Práctica 7

Internet Information Services (IIS)

Objetivos

Conocer los servicios básicos proporcionados por IIS así como su administración.

1 Introducción

IIS es un componente de Windows que permite convertir un sistema Windows en un servidor de Internet. Microsoft ha desarrollado múltiples versiones de IIS. La versión 6.0 que es la que se distribuye con Windows Server 2003 y es la que utilizaremos en esta práctica.

IIS proporciona, entre otros, los siguientes servicios:

- Servicio de ficheros mediante el protocolo HTTP/HTTPS (*Hypertext Transfer Protocol*.)
- Servicio de ficheros mediante el protocolo FTP (*File Transfer Protocol*.)
- Servicio de correo mediante el protocolo SMPT (*Simple Mile Transfer Protocol*.)
- Servicio de noticias mediante el protocolo NNTP (*Network News Transfer Protocol*.)

En esta práctica nos centraremos en los dos primeros servicios: el servicio HTTP, que es utilizado básicamente para que un servidor publique páginas *web*, y el servicio FTP, que convierte a un servidor en un repositorio de archivos que pueden ser accedidos a través de Internet.

Un servidor Windows que ejecuta IIS puede prestar sus servicios en Internet (ser accesible desde la Web), si cuenta con el soporte de un ISP (*Internet Service Provider*). Sin embargo, también puede prestar sus servicios dentro de una Intranet (red corporativa), como por ejemplo, la de la Universidad de Oviedo. En nuestro caso trabajaremos en un ámbito todavía más reducido: una mesa del laboratorio. Instalaremos IIS en el ordenador Windows Server 2003 y utilizaremos el ordenador XP como cliente. No obstante, los servicios proporcionados por el ordenador Windows Server 2003 podrían ser accedidos desde cualquier ordenador conectado a Internet, exactamente igual que son accedidos desde el ordenador XP, claro está, si el ordenador servidor contara con el soporte de red necesario para publicar sus servicios en Internet.

2 Instalación de IIS

IIS 6.0, al igual que otros muchos servicios y componentes de Windows, no viene instalado por defecto en Windows Server 2003. Para agregar IIS debes hacer lo siguiente:

H Abre el menú correspondiente al *Panel de control* y elige la opción *Agregar o quitar programas*. Se abre entonces la herramienta que nos permite gestionar los programas instalados en el sistema (Office, Acrobat Reader, Visual Studio, etc.) Esta misma herramienta es la que nos permite también agregar o quitar componentes del sistema operativo. Para ello, pulsa sobre el icono *Agregar o quitar componentes de Windows*. Entonces observarás una lista de componentes del sistema operativo que pueden ser agregados o eliminados a voluntad por el administrador del sistema.

IIS forma parte de otro componente más complejo, conocido como *Servidor de aplicaciones*, el cuál, además de contener IIS, contiene también otro conjunto de componentes relacionados con los servicios *web*.

H Busca el componente *Servidor de aplicaciones* y selecciónalo. Pulsa sobre el botón *Detalles*. Esto abrirá una ventana que muestra los componentes que están integrados en el componente *Servidor de aplicaciones*. Algunos de estos componentes ya se encuentran seleccionados. Se trata de los componentes que se instalarán al instalar el *Servidor de aplicaciones*. De nuevo, algunos de estos componentes contienen a su vez otros componentes. En concreto, el componente *Internet Information Services* contiene una serie de subcomponentes. Selecciona *Internet Information Services* y, después, pulsa sobre el botón *Detalles*. Indica a continuación que subcomponentes de IIS se encuentran seleccionados por defecto.

–Pregunta 1–

De todos estos componentes, el *World Wide Web* es el que convierte a un servidor Windows Server 2003 en un servidor *web*, ya que es el que permite al acceso a los ficheros del servidor mediante el protocolo HTTP.

H Además de los componentes de IIS que se encuentran seleccionados por defecto, selecciona también el *Servicio de Protocolo de transferencia de archivos (FTP)*, ya que en esta práctica vamos a trabajar también con este servicio. Finalmente, ubícate sobre el componente *Servicio World Wide Web* y pulsa sobre *Detalles*. Entonces observarás los subcomponentes de este servicio. Selecciona *Administración remota (HTML)*. Ahora acepta los elementos seleccionados en las sucesivas ventanas que has ido abriendo, hasta que llegues a la ventana *Componentes de Windows*. Entonces pulsa *Siguiente* para comenzar la instalación del *Servidor de aplicaciones*. Deberás utilizar el CD-ROM de Windows Server 2003, que está disponible en la caja de componentes de tu mesa de trabajo. Cuando finalice la instalación, cierra la

herramienta *Agregar o quitar programas* y retira el DC-ROM de Windows Server 2003 de la unidad de CD.

En este momento IIS ya se encuentra instalado en nuestro sistema. Vamos a realizar unas pruebas mínimas para comprobar que el servidor *web* está operativo.

Comprobación de la operatividad del servidor web

Lo primero que debes conocer es que un servidor *web* utiliza una estructura de directorios donde almacena la información (páginas *web* y otros tipos de ficheros) que el servidor publica en la red. Esta estructura de directorios tiene un directorio raíz, que en el caso de la instalación que hemos realizado (instalación por defecto) se encuentra en *C:\Inetpub\wwwroot*.

H Abre esta ubicación. Indica a continuación los ficheros que se encuentran en ella.

–Pregunta 2–

Enseguida veremos el cometido de estos ficheros. Vamos a colocar algún fichero adicional en esta ubicación.

H Abre el *Internet explorer*. Conéctate a la página de entrada de la Universidad de Oviedo. Vamos a almacenar en nuestro servidor una página del servidor de la Universidad. Colócate sobre el enlace *Órganos de gobierno* y pulsa sobre él con el botón derecho del ratón. En el menú que se abre elige *Guardar destino como*. Esto hará que, en vez de abrirse la página *html*, se descargue el fichero que contiene la página y se almacene en nuestro ordenador. ¿Qué ocurre? ¿Puedes descargar la página?

