Ángel Fabrizio Menendez Solorzano 0909-20-10024

Sistemas Operativos II

Servidores y sus tipos

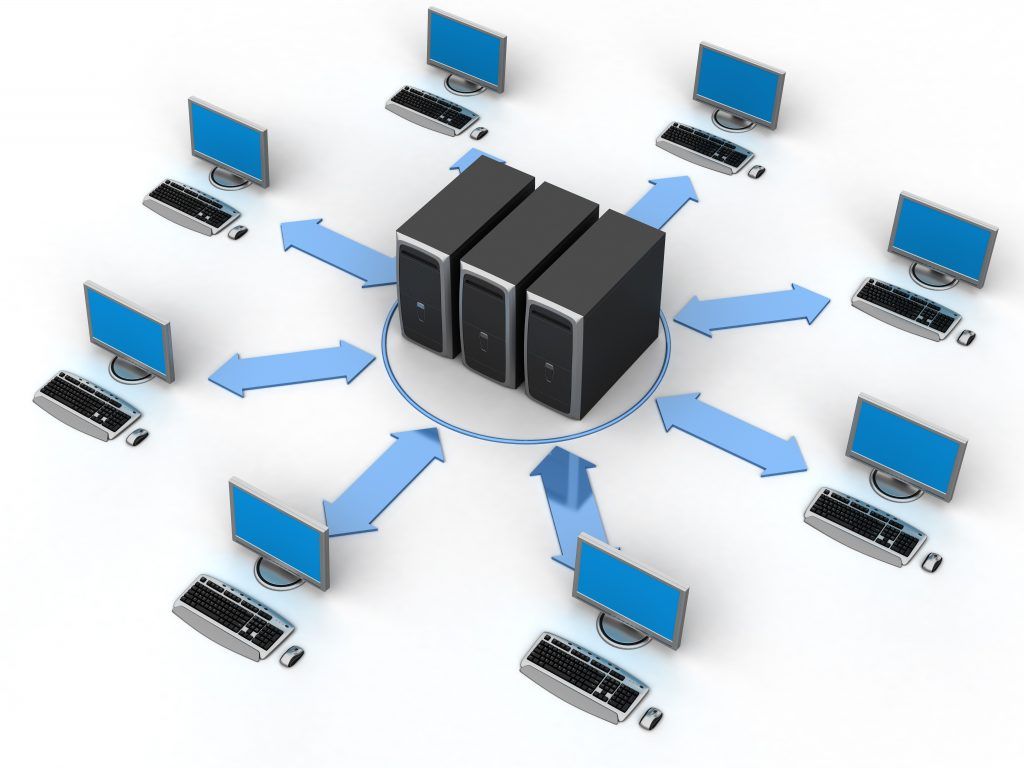
Que es un servidor: un servidor es un conjunto de computadoras en un solo equipo, capaz de poder atender las peticiones de un cliente u usuario, y poder devolver una respuesta a la petición.

Los servidores pueden ser capaces de ejecutarse en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como “servidor”. En la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento.

Los servidores operan a través de una arquitectura llamada CLIENTE-SERVIDOR. Un servidor es un conjunto de programas de computadora en ejecución que atienden las peticiones de otro programas.

Un **servidor** es un sistema informático que provee servicios, recursos o datos a otros dispositivos llamados **clientes** dentro de una red. Estos servidores pueden ser físicos (hardware dedicado) o virtuales (ejecutados sobre una plataforma de virtualización). Su función principal es responder a las solicitudes de los clientes y gestionar el tráfico de datos de manera eficiente.

Los servidores operan con software especializado que permite administrar los recursos y garantizar el funcionamiento de los servicios que ofrecen. Dependiendo de su uso, pueden estar diseñados para manejar tareas específicas como almacenamiento, procesamiento de datos, comunicación, seguridad, entre otros.



Tipos de servidores

1.Servidor Web: Un servidor web (server) es un ordenador de gran potencia que se encarga de “prestar el servicio” de transmitir la información pedida por sus clientes (otros ordenadores, dispositivos móviles, impresoras, personas, etc.)

Los servidores web (web server) son un componente de los servidores que tienen como principal función almacenar, en [web hosting](https://rockcontent.com/es/blog/que-es-un-host/), todos los archivos propios de una página web (imágenes, textos, videos, etc.) y transmitirlos a los usuarios a través de los navegadores mediante el protocolo HTTP (Hipertext Transfer Protocol).

**¿Para qué sirve un servidor web en Internet?**

El rol principal de un servidor web es **almacenar y transmitir el contenido solicitado de un sitio web al navegador del usuario**.

Este proceso, para los internautas no dura más que un segundo, sin embargo, a nivel del web server es una secuencia más complicada de lo que parece.

