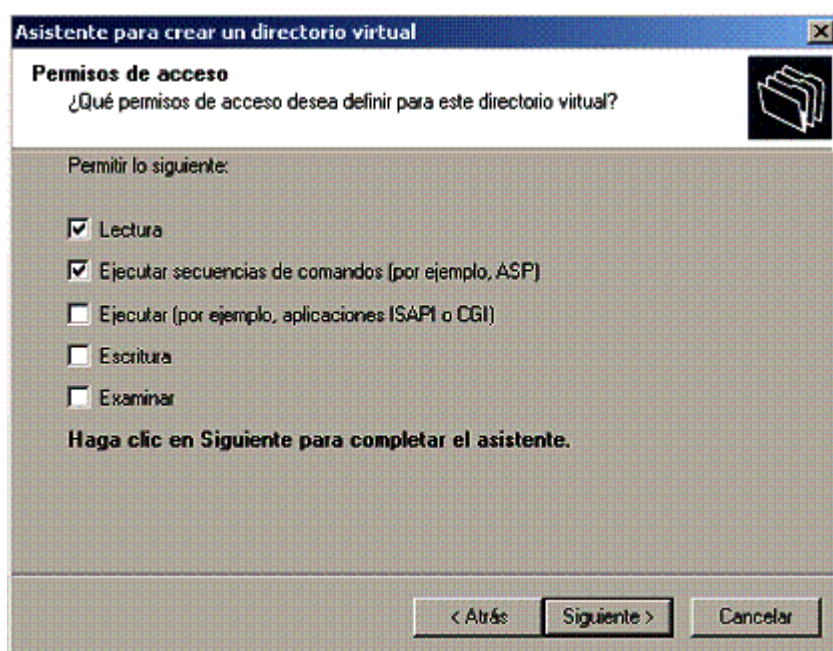
- 4) Luego debe accederse la ubicación del directorio virtual que puede ser un directorio local en la

forma `c:\directorio` o un directorio remoto usando UNC. En caso de seleccionar un directorio remoto, IIS pedirá las credenciales para conectarse y acceder a él. También es posible presionar en *Examinar* y seleccionar el directorio en el diálogo correspondiente:

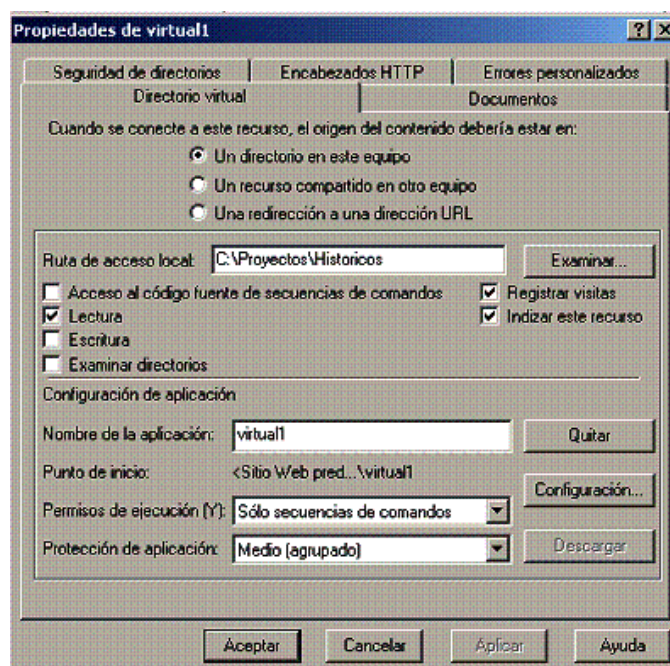


5) Luego se deben configurar los permisos de acceso al directorio en forma similar a lo realizado al crear un sitio Web, marcando las casillas correspondientes , como se ve en la siguiente figura:





Las propiedades del directorio virtual pueden modificarse de la misma forma que las propiedades del sitio mediante el diálogo de *Propiedades*.

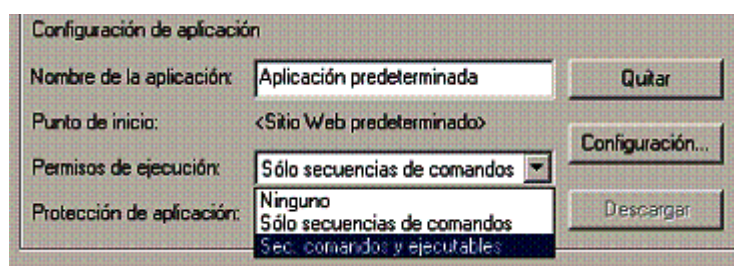


2.17 Instalando Soporte Para CGI/PERL

Si bien ASP es el método de desarrollo preferido para la realización de aplicaciones Web sobre IIS 5, existen otras opciones que son ampliamente usadas sobre la Web (fundamentalmente en sitios alojados en máquinas Linux / UNIX con servidores Apache). La interfaz de programación es conocida como CGI *Common Gateway Interface*.

CGI permite a un servidor Web interactuar con programas que pueden ser escritos en cualquier lenguaje. CGI no es un lenguaje, es una interfaz que puede ser utilizada por los desarrolladores. Los lenguajes más populares son: PERL y PHP aunque es posible utilizar casi cualquier lenguaje. Estos están particularmente adaptados al desarrollo de aplicaciones CGI.

El propio servidor Web es el encargado de disparar la ejecución de los programas CGI que deben residir en directorios con permisos suficientes como se muestra en la siguiente figura, dando permisos de ejecución a secuencia de comandos y ejecutables.



La comunicación entre el servidor Web y el programa se realiza según la especificación WinCGI mediante un parámetro de la línea de comandos el *cgi_data_file* que es un archivo creado por el servidor en un formato similar a los archivos .INI. Este archivo contiene toda la información necesaria para la ejecución del programa CGI.

Para desarrollar aplicaciones CGI en PERL (Practical Extration and Report Language) es necesario instalar el mismo. PERL es código abierto y los códigos fuente se encuentran disponibles en la Web. Existe una versión denominada ActivePerl que para un entorno Win32 como el de IIS cuenta con un conjunto de características específicas de la plataforma. ActivePerl puede descargarse de la página de ActiveState en www.activestate.com. La versión 5.8.3 en formato de instalación de Windows MSI tiene un tamaño de 12 MB. La instalación es sencilla pero para versiones de W2000 y 9X es recomendable tener la versión de MSI actualizada. Una vez instalado es posible poner programas PERL en los directorios habilitados.