–Pregunta 3–

Los problemas que tienes al descargar la página son debidos a la configuración de seguridad del Internet Explorer, que son mucho más restrictivos en un servidor (recuerda que estás ejecutando Windows Server 2003) que en una estación de trabajo (en la que ejecutamos XP). Vamos a resolver este pequeño problema.

H En el menú *Herramientas* del Navegador elige *Opciones de Internet*. Entonces selecciona la ficha *Seguridad* y en ella, el icono *Internet*. Pulsa en el botón *Nivel Personalizado*. Se abre entonces una ventana en la que se pueden configurar todos los aspectos de seguridad del navegador. Busca la opción *Descarga de archivos*, actívala y acepta la configuración. A partir de este momento el navegador quedará habilitado para descargar archivos. Ahora descarga la página *Órganos de gobierno* del servidor de la Universidad y almacénala en *C:\Inetpub\wwwroot*. Comprueba que el fiero que has descargado se llama `organos_gobierno.htm`.

Ahora vas a crear algunos elementos más en *C:\Inetpub\wwwroot*. Así iremos introduciendo contenidos en el servidor.

H Crea en *C:\Inetpub\wwwroot* dos carpetas, una llamada *horarios* y otra, *guiones*. Ahora usando el navegador entra en la página *web* de la asignatura. Entonces almacena en la carpeta *horarios* el fichero *html* que responde al enlace *Horarios* en la sección de *Teoría*. Después almacena en la carpeta *guiones* el fichero *html* que

responde al enlace *Guiones de prácticas*. Comprueba que los ficheros que has descargado se llaman `horarios-teor.htm` y `guiones-practicas.htm`.

En este momento ya tenemos un conjunto de información en el directorio de publicación de nuestro servidor *web*. Vamos a comprobar ahora que podemos acceder a ella desde el navegador de otro ordenador. Para ello utilizarás el ordenador XP de tu mesa de trabajo.

H Arranca el ordenador XP, autenticándote como *Alumno*. Abre el *Internet Explorer*. En el campo de direcciones del navegador se introduce la URL del recurso al que se desea acceder. Habitualmente esta URL se indica mediante un nombre DNS, como por ejemplo *www.microsoft.com* o *www.uniovi.es*. Pero ¿cuál es la URL de nuestro servidor *web* (ordenador Windows Server 2003)? De momento no tenemos esta información. Sin embargo, la URL puede indicarse también mediante una dirección IP, y esa sí la conocemos, ya que nuestro servidor tiene la dirección 156.35.151.XXX, donde XXX es la parte numérica del nombre del servidor. Por consiguiente, introduce en el campo de direcciones del navegador lo siguiente:

http://156.35.151.XXX/organos_gobierno.htm

Entonces el navegador accede utilizando el protocolo HTTP al servidor cuya dirección IP es 156.35.151.XXX. Además se indica que se accede al fichero `organos_gobierno.htm`, que se encuentra en el directorio raíz del área de publicación *web*. Utilizando las rutas adecuadas puedes acceder a cualquier fichero ubicado en las carpetas de dicho área de publicación.

H Utilizando de nuevo el navegador (en el ordenador XP), visualiza los ficheros `horarios-teor.htm` y `guiones-practicas.htm`.

De momento hemos comprobado que el servidor *web* está operativo. Nuestro siguiente objetivo es conocer las herramientas que proporciona el sistema operativo para administrar IIS.

3 Herramientas de administración de IIS

Hay dos herramientas básicas para administrar IIS, el *Administrador de Internet Information Services* y la *Herramienta de administración remota (HTML)*. Las presentaremos ahora brevemente y luego las utilizaremos indistintamente durante el resto de la sesión.

Administrador de Internet Information Services.

Para acceder a esta herramienta, haz lo siguiente:

H En el menú *Inicio*, elige *Herramientas administrativas*. Entonces selecciona *Administración de Internet Information Services (IIS)*. Esto abre la herramienta correspondiente.

Esta herramienta permite administrar tanto el servidor local como servidores remotos. No obstante, por defecto, se conecta al servidor local. Debido a ello, observarás ahora en el panel izquierdo una entrada con el nombre del servidor local (ATCXXX).

H Despliega el servidor local y observarás los servicios que está gestionando dicho servidor. Nosotros nos centraremos en dos elementos, *Sitios Web* y *Sitios FTP*.

Un *sitio* es un área de publicación de información. Si el sitio es de tipo *web*, se accederá a la información que contiene mediante el protocolo HTTP, y habitualmente una parte fundamental de su contenido estará formado por ficheros de hipertexto, que son navegables. Si el sitio es *ftp*, se accede a su contenido mediante el protocolo FTP. El objetivo de los sitios *ftp* es hacer accesible a través de Internet un repositorio de ficheros.

H Despliega *Sitios Web*. Observarás dos sitios: *Sitio Web predeterminado* y *Administración*. Selecciona *Sitio Web predeterminado*. En el panel derecho de la consola de administración aparecen los elementos que contiene el sitio seleccionado. Indica a continuación cuáles son estos elementos:

–Pregunta 4–

H Abre la carpeta *C:\Inetpub\wwwroot* y comprueba que observas los mismos elementos. La idea es que el *Administrador de Internet Information Services* nos muestra el contenido de los sitios.

El *Sitio Web predeterminado* es el área de publicación *web* que se crea por defecto cuando se instala IIS. Los clientes, cuando acceden al servidor *web* acceden, por defecto, al *Sitio Web predeterminado*. El sitio *Administración* es utilizado por la *Herramienta de administración remota HTML*.

El *Administrador de Internet Information Services* permite controlar y configurar todas las características posibles de un servidor *web*. Iremos viendo diversos aspectos de la configuración a lo largo de la práctica. Ahora, a modo de ejemplo, vamos a utilizar un comando de esta herramienta que nos permite detener o iniciar un sitio *web*.

Para comprobar si el sitio está activo o no utilizaremos el navegador del ordenador cliente. No obstante, debe tenerse en cuenta que los navegadores pueden "cachear" páginas. Puede ocurrir entonces que al repetir el acceso a una página de un servidor, el navegador sirva la página "cacheada" en vez de obtenerla realmente del servidor. Esto puede generar cierta confusión en nuestros experimentos. Para evitar este problema, cuando sea pertinente cerraremos y abriremos el navegador para cada nueva operación. Esto evitará los efectos de "cacheo".