Para cumplir con sus funciones el servidor deberá tener la capacidad de estar siempre encendido para evitar interrumpir el servicio que le ofrece a sus clientes. Si dicho servidor falla o se apaga, los internautas tendrán problemas al ingresar al sitio web.

**¿Cómo funciona un servidor web?**

La comunicación entre un servidor y sus clientes se basa en HTTP, es decir, en el protocolo de transferencia de hipertexto o en su variante codificada HTTPS.

Para saber cómo funciona, primero es necesario conocer que **el web server está permanentemente en espera de una solicitud de información**.

Además, ten en cuenta que toda computadora, smartphone o tablet tiene una dirección IP única e irrepetible que lo identifica de otro dispositivo en la red, así es como el servidor web envía la información exacta que el internauta está esperando.

Ahora bien, para que el web server pueda cumplir con su función es necesario que reciba la petición por parte de un navegador, en otras palabras, se envía un pedido desde una dirección IP hacia la dirección IP del servidor que aloja los archivos del sitio en cuestión.

A continuación, el servidor web busca en sus archivos la información que se le está solicitando, procede a interpretar las líneas de código y a enviar el resultado al navegador cuya dirección IP fue la solicitante.

Este resultado se le muestra a los internautas y es lo que siempre sucede cuando se navega en sitios de Internet. Cuando este proceso se completa podemos decir que el web server ha cumplido con su función.

**¿Cuáles son las características de un servidor web?**

Como características necesarias de un servidor web a nivel de [software y hardware](https://rockcontent.com/es/blog/hardware-y-software/), podemos encontrar:

**A nivel de software**

Sistema Operativo

Se encarga de que el hardware funcione y logre interactuar con los servicios que corre el sistema. Algunos ejemplos son:

* Unix,
* Linux,
* o Windows.

**Sistemas de archivos**

Es una guía lógica que permite que el sistema pueda ubicar, ordenar y filtrar datos en el disco duro, con el fin de que podamos leerlos, modificarlos o eliminarlos.

Software servidor HTTP

Son los diferentes tipos de servidores web especializados en transmitir el contenido vía web (Apache, Nginx, IIS, Caddy, etc.).

Virtual Hosting

Permite que bajo el mismo web server e IP se alojen en varios sitios web distinto.

Despacho de ficheros estáticos y dinámicos

Los ficheros estáticos brindan soporte para alojar y despachar archivos como:

* JPG,
* GIF,
* PNG,
* BMP,
* [CSS](https://rockcontent.com/es/blog/que-es-css/),
* TXT,
* HTML,
* Javascript,
* MP3
* y MP4.

Los ficheros dinámicos funcionan para información en PHP, ASP, Python, Ruby y GO.

Monitoreo de Red y Límites

Permite monitorear el tránsito de red, paquetes que entran y salen, así como servicios de sistema y uso de hardware como:

* el uso del Almacenamiento;
* consumo de RAM;
* porcentaje de ocupación del CPU;
* velocidad de la red;
* rendimiento de escritura/lectura en disco.

Sistema de seguridad

El sistema de seguridad de un servidor debe:

* imponer límites de acceso por dirección IP;
* denegar o permitirle acceso a ciertos archivos o URLs;
* solicitar usuario y contraseña para autenticación básica HTTP;
* realizar un filtrado de peticiones inseguras;
* dar soporte para despachar información cifrada con certificados de seguridad SSL vía HTTPS.

**A nivel de hardware**

Rack y gabinete

El rack se refiere al lugar donde se alojan los servidores físicamente y el gabinete es el armazón que sostiene los componentes de hardware de una computadora.

CPU

Es el centro de procesamiento de datos del servidor desde donde se realizan todos los cálculos lógicos y matemáticos para que el usuario pueda manipular y acceder a los datos como necesita.

Memoria RAM

Se utiliza para almacenar información y datos de forma temporal dependiendo de la demanda del usuario a través del sistema operativo.

Unidades de almacenamiento

El almacenamiento de servidores web se hace en discos duros, los cuales permiten almacenar la información del sistema operativo, los servicios de sistema, y en última instancia los datos cargados por el usuario.

Puerto de red

El ancho de banda es el que te permite tener un volumen suficiente para transmitir información de ida y vuelta hacia y desde tu servidor web.

**2. servidor de base de datos:** Un servidor de datos es un tipo de hardware que le permite instalar software de base de datos: un sistema SGBD (gestión de bases de datos) relacional. Esta aplicación de base de datos especializada le ofrece dos capacidades vitales: la primera es la infraestructura de backend adecuada para almacenar todos sus datos en tablas organizadas y personalizables. La segunda es los servicios orientados al cliente (usted, sus empleados y otras partes interesadas) que le permiten a usted y al personal autorizado recuperar, cambiar o actualizar archivos específicos donde y cuando desee.

