UNIVERSIDAD TECNOLOGICA DE PANAMA
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

# GUÍA DE SERVIDORES

Facilitador(a): Aris Castillo  Asignatura: Sistemas Operativos

Estudiante: _Gabriel Díaz_____ Fecha: 26/11/2020  Grupo: 1IF131

**DEFINICIÓN:**

Un **servidor** es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como «el servidor». En la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento. La ventaja de montar un servidor en computadoras dedicadas es la seguridad. Por esta razón la mayoría de los servidores son procesos diseñados de forma que puedan funcionar en computadoras de propósito específico.

**FUNCIONES:**

Comúnmente, los servidores proveen servicios esenciales dentro de una red, ya sea para usuarios privados dentro de una organización o compañía, o para usuarios públicos a través de Internet.

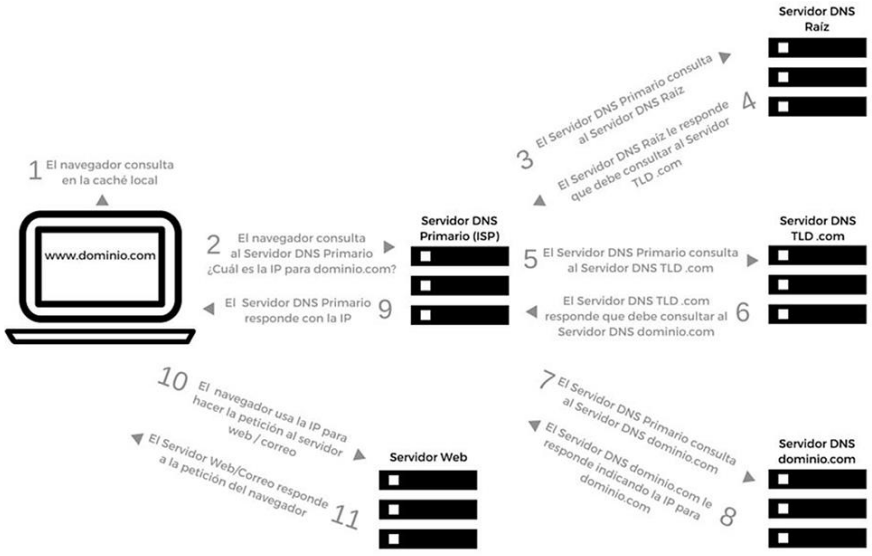
**TIPOS:**

1. Servidor de Sistema de Nombre de Dominio (DNS)
2. Servidor DHCP
3. Servidor alojamiento Web
4. Servidor FTP
5. Servidor Proxy
6. Servidor de Correo Electrónico
7. Servidor de Aplicaciones
8. Servidor VoIP

## 1. Servidor de Sistema de Nombres de Dominio (DNS)

Un **servidor de nombres** es un servidor de hardware o software que implementa un servicio de red para proveer respuestas a las consultas en un servicio de directorio. Traduce un identificador basado en texto a una identificación numérica o componente de direccionamiento interno de sistema. Este servicio es realizado por el servidor en respuesta a una petición de protocolo de servicio.

Un ejemplo de un servidor de nombres es el componente de servidor del Sistema de Nombres de Dominio (DNS), uno de los dos espacios de nombre principales del Internet. La función más importante de los servidores DNS es la traducción (resolución) de los nombres de dominios y nombres de host identificables por los humanos en sus direcciones numéricas del Protocolo de Internet (IP) correspondientes, el segundo principal espacio de nombres del Internet, que es usado para identificar y localizar a las computadoras y recursos en Internet.




## 2. Servidor DHCP

**Qué es DHCP**

En una red, cuando conectamos varios equipos, estos deben tener registrada una **dirección IP diferente dentro de un segmento o rango de red determinado**. Esto es así para que estos equipos puedan comunicarse y compartir información entre sí. En el pasado, esta comunicación era establecida manualmente, pero con el tiempo era evidente que no era viable dedicar recursos y tiempo de un administrador de sistemas a

configurar manualmente cada nuevo equipo que se conectaba a la red. Es en este punto donde aparece el término Servidor DHCP, para hacer una **administración centralizada y automática** de los parámetros de red.