H Selecciona *Sitio Web predeterminado*. Pulsa el botón derecho del ratón para abrir el menú contextual. Entonces elige le opción *Detener*. En el ordenador cliente, si tienes un navegador abierto, ciérralo y vuelve a abrirlo, debido a la razón expuesta anteriormente. Ahora intenta acceder desde el navegador del ordenador cliente a la página `organos_gobierno.htm` del servidor *web*, tal y como lo hiciste en la sección anterior. Observarás el error *The requested URL could not be retrieved*. Finalmente, abre de nuevo el menú contextual del *Sitio Web predeterminado* y selecciona la opción *Iniciar*. En el ordenador cliente cierra el navegador y vuelve a abrirlo, entonces intenta acceder de nuevo a la página `organos_gobierno.htm`, comprobando que ahora accedes correctamente.

Herramienta de administración remota (HTML)

Esta herramienta permite administrar un servidor *web* desde cualquier navegador que tenga acceso a dicho servidor. Así si el servidor está en Internet (recordar que también puede funcionar en una Intranet), cualquier ordenador con acceso a Internet serviría

para administrar dicho servidor. Esta herramienta utiliza el sitio *web* de *Administración* para llevar a cabo su cometido.

Algo que todavía no hemos indicado, pero que es necesario para el manejo de la *Herramienta de administración remota*, es que un servidor *web*, al igual que toda aplicación basada en el protocolo TPC/IP, necesita un número de puerto de red (estructura lógica gestionada por el SO), para establecer sus conexiones. Cuando un navegador se conecta a un servidor utiliza por defecto el puerto 80. Así las URLs que se indican a continuación son equivalentes:

http://156.35.151.XXX/organos_gobierno.htm

http://156.35.151.XXX:80/organos_gobierno.htm

H Prueba la segunda URL y comprueba que con ella accedes correctamente al servidor.

El sitio *web* de *Administración* responde en un puerto diferente al *Sitio Web predeterminado*. El puerto asignado al sitio *web* de *Administración* es el 8098. Además este sitio requiere una comunicación mediante el protocolo HTTPS, en vez del HTTP. El HTTPS es conocido como el protocolo HTTP seguro, es decir, que utiliza comunicaciones seguras mediante técnicas de encriptación. Por consiguiente, para acceder a este sitio debes utilizar la siguiente URL:

https://156.35.151.XXX:8098/

H Accede a esta URL utilizando el navegador del ordenador cliente. En principio observarás que no puedes acceder. Obtienes el error *Access denied*. Esto es debido a la configuración del navegador. Éste está configurado para utilizar el servidor *proxy* de la Universidad de Oviedo para acceder a Internet. Sin embargo, parece que este servidor filtra (por algún motivo desconocido) los accesos al *Sitio de administración* de servidores Windows. Para conseguir que el navegador acceda directamente a nuestro servidor sin pasar por el *proxy*, abre el menú *Herramientas* del navegador y selecciona *Opciones de Internet*. Elige entonces la ficha *Conexiones* y pulsa sobre *Configuración de LAN*. En el área de la ventana que se abre dedicada a la configuración del *Servidor proxy*, pulsa sobre *Opciones avanzadas*. Se abre entonces la ventana *Configuración de los servidores proxy*. En la parte inferior de esta ventana puedes observar el campo *No usar proxy para las direcciones que comiencen por*. Introduce en este campo la dirección IP de nuestro servidor *web* (ordenador Windows Server 2003) y *Acepta* esta nueva configuración. A partir de este momento, cada vez que el navegador del ordenador cliente acceda al servidor *web* del ordenador servidor, lo hará directamente, sin pasar por el servidor *proxy* y esto debe solucionar nuestros problemas. Accede de nuevo a la URL:

https://156.35.151.XXX:8098/

Ahora deberás acceder sin problemas al sitio *web Administración*. No obstante, como ahora estás llevando a cabo una comunicación segura (mediante el protocolo HTTPS) se muestra una alerta de seguridad, relacionada con las credenciales del servidor. El problema radica en que el servidor no ha sido configurado con un certificado de seguridad en el que el cliente confíe. Más adelante abordaremos este problema. De momento, pulsa sobre el enlace *Vaya a este sitio* web *(no recomendado)* para saltar la alerta de seguridad y acceder al servidor. Entonces, cuando se establece la conexión con el servidor, éste te pide que te autentiques. Esto es debido a que el sitio *web Administración* está configurado para que solo aquellos

usuarios que pertenezcan al grupo *Administradores* puedan acceder a él (observa la diferencia con el *Sitio Web predeterminado* en el que no se requiere autenticación). Autentícate utilizando la cuenta del *Administrador* y entrarás en el sitio *web Administración*.

De momento, haremos una prueba muy simple de administración mediante esta herramienta. Vamos a detener y luego a iniciar el *Sitio Web predeterminado*.

H Primero comprobamos que el *Sitio Web predeterminado* está funcionando. En el ordenador cliente, sin cerrar el navegador que tienes ahora abierto, abre un nuevo navegador. Accede mediante él a la página `organos_gobierno.htm`. Cierra este navegador.

H Conmuta al navegador con el que estás accediendo al sitio *web Administración*. Pulsa en él sobre el enlace *Sitios*. Se muestra una lista con los sitios *web* gestionados por el servidor. Selecciona *Sitio Web predeterminado*. Entonces pulsa sobre la opción *Detener*. Observa cómo en la columna *Estado* se indica el nuevo estado del sitio (*Detenido*.)

H Abre un nuevo navegador e intenta volver a acceder a la página `organos_gobierno.htm`. Lógicamente ahora no puedes acceder. Cierra esta navegador.

H Conmuta de nuevo al navegador con el que accedes al sitio *web Administración* e inicia el *Sitio Web predeterminado*.

H Abre un nuevo navegador y accede a la página `organos_gobierno.htm`. Ahora volverás a acceder a ella sin problemas.

En el resto de la sesión utilizaremos estas herramientas para configurar diversos aspectos del servidor *web*.

