

1 > Servidores web

1.1 > ¿Qué es HTTP?

El protocolo de transferencia de hipertexto o HTTP (*Hypertext Transfer Protocol*) es un protocolo de la capa de aplicación que permite distribuir y compartir información entre sistemas mediante páginas web.

Este protocolo fue desarrollado por Sir Timothy Berners-Lee y su equipo. Crearon asimismo el lenguaje de etiquetas de hipertexto o HTML (*Hypertext Markup Language*) y el sistema de localización de objetos en la web o URL (*Uniform Resource Locator*).

A partir de 1990 HTTP se convirtió en el protocolo de la World Wide Web o WWW (Red Global Mundial), también creada por Berners-Lee, que representa la unión de hipertexto e Internet.

La RFC 2616 especifica el estándar de la versión del HTML v1.1, que es la que se usa actualmente.

El IETF (Internet Engineering Task Force) o Grupo Especial sobre Ingeniería de Internet trabaja en la nueva versión de HTTP 2.0 que intentará mejorar la velocidad y la conexión con dispositivos de telefonía móvil.

1.2 > Localizador uniforme de recursos (URL)

Un localizador uniforme de recursos o URL se compone de una serie de elementos fijados por un estándar que se usan para nombrar recursos en Internet y permitir la localización o identificación de los mismos. Un URL identifica un único recurso.

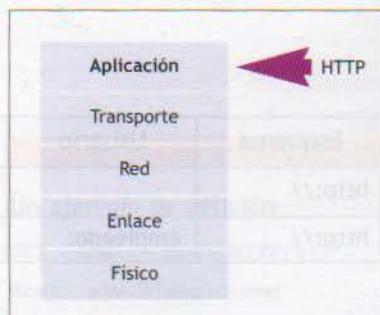
Un navegador web localiza y muestra un recurso de forma adecuada mediante la introducción de un URL. Este último contiene diversa información que permite realizar de manera adecuada el proceso descrito.

El formato general de un URL es:

esquema://usuario:contraseña@máquina:puerto/directorio/archivo

Donde:

- **Esquema:** especifica qué protocolo debe ser usado para acceder a cada documento. Como por ejemplo: HTTP, HTTPS, mailto, FTP... Utiliza los separadores «//» o «:».
- **Usuario:** indica el usuario. Le sigue como separador el símbolo de dos puntos (:).
- **Contraseña:** indica la contraseña. A continuación se añade como separador una arroba (@).
- **Máquina:** indica el nombre del equipo donde está alojado el contenido. Puede ser una FQDN, una dirección IP o un nombre de dominio.
- **Puerto:** indica el puerto de escucha. Va precedido por el separador dos puntos (:).
- **Directorio:** consta de una secuencia de directorios separados por barras que definen la ruta a seguir para llegar al documento.
- **Archivo:** indica el nombre del archivo que contiene el recurso.



4.1. HTTP en el modelo TCP/IP.

Niveles del protocolo TCP/IP

Aplicación	Transporte
HTTP	TCP (80) UDP (80)

Vocabulario

Hipertexto: en informática, es el texto que aparece en pantalla y que permite acceder a otros recursos: textos, imágenes, gráficos, etc., relacionados mediante pulsaciones de ratón o teclado.

En un URL no tienen por qué aparecer todos los campos, como vemos en los siguientes ejemplos:

<http://ejemplo.com/recurso.html>

<http://empleado:123abc@192.168.100.1:80/alberto/a.html>

Donde tenemos:

Esquema	Usuario	Contraseña	Máquina	Puerto	Directorio	Archivo
http://			ejemplo.com			/recurso.html
http://	empleado:	123abc@	192.168.100.1	:80	/alberto	/a.html

RFC 2616



http://xurl.es/rfc_2616

RFC 3986



http://xurl.es/rfc_3986

URN y URI

Cuando se habla de URL aparecen dos conceptos directamente relacionados con él: URN y URI.

- **URN (uniform resource name)** o nombre de recurso uniforme: identifica recursos en Internet, al igual que el URL, pero a diferencia de este último no indica cómo acceder a ellos. Un ejemplo de URN sería el ISBN de un libro, que identifica la obra, pero no nos indica en qué librería podemos conseguirla.
- **URI (uniform resource identifier)** o identificador uniforme de recurso: añade opcionalmente los campos *pregunta* y *fragmento* al final del URL:
 - *Pregunta*: son una o más variables separadas por punto y coma (;). Van precedidas por el separador «?». Con el separador «=» indicamos el valor de la variable.
 - *Fragmento*: es una zona del documento final. Va precedido del separador «#».

El URI puede ser clasificado como un localizador, un nombre o ambos.

La RFC 3986 indica que, en futuras especificaciones, se recomendará el uso del término URI en lugar de URL y URN, que son más restrictivos.

Ejemplo

A continuación se muestran algunos ejemplos de URI:

`foo://ejemplo.com:XXXX/over/there?name=exemple#nose`

`ftp://ftp.is.co.za/rfc/rfc1808.txt`

`http://www.ietf.org/rfc/rfc2396.txt`

`ldap://[2001:db8::7]/c=GB?objectClass?one`

`mailto:Jose.Dolz@ejemplo.com`

`news:comp.infosystems.www.servers.unix`

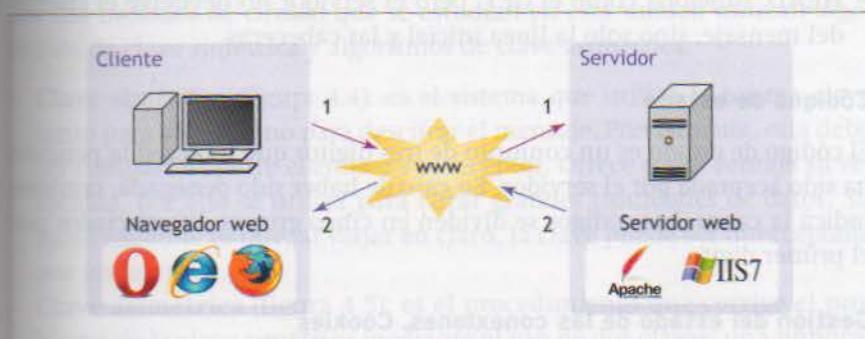
`telnet://192.0.2.16:80/`

`urn:oasis:names:specification:docbook:dtd:xml:4.1.2`

1.3 > Funcionamiento del protocolo HTTP

HTTP es un protocolo de pregunta/respuesta basado en el modelo cliente-servidor. Estos son los pasos que sigue en su funcionamiento:

- El navegador web envía un mensaje de petición al servidor web.
- El servidor que contiene los recursos o almacena los documentos envía un mensaje de respuesta.



4.2. Funcionamiento del protocolo HTTP.

Un navegador web o cliente web se denomina *user agent* o UA (agente de usuario) y la información transmitida se llama recurso. Este último, como se ha visto, se identifica con un URL.

Mensajes HTTP

El mensaje HTTP contiene el estado de la solicitud y puede incluir cualquier información que pida el cliente.

Los mensajes HTTP utilizan el formato estandarizado por la RFC 822 y pueden ser de petición o de respuesta:

- Mensaje de petición:** el cliente indica la acción que quiere realizar, el recurso sobre el que se quiere realizar esta acción y cualquier otro dato necesario para que el servidor pueda atender la petición.
- Mensaje de respuesta:** el servidor incluye en este paquete tanto información necesaria para el funcionamiento del protocolo, como, por ejemplo, el estado de la petición, como el recurso solicitado por el cliente.

Sesión HTTP

Una sesión HTTP consiste en una serie de transacciones de red entre el cliente y el servidor. El cliente realiza una petición y establece una conexión TCP estable con el puerto 80 del servidor, que permanece a la escucha. El servidor procesará la información y transmitirá una respuesta compuesta por un mensaje de estado (en HTTP v1.1: 200 OK) y un mensaje con el recurso solicitado.

En HTTP v1.0, cuando un cliente se comunica con un servidor, se abre una conexión. Una vez que el servidor le ha contestado, se cierra.

El HTTP v1.1 aumenta la velocidad al permitir que se realice por una misma conexión más de una transacción. Esto evita tener que volver a negociar la conexión TCP una vez enviada la primera petición.

obtener el resultado en tiempo

información (OK)

200 OK

se ha terminado de recibir la respuesta

Un ejemplo de petición

```
GET /indice.html HTTP/1.1
Host: www.ejemplo.com
User-Agent: Mozilla/5.0
(Windows; U; Windows NT 5.1;
en-US) AppleWebKit/525.13
(KHTML, like Gecko)
Chrome/0.X.Y.Z Safari/525.13
[Linea en blanco]
```

Un ejemplo de respuesta

```
HTTP/1.1 200 OK
Date: Fri, 31 Dec 2012
23:59:59 GMT
Content-Type: text/html
Content-Length: 1441
<html>
<body>
<h1>Página principal</h1>
<...>
</body>
</html>
```

Grupos de códigos de estado

1XX: informativo.

2XX: éxito.

3XX: redirección; para completar la acción se deben realizar más operaciones.

4XX: error en el cliente.

5XX: error en el servidor.

Métodos de petición

El método indica la acción que se quiere realizar con el recurso. HTTP v1.1 define ocho métodos diferentes, pero estos son los más usados:

- GET: realiza la petición de un recurso al servidor mediante el URL.
- POST: le indica al servidor que le va a llegar información del cliente que irá contenida en el cuerpo. Se suele utilizar en formularios.
- HEAD: funciona como el GET, pero el servidor no devuelve el cuerpo del mensaje, sino solo la línea inicial y las cabeceras.

Códigos de estado

El código de estado es un conjunto de tres dígitos que indica si la petición ha sido aceptada por el servidor. En caso de haber sido denegada, también indica la causa. Los códigos se dividen en cinco grupos diferenciados por el primer dígito.

Gestión del estado de las conexiones. Cookies

HTTP no tiene memoria, por lo tanto no guarda información de transacciones antiguas del cliente. Para ello deberemos utilizar un sistema externo: las llamadas cookies.

Una **cookie** es un conjunto de datos que recibe el cliente y almacena a petición del servidor web. Fueron desarrolladas por la empresa Netscape en el año 1994.

El servidor, gracias a las cookies, puede saber si un cliente se ha validado o no con antelación a la petición actual. De ese modo, puede brindarle servicios propios de usuarios registrados, como acceso a zonas privadas o configuración de entornos. También se puede hacer un seguimiento del usuario a través del sitio web. De este modo es posible generar estadísticas de uso del sitio.

Existen dos tipos de cookies:

- **Origen:** habilitadas por el sitio que estamos visitando.
- **Third-Party cookies** o cookies a terceros: producidas por anuncios u otros elementos externos al sitio visitado. Estas permiten realizar un seguimiento de los usuarios a través de la web recopilando información acerca de sus preferencias. Estos datos permitirán realizar perfiles no autorizados sobre los gustos de los usuarios. Existen leyes en diferentes países que las regulan.

Los usuarios pueden visualizar las cookies almacenadas por el UA y borrarlas. También pueden configurar su recepción, permitiendo bloquear el acceso a determinadas cookies.

RFC 6265

La RFC que estandariza las cookies es la 6265.



http://xurl.es/rfc_6265

Ejemplo

A continuación se muestra un ejemplo de una cookie:

```
Set-Cookie:ID=81.203.9.72-3163514960.30207365;lv=1332677651256;ss=1332677651256;
Domain=.mozilla.org;Path=/;Expires=miércoles, 23 de marzo de 2022 13:14:11;HttpOnly
```

1.4 > Sistema criptográfico

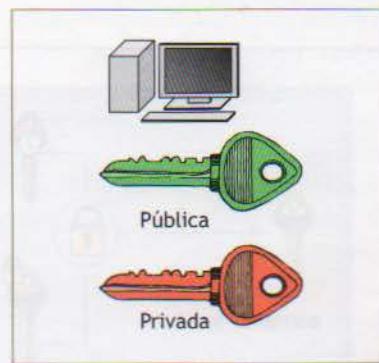
El sistema criptográfico es un conjunto de operaciones que permiten transmitir información de forma privada y segura entre emisor y receptor.

El mecanismo de cifrado consiste en aplicar un algoritmo sobre un texto en claro de forma que se obtenga otro compuesto por letras y símbolos que solo el receptor pueda leer.