2.18 Instalando Soporte Para ASP.NET

ASP.NET es el soporte de aplicaciones Web basado en el .NET Framework el cual ofrece un cambio radical en la forma de desarrollar aplicaciones. A las facilidades de desarrollar aplicaciones Web en diversos lenguajes como ser: VisualBasic, J#, el nuevo lenguaje de Microsoft C#, Eiffel, ComponentPascal, Delphi, etc. que es una característica notable del modelo de desarrollo .NET, se agregan una serie de mejoras con respecto a ASP. Entre las ventajas se encuentran:

- Ejecución compilada
- Soporte completo del .NET Framework
- Manejo de Caché superior.
- Administración de sesiones en granja de servidores.
- Sesiones pueden almacenarse en SQL Server 2000.
- Protección contra *deadlock* y caídas.
- Modelo de eventos del lado servidor
- Etc, etc.

Si se desarrollaran aplicaciones con MS Visual Studio entonces al instalar los prerequisites del mismo se instalará el *.NET framework* lo que dejará el servidor preparado para ASP.NET. No olvidar que es condición previa necesaria instalar las extensiones de FrontPage para el servidor.

Microsoft provee a su vez un entorno de desarrollo gratuito llamado *ASP.NET Web Matrix* que puede ser descargado de la Web (tiene un tamaño de solamente 1.3MB).

Previo a la instalación de *ASP.NET Web Matrix* (y de poder ejecutar aplicaciones ASP.NET) es necesario que se haya instalado el .NET Framework que puede obtenerse como actualización del sitio de Microsoft para Windows 2000 o XP (viene incluido en W2003 Server). Desde el sitio www.asp.net donde se encuentra el *ASP.NET Web Matrix* también puede descargarse el .NET Framework que tiene un tamaño de 23 MB.



2.19 Internet Information Services 6

MS Windows 2003 tiene integrada la nueva versión de IIS, la versión 6 presenta un cambio fundamental en la arquitectura para proveer servicios Web por parte de Microsoft. Los servicios de FTP, SMTP y NNTP no han cambiado notoriamente. Pero los servicios http han sido mejorados en varios aspectos.

La instalación de IIS6 no se realiza con el sistema operativo a diferencia de IIS 5 y Windows 2000. Por lo cual hay que proceder a su instalación separadamente de forma similar a instalar IIS 5 sobre un Windows 2000 que no lo tenga instalado. Para ello se utiliza *Agregar o quitar programas/Componentes de Windows* del panel de control.

Los pasos son:

1. En el panel de control click sobre *Agregar o quitar programas* para abrir el diálogo correspondiente
2. Click sobre *Agregar o quitar componentes de Windows*. Y abrirá el asistente de instalación de componentes de Windows
3. Realizar Click en *Servicios de Aplicación* y el botón de *Detalles*
4. Los componentes de IIS se localizan en el área de *Internet Information Services*

La parte más interesante es la de *World Wide Web Service* que provee los servicios donde se pueden ver los subcomponentes

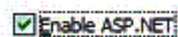
- *Active Server Pages*: Instala ASP.DLL que permite soportar páginas ASP (esta opción es instalada siempre pero se encuentra deshabilitada por defecto)
- *Internet Data Connector*: IDC permite la conectividad con bases de datos. Esta opción siempre es instalada.
- *Remote Administration HTML*: Permite la administración remota del IIS utilizando un navegador Web.
- *Remote Desktop Web Connection*: Instala un control ActiveX que permite que Internet Explorer se conecte a una sesión de Terminal Server. En Windows 2000 se conocía como Terminal Services Advanced Client.
- *WebDAV Publishing*: WebDAV significa *Web-based Distributed Authoring and Versioning* y es un conjunto de extensiones de http que permite el acceso y administración de archivos por parte de los usuarios en los directorios publicados como WebDAV.

- **World Wide Web Service:** Es el componente principal. Sin él casi nada trabaja.

Entre las ventajas de IIS6 que implican mayor confiabilidad, escalabilidad y seguridad se encuentra el soporte de ASP.NET ya que Windows 2003 incluye soporte para aplicaciones ASP.NET y el *.NET Framework versión 1.1*. Como ASP.NET no está habilitado por defecto hay dos formas de habilitarlo: una siguiendo el asistente de configuración del Server donde hay que elegir servidores de aplicación

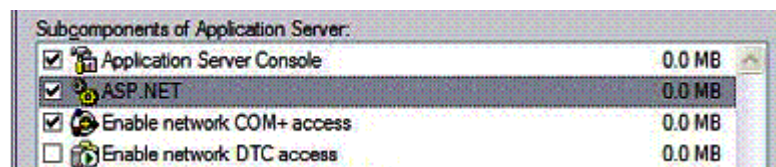
Server Role	Configured
File server	Yes
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	No

y en el otro paso marcar la casilla de ASP.NET



ASP.NET is a powerful programming framework for building Web-based applications and services that can target any browser or device.

La otra opción es seguir los pasos de instalación dados anteriormente y en los subcomponentes del servidor de aplicaciones elegir ASP.NET



2.20 Utilización De JSP/Servlets Con IIS

Para poder ejecutar JSP (Java Server Pages) y Servlets en Internet Information Server, es necesario instalar un contenedor para soportarlas. Se trata de un motor que soporte la ejecución de servlets.

Existen diversos tipos de motores independientes y algunos que pueden ser agregados (*adds-on*) como extensiones modulares IIS para soportar la ejecución de Servlets.

Entre los contenedores más conocidos se encuentra Tomcat (para una lista completa ver en <http://java.sun.com/products/servlet/industry.html>). Tomcat es el contenedor usado en la *Reference Implementation* oficial para las tecnologías Java Servlet y Java Server Pages .Por tal motivo, es el que se utilizará en este curso. Se desarrolla bajo la *Apache Software License* que es la licencia del popular servidor Web de la comunidad de software libre Apache (el cual se estudiará posteriormente).

Una vez instalado Tomcat (supongamos en c:\jakarta-tomcat), se encuentran los siguientes subdirectorios:

- c:\jakarta-tomcat\conf
- c:\jakarta-tomcat\webapps
- c:\jakarta-tomcat\bin

El subdirectorio *\conf* es el lugar donde se ubican los diversos archivos de configuración, el subdirectorio *\webapps* guarda las aplicaciones de ejemplo y en el subdirectorio *\bin* se ubican los *plugins* (extensiones insertables) del web server. Un proceso que acepta solicitudes desde el IIS es llamado *worker*.

Para poder enviar las solicitudes de JSP/Servlets a Tomcat se utilizan redirectores que deben instalarse como filtros en IIS. Es posible descargar una versión binaria del redirector ISAPI (ISAPI es la interface de programación de aplicaciones de IIS, y entre otras cosas permite la ejecución de procesos externos desarrollados como DLLs). La versión binaria es *isapi_redirect.dll*. Es posible descargarla desde el sitio de Tomcat en formato binario.