4 Configuración y funcionamiento de un sitio *web*

En esta sección vamos a utilizar el *Sitio Web predeterminado* para analizar diversos aspectos de la configuración y funcionamiento de un sitio *web*. Para acceder a la configuración de este sitio *web*, haz lo siguiente:

H Abre *Administrador de Internet Information Services (IIS)*. Selecciona *Sitio Web predeterminado*. Abre su menú contextual y selecciona *Propiedades*. Entonces se abre una ventana en la que podemos configurar todas las propiedades del sitio *web*.

Comenzaremos con la identificación del sitio *web*.

H Elige la ficha *Sitio Web*. En la parte superior de esta ficha se muestran los parámetros que identifican el sitio *web*. Estos son la dirección IP a la que responde y los puertos que utiliza para comunicarse. Indica a continuación el contenido del campo *Dirección IP*.

–Pregunta 5–

Esto significa que este sitio *web* responderá a todas las direcciones IP configuradas en el equipo, que de momento, es sólo una. Para verla pulsa en la fecha que está a la derecha del campo.

En el campo *Puerto TCP* se indica el puerto de comunicaciones que está utilizando este sitio *web*. Este campo es 80, ya que las comunicaciones HTTP utilizan este puerto por defecto. Vamos a probar a cambiar este puerto.

H Si tienes algún navegador abierto en el ordenador cliente, ciérralo. Configura el puerto TCP del *Sitio Web predeterminado* con el valor 50000[1]. Abre un navegador en el ordenador cliente y utilizando la URL apropiada accede a la página `organos_gobierno.htm` proporcionada por el *Sitio Web predeterminado*. Después vuelve a dejar el valor del puerto TCP en su valor original.

H ¿Qué es el puerto SSL? Repasa la URL que has utilizado para acceder al sitio *web* de *Administración*. Abre la ficha *Propiedades* del *web* de *Administración* y observando el valor del puerto SSL, contesta a esta pregunta.

–Pregunta 6–

H Ubícate de nuevo en la ventana de propiedades del *Sitio Web predeterminado*. Abre la ficha *Directorio particular*. En esta ficha se configura el directorio que es utilizado por el sitio *web* para publicar sus archivos en la red. Este directorio se indica en el campo *Ruta de acceso local*. Escribe a continuación el contenido de este campo.

–Pregunta 7–

H Abre este directorio. Es el que hemos utilizado antes para publicar un conjunto de páginas *web*. Cambia el nombre del fichero `iisstart.htm` por este otro: `Piisstart.htm`. Más adelante veremos por qué.

Ahora vamos a probar un parámetro de configuración del directorio de publicación: el *Examen de directorios*. Este parámetro determina si el sitio *web* va a permitir a los clientes navegar o no por su estructura de directorios. Vamos a ver qué significa esto mediante algunos ejemplos.

H Observa que en este momento el parámetro *Examen de directorios* está desactivado. Vamos a empezar estas pruebas accediendo a la página `organos_gobierno.htm`, situada en el directorio raíz de publicación. Para ello, abre un explorador en el ordenador cliente e introduce la URL

http://156.35.151.XXX/organos_gobierno.htm

Debes acceder a esta página sin ningún problema como ya habíamos visto antes. Si ahora en la URL no escribimos ninguna página en concreto, nuestro objetivo sería acceder a la carpeta raíz, es decir, abrir esta carpeta y mostrar su contenido. Introduce entonces la siguiente URL en el explorador del ordenador cliente:

http://156.35.151.XXX/

[1] Los números de puerto altos, en concreto por encima de 49152, son puertos de libre uso, que no se encuentran asignados a servicios o aplicaciones concretas.

Observarás que no se puede acceder. Indica a continuación el error que muestra el navegador.

–Pregunta 8–

Repite las dos pruebas anteriores, pero para acceder ahora a la página `guiones-practicas.htm` y a la carpeta `/guiones`, observando que obtienes los mismos resultados que en las pruebas anteriores.

Como puedes observar, tal y como está configurado el *Sitio Web predeterminado*, puedes acceder a sus páginas pero no puedes navegar por su estructura de carpetas.

H Activa el campo *Examen de directorios* del *Sitio Web predeterminado* y *Aplica* para que tenga efecto este cambio. Ahora, utilizando el navegador del ordenador cliente, accede a la URL "*http://156.35.151.XXX/*" y comprueba que puedes navegar por la estructura de directorios del sitio *web* sin que se produzcan errores.

Pasaremos ahora a otro aspecto de configuración que se maneja desde la ficha de *Documentos*.

H Abre la ficha *Documentos*. Observarás el campo *Habilitar página de contenido predeterminado*. En este momento este campo se encuentra habilitado. Utilizando la '?' de la esquina superior derecha, obtén ayuda sobre el significado de este campo. Indica a continuación los ficheros que están introducidos en este campo.

–Pregunta 9–

¿Se encuentra almacenado alguno de estos ficheros en el directorio raíz del *Sitio Web predeterminado*?

–Pregunta 10–

Recuerda que en este momento, en la ficha *Directorio particular* del *Sitio Web predeterminado* se encuentra habilitado el campo *Examen de directorios*. Por consiguiente al acceder desde un explorador en el ordenador negro al *Sitio Web predeterminado* observamos su estructura de directorios.

H Si tienes algún navegador abierto en el ordenador cliente, ciérralo. Abre un nuevo navegador y accede a la URL "*http://156.35.151.XXX/*". Ahora en el ordenador servidor abre el directorio raíz del *Sitio Web predeterminado*. Cambia el nombre del fichero `Piisstart.htm` por `iisstart.htm`. Ábrelo para ver su contenido (sigues en el ordenador servidor). Ten en cuenta que ahora este fichero (`iisstart.htm`) sí está en la lista de ficheros introducidos en el campo *Habilitar página de contenido predeterminado*. Por consiguiente, cuando se acceda desde un navegador al *Sitio Web predeterminado*, éste devolverá este fichero al navegador. Cierra el navegador que tienes abierto en el ordenador cliente y abre otro. Accede a la URL "*http://156.35.151.XXX/*". Observarás que se muestra la página `iisstart.htm`. Indica ahora con tus palabras cuál es el cometido del campo *Habilitar página de contenido predeterminado*.