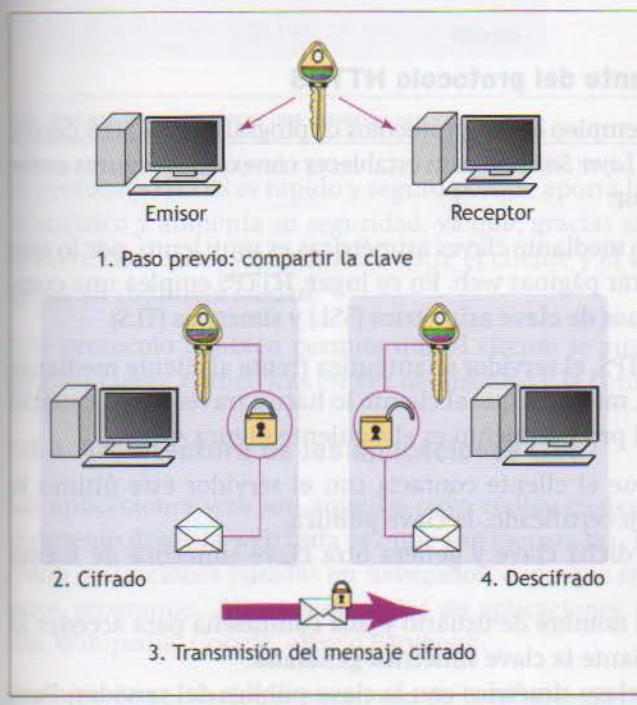
Los dos métodos de cifrado que se estudian en esta unidad utilizan algoritmos de clave simétrica y algoritmos de clave asimétrica:

- **Clave simétrica** (figura 4.4): es el sistema que utiliza la misma clave tanto para cifrar como para descifrar el mensaje. Previamente, esta debe ser compartida entre el emisor y el receptor. Ofrece como ventaja su velocidad, por ello se utiliza para cifrar grandes cantidades de datos. Su inconveniente es que, al viajar en claro, la clave puede ser interceptada por un tercero.
- **Clave asimétrica** (figura 4.5): es el procedimiento que corrige el problema de la clave simétrica mediante el uso de dos claves: una pública, que se puede enviar a todos los usuarios, y otra privada, que su propietario debe mantener en secreto. Estas claves son complementarias, es decir, lo que se cifra con una solamente lo puede descifrar la otra y viceversa. Su principal ventaja es que, como solo se transmite la clave pública, aunque sea interceptada, las transmisiones seguras no se verán comprometidas. Sus principales inconvenientes son que resulta un proceso muy lento y que debe existir el modo de asegurar que la clave pública realmente pertenezca a su dueño. Los dos elementos básicos utilizados por este sistema de cifrado son el certificado digital y la firma electrónica.

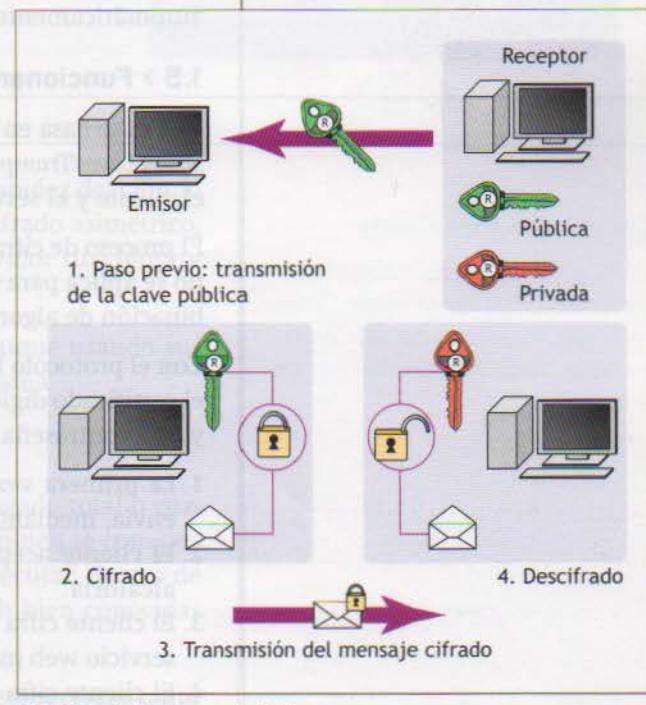
Este apartado trata sobre el cifrado simétrico y el cifrado asimétrico. El cifrado simétrico es más rápido y se usa para cifrar grandes cantidades de datos. El cifrado asimétrico es más lento pero más seguro porque usa dos claves: una pública y una privada.



4.3. Claves pública y privada.



4.4. Método de clave simétrica.



4.5. Método de clave asimétrica.

Función Hash

La función *Hash* es un algoritmo que al aplicarse sobre información de cualquier tamaño genera un conjunto de bits de longitud fija que representa un resumen único de dicha información.



Autoridades de certificación (CA)

Los navegadores web admiten los certificados firmados electrónicamente por las CA que tienen en su lista sin informar al usuario.



Firma electrónica

La firma electrónica amplía el concepto de firma manuscrita. Al firmar electrónicamente un documento, además de asegurar que el firmante original es el origen de dicho documento y que él no pueda negar que envió el mensaje, se verifica que su contenido no ha sido modificado. Estas características se denominan **autenticidad, no repudio e integridad** de datos.

El proceso de firma electrónica consiste en cifrar el resumen de un documento con la clave privada del emisor. Así, todos los destinatarios que tengan la clave pública del emisor podrán verificar su procedencia.

Certificado digital

Es el documento electrónico que acredita la correspondencia de una clave pública con su propietario. Mediante un certificado digital se resuelve el segundo problema en el cifrado de clave asimétrica, pero se plantea uno nuevo: saber si el certificado es auténtico o si ha sido falsificado.

Dado que las claves públicas son accesibles por todos los usuarios y que estos no suelen tener relación entre sí, es necesario encontrar el modo que permita que un usuario confíe en el certificado de otro.

Para ello se acude a las **autoridades de certificación** o CA (*Certification Authority*), entidades en las que todos los usuarios confían y que se encargan de distribuir y publicar los certificados digitales. Un ejemplo de CA es la Fábrica Nacional de Moneda y Timbre.

También existen los certificados que son firmados por la misma entidad cuya identidad se certifica, los llamados certificados **autofirmados**. La desventaja de estos certificados es que los navegadores no los reconocen automáticamente.

1.5 > Funcionamiento del protocolo HTTPS

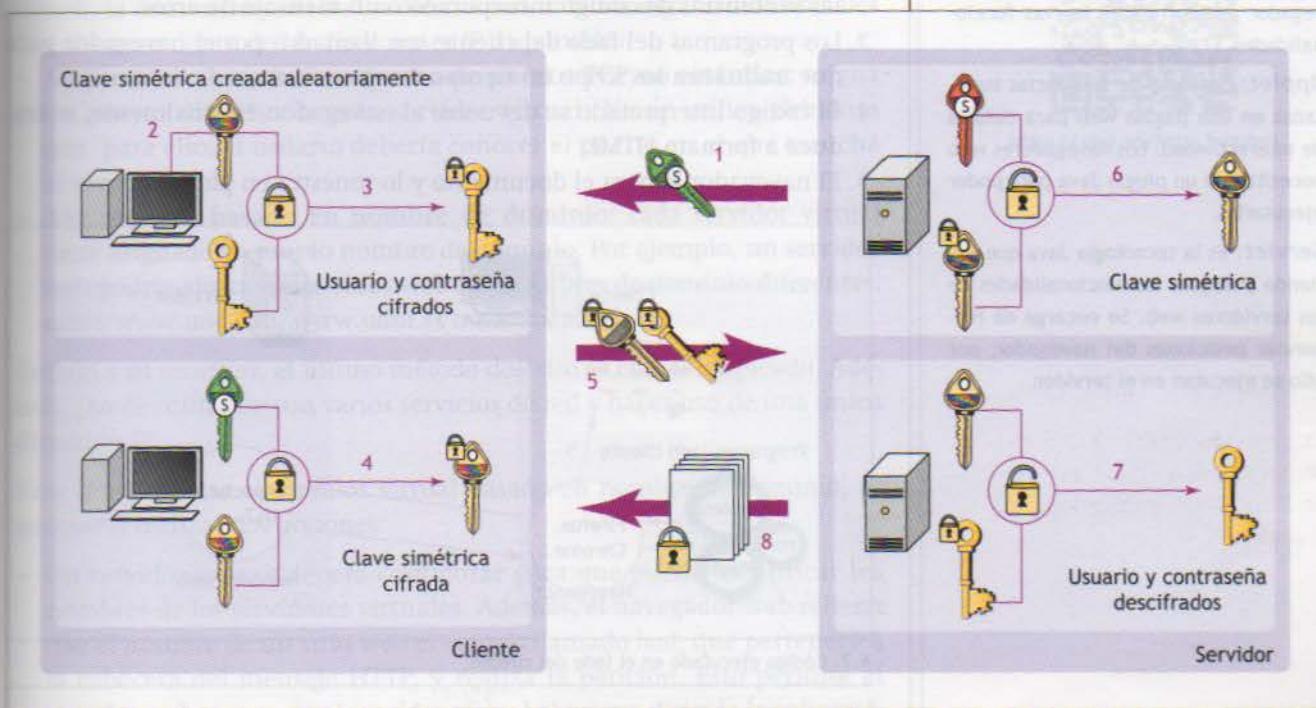
HTTPS se basa en el empleo de los protocolos criptográficos SSL/TLS (*Secure Socket Layer/Transport Layer Security*) para establecer conexiones seguras entre el cliente y el servidor.

El proceso de cifrado mediante claves asimétricas es muy lento, por lo que no se aplica para cifrar páginas web. En su lugar, HTTPS emplea una combinación de algoritmos de clave asimétrica (SSL) y simétrica (TLS).

Con el protocolo HTTPS, el servidor se autentica frente al cliente mediante el certificado digital, mientras que el cliente lo hace a través de un usuario y una contraseña. El procedimiento es el siguiente (figura 4.6):

1. La primera vez que el cliente contacta con el servidor este último le envía, mediante su certificado, la clave pública.
2. El cliente acepta dicha clave y genera otra clave simétrica de forma aleatoria.
3. El cliente cifra un nombre de usuario y una contraseña para acceder al servicio web mediante la clave simétrica generada.
4. El cliente cifra la clave simétrica con la clave pública del servidor. Para ello utiliza el sistema de criptografía asimétrica.

5. Se transmiten al servidor tanto el usuario y la contraseña cifrados como la clave simétrica cifrada.
6. El servidor descifra la clave simétrica a través de su clave privada.
7. La clave simétrica permite descifrar el nombre de usuario y la contraseña que han viajado cifrados a través de la red.
8. El servidor comprueba si el usuario tiene acceso al servicio web. En caso afirmativo, la conexión se habrá completado. A partir de este momento, cifrará las páginas web con la clave simétrica antes de transmitirlas y el cliente, una vez las reciba, podrá descifrarlas usando esta misma clave.



4.6. Proceso para establecer una conexión segura.

El protocolo HTTPS es rápido y seguro porque aporta la rapidez del cifrado asimétrico y aumenta su seguridad, ya que, gracias al cifrado asimétrico, la clave simétrica es transmitida entre el cliente y el servidor sin comprometer su confidencialidad.

Este protocolo también permite que el cliente se autentique usando sus propias claves asimétricas en vez del usuario y la contraseña.

1.6 > Arquitectura de las aplicaciones web

Las aplicaciones web son aquellas cuyo código es descargado total o parcialmente desde la web cada vez que son ejecutadas. También se conocen como aplicaciones basadas en navegador, dado que se ejecutan dentro de estos programas. Algunos ejemplos de aplicaciones web bien conocidas son Wikipedia, Google, eBay o Facebook.

Este tipo de aplicaciones hacen uso de la tecnología cliente-servidor tanto a través de una intranet como de Internet.

Función básica

La función básica de una aplicación web es la de informar la actividad en el sistema.

Vocabulario

Plugin o complemento: es un pequeño programa que se instala en el navegador para ofrecerle nuevas funcionalidades.

Applet: conjunto de sentencias insertadas en una página web para dotarla de interactividad. Los navegadores web necesitan de un plugin Java para poder ejecutarlas.

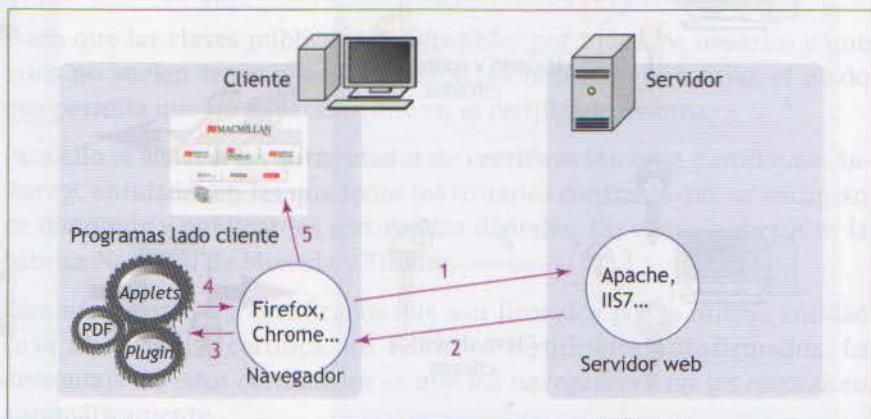
Servlet: es la tecnología Java que extiende y mejora las funcionalidades de los servidores web. Se encarga de responder peticiones del navegador, por ello se ejecutan en el servidor.