El redirector de Tomcat requiere tres archivos

1. *isapi_redirect.dll*: La isapi DLL que actúa como filtro
2. *workers.properties*: Es un archivo que tiene la información sobre los puertos y máquinas que usan los workers.

3. `uriworkermapping.properties`. Este archivo, como su nombre lo indica, permite el mapeo entre URIs y workers.

De todas formas, existen archivos de ejemplo de estos dos últimos ubicados en el directorio de configuración (`\conf`).

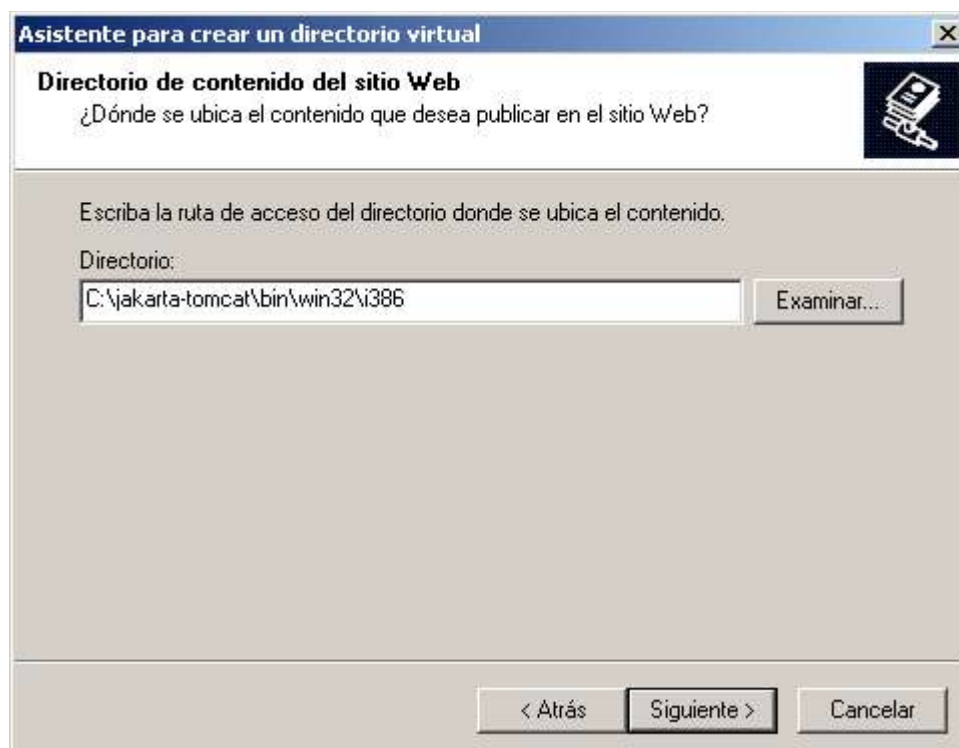
Los siguientes pasos permiten configurar el redirector:

- El registro de Windows (invocando Ejecutar\regedit) agregar una nueva clave:
 - "HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0"
- Agregar un valor de tipo string (cadena) con `extension_uri` como nombre y valor `/jakarta/isapi_redirect.dll`
- Agregar un valor de tipo string (cadena) con `log_file` como nombre y como valor el lugar donde se quiere que se ubiquen el archivo de log por ejemplo: `c:\jakarta-tomcat\logs\isapi.log`
- Agregar un valor de tipo string (cadena) con `log_level` como nombre y como valor el nivel de detalle que se quiere en el archivo de log (esto, luego, puede modificarse para ajustar la depuración del servicio. Los valores posibles pueden ser
 - debug (depuración)
 - info (información)
 - error (error)
 - emerg (emergencias)
- Agregar un valor de tipo string (cadena) con `worker_file` como nombre y como valor el camino completo al archivo `workers.properties`.
- Agregar un valor de tipo string (cadena) con `worker_mount_file` como nombre y como valor el camino completo al archivo `uriworkermapping.properties`.
- Luego se utiliza la consola de administración del IIS para agregar un directorio virtual nuevo.
- El nombre del directorio virtual debe ser `jakarta`

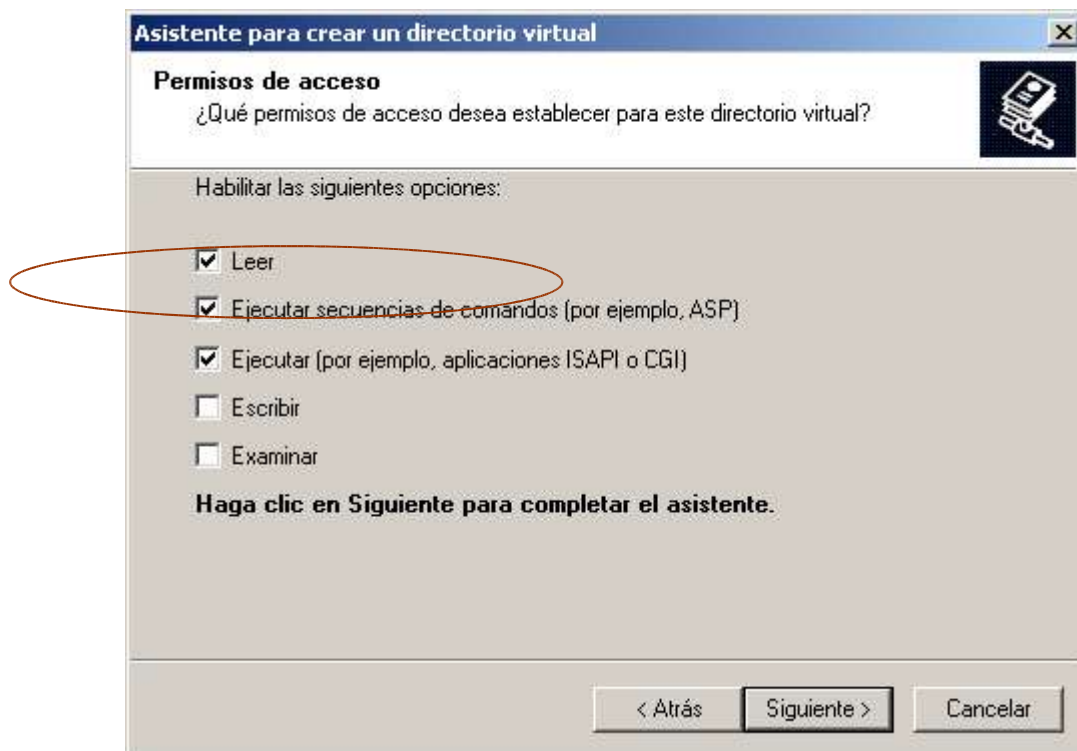




- El lugar físico debe ser el directorio donde se ubica la isapi_redirect.dll.