–Pregunta 11–

H Vuelve a cambiar el nombre del fichero `iisstart.htm` por `Piisstart.htm`. Nos interesa así para abordar el siguiente apartado.

Seguridad de directorios

Un aspecto crucial en los sistemas Windows es la seguridad. Hasta ahora hemos podido acceder desde los clientes al *Sitio Web predeterminado* sin ningún problema, es decir, los clientes entran al sitio *web* sin necesidad de autenticación y acceden a los ficheros que hay en él sin restricciones.

H En *Propiedades de Sitio Web predeterminado*, elige la ficha *Seguridad de Directorios*. En el apartado *Autenticación y control de acceso*, pulsa en *Modificar*. Aparece entonces la ventana *Métodos de autenticación*. En este momento observarás la opción *Habilitar acceso anónimo* seleccionada. Esto significa que se accede al sitio *web* sin autenticación. Deshabilita esta opción. Si ahora pulsas en *Aceptar*, obtendrás un mensaje indicando que se denegará todo tipo de acceso. Esto es debido a que si deshabilitamos el acceso *anónimo*, será necesario habilitar otro tipo de acceso al servidor, como por ejemplo, *Autenticación de Windows integrada*. Entonces definitivamente deselecciona *Habilitar acceso anónimo* y selecciona *Autenticación de Windows integrada*. Esto significa que cuando accedas mediante un cliente a este sitio *web*, deberás autenticarte con un usuario registrado en el servidor. Vamos a probar esto. En el ordenador cliente, abre un explorador y accede al *Sitio web predeterminado* mediante la URL "*http://156.35.151.XXX/*". ¿Qué ocurre?

–Pregunta 12–

Autentícate utilizando el usuario *administrador*. Comprueba entonces que puedes navegar por el sitio *web* sin problema alguno.

Ahora lo que vamos a ver es cómo podemos limitar la capacidad de realizar operaciones de los usuarios anónimos en el sitio *web*.

H Indica a continuación qué cuenta de usuario utilizan los usuarios anónimos para acceder al servidor.

–Pregunta 13–

Observarás que el nombre de este usuario se compone mediante un prefijo y el nombre del servidor. Dicho usuario es utilizado en la ACL de las carpetas y ficheros del servidor para conceder acceso a estos recursos al usuario anónimo.

H En el sitio *web* deshabilita la autenticación de Windows integrada y vuelve a habilitar el acceso anónimo. Abre el directorio raíz de publicación de archivos del *Sitio Web predeterminado*. Abre la ficha *Seguridad* del fichero `organos_gobierno.htm`. Observarás un conjunto de usuarios y grupos en la ACL de este fichero. Entre ellos debe estar el usuario:

Cuanta de invitado para Internet (ATCXXX\IUSR_ATCXXX)

Esta es la cuenta de usuario que utilizan los clientes anónimos. Deniega el permiso *leer* a este usuario. Abre un navegador en el ordenador cliente e intenta acceder desde él al fichero `organos_gobierno.htm`. Indica a continuación el error que se produce.

–Pregunta 14–

Si al acceso anónimo está habilitado y denegamos el acceso anónimo a ciertos recursos (ficheros y carpetas), ¿habrá alguna forma de acceder a estos recursos? La respuesta es sí. Para ello habrá que habilitar también la *Autenticación de Windows integrada*. Entonces, cuando desde un explorador se intenta acceder a un recurso del sitio *web*, el comportamiento es el siguiente:

1) Si el recurso permite que sea accedido por el usuario anónimo, se le da el acceso.
2) Si el recurso no permite que sea accedido por el usuario anónimo, se piden unas credenciales para acceder al recurso: nombre de usuario y contraseña. Entonces se concede acceso o no al recurso en función de si las credenciales proporcionadas por el usuario permiten acceso o no al recurso.

H Para comprobar este comportamiento, en el *Sitio Web predeterminado*, manteniendo habilitado el acceso anónimo, habilita también *Autenticación de Windows Integrada* y *Acepta* para que tenga efecto la nueva configuración. Abre un nuevo navegador en el ordenador cliente. Entonces primero vas a acceder al fichero `Piisstart.htm`, sobre el que usuario anónimo tiene permiso de lectura y luego vas a acceder al fichero `organos_gobierno.htm`, para el que el usuario anónimo no tiene permiso de lectura. Accede a `Piistart.htm`, comprobando que no necesitas autenticarte. Ahora accede a `organos_gobierno.htm`. Deberás autenticarte para acceder a él. Utiliza el usuario *Administrador*.

H Vuelve a dejar el permiso *Leer* de la *Cuenta de invitado para Internet* del fichero `organos_gobierno.htm` como estaba originalmente.

Utilizando estas características que acabamos de ver se puede organizar fácilmente la gestión de acceso a los recursos de un sitio *web*. Vamos a plantear un ejercicio simple sobre este asunto.

Imagina que el *Sitio Web predeterminado* fuera el sitio *web* de la asignatura Tecnología de Computadores. Se pretende que el sitio *web* sea de libre acceso, pero que sólo los alumnos de la asignatura tengan acceso a la carpeta en la que se encuentran los guiones de prácticas.

Para llevar a cabo este ejercicio utilizaremos un conjunto de usuarios que ya se encuentran registrados en el servidor y que fueron utilizados en la Práctica 2 de la asignatura. Se trata de los usuarios *AlumnoTC1* y *AlumnoTC2*. Utilizaremos estos usuarios para representar a los alumnos de la asignatura. También se encuentra registrado en el servidor el grupo *AlumnosTC*. Este grupo contiene como miembros a *AlumnoTC1* y *AlumnoTC2*. También el usuario *Alumno* está registrado en el servidor. Utilizaremos este usuario como un ejemplo de usuario que no pertenece a los alumnos de la asignatura. En concreto, el usuario *Alumno* no debe tener acceso a la carpeta *Guiones*.

H Comprueba que los usuarios *AlumnoTC1*, *AlumnoTC2* y *Alumno*, así como el grupo *AlumnosTC* se encuentran registrados en el servidor.