**¿Para qué sirve un servidor de bases de datos?:** Los mejores ejemplos de servidores ofrecen varias características críticas para el funcionamiento que una organización puede aprovechar. Algunos de los tipos de servidor de bases de datos más populares que se utilizan en la actualidad incluyen:

**Administrar mejor los datos:** Los servidores de bases de datos le permiten reunir todos sus datos, ya provengan, por ejemplo, de clientes de correo electrónico o software críticos, creando la solución única definitiva para sus necesidades de administración y almacenamiento de datos e información. Son ideales si necesita consultar información con frecuencia o administrar mejor sus bases de datos usando un sistema de red fiable.

**Hacer los datos accesibles:** Se pueden asignar permisos para que los usuarios puedan compartir datos entre varios tipos de dispositivos. Pueden ser páginas web, información de investigación, programas de Microsoft Windows o una nueva versión de una aplicación.  Esto proporciona a los empleados o partes interesadas acceso instantáneo a cualquier dato e información que necesiten, tanto si se desplazan como si están en la oficina. Estas características permiten aumentar el rendimiento y la eficiencia en todos los niveles de la red y proporcionan el soporte necesario para desempeñar un papel de forma eficaz.

**Reforzar los niveles de seguridad:** Al ofrecer una protección mucho mayor contra los ciberataques y otras amenazas, el uso de un servidor de datos le permite hacerse cargo de sus datos e información. Decida exactamente quién puede acceder, modificar y modelar sus valiosas tablas de conjuntos de datos, todo mientras se asegura de que se cumplan los requisitos de gestión de riesgos y conformidad de datos.

**Hacer copia de seguridad de los datos:** Un ejemplo óptimo de servidor de base de datos es aquel que permite a los usuarios realizar backup de los datos. Esta característica crucial garantiza que, incluso en los peores casos, si el negocio es hackeado, cualquier dato se almacena en la memoria de la red para ser recuperado y restaurado, lo que a su vez proporciona una continuidad vital del negocio para las operaciones de la empresa.

**Obtener información vital:** El sistema de administración de bases de datos adecuado le ofrece acceso a poderosas herramientas de análisis, lo que le permite consultar conjuntos de datos y extrapolar métricas clave y conocimientos para informar todas las estrategias de negocio en el futuro. Desde artículos web y blogs hasta redes sociales, cada versión de estas herramientas de marketing requiere un análisis detallado en forma de una tabla fácil de interpretar. Entre los ejemplos de uso de los resultados para mejorar el negocio se incluyen la mejora de la atracción de los motores de búsqueda en la web, la comprensión de una consulta del cliente o por qué las palabras clave lo son todo.

**¿Cómo funciona un servidor de base de datos?**

En primer lugar, es importante comprender qué significa realmente «[**base de datos**](https://www.ovhcloud.com/es/learn/what-is-cloud-database/)» y «servidor». Una base de datos es una aplicación que permite almacenar los datos y mantenerlos almacenados en una memoria. Un servidor puede estar basado en hardware o software y ofrece funciones específicas a los usuarios. Por ejemplo, puede implementarse para alojamiento web, correo electrónico, aplicaciones y mucho más.

Al migrar los sistemas de bases de datos a un servidor, se crea un servidor de bases de datos, una ubicación en la que ahora se almacenan todos los datos y que se gestiona mediante el SGBD o el SGBDR. Los usuarios pueden utilizar ambos para acceder rápidamente a los datos con una simple consulta de la interfaz de usuario, además de enviar comandos sobre los que el SGBD actúa inmediatamente (ver a continuación). Los comandos incluyen acceso y recuperación de datos, modificación de privilegios de acceso, carga de nuevos conjuntos de datos y más.

**¿Cómo utilizar un servidor de bases de datos?**

El uso de un servidor de base de datos ofrece una administración eficiente de la información mediante un motor dedicado, lo que garantiza sistemas óptimos de almacenamiento y recuperación de datos. Los comandos utilizan «lenguajes de programación aplicables» que permiten a los usuarios interactuar con una base de datos relacional mediante el SGBD. Varios sistemas lingüísticos diferentes ofrecen sus propias funciones y conjuntos de funciones exclusivos. Esta diversidad permite seleccionar un lenguaje que se ajuste a necesidades operativas específicas, utilizando funciones de memoria y programación con el fin de respaldar su negocio en general.

Algunos ejemplos populares de lenguajes de programación de servidores de bases de datos son:



**MySQL:** [**MySQL**](https://www.ovhcloud.com/es/public-cloud/mysql/) es una solución extremadamente popular optimizada para la escalabilidad y el rendimiento, ideal para sitios web, e-commerce o aplicaciones de terceros desarrolladas por editores de software. SQL significa «Structured Query Language» (o lenguaje de consulta estructurado), es decir, permite manipular bases de datos sin necesidad de tener un amplio conocimiento de programación.