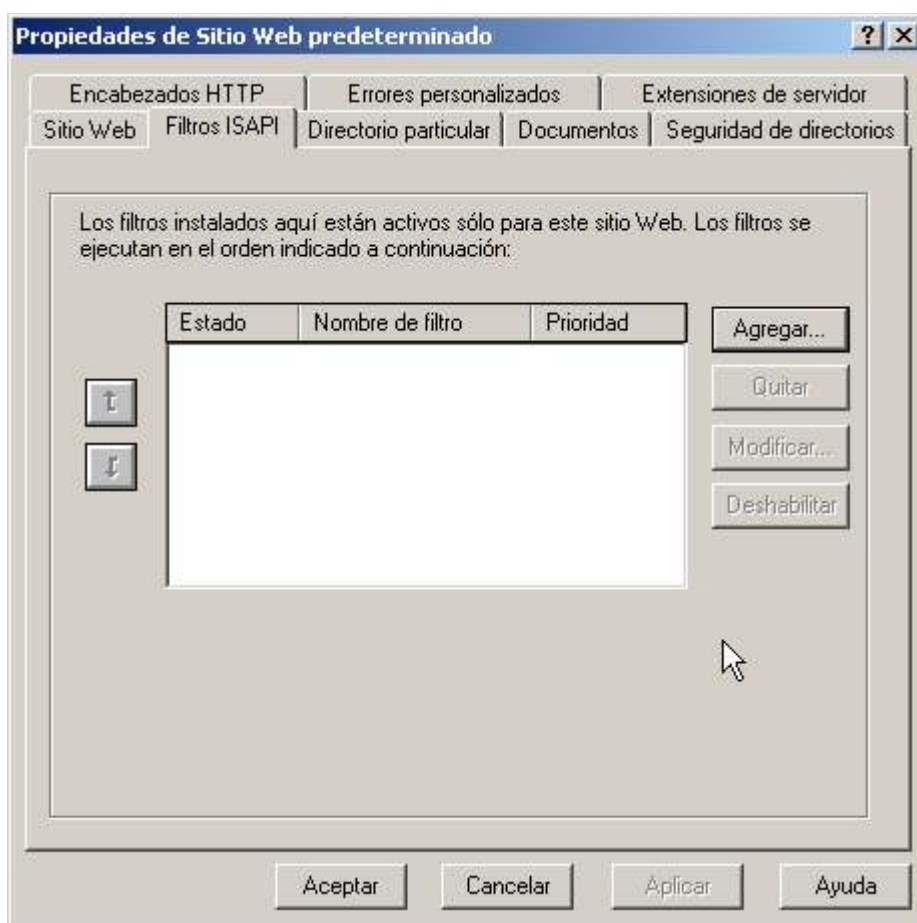


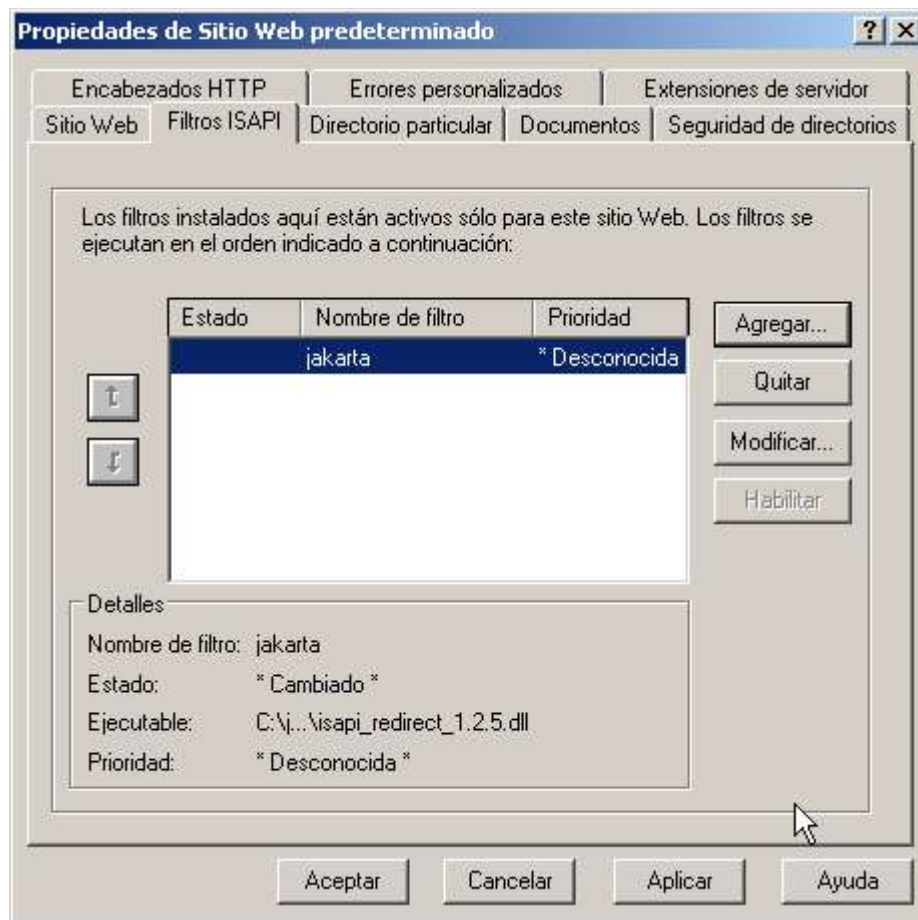
- Asignarle al directorio permiso de ejecución



- Luego se debe agregar el filtro al IIS. El ejecutable del filtro debe ser el isapi_redirect.dll. Las siguientes figuras muestran el agregado del filtro al servidor.