H Modifica la ACL de la carpeta *guiones* del *Sitio Web predeterminado* como consideres oportuno. Indica a continuación las acciones que vas a llevar cabo en dicha ACL:

–Pregunta 15–

H Configura la *Autenticación y control de accesos* del *Sitio Web predeterminado* según sea necesario.

H Ahora vas a comprobar que la configuración que has realizado funciona de la forma esperada. Para ello accederás al Sitio Web predeterminado utilizando un navegador en el ordenador cliente. Para cada prueba abre un nuevo navegador, cerrando previamente el que tengas abierto. Todas las comprobaciones a realizar se indican en el cuadro siguiente. Cada vez que pases una prueba, marca la casilla blanca que se muestra a su izquierda. Si algo falla revisa la configuración.

- Accedes sin necesidad de autenticarte a todos los elementos del *Sitio Web predeterminado*, salvo a la carpeta guiones.
- Puedes entrar en la carpeta *guiones* autenticándote como TC1 y como TC2.
- No puedes entrar en la carpeta *guiones* autenticándote como alumno.

5 Configuración de un sitio *web* seguro

Los sitios *web* seguros implementan su seguridad mediante una tecnología conocida como infraestructura de clave pública (o en inglés, PKI, *Public Key Infrastructure*).

H En la Wikipedia encontrarás el artículo Infraestructura de clave pública. Lee la introducción y la sección *Propósito y funcionalidad* de este artículo.

Una clave es una entidad de información que controla el funcionamiento de un algoritmo de criptografía. Los algoritmos de clave pública se basan en el uso de una pareja de claves para cifrar y descifrar secuencias de información. La información se cifra con la clave pública y se descifra con la clave privada. Un servidor seguro cuenta con una clave pública y otra privada. El servidor seguro proporciona la clave pública a todo cliente que quiera comunicar con él usando información cifrada. El cliente cifra la información con la clave pública del servidor y cuando éste recibe la información, la descifra con su clave privada. Como sólo este servidor "conoce" la clave privada correspondiente a la clave pública utilizada por el cliente, la información cifrada por el

cliente solo es descifrable por este servidor. La clave pública junto con diversa información de identificación del servidor se almacena en un certificado digital.

H Lee el artículo certificado digital disponible en la Wikipedia. Entonces indica a continuación los datos que como mínimo debe contener un certificado digital:

–Pregunta 16–

Lo primero que necesitamos para poder configurar un servidor *web* seguro es un certificado digital para el servidor. Los certificados digitales son emitidos por autoridades de certificación (en inglés, CA, *Certification Authority*). Hay autoridades de certificación de ámbito global, como por ejemplo VeriSign. Los certificados emitidos por este tipo de autoridades son reconocidos y aceptados por cualquier ordenador cliente, ya que las plataformas Windows contienen la información necesaria para reconocer como fiables dichas autoridades de certificación. No obstante, obtener un certificado de VeriSign tiene un conste económico y requiere hacer una serie de trámites. Los servidores seguros de las empresas que realizan transacciones comerciales en Internet tienen certificados emitidos por este tipo de autoridades de certificación.

H Busca VeriSign en la Wikipedia.

No siempre es necesario utilizar certificados emitidos por autoridades como VeriSign. Por ejemplo, para realizar comunicaciones seguras en el ámbito de una compañía, se pueden utilizar certificados generados en el propio seno de la compañía por una autoridad de certificación interna. El sistema operativo Windows Server 2003 proporciona las herramientas y componentes software necesarios para crear una autoridad de certificación en un servidor. Si tuviéramos disponible en el laboratorio un servidor con una autoridad de certificación operativa, podríamos solicitarle a dicho servidor un certificado para configurar nuestro servidor *web* seguro. Sin embargo, como no tenemos disponible dicho servidor, tendremos que convertir el servidor en el que estamos trabajando en una autoridad de certificación, que nos proporcionará el certificado que necesitamos para configurar nuestro servidor *web* seguro. El componente de Window Server 2003 que proporciona el servicio de autoridad de certificación se conoce como *Servicios de Certificate Server*. Vamos a instalar dicho componente.

H En el menú correspondiente al *Panel de control* elige *Agregar o quitar programas*. Entonces pulsa sobre *Agregar o quitar componentes de Windows*. Busca el componente *Servicios de Certificate Server* y selecciónalo. Un mensaje nos indica que tras instalar *Servicios de Certificate Server* no se podrá cambiar el nombre del

equipo. Acepta este mensaje. Si pulsas en el botón *Detalles*, observarás los componentes que se van a instalar. El componente *Entidad emisora de Servicios de Certificate Server* se explica por sí mismo. El componente *Compat. De inscripción Web de Servicios de Certificate Server* corresponde a un conjunto de páginas *web* que van a permitir que clientes externos a este sistema soliciten certificados vía *web*. *Acepta* para volver a la ventana anterior y pulsa *Siguiente* para completar la instalación del componente *Servicios de Certificate Server*. En la ventana *Tipo de entidad emisora de certificados*, elige *Entidad emisora raíz independiente*, ya que se va a trabajar con una sola entidad de certificación. En la parte inferior de esta ventana selecciona también *Usar la configuración personalizada para generar el par de claves y el certificado de la entidad emisora*. Se abre entonces la ventana en la que se configuran las opciones para la generación de las claves pública y privada. En el proveedor de servicios de cifrado, selecciona *Microsoft Enhanced Cryptographic Provider v1.0*, y justo debajo, selecciona *Permitir a este proveedor interactuar con el escritorio*. En *Algoritmo hash* elige *SHA-1*, y en *Longitud de la clave*, 1024. Pulsa *Siguiente* para completar esta fase. A continuación se muestra la ventana de *Identificación de la entidad emisora de certificados*. En el campo *Nombre común para esta entidad emisora de certificados* tenemos que introducir el nombre de la entidad. Introduce por ejemplo CA-ATCXXX (donde XXX indica el número del servidor). En el resto de los campos no hagas ninguna modificación. En la siguiente ventana, *Configuración de la base de datos de certificados*, hay que indicar las rutas de los archivos en las que se almacenarán los certificados generados. Deja los valores por defecto proporcionados en esta ventana. Después, un mensaje indica que hay que detener *Servicios de información de Internet* (o sea, el servidor de aplicaciones que instalaste anteriormente) para completar la instalación. Acepta este mensaje. Comienza entonces la instalación de *Servicios de Certificate Server*. Deberás introducir el CD de Windows Server 2003 para completar la instalación.