[1]

**PostgreSQL:** Otro formato SQL, PostgreSQL se centra en el procesamiento de datos de contabilidad o transacciones. [**PostgreSQL**](https://www.ovhcloud.com/es/public-cloud/postgresql/) está diseñado para proteger la integridad de sus conjuntos de datos mientras ofrece excelentes opciones de personalización a través de la gestión del soporte de bases de datos.



**MongoDB:** [**MongoDB**](https://www.ovhcloud.com/es/public-cloud/mongodb/) le permite almacenar y administrar tanto archivos estructurados (información numérica) y archivos no estructurados como imágenes, videos y publicaciones en redes sociales.

**3. Servidor de archivos:** Un servidor de archivos es una computadora responsable del almacenamiento y la administración de archivos de datos para que otras computadoras en la misma red puedan acceder a los archivos. Permite a los usuarios compartir información a través de una red sin tener que transferir archivos físicamente.

El servidor de archivos asume la función de computadora o servidor para almacenar y poner a disposición blobs de datos para los clientes, sirviendo como una ubicación central para almacenar y compartir archivos para una red. Pueden estar limitados a una única red de área local (LAN) o pueden estar abiertos a internet.

Los servidores de archivos simplifican el almacenamiento, la protección y el intercambio de archivos en una organización. Los servidores de archivos son un objetivo común para los piratas informáticos y el ransomware, por lo que se debe prestar especial atención a protegerlos contra ataques.

Todas las organizaciones necesitan compartir información y datos entre personas. En lugar de enviar por correo electrónico o usar unidades de bus serie universal para mover datos, por ejemplo, un servidor de archivos puede usarse como un lugar central para que muchas personas almacenen archivos. Esto puede facilitar la colaboración entre personas en diferentes ubicaciones y se puede utilizar para transferir archivos grandes que de otra manera serían difíciles de mover.

Un servidor de archivos es fundamental para la mayoría de las operaciones comerciales. Puede ser tan simple como compartir una carpeta con un solo escritorio o tan complejo como un dispositivo virtual redundante disponible a nivel mundial.

**¿Cómo funcionan los servidores de archivos?**

Los servidores de archivos solo hacen que un sistema de archivos remoto sea accesible para los clientes. Pueden almacenar cualquier tipo de datos —por ejemplo, ejecutables, documentos, fotos o videos.

Por lo general, almacenan los datos como [blobs de datos o archivos binarios](https://searchdatacenter.techtarget.com/es/definicion/Objeto-Binario-Grande-o-BLOB?_gl=1*1ae3qy5*_ga*NjgyMjI2MzEuMTYyODU0ODc0NQ..*_ga_TQKE4GS5P9*MTYzMTEyMTE5Ny40Mi4xLjE2MzExMjE4NTYuMA..&_ga=2.117251782.1114768452.1631121198-68222631.1628548745). Esto significa que no realizan una indexación o procesamiento adicional de los archivos almacenados en ellos. Sin embargo, puede haber complementos o funciones de servidor adicionales que pueden proporcionar funciones adicionales.

Un servidor de archivos no proporciona formas integradas de interactuar con los datos y depende del cliente para usarlos. Las bases de datos no se consideran servidores de archivos porque las bases de datos solo tratan con datos estructurados a los que se accede mediante una consulta.

Los servidores de archivos suelen incluir funciones adicionales para permitir que varios usuarios accedan a ellos simultáneamente:

* La **gestión de permisos** se utiliza para establecer quién puede acceder a qué archivos y quién tiene derechos para editar o eliminar los archivos.
* El **bloqueo de archivos** impide que varios usuarios editen el mismo archivo al mismo tiempo.
* La**resolución de conflictos** mantiene la integridad de los datos en caso de que se sobrescriban archivos.
* Un**sistema de archivos distribuido** puede hacer que los datos sean redundantes y de alta disponibilidad al copiarlos en varios servidores en diferentes ubicaciones.

**Ventajas y desventajas del servidor de archivos**

El uso de servidores de archivos tiene sus ventajas y desventajas:

* Ventajas de un servidor de archivos
  + costo relativamente bajo
  + fácil de ampliar y personalizar
  + puede ser de alta capacidad
  + puede ser de alto rendimiento

* Desventajas de un servidor de archivos
  + requiere administración
  + necesita ser asegurado
  + limitada manipulación de archivos y metadatos incorporados
  + se necesita planificar en caso de querer aumentar la capacidad

**4. Servidor de correo electrónico:** Un servidor de correo es un sistema que se encarga de enviar correos electrónicos desde un cliente de correo a otro. Sin un servidor de correo, no puedes enviar ni recibir correos electrónicos. Los servidores de correo utilizan distintos protocolos de red para comunicarse entre sí.