Ejecución de código en el cliente

El cliente representa en pantalla un documento generado a partir del código HTML. Además, se hace cargo de la ejecución de las sentencias que componen los scripts (programas), que se encuentran incorporados en el código de las mismas. Por ejemplo, plugins como PDF o applets.

En la figura 4.7 se muestra el funcionamiento de una aplicación web, cuyos pasos se describen a continuación:

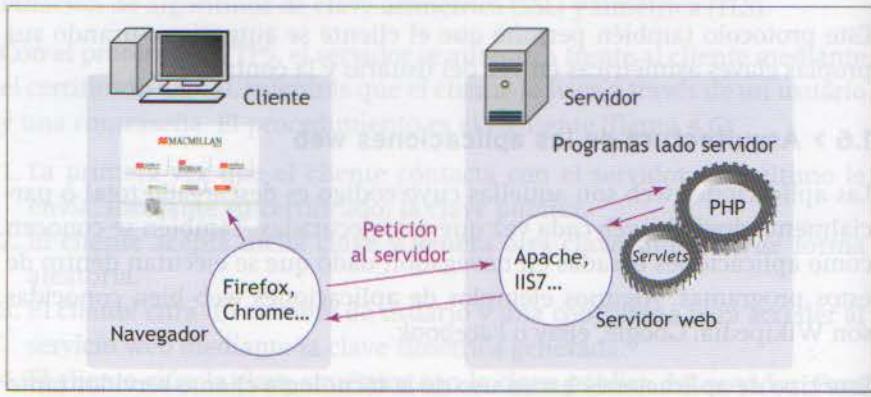
1. El navegador realiza una petición al servidor web.
2. El servidor envía el documento completo en formato HTML junto con las sentencias de código incorporado o un mensaje de error.
3. Los programas del lado del cliente son llamados por el navegador para que traduzcan los scripts en tiempo de ejecución.
4. El código interpretado se devuelve al navegador. Normalmente, se traduce a formato HTML.
5. El navegador genera el documento y lo muestra en pantalla.



4.7. Código ejecutado en el lado del cliente.

Ejecución de código en el servidor

La diferencia respecto a la ejecución de código en el lado del cliente consiste en que son los programas del lado del servidor quienes interpretan y ejecutan los scripts, para luego generar como resultado código HTML, que posteriormente enviarán al navegador web.



4.8. Código ejecutado en el lado del servidor.

1.7 > Servidor virtual

Se denomina **alojamiento virtual** la técnica que permite hospedar diversos sitios web sobre un mismo servidor de páginas web. A cada uno de estos sitios se le llama **servidor virtual**.

Los servidores virtuales pueden crearse utilizando varios métodos:

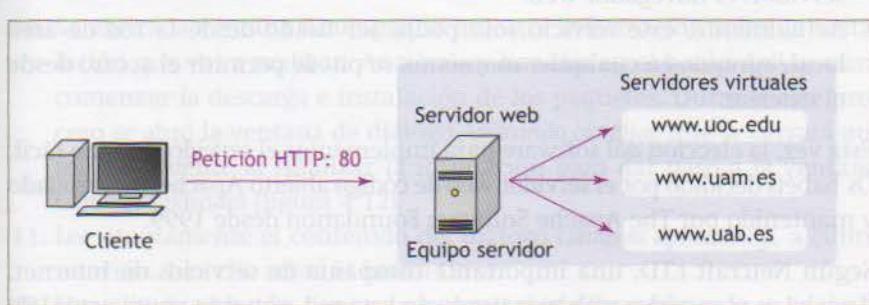
- **Alojamiento basado en dirección IP:** cada servidor virtual debe tener asignada una dirección IP diferente. Este método tiene varias desventajas, entre las que se encuentran la gestión que comporta la asignación de las direcciones IP o la creación de interfaces virtuales en el servidor web, la administración de las direcciones ante los organismos oficiales y el agotamiento de las direcciones IP disponibles.
- **Alojamiento basado en número de puerto TCP no estándar:** asigna un puerto diferente a cada servidor virtual. No se utiliza debido a que, para ello, el usuario debería conocer el puerto en el que escucha el servidor web.
- **Alojamiento basado en nombre de dominio:** cada servidor virtual tiene asignado su propio nombre de dominio. Por ejemplo, un servidor web podría alojar varios sitios web con nombres de dominio diferentes, como www.uoc.edu, www.uam.es o www.uab.es.

Debido a su sencillez, el último método descrito es el más empleado. Además, puede utilizarse con varios servicios de red y hacer uso de una única dirección IP.

Para implementar el servidor virtual basado en nombre de dominio, es necesario realizar dos acciones:

- Un servidor web se deberá configurar para que pueda identificar los nombres de los servidores virtuales. Además, el navegador web rellena con el nombre de un sitio web el campo llamado *host*, que pertenece a la cabecera del mensaje HTTP, y realiza la petición. Esto permite al servidor web reconocer el servidor virtual al que va dirigida la solicitud. En la versión 1.1 del protocolo HTTP aparece por primera vez esta nueva característica.
- Los nombres de *host* deberán registrarse en el servidor DNS para que pueda resolver la dirección IP del servidor web.

A veces se realizan peticiones a servidores virtuales que ya no existen. Si se configura un servidor virtual por defecto, se asegura que la petición será atendida.



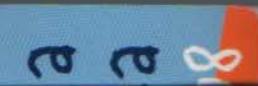
4.9. Servidores web virtuales basados en el nombre de dominio.

Lista de campos de cabecera HTTP

Encontrarás la lista de campos de cabecera de los mensajes HTTP y concretamente el campo host en el siguiente URL:



http://xurl.es/http_headers



2 >> Servicios web en sistemas GNU/Linux

Para saber más

Sitio web de The Apache Software Foundation:



<http://www.apache.org>

Servidor web: la tecnología Java que maneja y sirve las funcionalidades de los servicios web. Se encarga de gestionar peticiones del navegador, para ello se organiza en el protocolo

Clasificación de código abierto

Es una muestra de los dos modelos visto con anterioridad, donde existe código de programación para ejecutar en los servidores, tanto en el cliente como en el servidor.

En esta ocasión, el trabajo que vais a desarrollar en ServPubli consistirá en la instalación y configuración de un servicio que permita a los usuarios acceder, por ejemplo, a distintos tipos de información, a servicios internos de comunicaciones para tener la posibilidad de realizar videoconferencias, mensajería instantánea, etc.

En los contactos previos, la empresa os comunicó algunos de los problemas que venía sufriendo: replicación de la misma información en distintos ordenadores, inconsistencia de los datos almacenados, ausencia de control sobre quién accede a la información más sensible y falta de fluidez en las comunicaciones internas.

Por tanto, el plan de trabajo pactado con los representantes de la empresa incluye cubrir las siguientes necesidades:

- Disponer de acceso centralizado a través de la red a determinada información, como puede ser documentación, programas, archivos multimedia, etc.
- El método de trabajo tiene que ser sencillo y utilizará herramientas intuitivas y fáciles de usar.
- Los trabajadores de la empresa deben poder acceder a los mismos documentos independientemente del ordenador que estén usando en cada momento.
- Cada trabajador solo podrá acceder a los datos que el administrador del sistema le permita.

Una vez analizados estos requerimientos y valoradas las distintas alternativas, optáis por implantar el servicio web como solución a las necesidades actuales.

Las justificaciones que presentáis a la empresa sobre el uso de este servicio son las siguientes:

- Todos los datos están organizados y centralizados evitando duplicidades y garantizando la integridad.
- Este servicio permite alojar distintos tipos de datos.
- El acceso a estos datos se puede restringir, de forma que cada usuario vea solo la información para la que está autorizado. Además la información podrá ser cifrada.
- Los usuarios ya conocen la herramienta que les permitirá acceder al servidor: el navegador web.
- Actualmente, este servicio solo podrá ser usado desde la red de área local, aunque, en cualquier momento, se puede permitir el acceso desde el exterior.

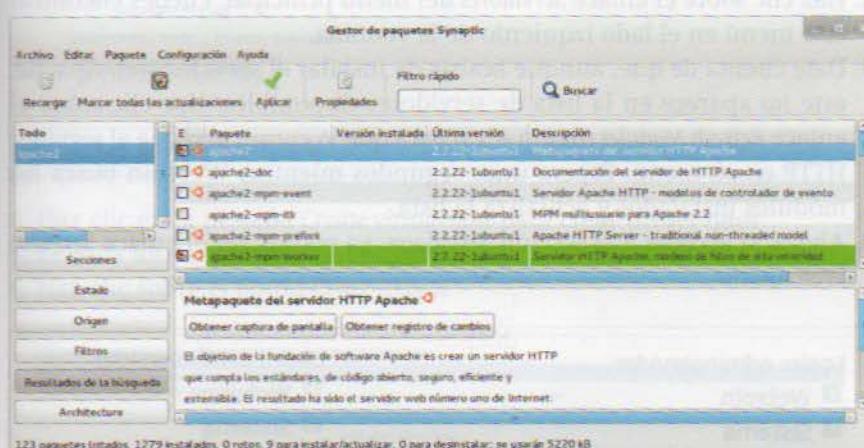
Esta vez, la elección del software para implementar el servidor ha sido fácil. Os habéis decidido por el servidor web de código abierto Apache, desarrollado y mantenido por The Apache Software Foundation desde 1999.

Según Netcraft LTD, una importante compañía de servicios de Internet, Apache es el servidor web más usado en esta red, con una cuota actual de mercado próxima al 65%.

2.1 > Instalación del servidor < Consultar el ejercicio de desarrollo de la actividad

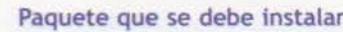
Sigue las indicaciones que se realizan a continuación para proceder a la instalación del servidor HTTP:

1. Abre una sesión gráfica en el servidor.
 2. Abre el gestor de paquetes Synaptic.
 3. Haz clic en el botón *Recargar* para actualizar la lista de paquetes disponibles en los repositorios de Internet que están configurados. Espera unos segundos mientras termina este proceso.
 4. Haz clic sobre el botón *Buscar* para acceder a la herramienta de búsqueda.
 5. Escribe *apache2* en el cuadro de texto y haz clic en el botón *Buscar* (figura 4.10).
 6. Selecciona *apache2* haciendo clic sobre el nombre del paquete y lee la información adicional mostrada debajo de la lista.
 7. Haz clic sobre la casilla de verificación que se encuentra delante del nombre del paquete que has seleccionado, de esta manera lo marcas para instalar.
 8. Se abrirá un diálogo que te advierte que para poder instalar apache2 es necesario marcar otros paquetes. Haz clic en el botón *Marcar* para permitir estos cambios adicionales.
 9. Asegúrate de que la casilla de verificación correspondiente al paquete apache2 se encuentra marcada y haz clic sobre el botón *Aplicar* para iniciar la instalación.

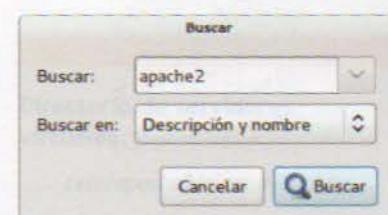


4.11. Selección de paquetes.

10. Se abrirá la ventana *Resumen* que muestra información sobre la instalación que vas a realizar. Analízala y haz clic en el botón *Aplicar* para comenzar la descarga e instalación de los paquetes. Durante este proceso se abre la ventana de diálogo *Aplicando cambios*, que se cerrará automáticamente al finalizar la instalación para dar paso a la ventana *Cambios aplicados* (figura 4.12).
 11. Lee atentamente el contenido del diálogo *Cambios aplicados* y, a continuación, haz clic sobre el botón *Cerrar*.
 12. Haz clic en el botón *Cerrar* de la ventana de Synaptic para salir de la aplicación.



apache2



4.10. Herramienta Buscar



4.12. Ventana Cambios aplicados

2.2 > Configuración del servidor

Después de instalar el servidor web, el siguiente paso es crear y configurar estos servidores virtuales basados en el nombre:

- www.servpubli.com: servidor de uso general con acceso anónimo.
- webapp.servpubli.com: aplicación segura de comunicaciones.
- software.servpubli.com: almacena software de uso general y los manuales correspondientes.