H Para comprobar que la instalación fue correcta puedes comprobar que en el menú *Herramientas administrativas* se encuentra disponible la herramienta *Entidad emisora de certificados*. Abre esta herramienta y observa que muestra la entidad emisora que acabamos de crear, es decir, CA-ATCXXX.

H Abre la herramienta *Administrador de Internet Information Services (IIS)*. Abre *Sitio Web predeterminado* y observa que se han registrado en él nuevos elementos. En concreto el elemento CertSrv. Se trata de una página *web* que permite a clientes externos solicitar certificados a al entidad de certificación instalada en este servidor.

Una vez instalada la autoridad de certificación (CA-ATCXXX), vamos a utilizarla para generar un certificado para nuestro servidor *web*. El certificado se solicitará a través de la página web CertSrv. Otras páginas lanzadas a partir de ésta utilizan componentes ActiveX (*plugins* que se acoplan al navegador) que requieren un ajuste de la configuración de seguridad del navegador que se utilice para acceder a ellas. En nuestro caso, la autoridad de certificación y el servidor *web* para el que queremos generar el certificado están en el mismo servidor (la máquina Windows Server 2003 de nuestro puesto de trabajo). Por tanto, utilizaremos el propio navegador del servidor para acceder a la página CertSrv y sucesivas. Consecuentemente, es el navegador del servidor el que debe ser configurado apropiadamente para permitir la ejecución de componentes ActiveX. Empecemos entonces por ajustar la configuración de seguridad del navegador del servidor.

H Abre el navegador. A continuación abre *Opciones de Internet* a las que se accede a través del menú *Herramientas*. Selecciona la ficha *Seguridad*. Y en el campo titulado *Seleccione una zona para ver o cambiar la configuración de seguridad*, elige *Internet*. Pulsa el botón *Nivel personalizado*. Se abre una ventana en la que se muestran múltiples aspectos de la configuración de seguridad del navegador. Tienes que modificar la configuración de los aspectos de seguridad que se indican a continuación:

- En el apartado *Automatización*
  - Habilitar la opción *Active scripting*.
- En el apartado *Controles y complementos de ActiveX*
  - Habilitar la opción *Ejecutar controles y complementos de ActiveX*.
  - Habilitar la opción *Generar scripts de los controles ActiveX marcados como seguros para scripting*.

Acepta la nueva configuración de seguridad y el navegador del servidor estará preparado para ejecutar apropiadamente las páginas *web* que le permitirán gestionar un certificado.

Vamos a gestionar el certificado para el servidor.

H Abre el navegador del servidor y accede desde él a la página CertSrv. Para ello tendrás que utilizar la URL:

http://156.35.151.XXX/CertSrv

Se abre una página de bienvenida en la que se indica que se está accediendo a un sitio *web* que permite solicitar un certificado. En la parte inferior de esta página se indican las tareas que se pueden llevar a cabo desde ellas. Una de estas tareas es *Solicitar un certificado.*

H Pulsa sobre el enlace *Solicitar un certificado*. Se abre una página en la que debe indicarse el tipo de certificado que se desea solicitar. Pulsa sobre el enlace *Solicitud avanzada de certificado* y en la nueva página que se abre selecciona el enlace *Crear y enviar una solicitud a esta CA*, lo que te lleva a la página *Solicitud de certificado avanzada*.

H Si es la primera vez que se utiliza la página *Solicitud de certificado avanzada*, ésta requerirá la ejecución de un componente ActiveX, que en principio será bloqueada por los mecanismos de seguridad del navegador. Esto se indica mediante un mensaje justo debajo de las pestañas de navegación del navegador. Pulsa con el botón derecho del ratón sobre este mensaje y elije la opción *Ejecutar control ActiveX*. Una vez que este control se haya ejecutado, la página estará lista para ser utilizada. Ahora hay que rellenar los campos de esta página para proporcionar a la autoridad de certificación la información necesaria para generar el certificado. A continuación se indican los datos que tienes que proporcionar. Los campos no indicados, déjalos en blanco.

- En el apartado *Identificando información*
  - Campo *Nombre*: **ATCXXX** (Donde XXX es el número del servidor). Este campo debe coincidir siempre con el nombre del servidor.
  - Campo *Compañía*: **Universidad de Oviedo**.

  - Campo *Departamento*: **Informática**.
- En el apartado *Tipo de certificado necesario* selecciona **Certificado de autenticación de servidor**.
- En el apartado *Opciones de clave*
  - Selecciona **Crear un conjunto de claves nuevo**.
  - Campo *Proveedor de servicios de cifrado (CSP)*: **Microsoft Enhanced Cryptographic Provider v1.0**.
  - Campo *Uso de clave*: **Ambos**.
  - Campo *Tamaño de clave*: **1024**.
  - Selecciona **Nombre automático ce contenedor de claves**.
  - Selecciona **Almacenar el certificado en el almacén de certificados del equipo local**.
- En el apartado *Opciones adicionales*
  - Campo *Formato de solicitud*: **CMC**.
  - Campo *Algoritmo hash*: **SHA-1**.

Una vez completado este formulario pulsa *Enviar*. Entonces recibirás una página de respuesta en la que se indica que se ha recibido la solicitud de certificado. Se indica también el ID de la solicitud, que es 2.

En este momento la autoridad de certificación CA-ATCXXX ha recibido una solicitud de certificado. Ahora hay que crear el certificado correspondiente a la solicitud recibida, para lo que se utilizará la herramienta *Entidad emisora de cerificados*.