Un servidor de correo es un sistema informático configurado con las aplicaciones necesarias para enviar y recibir correo electrónico. El servidor de correo es el hardware central de un proceso complejo en el que intervienen múltiples redes y protocolos de red. Estos protocolos son las normas que rigen la comunicación entre los distintos sistemas online.

Cuando envías un mensaje, el servidor de correo se asegura de que se envía al destinatario correcto. Si hay algún error, intentará enviarlo varias veces, sin que tengas que hacer nada. A su vez, si tu servidor de correo recibe un mensaje que no tiene un destinatario válido, informará al remitente de que algo ha fallado. El servidor de correo se encarga de que tu correo funcione como debe, para que tú no tengas que preocuparte de nada. Otra tarea que tiene un servidor de correo es comunicarse con el cliente de correo que tienes en tus dispositivos o en tu webmail. Cuando tu servidor de correo recibe un nuevo mensaje, lo reenvía a tu cliente de correo. Allí puedes leer el mensaje, moverlo a una carpeta, añadirle una etiqueta, o borrarlo. El servidor de correo guarda cualquier cambio que hagas en el mensaje, con lo que puedes, por ejemplo, borrar un correo en tu móvil y no tener que volver a borrarlo en tu webmail.

**5. servidor DNS (Domain Name System):** El sistema de nombres de dominio o DNS (Domain Name System) es un conjunto de protocolos y servicios que nació con la finalidad de evitar a las personas usuarias el esfuerzo de tener que recordar una dirección IP. Sin lugar a duda, nos resulta más fácil recordar un nombre, y además la dirección numérica podría cambiar por diferentes razones, sin que por ello cambie el nombre.

En este sistema estructurado en árbol participan tres partes diferenciadas:

**Clientes DNS:** es un programa cliente DNS usado por cualquier persona usuaria a través de su equipo o dispositivo para realizar una petición a través de la red (una web, un envío de correo, etc).

**Servidores DNS:** es el software o máquina encargada de atender y dar respuesta a la petición de los clientes DNS, por ejemplo, indicando en que dirección se aloja una determinada página web. Los servidores recursivos tienen la capacidad de reenviar la solicitud hacia otro servidor en caso de que ellos no dispongan de la dirección solicitada.

**Zona de autoridad:** servidores o grupos de servidores que se encargan de resolver un conjunto de dominios determinado (por ejemplo .ES, .COM, etc).

**6. Servidor Proxy:** Un servidor proxy proporciona una puerta de enlace entre los usuarios e Internet. Es un servidor denominado “intermediario”, porque está entre los usuarios finales y las páginas web que visitan en línea.

Cuando una computadora se conecta a Internet, utiliza una dirección IP. Esto es similar a la dirección de su casa: le indica a los datos entrantes adónde ir y marca los datos salientes con una dirección de devolución para que otros dispositivos se autentiquen. Un servidor proxy es esencialmente una computadora en Internet que tiene una dirección IP propia.

Los servidores proxy proporcionan una valiosa capa de seguridad para su computadora. Pueden configurarse como filtros web o firewalls, y protegen a su computadora contra amenazas de Internet como el malware.

Esta seguridad adicional también es valiosa cuando se combina con una puerta de enlace web segura o con otros productos de seguridad de correo electrónico. De esta manera, puede filtrar el tráfico de acuerdo con su nivel de seguridad o la cantidad de tráfico que su red, o las computadoras individuales, pueden manejar.

Algunas personas usan los proxies para fines personales, como ocultar su ubicación mientras miran películas en línea. Sin embargo, para una compañía, pueden utilizarse para realizar varias tareas clave como las siguientes:

1. Mejorar la seguridad.
2. Proteger la actividad de los empleados en Internet de las personas que intentan espiarlas.
3. Equilibrar el tráfico de Internet para evitar choques.
4. Controlar el acceso de los empleados a los sitios web.
5. Guardar el ancho de banda almacenando archivos en caché o comprimiendo el tráfico entrante.

**Cómo funciona un proxy** Debido a que un servidor proxy tiene su propia dirección IP, actúa como un mediador para una computadora e Internet. Su computadora conoce esta dirección y, cuando usted envía una solicitud en Internet, se enruta al proxy, que luego obtiene la respuesta del servidor web y reenvía los datos de la página al navegador de su computadora, como Chrome, Safari, Firefox o Microsoft Edge.