Para dotar de seguridad a los servidores virtuales aplicarás, por separado o en conjunto, estas tareas:

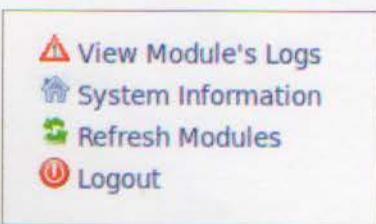
- Crear los mecanismos necesarios para permitir o denegar el acceso al servidor, dependiendo de las credenciales que presente el cliente.
- Configurar el servidor virtual para que, mediante el cifrado de la información, se garantice tanto la confidencialidad como la autenticación del servidor frente al cliente.

Repasa la información de configuración de la red y del hardware de ServPubli antes de seguir estas indicaciones y realizar las actividades. Esta información está detallada en el epígrafe 2.1 de la Unidad 1.

Acceso al módulo Servidor Web Apache

Sigue estas indicaciones para actualizar la lista de servidores en Webmin:

1. Abre el navegador web en el servidor y accede a Webmin.
2. Haz clic sobre el enlace **Servidores** del menú principal. Puedes encontrar este menú en el lado izquierdo de la ventana.
3. Date cuenta de que, aunque acabas de instalar el servidor web Apache, este no aparece en la lista de servidores disponibles. Haz clic sobre el enlace **Refresh Modules** (figura 4.13) para que Webmin agregue el servidor HTTP en su menú. Espera unos segundos mientras Webmin busca los módulos instalados y actualiza la lista.
4. Ahora, si accedes a la sección **Servidores**, ya podrás ver el enlace **Servidor Web Apache**.



4.13. Refrescar módulos.

Login: adminservidor <input checked="" type="checkbox"/> Webmin <input checked="" type="checkbox"/> Sistema <input checked="" type="checkbox"/> Servidores Lectura de Correo de Usuarios Servidor de DHCP Servidor de DNS BIND <input checked="" type="checkbox"/> Otros <input checked="" type="checkbox"/> Red <input checked="" type="checkbox"/> Hardware <input checked="" type="checkbox"/> Cluster <input checked="" type="checkbox"/> Un-used Modules		Login: adminservidor <input checked="" type="checkbox"/> Webmin <input checked="" type="checkbox"/> Sistema <input checked="" type="checkbox"/> Servidores Lectura de Correo de Usuarios Servidor Web Apache Servidor de DHCP Servidor de DNS BIND <input checked="" type="checkbox"/> Otros <input checked="" type="checkbox"/> Red <input checked="" type="checkbox"/> Hardware <input checked="" type="checkbox"/> Cluster <input checked="" type="checkbox"/> Un-used Modules
--	--	---

4.14. Servidores disponibles.

Creación de un servidor virtual de acceso anónimo

Sigue estos pasos para crear un servidor virtual de acceso anónimo:

1. Para dar contenido al servidor www.servpubli.com, crea el archivo /var/www-anonimo/index.html de forma que, al visualizarlo desde el navegador, se lea el mensaje: Portal web de uso general de ServPubli.
2. Abre Webmin y accede al enlace *Servidor Web Apache* de la sección *Servidores* del menú principal.
3. En la pestaña *Existing virtual hosts* (figura 4.15) encontrarás los servidores virtuales creados en el servidor web Apache. Después de la instalación serán:
 - Servidor por defecto: se usa como plantilla para crear servidores web.
 - Servidor virtual automático: si la petición del cliente no corresponde al nombre de ningún otro servidor, será este servidor quien la atienda.

4.15. Módulo *Servidor Web Apache*.

4. Haz clic en la pestaña *Create virtual host* para crear un servidor.
5. Rellena los campos según la figura 4.16.
6. Haz clic sobre el botón *Crear Ahora*.

4.16. Crear el servidor virtual.

7. Haz clic sobre el enlace *Aplicar cambios*. Lo encontrarás en la esquina superior derecha del módulo *Servidor Web Apache* (figura 4.17).

Advertencia

Es posible que necesites permisos de superusuario para crear el contenido de los servidores virtuales.

Directorio de servidores virtuales

/etc/apache2/sites-available

Directorio de servidores virtuales habilitados

/etc/apache2/sites-enabled

**Aplicar Cambios
Parar Apache
Buscar Documentos..**

4.17. Aplicar cambios.

Emisión de un certificado autofirmado

El primer paso para configurar un servidor seguro es obtener un certificado que será usado en la comunicación HTTPS. Este certificado puede ser emitido por autoridades certificadoras reconocidas o por la propia empresa u organización actuando como autoridad certificadora para sí misma. En este último caso, se denominan certificados autofirmados.

Como ServPubli va a usar el certificado internamente y no quiere invertir dinero para conseguirlo, le proponemos generar su propio certificado. Sigue estos pasos para crear un certificado autofirmado:

1. Abre Webmin y despliega la sección Webmin del menú principal.
2. Accede al enlace *Configuración* de Webmin.
3. Acabas de acceder al módulo que permite la configuración general de esta aplicación (figura 4.18). Haz clic sobre el enlace *Encriptación SSL*.



4.18. Módulo Configuración de Webmin.

4. Esta página te permite gestionar los certificados que usa Webmin; podrás, por ejemplo, crearlos, importarlos, etc. Accede a la pestaña *Create Certificate* para crear una clave y un certificado nuevos.

Indice de Módulo

[SSL settings](#) [Current certificate](#) [Per-IP certificates](#) [Create certificate](#) [Upload certificate](#)

La máquina en que Webmin se está ejecutando parece tener el módulo SSLeay de Perl instalado. Usándolo, Webmin soporta comunicaciones SSL cifradas entre el navegador y el servidor. Si está accediendo a su servidor Webmin a través de Internet, debe de considerar de manera definitiva el utilizar SSL para prevenir que cualquiera capture su clave de acceso a Webmin.

Aviso - active el soporte SSL sólo si tiene un navegador que lo soporta a su vez (como p.ej. Netscape o IE), y no tiene un cortafuegos bloqueando las peticiones https entre su navegador y la máquina de Webmin.

Encriptación SSL

4.19. Módulo Encriptación SSL.

5. Comprueba que la opción *localhost* del control *Nombre de servidor en URL* esté marcada.
 6. Elimina el contenido del campo *Organización* y escribe el nombre de la empresa: *ServPubli*.
 7. El código ISO para España es *ES*. Escríbelo en el cuadro de texto *Código de país*.
 8. En el campo *Escribir clave a archivo* se especifica el fichero donde se almacenará tanto el certificado como la clave privada. Introduce en este campo */etc/apache2/CertificadoServPubli.pem*.
 9. Selecciona la opción *No* del control *¿Utilizar la nueva clave inmediatamente?* Si no lo haces así, el propio Webmin cambiaría el certificado que usa actualmente para su conexión HTTPS por el que vas a crear. Esta situación conllevaría que tu navegador web, al no reconocer el nuevo certificado, mostrará un mensaje de advertencia indicando que la conexión con Webmin no está verificada.
 10. Haz clic sobre el botón *Crear ahora* para crear el archivo con la clave privada y el certificado.

Indice de Módulo

Encriptación SSL

[SSL settings](#) | [Current certificate](#) | [Per-IP certificates](#) | **Create certificate** | [Upload certificate](#)

Este formulario se utiliza para crear una nueva clave SSL para su servidor Webmin.

Crear clave SSL

Nombre de servidor en URL	<input checked="" type="radio"/> Cualquier nombre de máquina <input type="radio"/> localhost
Dirección de correo	<input type="text"/>
Departamento	<input type="text"/>
Organización	ServPubli
City or locality	<input type="text"/>
Estado	<input type="text"/>
Código de País	ES
Tamaño de clave RSA	<input checked="" type="radio"/> Defecto (2048) <input type="radio"/> <input type="text"/> bits
Días antes de expirar	1825
Escribir clave a archivo	/etc/apache2/CertificadoServPubli.pem
¿Utilizar la nueva clave inmediatamente? <input type="radio"/> Si <input checked="" type="radio"/> No	
Crear Ahora	

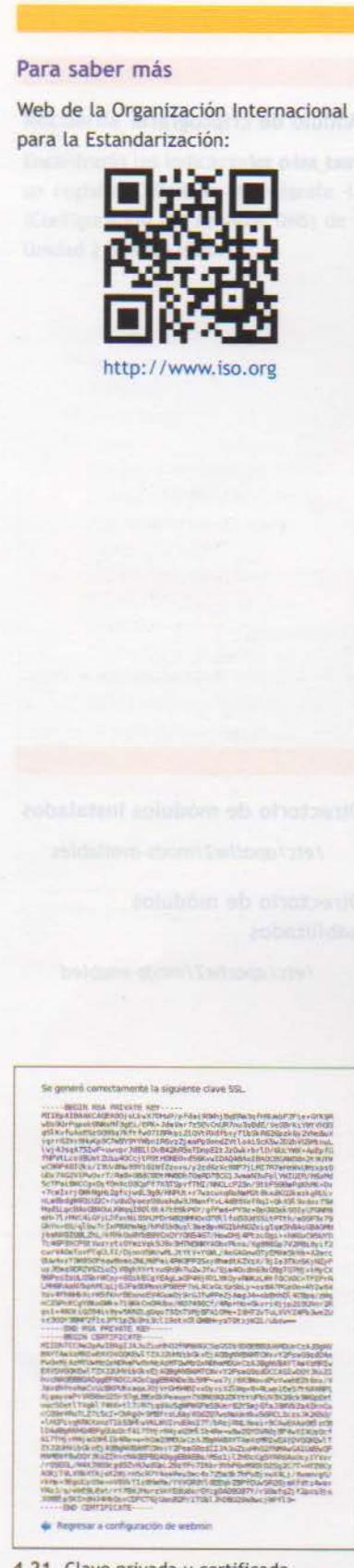
4.20. Crear un certificado

11. Despues de crearlo, se muestra el contenido del archivo que se acaba de crear, CertificadoServPubli.pem (figura 4.21):

 - La primera parte del archivo contiene la clave privada.
 - La segunda parte del fichero guarda el certificado y, por tanto, la clave pública.

Este archivo es de vital importancia para la seguridad del servidor virtual, por lo que no debe estar al alcance de otros usuarios del sistema ni, por supuesto, ser accesible mediante el propio servidor web.

12. Haz clic sobre el enlace **Regresar a configuración de Webmin** para volver al módulo *Configuración de Webmin*.



4.21. Clave privada y certificado

Módulo de criptografía
mod_ssl o ssl



Directorio de módulos instalados

/etc/apache2/mods-available

Directorio de módulos habilitados

/etc/apache2/mods-enabled

Activación del módulo de criptografía

Para poder crear un servidor seguro y usar el protocolo HTTPS es necesario activar el módulo *mod_ssl* (o *ssl*). Sigue estas indicaciones:

1. Abre Webmin y accede al enlace *Servidor Web Apache* de la sección *Servidores* del menú principal.
2. Accede a la pestaña *Global configuration*.
3. Haz clic sobre el enlace *Configure Apache Modules* (figura 4.22).