El **protocolo DHCP**, en inglés, **Dynamic Host Configuration Protocol**, es una **extensión del protocolo Bootstrap (BOOTP)** desarrollado en 1985 para conectar dispositivos como terminales y estaciones de trabajo sin disco duro con un **Bootserver**, del cual reciben su sistema operativo. Su función fue la de ofrecer solución a redes de gran tamaño y la incipiente presencia de puestos de trabajo móviles como portátiles o think-clients, asignando direcciones de red automáticamente de modo que fueran reutilizables.

DHCP ya tiene casi 40 años entre nosotros y como todo protocolo ha pasado por diferentes revisiones que lo han ido adaptando hasta nuestros días, aunque quizá la más importante fue en 1997 con el RFC 2131 y su especificación definitiva.

**Cómo funciona el protocolo DHCP**

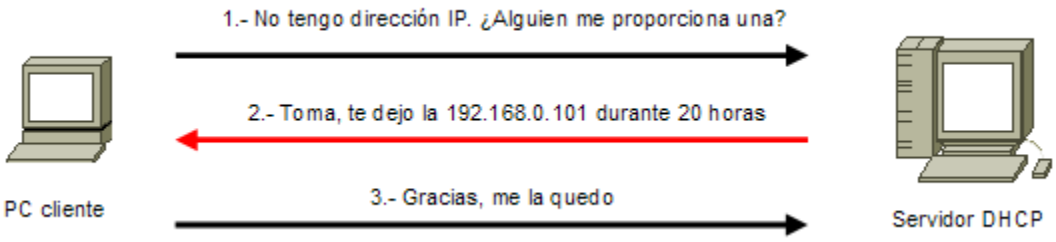
Este protocolo de red se basa en un **modelo cliente-servidor**. En este escenario, un dispositivo (un portátil, móvil, etc.) solicita en el momento de conectarse a una red la configuración IP a un servidor DHCP a través de los puertos UDP 67 y 68 (para IPv6, los puertos 546 y 547), que por su parte consulta en una base de datos las direcciones y parámetros de red asignables antes de dar una respuesta. Una vez realizada la consulta, el servidor envía los siguientes parámetros al cliente a través de la red:

- Dirección IP única
- Máscara de subred
- Puerta de enlace estándar
- Servidores DNS
- Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol)

Pero, ¿cómo se logra esta asignación? el proceso es automático pero también es el resultado de finalizar con éxito cuatro pasos consecutivos:

1. **Difusión amplia o broadcast**: El cliente DHCP envía un paquete DHCPDISCOVER a la dirección 255.255.255.255 desde la dirección 0.0.0.0. De este modo se intenta establecer una comunicación con todos los integrantes de la red, la idea de fondo es localizar los servidores DHCP disponibles y así continuar con la petición.
2. **Oferta**: Los servidores DHCP presentes en la red se encuentran a la escucha de peticiones a través del puerto 67. En cuanto detectan la petición de un cliente envían un paquete DHCPOFFER, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.

3. **Solicitud**: El cliente DHCP que recibe el paquete contacta con el servidor correspondiente con DHCPREQUEST. De este modo, los demás servidores quedan enterados de la asignación al mismo tiempo que el cliente confirma al servidor que acepta los parámetros asignados anteriormente.
4. **Confirmación**: Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete DHCPACK (DHCP acknowledged o «reconocido»). La dirección asignada se guarda en la base de datos del servidor junto con la dirección MAC del cliente.




## 3. Servidor alojamiento Web

Un servidor web o servidor HTTP es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o aplicación del lado del cliente. El código recibido por el cliente es renderizado por un navegador web. Para la transmisión de todos estos datos suele utilizarse algún protocolo. Generalmente se usa el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del modelo OSI. El término también se emplea para referirse al ordenador.