**Beneficios de un servidor proxy** Los proxies vienen con varios beneficios que pueden darle a su negocio una ventaja:

1. **Seguridad mejorada:** Pueden actuar como un firewall entre su sistema e Internet. Sin ellos, los piratas informáticos tienen fácil acceso a su dirección IP y pueden usarla para infiltrarse en su computadora o red.
2. **Navegación, observación, escucha y compras privadas:** Utilice diferentes proxies para que no lo inunden los anuncios no deseados o recopilen datos específicos de IP.
3. **Acceso al contenido específico de la ubicación:** Puede designar un servidor proxy con una dirección asociada con otro país. De hecho, puede hacer que parezca que usted se encuentra en ese país y obtener acceso total a todas las computadoras de contenido de ese país con las que puede interactuar.
4. **Evitar que los empleados exploren sitios inapropiados o que distraigan:** Puede usarlo para bloquear el acceso a sitios web que están en contra de los principios de su organización. Además, puede bloquear sitios que suelen terminar distrayendo a los empleados de tareas importantes. Algunas organizaciones bloquean los sitios de redes sociales como Facebook y otros para eliminar las tentaciones que los hacen perder tiempo.

**Tipos de servidores proxy** Si bien todos los servidores proxy les dan a los usuarios una dirección alternativa con la cual usar Internet, hay varios tipos diferentes, cada uno con sus propias funciones.

**Proxy de reenvío** Un proxy de reenvío se encuentra frente a los clientes y se utiliza para obtener datos para grupos de usuarios dentro de una red interna. Cuando se envía una solicitud, el servidor proxy la examina para decidir si debe continuar y realizar una conexión.Un proxy de reenvío es más adecuado para redes internas que necesitan un único punto de entrada. Proporciona seguridad de dirección IP para quienes están en la red y permite un control administrativo directo. Sin embargo, un proxy de reenvío puede limitar la capacidad de una organización para satisfacer las necesidades de los usuarios finales individuales.

**Proxy transparente** Un proxy transparente puede brindar a los usuarios una experiencia idéntica a la que tendrían si usaran su computadora personal. Es por esto que es “transparente”. También puede “forzarse” en los usuarios, lo que significa que están conectados sin saberlo.

Los proxies transparentes son adecuados para las empresas que desean utilizar un proxy sin que los empleados sepan que están usando uno. Tiene la ventaja de proporcionar una experiencia de usuario perfecta. Por otro lado, los proxies transparentes son más susceptibles a ciertas amenazas de seguridad, como los ataques de denegación de servicio de SYN-flood.

**Proxy anónimo** Un proxy anónimo se basa en hacer que la actividad de Internet sea imposible de rastrear. Funciona accediendo a Internet en nombre del usuario mientras oculta su identidad y la información de su computadora.

Un proxy transparente es más adecuado para los usuarios que desean tener anonimato completo mientras acceden a Internet. Si bien los proxies transparentes brinda algunas de las mejores protecciones de identidad posible, no carecen de desventajas. Muchos consideran que el uso de proxies transparentes es insuficiente, y los usuarios a veces enfrentan resistencias o discriminación como resultado.

**Proxy de alto anonimato** Un proxy de alto anonimato es un proxy anónimo que lleva el anonimato un paso más allá. Funciona borrando su información antes de que el proxy intente conectarse al sitio de destino.

El servidor es más adecuado para los usuarios para quienes el anonimato es una necesidad absoluta, como los empleados que no desean que su actividad se rastree hasta la organización. En lo que respecta a la desventaja, algunos de ellos, en particular los gratuitos, son señuelos configurados para atrapar usuarios con el fin de acceder a su información o datos personales.

**Proxy de distorsión** Un proxy de distorsión se identifica como un proxy de un sitio web, pero oculta su propia identidad. Y hace esto cambiando su dirección IP a una incorrecta.

Los proxies de distorsión son una buena opción para las personas que desean ocultar su ubicación mientras acceden a Internet. Este tipo de proxy puede hacer que parezca que está navegando desde un país específico y le da la ventaja de ocultar no solo su identidad, sino también la del proxy. Esto significa que, incluso si usted está asociado con el proxy, su identidad sigue siendo segura. Sin embargo, algunos sitios web bloquean automáticamente los proxies de distorsión, lo que podría impedir que un usuario final acceda a los sitios que necesita.

**Proxy del centro de datos** Los proxies del centro de datos no están afiliados a un proveedor de servicios de Internet (ISP), sino que otra corporación los proporciona a través de un centro de datos. El servidor proxy existe en un centro de datos físico y las solicitudes del usuario se enrutan a través de ese servidor.

Los proxies de centros de datos son una buena opción para las personas que necesitan tiempos de respuesta rápidos y una solución económica. Por lo tanto, son una buena opción para las personas que necesitan recopilar inteligencia sobre una persona u organización muy rápidamente. Ofrecen el beneficio de darles a los usuarios el poder de recolectar datos de manera rápida y económica. Pero por otro lado no ofrecen el más alto nivel de anonimato, lo que puede poner en riesgo la información o identidad de los usuarios.