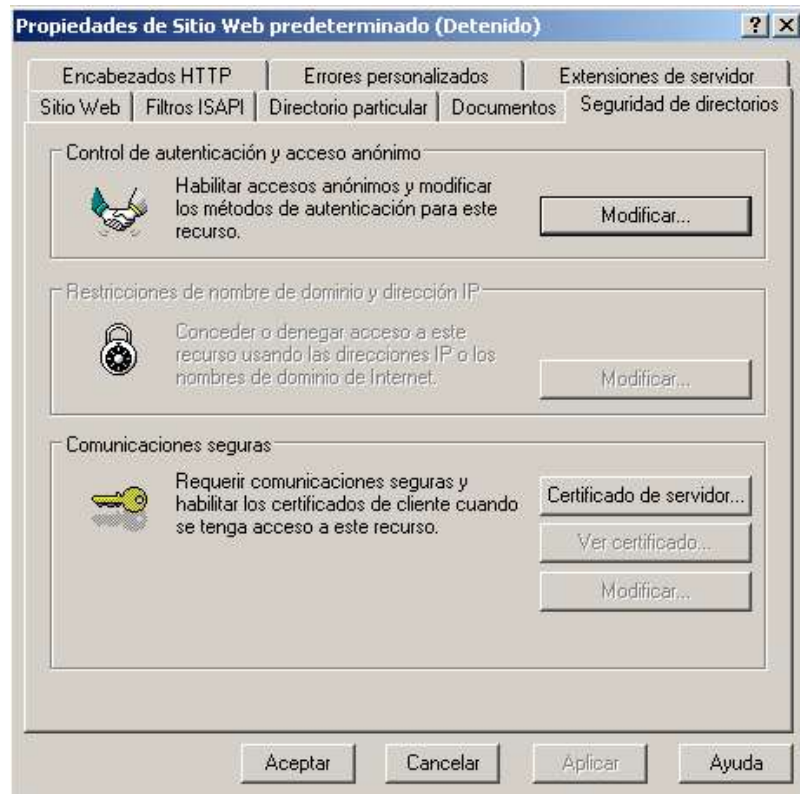
- Se debe reinicializar el servicio.

De esta forma, se tiene instalado el servicio de redirector de Tomcat para IIS. Como existen numerosos contenedores de JSP/Servlets es imposible generar una configuración estándar y cada uno tendrá sus opciones técnicas particulares. Lo importante es notar que IIS no tiene el soporte nativo para JSP/Servlets como tiene para ASP. Esto obliga a la instalación de un contenedor de terceras partes.



2.21 Soporte De SSL En IIS

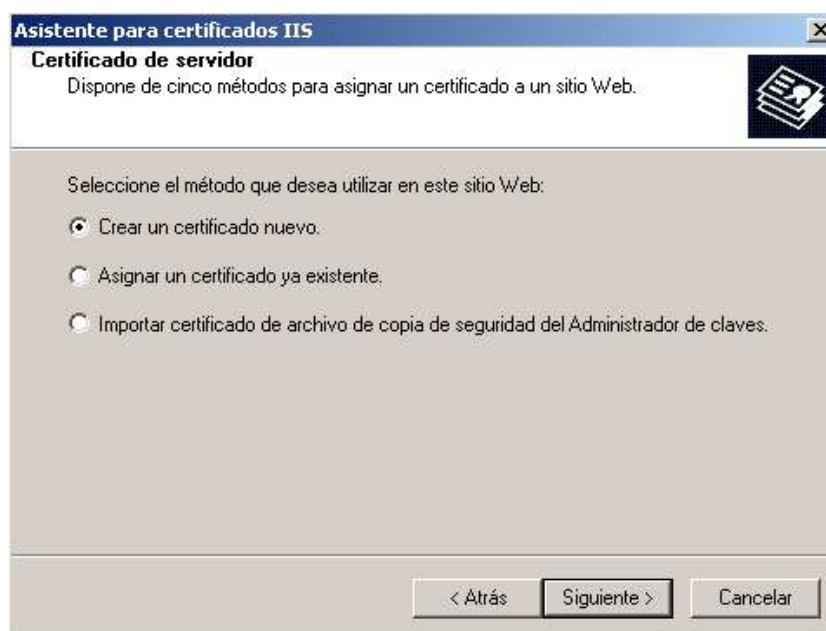
Para poder utilizar soporte de SSL en IIS es necesario instalar un certificado. Para ello hay que ir a la ventana de propiedades del sitio Web y hacer click en *Certificado de servidor*



Esto lanza el asistente para certificados Web:



Simplemente, siguiendo el asistente como se muestra en las siguientes figuras, se obtiene un archivo de texto:



Se elige crear un certificado nuevo.



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

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:

miempresa.com

< Atrás Siguiente > Cancelar



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.

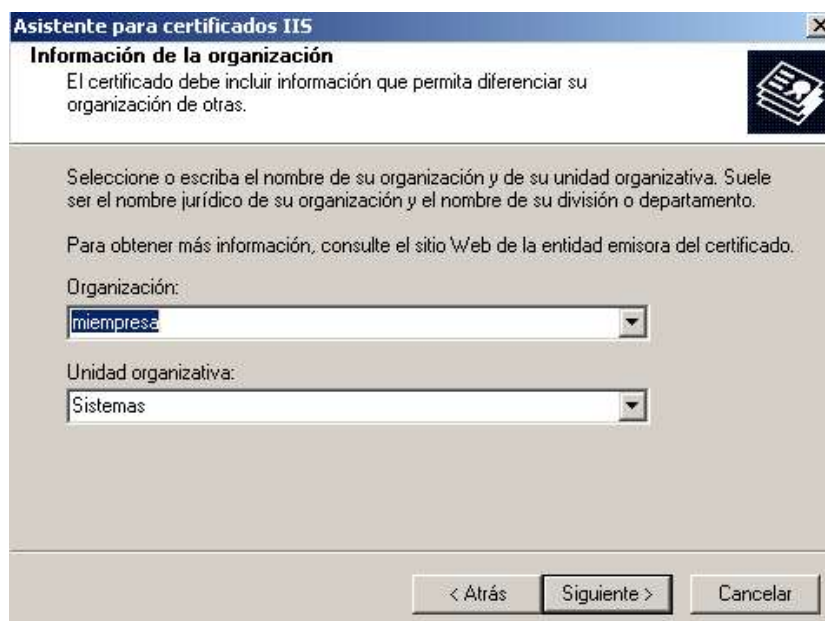
Nombre:

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:

☐ Certificado de criptografía activada por servidor (SGC) (sólo para las versiones exportadas)
☐ Seleccionar el proveedor de servicios criptográficos (CSP) para este certificado

Se debe ingresar un nombre al certificado. Luego se deben completar los datos de empresa y ubicación geográfica:



Asistente para certificados IIS

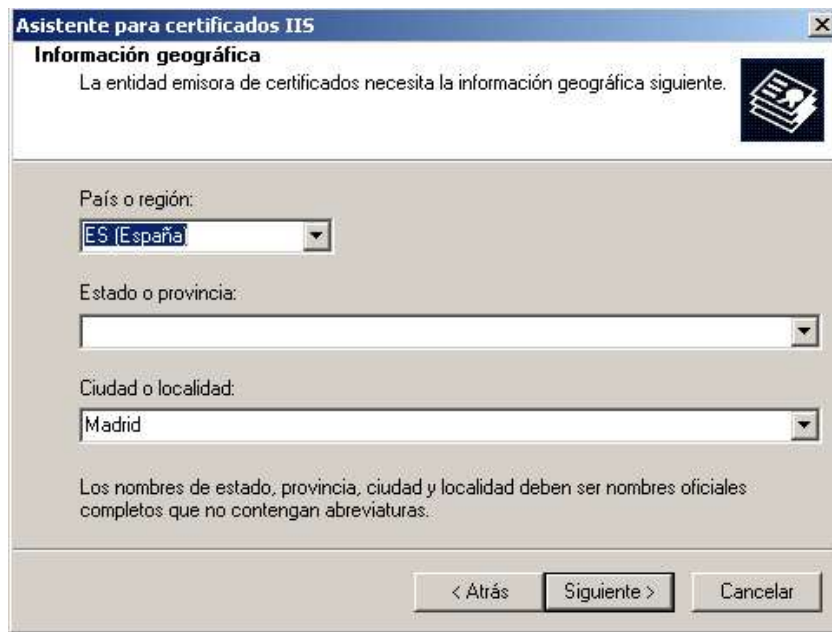
Información de la organización
El certificado debe incluir información que permita diferenciar su organización de otras.