**Funcionamiento**

El servidor web se ejecuta en un ordenador manteniéndose a la espera de peticiones por parte de un cliente (un navegador web) y responde a estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error. A modo de ejemplo, al teclear www.wikipedia.org en nuestro navegador, este realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo exhibe en pantalla. Como vemos con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se

limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Además de la transferencia de código HTML, los servidores web pueden entregar aplicaciones web. Estas son porciones de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

Aplicaciones en el lado del cliente: el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java "applets" o Javascript: el servidor proporciona el código de las aplicaciones al cliente y este, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Comúnmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje Javascript y Java, aunque pueden añadirse más lenguajes mediante el uso de plugins.

Aplicaciones en el lado del servidor: el servidor web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor muchas veces suelen ser la mejor opción para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, este no necesita ninguna capacidad añadida, como sí ocurre en el caso de querer ejecutar aplicaciones Javascript o Java. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones.

El hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un lenguaje de marcas y HTTP es un "protocolo".

**Algunos servidores web importantes son:**

- Nginx
- Apache
- Internet Information Services (IIS)
- Cherokee
- Tomcat

**Otros servidores, más simples pero más rápidos, son:**

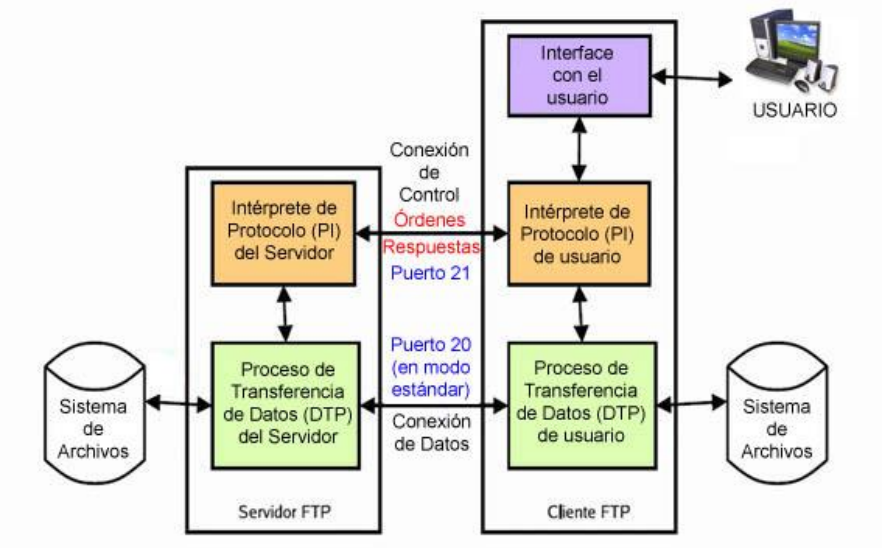
- lighttpd
- thttpd

## 4. Servidor FTP

El Protocolo de transferencia de archivos (en inglés File Transfer Protocol o FTP) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