H Abre la herramienta *Entidad emisora de certificados*. Despliega la autoridad de certificación CA-ATCXXX. Abre la carpeta *Peticiones pendientes*. Observarás la petición con ID 2, que es la que se ha realizado anteriormente. Ahora hay que emitir el certificado correspondiente a dicha petición. Pulsa con el botón derecho del ratón sobre la petición. Entonces elige *Todas las tareas* **à** *Emitir*. La petición desaparecerá de la carpeta *Peticiones pendientes*. Abre ahora la carpeta *Certificados emitidos* y observarás el certificado que se acaba de generar. Pulsa sobre él y un visor de certificados te mostrará la información contenida en el certificado. Indica a continuación cuál es la ruta de certificación de este certificado.

–Pregunta 17–

Resta ahora instalar el certificado en el servidor que lo solicitó. Para ello, desde el servidor solicitante se accederá vía *web* al servidor que contiene la autoridad de certificación, para lo que se utilizará de nuevo la página *CertSrv*.

H Abre el navegador del servidor y accede desde él a la página CertSrv. Selecciona entonces el enlace *Ver el estado de una solicitud de certificado pendiente*. En la página que se abre debe haber un enlace a la solicitud de certificado que tenemos en trámite, que será del tipo *Certificado de autenticación de servidor*. Pulsa sobre este enlace. Se abre otra página que indica que se ha generado el certificado solicitado y proporciona un enlace para instalar el certificado. Pulsa sobre dicho enlace. Se

muestra un aviso de seguridad, acéptalo y en este momento el certificado quedará almacenado en el almacén de certificados del servidor.

Todo este proceso ha sido necesario para tener un certificado para el servidor. Una vez que éste ya está disponible podemos configurar el sitio *web* seguro. Para ello, llevaremos a cabo los pasos que se indican a continuación.

H Abre la herramienta *Administrador de Internet Information Services*. Abre *Propiedades* del *Sitio Web predeterminado*. Entonces elige la ficha *Seguridad de directorios*. Pulsa sobre el botón *Certificado de servidor*. Esto hace que se abra el *Asistente para certificados de servidor Web*. En la ventana *Certificado de servidor*, elige *Asignar un certificado ya existente*. Se muestra una ventana con los certificados disponibles en el servidor. El certificado que queremos asignar al *Sitio Web predeterminado* es que el ha sido emitido para nuestro servidor (ATCXXX) por nuestra autoridad de certificación (CA-ATCXXX). Para ello fíjate en los campos *Emitido para* y *Emitido por* del cuadro en el que se muestran los certificados. A continuación hay que indicar el puerto de comunicación utilizado para las comunicaciones seguras (puerto SSL). Deja el valor proporcionado por defecto. Finaliza los pasos del asistente. Ahora en la ficha *Seguridad de directorios* pulsa en el botón *Modificar*. Se abre la ventana *Comunicaciones seguras*. Selecciona el campo *Requerir canal seguro*. Esto hará que sólo se pueda acceder a este sitio *web* utilizando comunicaciones seguras, es decir, mediante el protocolo *https*. Acepta las veces que sean necesarias para que todas estas modificaciones tengan efecto.

H Comprobemos primero que ya no podemos acceder al sitio *web* mediante el protocolo *http*. Intenta acceder a la página `organos_gobierno.htm` utilizando el navegador del servidor. Usa la URL

http://156.35.151.XXX/organos_gobierno.htm

Observa que el servidor responde que se debe ver la página utilizando un canal seguro. Utiliza entonces la siguiente URL

https://156.35.151.XXX/organos_gobierno.htm

Observarás que ahora sí podrás acceder a la página.

La configuración del servidor web seguro ha conluido.

6 Configuración y funcionamiento de un sitio *ftp*

Como ya hemos comentado, el objetivo de un sitio *ftp* es proporcionar un repositorio de archivos que pueda ser manejado a través de Internet. Para administrar un sitio *ftp* se utiliza también el *Administrador de Internet Information Services (IIS)*. Empecemos viendo qué sitios *ftp* tenemos instalados en nuestro sistema.

H Abre el *Administrador de Internet Information Services (IIS)*. Despliega el *equipo local* y a continuación *Sitios FTP*. Observarás entonces el *Sitio FTP predeterminado*. Abre la ventana de *Propiedades* de este sitio. Elige la ficha *Directorio particular*. Entonces, indica a continuación cuál es el directorio raíz de publicación de ficheros de este sitio *ftp*.

–Pregunta 18–

H Abre este directorio. Vamos a crear en él una estructura de carpetas mínima. Crea por ejemplos las carpetas *Asignaturas* y *Examenes*, y dentro de *Asignaturas*, las carpetas *Matematicas* y *Tecnoloagia*. Crea un fichero de texto dentro de cada una de estas carpetas que ponga cualquier cosa.

Para acceder a un sitio *ftp*, se puede utilizar un programa específicamente diseñado para el manejo de sitios *ftp*, o bien se pude utilizar un navegador, como el Internet Explorer. Utilizaremos esta opción.

H Para acceder al *Sitio FTP predeterminado*, abre un navegador en el ordenador cliente. Accederemos a este sitio igual que lo hacíamos al *Sitio Web predeterminado*, pero cambiando en la URL el protocolo *http* por *ftp*. Es decir, utiliza la siguiente URL:

ftp://156.35.151.XXX/

H Observa que puedes navegar por las carpetas. Intenta copiar al sitio *ftp* algún archivo o carpeta. Observarás que no podrás. Busca entre las fichas de configuración del *Sitio FTP predeterminado* la opción adecuada para que puedas crear carpetas y subir ficheros al sitio. ¿Qué opción es ésta y en qué ficha se encuentra? Indícalo a continuación:

–Pregunta 19–

Ficha:	Opción:

Haz las pruebas necesarias para comprobar que tras habilitar esta opción puedes crear carpetas y subir ficheros al sitio *ftp*.

7 Pasos finales

Ordenador Windows XP

- Vuelve a la configuración del servidor *proxy* del navegador y en el campo *No usar proxy para las direcciones que comiencen por* elimina la dirección IP que has introducido.

Ordenador Windows Server 2003

- Utilizando *Agregar o quitar programas* y después *Agregar o quitar componentes de Windows* desinstala primero *Servicios de Certificate Server* y después *Servidor de aplicaciones.*