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:

Unidad organizativa:



Asistente para certificados IIS

Información geográfica

La entidad emisora de certificados necesita la información geográfica siguiente.

País o región:

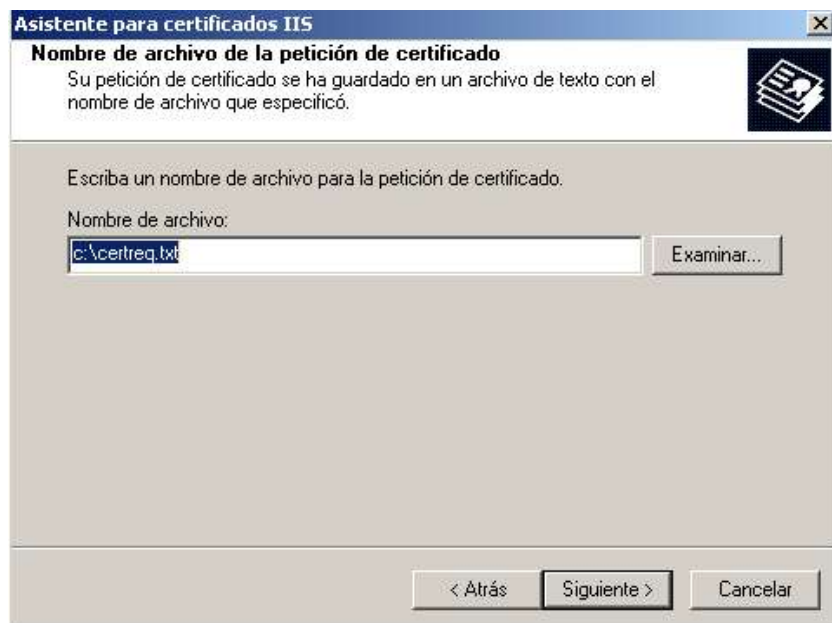
Estado o provincia:

Ciudad o localidad:

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

< Atrás Siguiendo > Cancelar

Luego se debe ingresar el nombre del archivo y la ubicación



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.

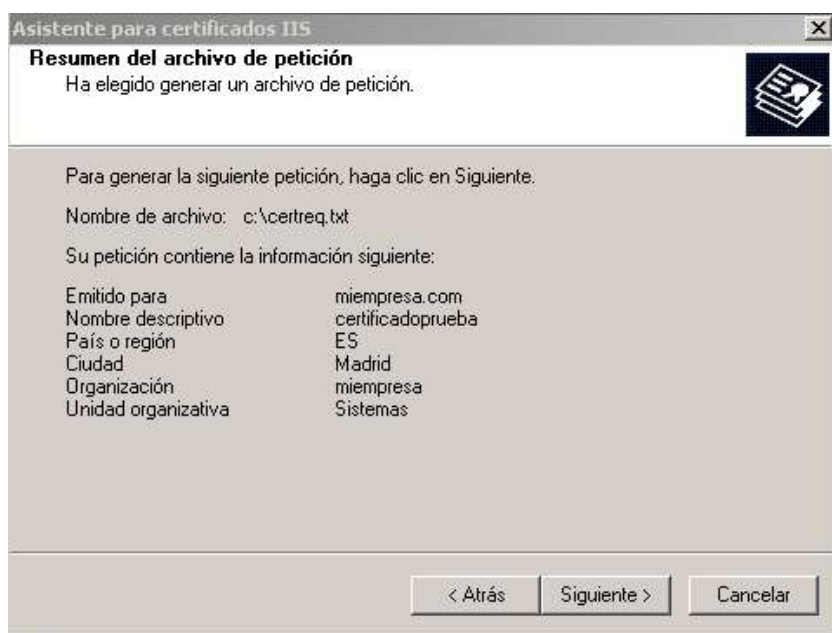
Escriba un nombre de archivo para la petición de certificado.

Nombre de archivo:
 Examinar...

< Atrás Siguiendo > Cancelar

La última pantalla muestra un resumen de lo configurado





Finalmente, se genera la petición de certificado. Esta petición es posible enviarla a una autoridad de certificación. Es posible para fines de prueba que uno mismo sea la propia autoridad de certificación.

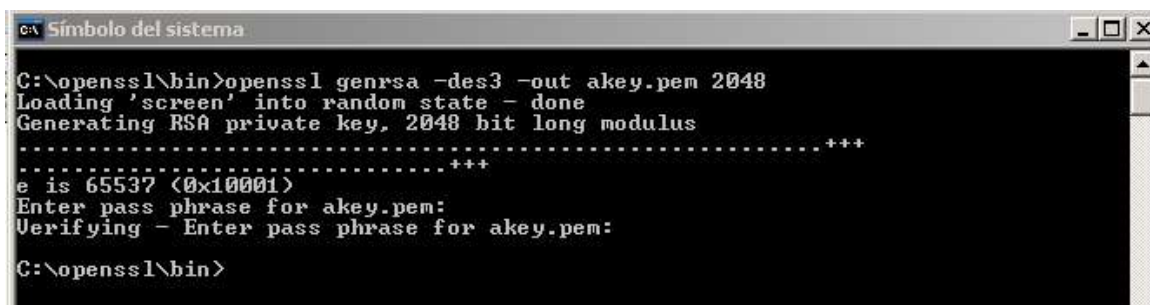
Para transformarse uno mismo en una empresa de certificación (ficticia pero útil para pruebas) se debe usar el software OpenSSL. Existen versiones compiladas para Windows disponibles (o se puede optar por bajar los códigos fuentes y compilarlo). En el sitio <http://www.shininglightpro.com/> es posible buscar una versión compilada. Por lo tanto, conviene bajarla e instalarla como cualquier programa Windows.

Una vez instalada, se procede a generar las claves y el certificado. Para ello, se abre una ventana de línea de comandos y se posiciona en el directorio correspondiente a los binarios de OpenSSL.