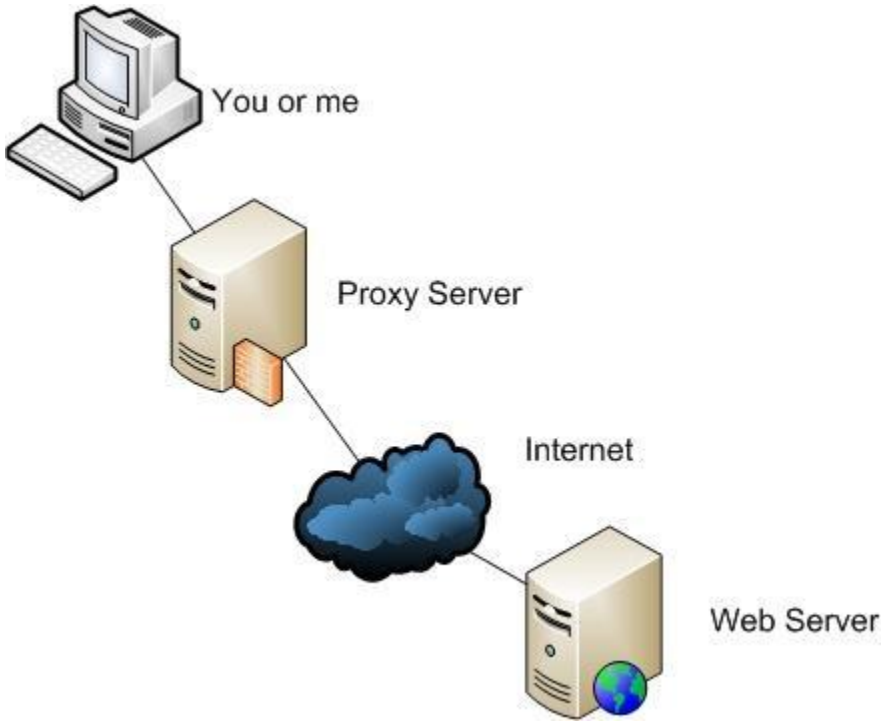
Para solucionar este problema son de gran utilidad aplicaciones como SCP y SFTP, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.




## 5. Servidor Proxy

Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica

de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc. Dependiendo del contexto, la intermediación que realiza el proxy puede ser considerada por los usuarios, administradores o proveedores como legítima o delictiva y su uso es frecuentemente discutido.




**Características**

Comúnmente un servidor proxy es un equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino.

El más popular es el servidor proxy de web. Interviene en la navegación por la web, con distintos fines: seguridad, rendimiento, anonimato, etc.

Existen proxys específicos para otros protocolos, como el proxy de FTP.

El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

Un componente hardware también puede actuar como intermediario para otros.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo que la solicitó.

Hay dos tipos de proxys atendiendo a quién es el que quiere implementar la política del proxy:

proxy local: En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).

proxy de red o proxy externo: El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

**Ventajas**

Control: solamente el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos únicamente al servidor proxy.

Ahorro: solamente uno de los usuarios (el proxy) ha de estar preparado para hacer el trabajo real. Con estar preparado se entiende que es el único que necesita los recursos necesarios para hacer esa funcionalidad. Ejemplos de recursos necesarios para hacer la función pueden ser la capacidad y lógica de la dirección de red externa (IP).

Velocidad: si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

Filtrado: el proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

Modificación: como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

Anonimato: Conectarse de forma anónima a un recurso externo sin revelar nuestra IP, pues es la IP pública del Proxy la que es usada para la obtención del recurso.

**Desventajas**

Anonimato: si todos los usuarios se identifican como uno solo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Abuso: al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.

Carga: un proxy tiene que hacer el trabajo de muchos usuarios.

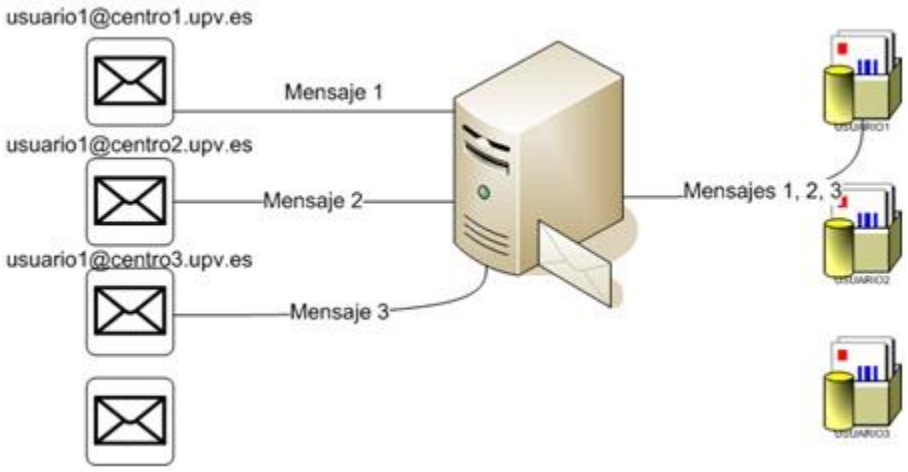
Intromisión: es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.