**Proxy residencial** Un proxy residencial le da una dirección IP que pertenece a un dispositivo físico específico. Todas las solicitudes se canalizan a través de ese dispositivo.

Los proxies residenciales sirven para los usuarios que necesitan verificar los anuncios que van a su sitio web, de modo que usted pueda bloquear anuncios sospechosos o no deseados de competidores o malhechores. Los proxies residenciales son más confiables que otras opciones de proxy. Sin embargo, a menudo cuestan más dinero, por lo que los usuarios deben analizar cuidadosamente si los beneficios valen la inversión adicional.

**Proxy público** Cualquier persona puede acceder a un proxy público sin cargo. Funciona dándoles a los usuarios acceso a su dirección IP y ocultan su identidad cuando visitan sitios.

Los proxies públicos son más adecuados para aquellos usuarios para quienes el costo es una preocupación importante, mientras que la seguridad y la velocidad no lo son. Aunque son libres y de fácil acceso, a menudo son lentos porque se atascan con usuarios libres. Cuando utiliza un proxy público, también corre un mayor riesgo de que otros accedan a su información en Internet.

**Proxy compartido** Los proxies compartidos son utilizados por más de un usuario a la vez. Le dan acceso a una dirección IP que puede compartirse con otras personas, y luego usted puede navegar por Internet mientras parece que navega desde una ubicación de su elección.

Los proxies compartidos son una opción sólida para las personas que no tienen mucho dinero para gastar y no necesariamente necesitan una conexión rápida. La principal ventaja de un proxy compartido es su bajo costo. Debido a que otras personas lo comparten, es posible que le echen la culpa por las malas decisiones de otra persona, lo que podría hacer que lo prohíban en un sitio.

**Proxy de SSL** Un proxy de capa de sockets seguros (SSL) proporciona descifrado entre el cliente y el servidor. Dado que los datos se cifran en ambas direcciones, el proxy oculta su existencia tanto del cliente como del servidor.

Estos proxies son más adecuados para organizaciones que necesitan protección mejorada contra las amenazas que el protocolo SSL revela y detiene. Debido a que Google prefiere servidores que usan SSL, un proxy SSL puede ayudar a su clasificación de motores de búsqueda cuando se lo usa en relación con un sitio web. Lo negativo es que el contenido cifrado en un proxy SSL no se puede almacenar en caché; entonces, cuando visita sitios web varias veces, es posible que experimente un rendimiento más lento de lo que experimentaría de otro modo.

**Proxy rotativo** Un proxy rotativo asigna una dirección IP diferente a cada usuario que se conecta a él. Cuando los usuarios se conectan, se les da una dirección que es exclusiva del dispositivo que se conectó antes.

Los proxies rotativos son ideales para los usuarios que necesitan hacer un gran volumen de raspado de red continuo. Permiten volver al mismo sitio web una y otra vez de forma anónima. Sin embargo, debe tener cuidado al elegir servicios de proxy rotativos. Algunos de ellos contienen proxies públicos o compartidos que podrían exponer sus datos.

**Proxy inverso** A diferencia de un proxy de reenvío, que se encuentra delante de los clientes, un proxy inverso se coloca delante de los servidores web y reenvía las solicitudes desde un navegador a los servidores web. Funciona interceptando las solicitudes del usuario en el borde de la red del servidor web. Luego envía las solicitudes al servidor de origen y recibe las respuestas de este.

Los proxies inversos constituyen una opción sólida para sitios web populares que necesitan equilibrar la carga de muchas solicitudes entrantes. Pueden ayudar a que una organización reduzca la carga del ancho de banda porque actúan como otro servidor web que administra las solicitudes entrantes. La desventaja es que los proxies inversos pueden exponer potencialmente la arquitectura del servidor HTTP si un atacante logra penetrar en ella. Esto significa que es posible que los administradores de red tengan que reforzar o reposicionar su firewall si están usando un proxy inverso.

**7. Servidor de Aplicaciones**: Los servidores de aplicaciones son componentes fundamentales en el mundo de la tecnología y el desarrollo web. Son los encargados de proporcionar servicios y funcionalidades a las aplicaciones, lo que permite que estas puedan comunicarse con otras aplicaciones, bases de datos, servidores web y realizar tareas específicas para el correcto funcionamiento de los sistemas.

En términos sencillos, un servidor de aplicaciones es como un anfitrión que sirve y gestiona las aplicaciones web para que los usuarios puedan interactuar con ellas. Estos servidores están diseñados para manejar múltiples solicitudes y proporcionar los recursos necesarios para que las aplicaciones funcionen correctamente.