4.22. Configuración global.

4. Marca la casilla de verificación del módulo *ssl*.
5. Luego haz clic sobre el botón *Enable Selected Modules*.

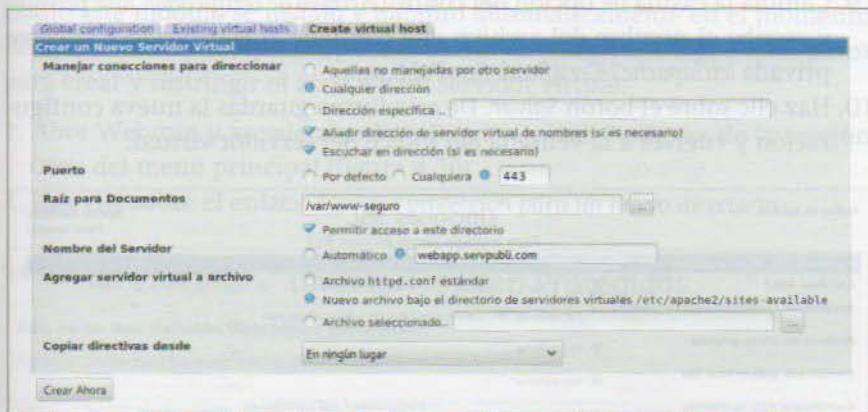
Module	Current state	Module	Current state
<input type="checkbox"/> actions	Disabled	<input type="checkbox"/> file_cache	Disabled
<input checked="" type="checkbox"/> alias	Enabled	<input type="checkbox"/> filter	Disabled
<input type="checkbox"/> asis	Disabled	<input type="checkbox"/> headers	Disabled
<input checked="" type="checkbox"/> auth_basic	Enabled	<input type="checkbox"/> ident	Disabled
<input type="checkbox"/> auth_digest	Disabled	<input type="checkbox"/> imagemap	Disabled
<input type="checkbox"/> authn_alias	Disabled	<input type="checkbox"/> include	Disabled
<input type="checkbox"/> authn_anon	Disabled	<input type="checkbox"/> info	Disabled
<input type="checkbox"/> authn_default	Disabled	<input type="checkbox"/> mem_cache	Disabled
<input checked="" type="checkbox"/> authn_file	Enabled	<input checked="" type="checkbox"/> mime	Enabled
<input type="checkbox"/> authz_ldap	Disabled	<input type="checkbox"/> mime_magic	Disabled
<input type="checkbox"/> authz_dbm	Disabled	<input checked="" type="checkbox"/> negotiation	Enabled
<input checked="" type="checkbox"/> authz_default	Enabled	<input type="checkbox"/> proxy	Disabled
<input checked="" type="checkbox"/> authz_groupfile	Enabled	<input type="checkbox"/> proxy_ajp	Disabled
<input checked="" type="checkbox"/> authz_host	Enabled	<input type="checkbox"/> proxy_balancer	Disabled
<input type="checkbox"/> authz_owner	Disabled	<input type="checkbox"/> proxy_connect	Disabled
<input checked="" type="checkbox"/> authz_user	Enabled	<input type="checkbox"/> proxy_ftp	Disabled
<input checked="" type="checkbox"/> autoindex	Enabled	<input type="checkbox"/> proxy_http	Disabled
<input type="checkbox"/> cache	Disabled	<input type="checkbox"/> proxy_scgi	Disabled
<input type="checkbox"/> cern_meta	Disabled	<input checked="" type="checkbox"/> readline	Enabled
<input type="checkbox"/> cgi	Disabled	<input type="checkbox"/> rewrite	Disabled
<input checked="" type="checkbox"/> cgid	Enabled	<input checked="" type="checkbox"/> setenvif	Enabled
<input type="checkbox"/> charset_lite	Disabled	<input type="checkbox"/> spelling	Disabled
<input type="checkbox"/> dav	Disabled	<input checked="" type="checkbox"/> ssl	Disabled
<input type="checkbox"/> dav_fs	Disabled	<input checked="" type="checkbox"/> status	Enabled
<input type="checkbox"/> dav_lock	Disabled	<input type="checkbox"/> substitute	Disabled
<input type="checkbox"/> dbd	Disabled	<input type="checkbox"/> suexec	Disabled
<input checked="" type="checkbox"/> deflate	Enabled	<input type="checkbox"/> unique_id	Disabled
<input checked="" type="checkbox"/> dir	Enabled	<input type="checkbox"/> userdir	Disabled
<input type="checkbox"/> disk_cache	Disabled	<input type="checkbox"/> usertrack	Disabled
<input type="checkbox"/> dump_io	Disabled	<input type="checkbox"/> version	Disabled
<input checked="" type="checkbox"/> env	Enabled	<input type="checkbox"/> vhost_alias	Disabled
<input type="checkbox"/> expires	Disabled		
<input type="checkbox"/> ext_filter	Disabled		

4.23. Configuración de módulos de Apache.

Creación de un servidor virtual cifrado con HTTPS

Una vez habilitado el módulo SSL ya se puede crear un servidor virtual cifrado. Para esto, primero vas a crear un servidor que escuche las peticiones de los clientes por el puerto HTTPS (443) y, luego, configurarás sus parámetros SSL. Sigue estos pasos:

1. Para dar contenido al servidor webapp.servpubli.com, crea el archivo /var/www-seguro/index.html de forma que, al visualizarlo desde el navegador, se lea el mensaje: *Portal web seguro de ServPubli*.
 2. Para acceder a este servidor se usará el nombre webapp.servpubli.com. Crea un registro de alias de este nombre en el servidor DNS.
 3. Abre Webmin y accede al enlace *Servidor Web Apache* de la sección *Servidores* del menú principal.
 4. Haz clic en la pestaña *Create virtual host* para crear un servidor.
 5. Rellena los campos según la figura 4.24 y haz clic en el botón *Crear Ahora*.



4.24. Crear servidor virtual con puerto HTTPS.

6. Fijate en que el servidor que acabas de crear ya aparece en la lista. Haz clic sobre su correspondiente enlace **Servidor Virtual**.



4.25. Servidores virtuales existentes.

Recuerda

Encontrarás las indicaciones para crear un registro CNAME en el epígrafe 4.2 (Configuración del servidor DNS) de la Unidad 2 de este libro.

Módulo de criptografía: abierta SSL
Este módulo proporciona las herramientas para administrar el cifrado SSL. Al activarlo se nos brindan las siguientes funcionalidades:

- Límites y Procesos
- Redes y Direcciones
- Archivos de bitácora
- Opciones de Documento
- Tipos MIME
- Manejo de Errores
- Alias y Redirecciones
- Programas CGI
- Indizado de Directorio
- Filtros
- Idiomas
- Mostrar Directivas
- Editar Directivas

Advertencia

No se cumplimentará el campo Archivo de clave privada porque esta clave y el certificado se guardan en el mismo archivo.

Dirección de módulos habilitados:

Dirección de módulos habilitados:

Aplicar cambios / Parar Apache / Buscar Documentos..

4.29. Aplicar cambios.

7. Ahora haz clic en el icono Opciones SSL.

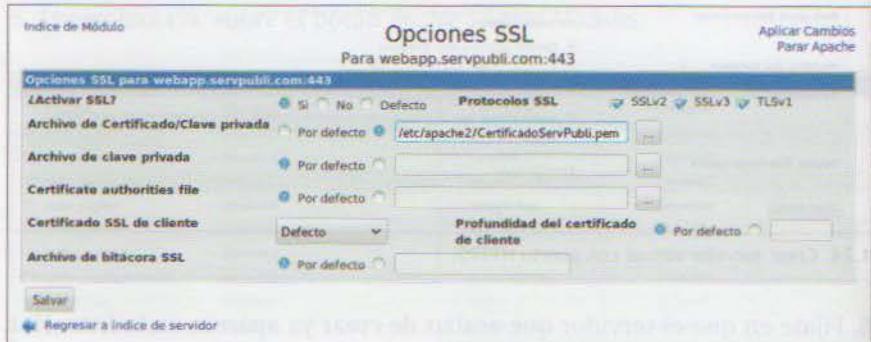


4.26. Índice del servidor virtual.

8. Selecciona Sí en el control ¿Activar SSL?

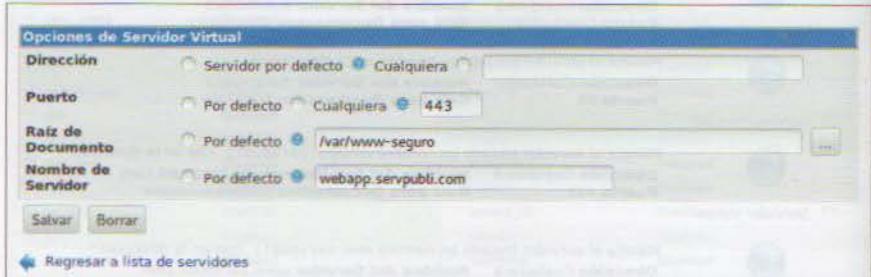
9. Cambia la casilla de opción del control Archivo de certificado/Clave privada y escribe el nombre del archivo que contiene el certificado y la clave privada /etc/apache2/CertificadoServPubli.pem.

10. Haz clic sobre el botón Salvar. De esta forma guardas la nueva configuración y vuelves a la ventana del índice del servidor virtual.



4.27. Opciones SSL del servidor virtual.

11. Al final de esta ventana, bajo la sección Opciones de Servidor Virtual, encontrarás el enlace Regresar a lista de servidores. Haz clic en él.



4.28. Opciones del servidor virtual.

12. El servidor virtual no estará disponible para los clientes hasta que se apliquen los cambios. Haz clic sobre el enlace Aplicar cambios que encontrarás en la esquina superior derecha (figura 4.29).

Configuración de un servidor virtual con autenticación básica

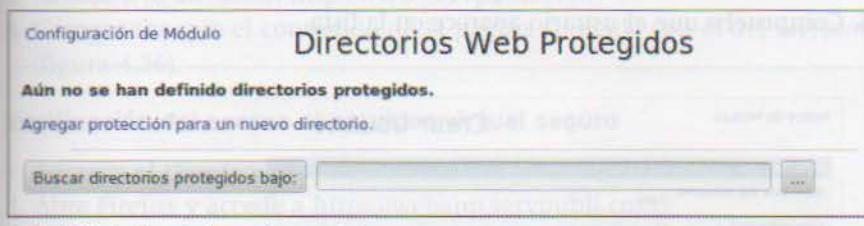
Ya has configurado el servidor webapp.servpubli.com para que la información viaje cifrada entre él y los clientes. De modo que, si alguien interceptara el mensaje, sería muy difícil saber su contenido real.

Además, gracias al protocolo HTTPS, el cliente tiene la certeza de que la información que recibe proviene del servidor original, es decir, que ningún atacante ha suplantado su identidad.

Ahora es el servidor quien debe asegurarse de que solo contesta a los clientes autorizados para acceder a la información que guarda. Cuando se crea un nuevo servidor virtual, por defecto, se puede acceder a él de forma anónima. Si se quiere tener un control de acceso, una de las posibilidades es usar el módulo de autenticación básica, ya que permite al cliente introducir un usuario y una contraseña. Después de comprobar estos datos, el servidor permitirá o denegará el acceso.

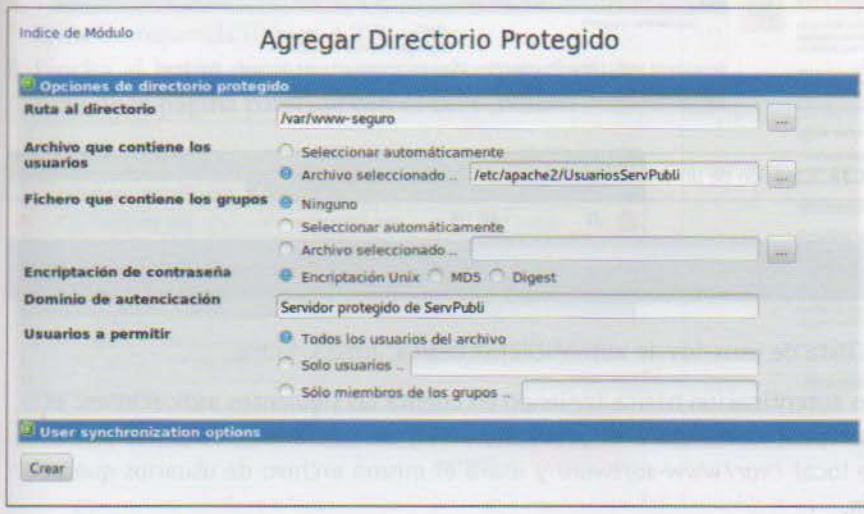
Como este módulo se instaló y habilitó automáticamente en el momento de la instalación de Apache, puedes usarlo directamente. Sigue estos pasos para crear y restringir el acceso a un servidor virtual:

1. Abre Webmin y accede al enlace Directorios Web Protegidos de la sección Otros del menú principal (figura 4.30).
2. Haz clic sobre el enlace Agregar protección para un nuevo directorio.



4.31. Módulo Directorios web protegidos.

3. Rellena los campos según la figura 4.32.
4. Pincha el botón Crear para volver a la lista de directorios protegidos.



4.32. Agregar directorio protegido.

Módulo de autenticación básica

mod_auth_basic o auth_basic

Configuración de mod_auth_basic

Login: adminservidor
 Webmin
 Sistema
 Servidores
 Otros
 Cargas y Descargas
 Comandos Personalizados
 Comandos de Consola
 Conexión SSH
 Directorios Web Protegidos
 Estado de Sistema y de Servidor
 Explorador de Archivos
 Módulos de Perl (CPAN)
 Túnel HTTP
 Text Login
 Red
 Hardware
 Cluster
 Un-used Modules

4.30. Menú Webmin.

Advertencia

El archivo que contiene los usuarios es muy importante para la seguridad del servidor virtual. Crear este archivo en directorios con acceso restringido a la mayoría de usuarios es una muy buena práctica.

Gestión de usuarios de autenticación básica

Ya has protegido un directorio web asociándolo a un archivo de usuarios y contraseñas vacío. Sigue estos pasos para añadir usuarios a este fichero:

1. Abre Webmin y accede al enlace *Directarios Web Protegidos* de la sección *Otros* del menú principal.
2. Observa en la lista de directorios y usuarios que no se han definido usuarios para la carpeta */var/www-seguro*.
3. Haz clic sobre el enlace *Agregar un nuevo usuario*.