Incoherencia: si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.

Irregularidad: el hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

## 6. Servidor de Correo Electrónico

Un servidor de correo es una aplicación de red de computadoras ubicada en un servidor de Internet, para prestar servicio de correo electrónico (correo-e o e-mail). De forma predeterminada, el protocolo estándar para la transferencia de correos entre servidores es el Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP). Está definido en el RFC 2821 y es un estándar oficial de Internet.



**Intercambio de correo**

Un servidor de correo realiza una serie de procesos que tienen la finalidad de transportar información entre los distintos usuarios.

Usualmente el envío de un correo-e tiene como fin que un usuario (remitente) cree un correo-e y lo envíe a otro (destinatario). Esta acción tiene típicamente cinco pasos:

El usuario inicial crea un "correo electrónico", un archivo que cumple los estándares de un correo-e. Usará para ello una aplicación ad-hoc. Algunas de las aplicaciones cliente de correo-e más usadas, en indistinto orden son:

- Lotus Notes (IBM),
- Microsoft Outlook,
- Mozilla Thunderbird (Fundación Mozilla),
- Outlook Express (Microsoft),
- Windows Mail Desktop (Microsoft),
- Gmail (Google).

El archivo creado es enviado a un almacén, administrado por el servidor de correo local al usuario remitente del correo, donde se genera una solicitud de envío.

El servicio MTA local al usuario inicial recupera este archivo e inicia la negociación con el servidor del destinatario para el envío del mismo.

El servidor del destinatario corrobora la operación y recibe el mensaje de correo, depositándolo en el "buzón" correspondiente al usuario receptor del correo. El "buzón" no es otra cosa que un registro en una base de datos.

Finalmente, el software del cliente receptor del correo recupera este archivo o "correo" desde el servidor almacenando una copia en la base de datos del programa cliente de correo electrónico, ubicada en la computadora del cliente que recibe el correo.

A diferencia de un servicio postal clásico, que recibe un único paquete y lo transporta de un lugar a otro, el servicio de correo-e copia varias veces la información que corresponde al correo electrónico.

Este proceso que en la vida real ocurre de manera muy rápida involucra muchos protocolos. Por ejemplo, para ubicar el servidor de destino se utiliza el servicio Domain Name System (DNS), el que reporta un tipo especial de registro para servidores de correo o registro MX (Mail eXchange record). Una vez ubicado, para obtener los mensajes del servidor receptor de correos, los usuarios se sirven de clientes de correo que utilizan el protocolo Post Office Protocol (POP3) o el protocolo Internet Message Access Protocol (IMAP) para recuperar los mensajes de correos-e del servidor y almacenarlos en sus computadores locales.

## 7. Servidor de Aplicaciones

En informática, se denomina servidor de aplicaciones a un servidor en una red de computadores que ejecuta ciertas aplicaciones.

Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negociación y de acceso a los datos de las aplicaciones. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.


**Usos**

Un ejemplo común del uso de servidores de aplicación (y de sus componentes) son los portales de Internet, que permiten a las empresas la gestión y divulgación de su información, y un punto único de entrada a los usuarios internos y externos. Teniendo como base un servidor de aplicación, dichos portales permiten tener acceso a información y servicios (como servicios Web) de manera segura y transparente, desde cualquier dispositivo.

## 8. Servidor VoIP

Voz sobre protocolo de internet o Voz por protocolo de internet, también llamado voz sobre IP, voz IP, vozIP o VoIP (siglas en inglés de Voice over IP: 'voz sobre IP'), es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a

través de circuitos utilizables solo por telefonía convencional, como las redes PSTN (siglas de Public Switched Telephone Network, red telefónica pública conmutada).

Los protocolos de internet que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la «red experimental de protocolo de voz» (1973), inventada por ARPANET.