Allí se ejecuta el siguiente comando:

openssl genrsa -des3 -out akey.pem 2048

como se muestra en la siguiente figura:



Con esto se ha generado una clave privada. Hay que prestar atención a la contraseña y no olvidarla.

La clave generada es un archivo de texto con un contenido similar al siguiente

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,621BCA36271256A2

NERNJlzeOB7/Q4yhiaRL93RLejHOabbRxxBMdcPmE6CwcAD5EdFM2eX7raJbjYsq
UOzClhhV2vrixhS5/jmS0fFgT6lPphULHhMvQqTidyKYZPmCccGOQWmnXxAcDA2G
oWtE20RM9rvUYG6ZlQAvHsZPgXv4lcKLrt35F7GyDs8tojalGtJoUVp7uyODE5Ll
NLXWwhoZ3Vt5XZUyhtjdwVZrFRNf1xayHjAfgeR8hAWKnlSp/pvFZFY9ce75Ys78
GktGlvTV3cdjVftxRfeNu6hSK/OfL6yJHlaYPHjw9t9ElfYpQsoMO4ZQ/InT6Rshp
mdThSrTXZ4rkEqS4TYpD9DZJ4l7LtcXiVRzMJzMSnZLvlzrG4KDEXpGn8v4Ubxsu
dgSnqHkfGCBnz1sgfea0a5Xc9hsCk5iFORCwnKGFGHEidCZtfO5nAdN9zn7tLO2
3tpRoRXr5f7+36Mtl1T9tRo16zpSmzeM7VvURtNYhakCw92hZU42Vrsh7Yyptq
vBaF4CsSsxJ0XvAEuuB4UWkLD453DlgeVNIDJTtSeD7/LmtkxpcQx70KFWnmkPX/
jV0g5iNfdjh2ELje9Q8r4TETrotY/3tBrfSa+nNrWQGRSDbnYP9lo1N0qJQPlquZ
oHmHQUM00jTHnCie7D8X5BGNktXjm2Q3+48/RuVzdZfiAEcXVSm098sw0PRPykc6
y9JRyJA/p3t3u1lVZGvv6h8rmlNhpDQShePoqLEGBtk1W9/gtbnZrDYJSehGdZB
i78gJYZydhRtF8f7a2SNP8T4QdJ+CglPrh+dWdafLO9yH7/62/a0rlmJ4zEH4VR/
9KyT59T4gF/eM+WnjCHLTH0HIXH9j59bMwbSOjLEZqnRjo9Nz+GjxJO7ocREdhaF
kr80Pl2lerhjiWgEv5A7P12XqbQ/4nYD/6HPpCIUtifMLaVMSEIYhDXltrWYi8Jm
Ri8tXSswEvEirFGw9EhEuEZW/Gs7sThkrX9acDsNT/VTYZucD9EPqlKugR9vzebxV
TozATlvceWfrcjPrcYnE1M1jFQ6aGeHPZkBGQSq8S5DrFg8dPFOnr9WtAxOxLD2F
cvlhj+RZKydyI+VV7Uwbu5dPbrR+fEii/K5ebkvFz2Na+qg74cytWgZoBJ2MHuCc
SJ9K6F/0wa3WZdBg3BZ8KbEEPba+Ws/RefoUloJpZlSWJlaBLoFpeJc/Ueicrm+D
VE11jKUmlly1xBGEGwQhRalfLxFRaldGD3jfvli69sozOzUDEP1Bsve/7WQDAT
6SWaqYMXEQra7TdyjCWYsD9dYqR8CwMKcPID2HQLG1ccUycNvPFfrS0g0z+wc6lY
tKPgtxzOZySlmwtYgvGko+YrF25vCpRcu7FEEYFAxQEnhqLY4oWfo5nBP4QvTNAA
w0yzesOJkdbeQKCZai+YZpZHf2b9kBV3m/808KRQJp94cNMkc6Lz8a/hphHi7v5r
6zEoMUuu7aDMFHSnfzcyB8U8bakdA9VLzBqywwxymQ/VwR7/E4xlmxpMj3/UGbjv
axBnYsANefGk0Qdc+4D4AZS9em8myj//M8Fxva7mihd0W/kYsTJ+Pg==
-----END RSA PRIVATE KEY-----
```

A continuación con el siguiente comando

openssl req -new -x509 -key akey.pem -out acert.pem -days 365

se crea un certificado digital de Autoridad de Certificación (en este caso ficticia) con la información que se solicite, válido por un año, tal cual se ve en la siguiente figura:



```
C:\OpenSSL\bin>openssl req -new -x509 -key akey.pem -out acert.pem -days 365
Enter pass phrase for akey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MiEmpresa
Organizational Unit Name (eg, section) []:Sistemas
Common Name (eg, YOUR name) []:Juan
Email Address []:juan@miempresa.com

C:\OpenSSL\bin>
```

A continuación, se debe crear el certificado del sitio Web en cuestión. Para ello, es necesario copiar el archivo que se generó con el IIS, certreq.txt, al directorio donde se esté trabajando y ejecutar el siguiente comando:

```
openssl x509 -req -days 365 -in certreq.txt -CA acert.pem -CAkey akey.pem -CAcreateserial -out iis.crt
```

```
C:\OpenSSL\bin>openssl x509 -req -days 365 -in certreq.txt -CA acert.pem -CAkey
akey.pem -CAcreateserial -out iis.crt
Loading 'screen' into random state - done
Signature ok
subject=/CN=gordixp/OU=sistemas/O=miempresa/L=Madrid/ST=/C=ES
Getting CA Private Key
Enter pass phrase for akey.pem:

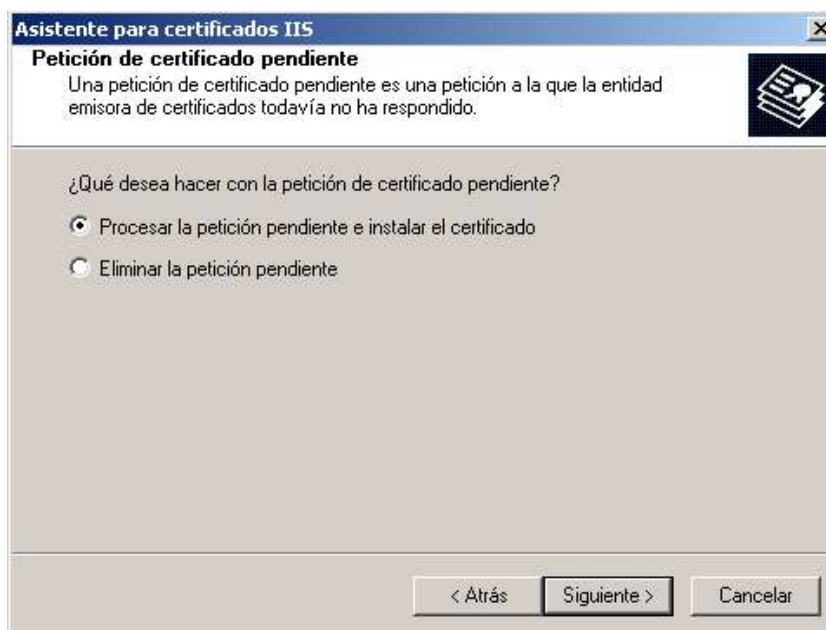
C:\OpenSSL\bin>
```

De esta forma se consiguió un certificado iis.crt firmado por una autoridad de certificación, que se creó para propósitos de prueba. El último paso es importar el certificado al IIS. Para ello, debe volverse a la pantalla del asistente de certificados Web:

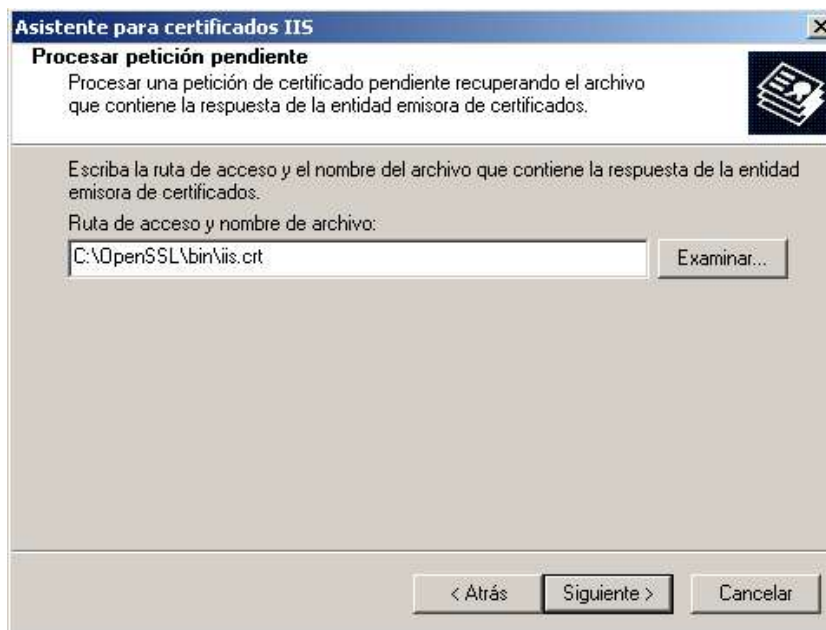




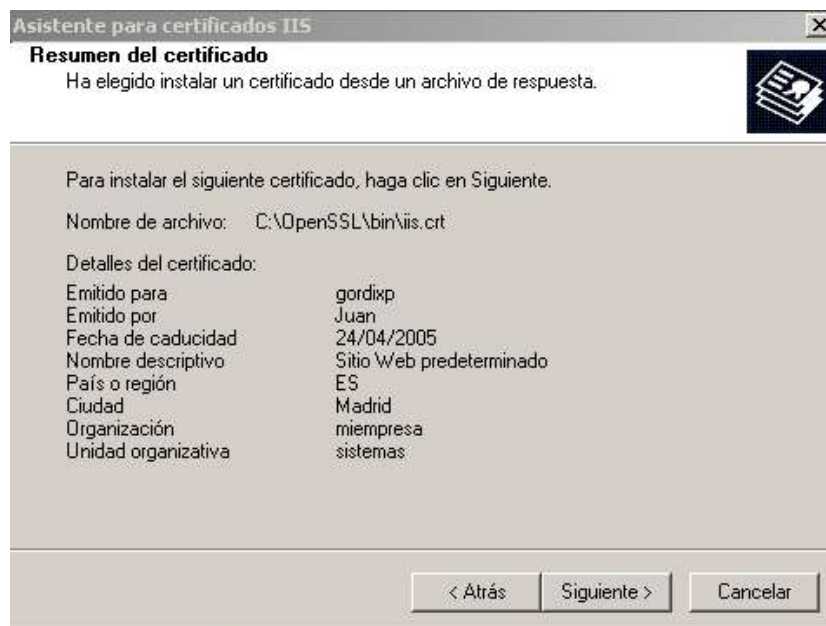
En este caso, la segunda pantalla del asistente cambia y pregunta si se quiere procesar la certificación pendiente (la que se creó al comienzo con en el archivo certreq.txt). Además, es posible eliminarla si no se quiere procesarla o se tuvo algún problema (y se debe entonces empezar todo de nuevo).



Luego se ingresa el certificado que se acaba de generar con OpenSSL tal cual se ve en la siguiente figura:



Luego se muestra una ventana con la información del certificado para verificar que los datos sean correctos:



De esta manera finaliza el asistente, indicando que tuvo éxito en la instalación de certificados.

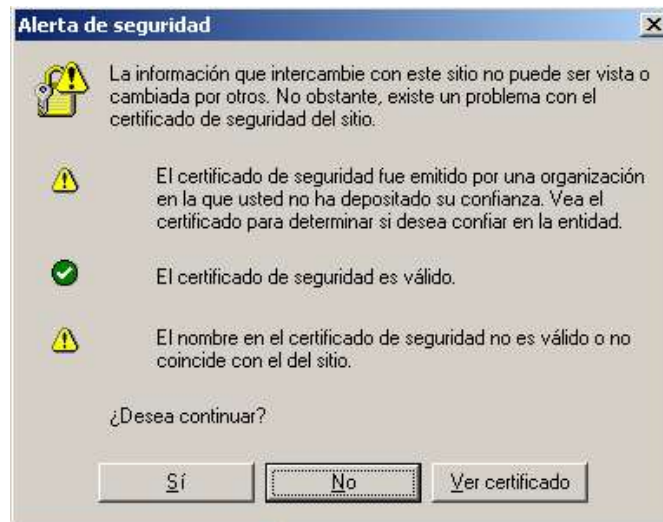




Si luego, en la pantalla de propiedad, se elige ver certificado, se muestra el diálogo con la información pertinente:



Si en el navegador se ingresa una dirección local, pero en lugar de http:// se escribe https:// (o sea una comunicación segura), se tiene un mensaje de advertencia:



La advertencia afirma que el certificado no fue emitido por una organización de confianza (lógico si fue certificado por nosotros mismos). Es posible ver el certificado con la opción *Ver certificado* (esta opción es útil en caso de acceder a otros sitios y se quiere saber quien firmó el certificado).

Si se elige la opción *Sí*, entonces se ingresa al sitio utilizando una comunicación segura mediante SSL.