The screenshot shows the 'Configuración de Módulo' (Module Configuration) section for 'Directorios Web Protegidos'. On the left, there's a sidebar with various links like 'Administración de usuarios', 'Administración de grupos', 'Administración de direcciones IP', etc. The main area has two tabs: 'Directorio protegido' (Protected Directory) and 'Usuarios y grupos asociados' (Associated Users and Groups). Under 'Directorio protegido', it shows '/var/www-seguro' selected. Under 'Usuarios y grupos asociados', it says 'Aún no se han definido usuarios.' (No users have been defined yet.) There are buttons for 'Un-Protect Selected Directories' and 'Un-Protect and Remove Files'. At the bottom, there's a search bar for 'Buscar directorios protegidos bajo:' (Search protected directories under:).

4.33. Lista de directorios protegidos y usuarios asociados.

4. Rellena los campos del formulario *Crear Usuario* según la figura 4.34.
5. Haz clic sobre el botón *Crear* para dar de alta al nuevo usuario.
6. Comprueba que el usuario aparece en la lista.

This screenshot shows two overlapping windows. The top window is the 'Crear Usuario' (Create User) form, which has fields for 'Nombre de usuario' (User name) set to 'juan', '¿Habilitado?' (Enabled) with 'Si' (Yes) selected, and 'Contraseña' (Password) set to 'Spr1pZ'. Below this is a 'Configuración de Módulo' (Module Configuration) section for 'Directorios Web Protegidos'. The bottom window is the same 'Directorios Web Protegidos' configuration page as in figure 4.33, showing the list of protected directories and users. The user 'juan' is listed under 'Users and groups associated'.

4.34. Creación de un usuario asociado a un directorio protegido.

Actividades propuestas

1. Añade los siguientes usuarios a la lista de usuarios de autenticación básica: luisa y jaime.
2. Crea un nuevo servidor virtual con autenticación básica teniendo en cuenta las siguientes indicaciones: el nombre del servidor será *software.servpubli.com*, usará el protocolo *HTTP*, atenderá las peticiones por el puerto *80*, se alojará en el directorio local */var/www-software* y usará el mismo archivo de usuarios que el servidor virtual *webapp.servpubli.com*.

2.3 > Comprobaciones

Verificación del estado del servicio

Sigue estos pasos para asegurarte de que el servidor está en ejecución:

1. Abre Webmin en el navegador web del servidor, despliega el menú *Otros* y haz clic sobre el enlace *Estado de sistema y de Servidor*.
2. Busca el servicio *Apache Webserver* y comprueba que, a su derecha, hay un símbolo de color verde que indica que está iniciado.

Monitorizando	En host	Estado	Monitorizando	En host	Estado
DHCP Server	Local	✓	PostgreSQL Database Server	Local	✗
Internet and RPC Server	Local	✗	MySQL Database Server	Local	✗
Postfix Server	Local	✗	Apache Webserver	Local	✓
NFS Server	Local	✗	Squid Proxy Server	Local	✗
Extended Internet Server	Local	✗	QMail Server	Local	✗
BIND DNS Server	Local	✓	Samba Servers	Local	✗
Sendmail Server	Local	✗			

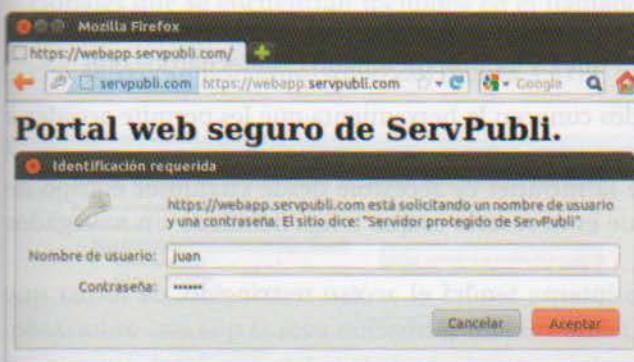
4.35. Estado del sistema y del servidor.

Verificación del acceso al servidor virtual anónimo

1. Arranca el cliente y abre una sesión con el usuario admincliente.
2. Haz clic sobre el icono *Navegador web Firefox* que se encuentra en el panel lateral.
3. Accede a la dirección <http://www.servpubli.com>.
4. Comprueba que el contenido de la página coincide con el del servidor (figura 4.36).

Verificación del acceso al servidor virtual seguro

1. Arranca el cliente y abre una sesión con el usuario admincliente.
2. Abre Firefox y accede a <https://webapp.servpubli.com>.
3. Haz clic con el ratón sobre *Entiendo los riesgos* y sobre el botón *Añadir excepción* (figura 4.38).
4. Lee el contenido de la nueva ventana y haz clic sobre el botón *Confirmar excepción de seguridad* (figura 4.38).
5. Teclea el usuario y su contraseña en la ventana *Identificación requerida* (figura 4.37).
6. Pincha el botón *Aceptar* y comprueba que el contenido de la página coincide con el del servidor.



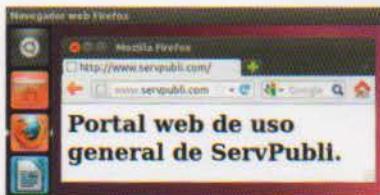
4.37. Acceso al servidor seguro con Firefox.

Datos de acceso

Usuario: admincliente
Contraseña: Cli3nt@

Proceso del servidor HTTP

/usr/sbin/apache2



4.36. Acceso al servidor anónimo con Firefox.

Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a webapp.servpubli.com, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intenta conectar de forma segura, los sitios presentan información verificable para asegurar que están en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio y puede estar ocurriendo porque suplanta el sitio, y no debe:

[Añadir excepción de seguridad](#)

Detalles técnicos

Entiendo los riesgos

Si sabe lo que está haciendo, confiar en la identificación de confie en este sitio, este sitio o alguien está intentando interceptar tu conexión.

No añada una excepción a este sitio por lo que este sitio no es seguro.

[Añadir excepción](#)

Estado del certificado

Este sitio intenta identificarse a sí mismo con información no válida.

Sí es seguro

El certificado pertenece a un sitio diferente, lo que podría indicar una suplantación de identidad.

Identidad desconocida

No se confía en el certificado, porque no ha sido verificado por una autoridad reconocida.

Guardar esta excepción de manera permanente

[Confirmar excepción de seguridad](#)

[Cancelar](#)

4.38. Verificación de la conexión.

3 > Servicio web en sistemas Windows

Para saber más

Puedes obtener soporte técnico de Microsoft para el servicio HTTP en el siguiente URL:

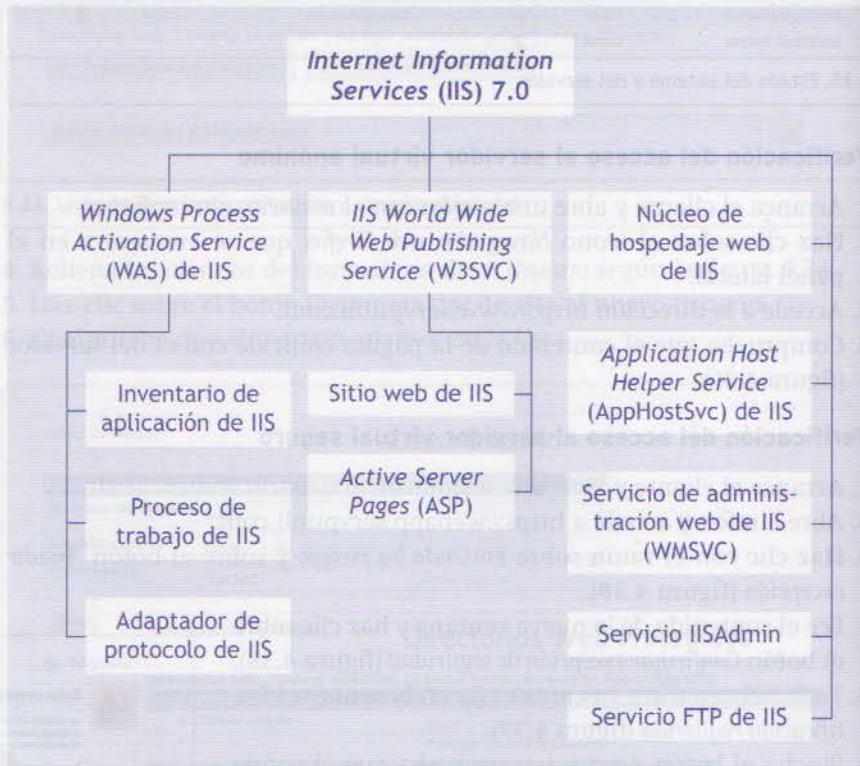


http://xurl.es/http_ms

Según la propuesta de trabajo pactada con la empresa ConRecuerdos.org, la tercera tarea que debéis realizar es la implantación de un servidor web que permita a los empleados compartir diversa información de la empresa:

- Página web de la intranet, donde se publican las novedades acerca de la empresa, como por ejemplo sus nuevos objetivos y políticas.
- Aplicación web interna, donde se realiza la comunicación entre empleados, mediante videoconferencia o mensajería instantánea.

Internet Information Services (IIS) es el servidor web que ya viene incorporado en Windows Server 2008.



4.39. Infraestructura IIS en Windows Server 2008.

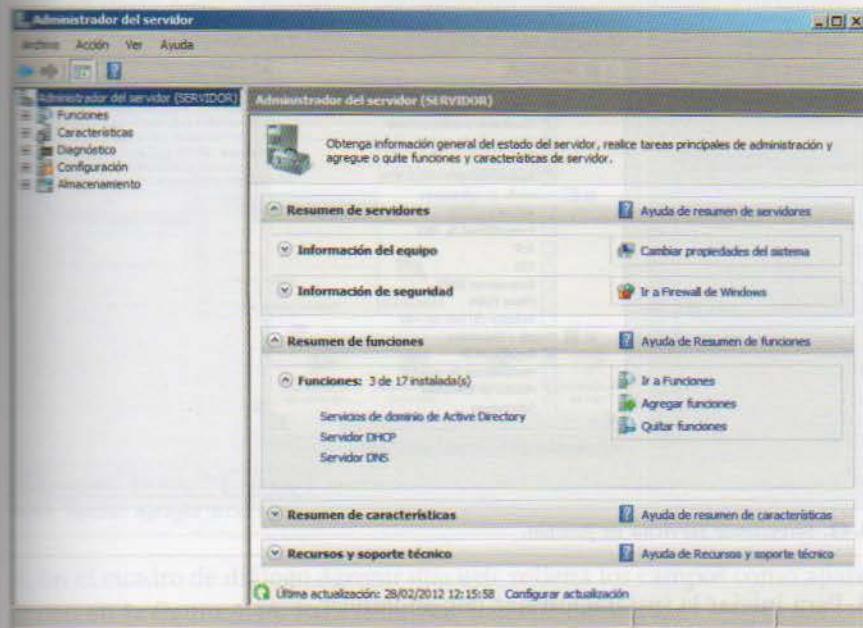
Antes de empezar a trabajar con el servidor web, debéis estudiar los requisitos y la información que os ha proporcionado ConRecuerdos.org:

- Todos los empleados conocen la herramienta que les permite acceder a cualquiera de los servicios: un navegador web.
- La página web de la intranet es accesible desde cualquier equipo de la red, lo único que es necesario es que tenga instalado un navegador web.
- La aplicación web interna tendrá el acceso restringido, de forma que cada usuario solo podrá ver la información para la que está autorizado.
- Este servicio solo podrá ser usado desde la red de área local, aunque, en cualquier momento, se puede permitir el acceso desde el exterior.

3.1 > Instalación del servidor

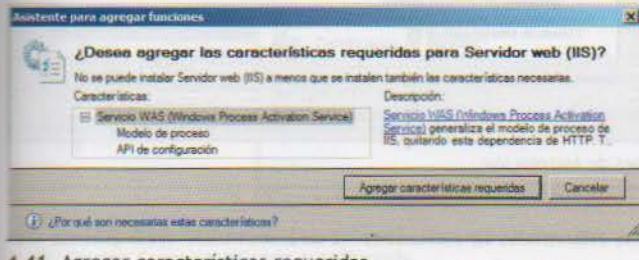
Sigue estas indicaciones para instalar el servidor IIS:

1. Haz clic en el botón *Inicio* y, a continuación, selecciona la opción *Administrador del servidor*.
2. En la ventana que aparece, pincha la opción *Agregar funciones*, que se encuentra en el bloque *Resumen de funciones* de la parte derecha de la ventana.



4.40. Sección Administrador del servidor.

3. En la primera ventana del Asistente para agregar funciones se te informa de las comprobaciones previas que debes realizar para instalar correctamente cualquier tarea en el servidor. Léelas atentamente y haz clic sobre el botón *Siguiente*.
4. En la ventana *Seleccionar funciones de servidor*, marca la casilla de verificación *Servidor web (IIS)* y haz clic en *Siguiente* (figura 4.42).
5. La instalación de IIS requiere agregar servicios adicionales que se encuentran incluidos en el llamado *Servicio WAS (Windows Process Activation Service)*. Pincha *Agregar características requeridas* (figura 4.41).

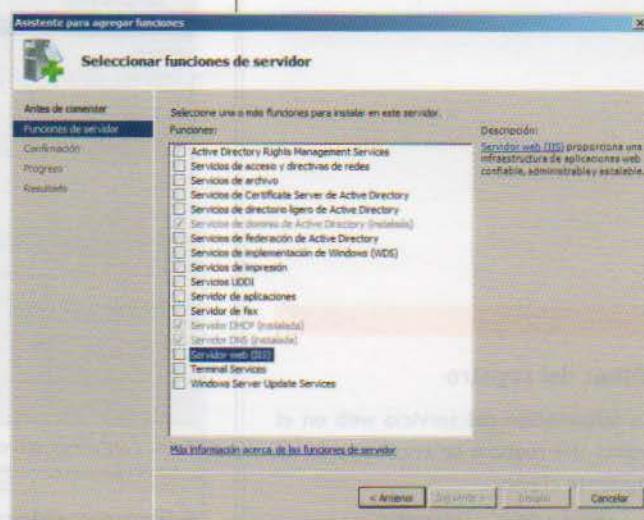


4.41. Agregar características requeridas.

Recuerda

Los datos para acceder como usuario administrador son:

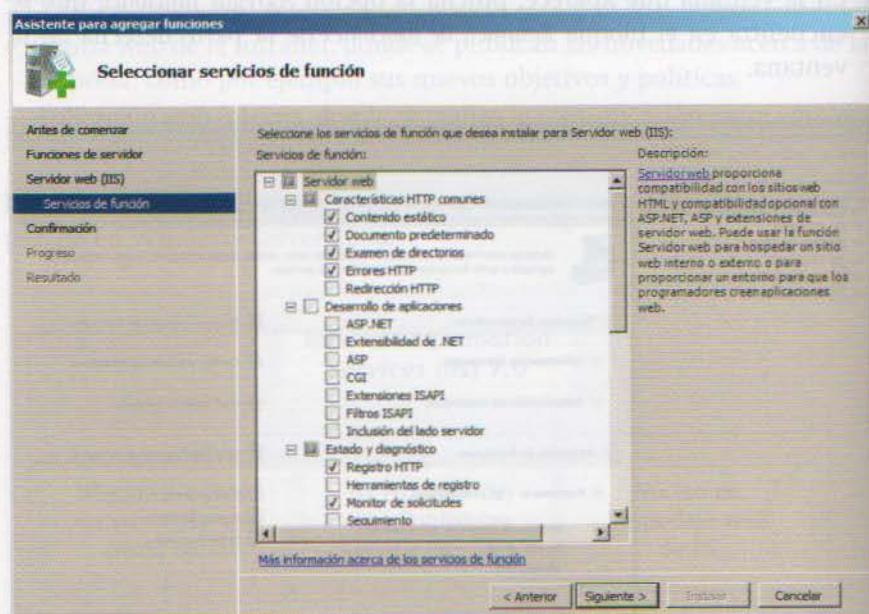
- Usuario: adminservidor
- Contraseña: S3rvid@r



4.42. Seleccionar funciones del servidor.

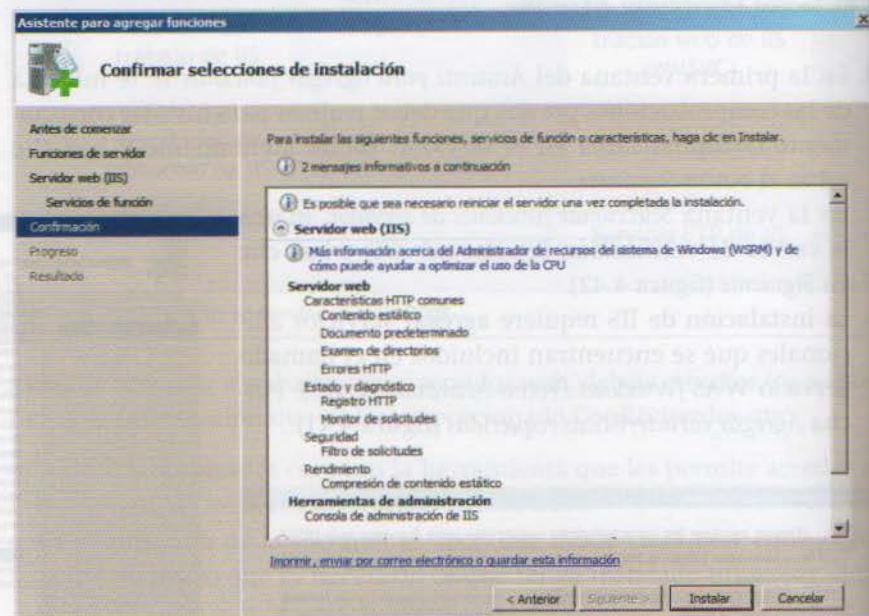
Para saber más
acerca de los servicios que se instalan en el sistema operativo Windows Server 2008, consulta la guía de instalación.

6. La ventana *Servidor web (IIS)* indica algunos factores que se deben tener en cuenta antes de instalar el servidor web. Una vez hayas leído y entendido dicha información, haz clic sobre el botón *Siguiente*.
7. En la ventana que aparece deja marcadas las casillas que ya lo están y pincha *Siguiente*.



4.43. Seleccionar servicios de función.

8. Para iniciar la instalación haz clic en *Instalar*.



4.44. Confirmar selecciones de instalación.

9. Transcurridos unos minutos, la instalación del servidor web habrá terminado. Si todo es correcto, finaliza haciendo clic en *Cerrar*.

Editor del registro

La información del servicio web en el editor del registro se encuentra en la siguiente clave:

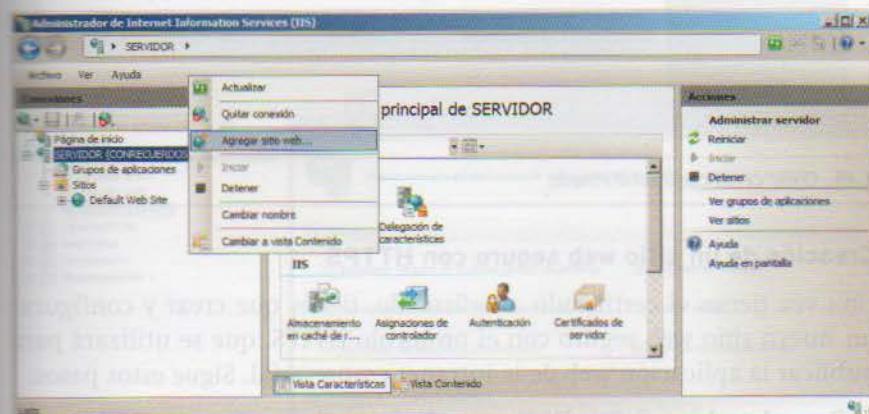
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W3SVC

3.2 > Configuración del servidor

Creación de un sitio web

Vas a crear un sitio web que se utilizará para publicar la web de la intranet empresarial. Sigue estos pasos:

1. Crea el archivo C:\SitiosWeb\www\index.html, con formato HTML, que muestre el siguiente contenido: *Portal web de ConRecuerdos.org.*
2. Abre el administrador de IIS.
3. Selecciona y haz clic con el botón secundario del ratón en SERVIDOR. Elige la opción *Agregar sitio web* del menú contextual.



4.45. Opción Agregar sitio web...

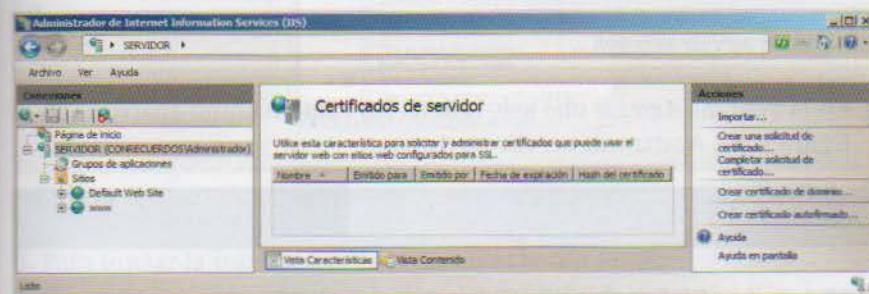
4. En el cuadro de diálogo *Agregar sitio web*, rellena los campos como aparecen en la figura 4.46. Para finalizar, haz clic en *Aceptar*.

Podrás ver una nueva entrada en la lista desplegable *Sitios* llamada **WWW**.

Creación de un certificado

Ahora vas a crear un certificado, de tipo autofirmado, que es un requisito previo para poder configurar un sitio web seguro. Sigue estos pasos:

1. Abre el administrador de IIS.
2. Selecciona *SERVIDOR* y haz doble clic en el ícono *Certificados de servidor*, que está en la parte central de la ventana.
3. En el apartado *Acciones*, que se encuentra en la parte derecha de la ventana, pincha la opción *Crear certificado autofirmado*.

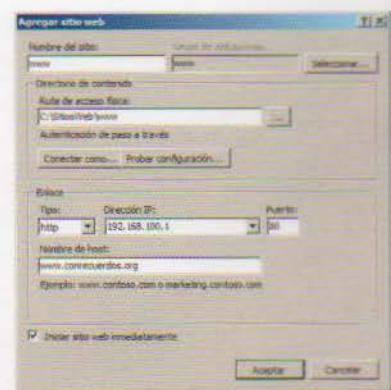


4.47. Opción Crear certificado autofirmado.

Administrador de IIS

Una vez instalado el servicio HTTP, puedes administrarlo si vas a la siguiente ruta:

Inicio / Herramientas administrativas / Administrador de Internet Information Services (IIS)

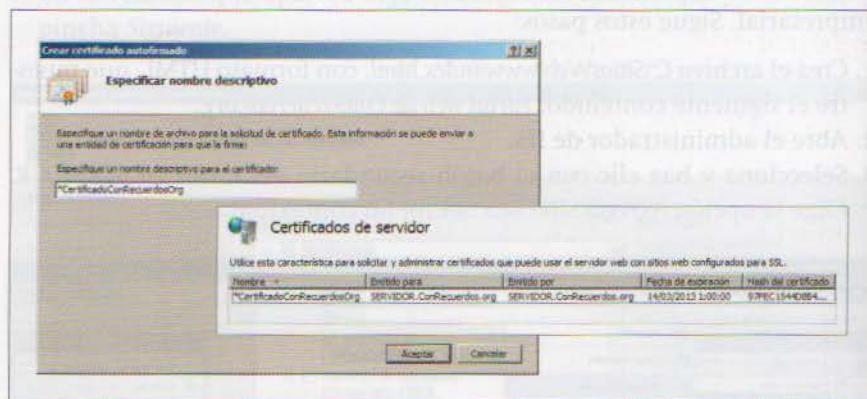


4.46. Agregar sitio web.

Nombre del certificado

En el caso de que se vaya a crear un servidor virtual para un sitio web seguro (HTTPS), es obligatorio que el nombre del certificado empiece con el símbolo asterisco (*). Si no se hace esto, IIS no permite configurar el encabezado de host del servidor virtual.

4. En la ventana *Crear certificado autofirmado*, escribe un nombre para el certificado, por ejemplo *CertificadoConRecuerdosOrg. Haz clic en *Aceptar*. Aparecerá el nuevo certificado en la lista *Certificados de servidor*.

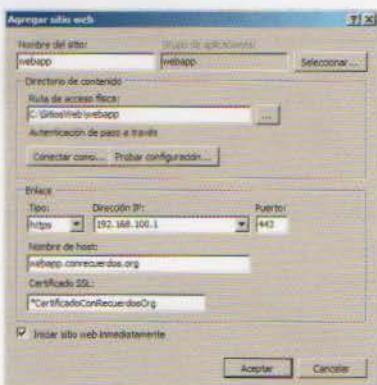


4.48. Crear certificado autofirmado.

Creación de un sitio web seguro con HTTPS

Una vez tienes el certificado autofirmado, tienes que crear y configurar un nuevo sitio web seguro con el protocolo HTTPS, que se utilizará para publicar la aplicación web de la intranet empresarial. Sigue estos pasos:

1. Crea el archivo *C:\SitiosWeb\webapplindex.html*, con formato HTML, que muestre el siguiente contenido: *WebApp de ConRecuerdos.org*.
2. Abre el administrador de IIS.
3. Selecciona y haz clic con el botón secundario del ratón en SERVIDOR. Elige la opción *Agregar sitio web* del menú contextual.



4.49. Ventana Agregar sitio web.



4.50. Opción Agregar sitio web...

4. En la ventana *Agregar sitio web*, rellena los campos como aparecen en la figura 4.49. Acaba con un clic en *Aceptar*.

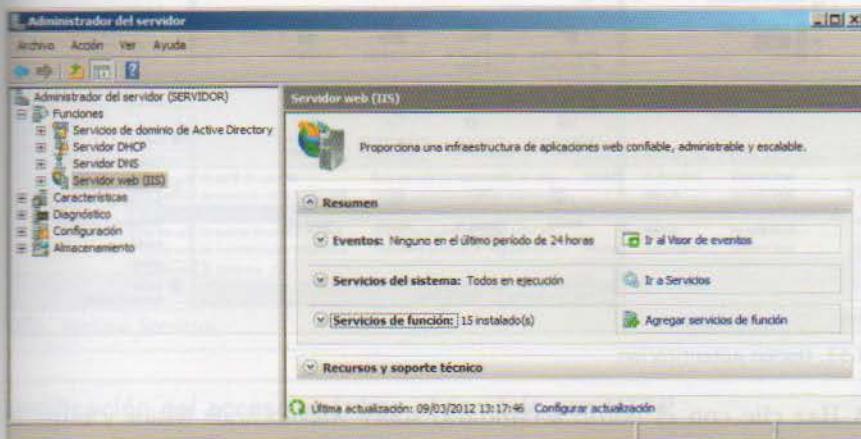
Actividades propuestas

3. En el servidor DNS, crea el RR CNAME con el nombre webapp para que resuelva el sitio web seguro.

Instalación del módulo de autenticación básica

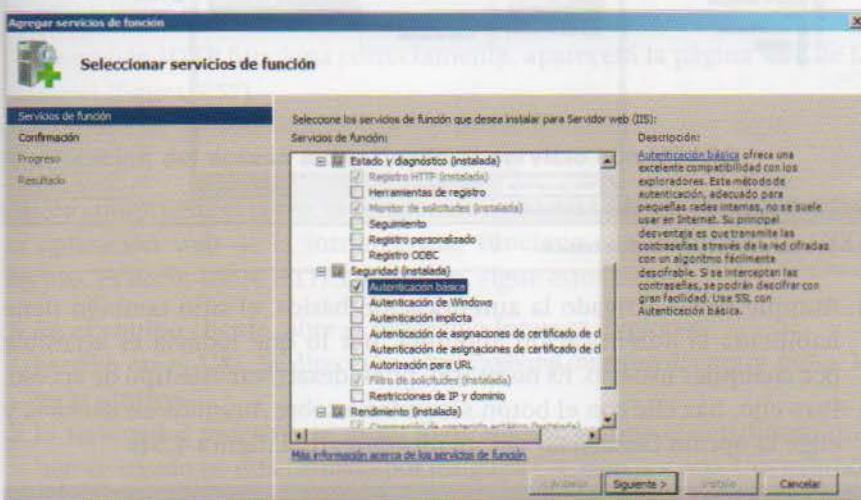
Además de configurar el sitio con HTTPS, es necesario que los usuarios se autentiquen para poder acceder a la información que se encuentra publicada en la aplicación web de la intranet empresarial. Para ello, se debe instalar el módulo de autenticación básica. Sigue estos pasos:

1. Abre el administrador del servidor.
2. Haz clic sobre la opción *Servidor web (IIS)* que se encuentra en la ruta *Administrador del servidor (SERVIDOR) / Funciones*.
3. Haz clic sobre la opción *Agregar servicios de función* que puedes localizar en el bloque *Resumen / Servicios de función*.



4.51. Sección Administrador del servidor.

4. En la ventana *Seleccionar servicios de función*, marca la casilla de verificación *Autenticación básica* dentro de la subcategoría *Seguridad*. A continuación, haz clic en *Siguiente*.



4.52. Seleccionar servicios de función.

5. Para iniciar la instalación, haz clic en el botón *Instalar*.
6. Tras unos minutos, la instalación del módulo de autenticación ha terminado. Si la instalación es correcta, finaliza con un clic en *Cerrar*.

Seguridad de la autenticación básica

La autenticación básica solicita al usuario un nombre y una contraseña.

Esta información se envía sin cifrar y, por tanto, es muy recomendable emplear el método de autenticación básica junto a un medio de transporte encriptado, como HTTPS.

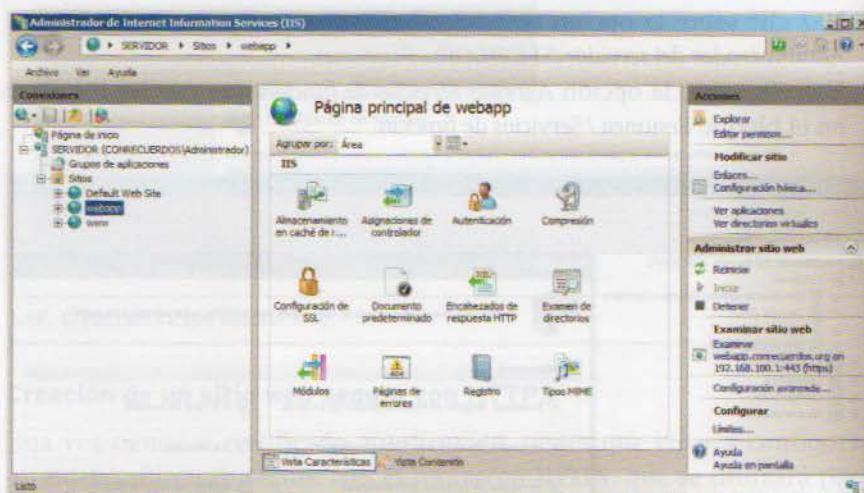
Usuarios de la autenticación básica

Los usuarios que pueden acceder a un sitio web configurado con autenticación básica son aquellos que tienen una cuenta de Windows (credenciales) en el servidor.

Configuración del sitio seguro con autenticación básica

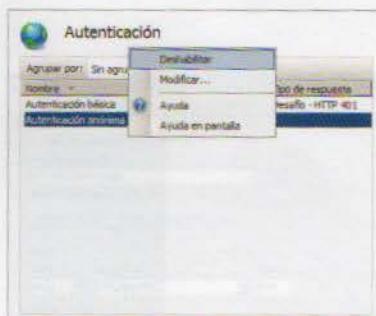
Una vez instalado el módulo de autenticación, ya es posible configurar un sitio para que sea accesible con usuario y contraseña. Sigue estos pasos:

1. Abre el administrador de IIS.
2. Selecciona el sitio SERVIDOR/Sitios/webapp y haz doble clic sobre el ícono Autenticación, que está en la parte central de la ventana.

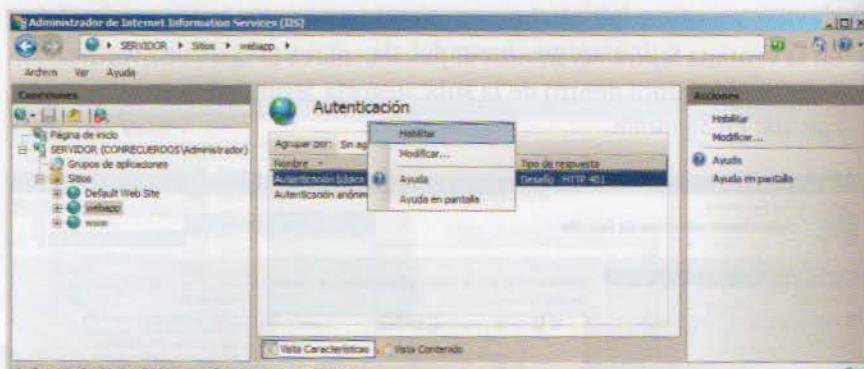


4.53. Opción Autenticación.

3. Haz clic con el botón secundario sobre Autenticación básica y elige la opción *Habilitar* del menú contextual.



4.54. Deshabilitar autenticación anónima.



4.55. Habilitar autenticación básica.

4. Aunque hayas activado la autenticación básica, el sitio también tiene habilitada la autenticación anónima, por lo que todavía es accesible por cualquier usuario. Es necesario, pues, desactivar este tipo de acceso. Para ello, haz clic con el botón secundario sobre Autenticación anónima y elige la opción *Deshabilitar* del menú contextual (figura 4.54).

Actividades propuestas

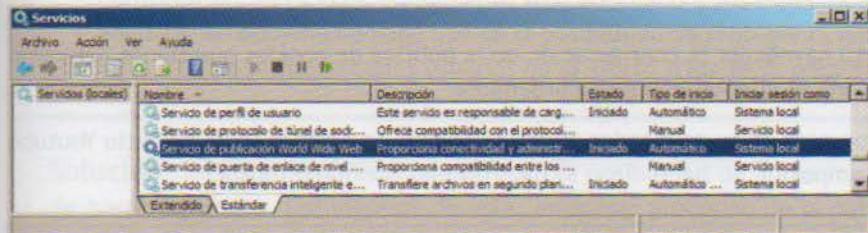
4. En Active Directory, crea un usuario de nombre prueba y contraseña U\$u4r1o y comprueba si puedes autenticarte en el sitio web seguro.

3.3 > Comprobación del servicio

Se deben realizar comprobaciones tanto en el servidor como en el cliente. Por una parte, en el servidor se verifica el estado del proceso y, por otra, en el cliente se confirma que se puede acceder a los sitios web internos.

Verificación del estado del servicio

Para comprobar el estado del servicio web, ve a la ruta *Inicio / Herramientas administrativas* y haz clic sobre *Servicios*. En la ventana que aparece busca *Servicio de publicación WWW*. Una vez lo hayas encontrado, si el campo *Estado* tiene el valor *Iniciado* y en *Tipo de inicio* aparece *Automático*, quiere decir que el servicio web está en funcionamiento y que se iniciará automáticamente cada vez que arranque el equipo servidor.

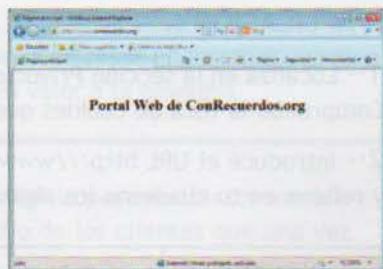


4.56. Ventana *Servicios*.

Estado del servicio web

El servicio web tiene tres posibles estados de inicio:

- Automático: está iniciado y se iniciará cada vez que arranca el ordenador.
- Manual: está detenido y se debe iniciar manualmente.
- Deshabilitado: está detenido y no se puede iniciar de ningún modo.



4.57. Acceso anónimo al sitio www.

Verificación del acceso anónimo al servicio con HTTP

Sigue estos pasos para comprobar si se abre correctamente la URL donde se aloja la web de la intranet, que funciona sobre el protocolo HTTP:

1. En el equipo cliente abre el programa Internet Explorer, que puedes encontrar en la ruta *Inicio / Todos los programas*.
2. Escribe la dirección <http://www.conrecuerdos.org> en el URL del navegador web y pulsa la tecla <Intro>.

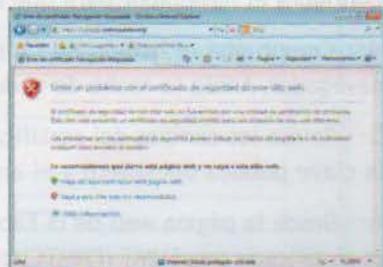
Si el servicio HTTP funciona correctamente, aparecerá la página web de la intranet (figura 4.57).

Verificación del acceso autenticado al servicio con HTTPS

Ahora comprueba el correcto funcionamiento del URL donde se encuentra la aplicación web de la intranet, que funciona con el protocolo HTTPS seguro, es decir, sobre HTTPS. Para ello, sigue estos pasos:

1. En el equipo cliente, abre el programa Internet Explorer.
2. Escribe en el URL la dirección <https://webapp.conrecuerdos.org> y pulsa la tecla <Intro>.
3. El navegador muestra un aviso (figura 4.58), ya que el certificado que hemos creado no está firmado por ninguna CA, sino por nosotros mismos (autofirmado). Haz clic en *Vaya a este sitio web (no recomendado)*.
4. En la ventana que aparece, introduce el nombre y la contraseña del usuario prueba que has creado en una actividad del epígrafe anterior.

Si el servicio HTTPS funciona correctamente, aparece la página de la aplicación web (figura 4.59).



4.58. Aviso de certificado no firmado.



4.59. Acceso autenticado al sitio webapp.