**El papel de los servidores de aplicaciones** Cuando una aplicación necesita acceder a una base de datos, procesar información o realizar tareas complejas, se requiere un servidor de aplicaciones para gestionar estas acciones. Estos servidores actúan como intermediarios entre el usuario y la aplicación, encargándose de ejecutar la lógica de negocio, procesar datos y proveer respuestas adecuadas.

Los servidores de aplicaciones se basan en la tecnología de Internet Información Services (IIS) o en otras soluciones de servidor web, que les permiten recibir y procesar solicitudes HTTP/HTTPS de los usuarios y proporcionar respuestas en forma de páginas web o servicios.

**Funcionalidades clave de los servidores de aplicaciones** Los servidores de aplicaciones ofrecen una variedad de funcionalidades esenciales para el desarrollo y despliegue de aplicaciones. Algunas de estas funcionalidades son:

**Ejecución de código** Los servidores de aplicaciones son capaces de ejecutar código en diferentes lenguajes de programación, como Java, C#, Python o Ruby, entre otros. Esto permite que las aplicaciones puedan desarrollarse en el lenguaje de programación más adecuado para cada caso.

**Acceso a bases de datos** Los servidores de aplicaciones brindan acceso a bases de datos, lo que les permite a las aplicaciones almacenar, recuperar y modificar datos de manera eficiente. Esta integración con bases de datos es crucial para muchas aplicaciones, ya que les permite gestionar información de forma persistente.

**Gestión de la lógica de negocio** La lógica de negocio de una aplicación, es decir, las reglas y procesos que determinan su funcionamiento, se gestiona y ejecuta en los servidores de aplicaciones. Esto permite separar la lógica del negocio del resto de los componentes de la aplicación, facilitando su mantenimiento y escalabilidad.

**Interfaz para programación de aplicaciones (API)** Los servidores de aplicaciones también proporcionan una interfaz para la programación de aplicaciones (API), que le permite a otras aplicaciones o servicios acceder y utilizar las funcionalidades de una aplicación. Esto posibilita la integración entre diferentes sistemas y aplicaciones, creando ecosistemas tecnológicos más amplios y colaborativos.

**8. Servidor de Videojuegos:** Un servidor de videojuego es un servidor local o remoto usado por clientes de videojuegos para jugar videojuegos multijugador. La mayoría de los videojuegos jugados a través de Internet funcionan mediante una conexión a un servidor de videojuego.

**Alojamiento de servidores de videojuegos**

Los proveedores de servidores de videojuegos son empresas que alquilan servidores de videojuegos. Los clanes de videojuegos a menudo alquilarán uno o más servidores para el videojuego que jueguen, y los miembros contribuirán a pagar el alquiler. Los proveedores de servidores de videojuegos a menudo ofrecen herramientas web para controlar y configurar los servidores; la mayoría permiten que los alquiladores modifiquen los videojuegos alquilados.

**Servidores de videojuegos dedicados**

La mayoría de los videojuegos hacen uso de una aplicación de servidor dedicado. Este programa recolecta datos de los jugadores y los distribuye a los otros jugadores. Esto es más eficiente y efectivo que un sistema peer-to-peer, pero necesita de una computadora aparte para alojar la aplicación de servidor. Esta computadora adicional es el servidor. El ancho de banda de red, en particular el ancho de banda de subida es muy a menudo una de las mayores limitaciones al momento de alojar servidores de videojuegos. Las conexiones de Internet con anchos de banda hogareños raramente proveen el ancho de banda de subida necesario para alojar servidores de videojuegos dedicados con más de cuatro a diez clientes.

**Tipos de servidores de videojuegos**

Los servidores de videojuegos pueden clasificarse como servidores de escucha o servidores dedicados. En los servidores de escucha, el servidor funciona en el mismo proceso que el cliente de videojuego, permitiéndole a un jugador alojar y participar del videojuego al mismo tiempo. Pero, cuando se cierra el cliente, al servidor le ocurre lo mismo. Los servidores de escucha son operados en su mayoría por individuos, más comúnmente en LAN parties que a través de Internet, y generalmente con un reducido número de jugadores debido a los grandes requisitos de procesamiento y ancho de banda que exigen los servidores y clientes funcionando en una misma máquina. Los servidores dedicados son servidores que funcionan independientemente del cliente. Estos servidores pueden ser operados por individuos, pero usualmente son operados en computadoras dedicadas ubicadas en centros de procesamiento de datos, que pueden proveer un mayor ancho de banda y un poder de procesamiento dedicado. Los servidores dedicados son el método preferido para alojar servidores de videojuegos para la mayoría de los videojuegos multijugador de PC. Los videojuegos multijugador masivos en línea funcionan en servidores dedicados usualmente operados por la empresa de software propietaria del videojuego, permitiéndoles controlar y actualizar el contenido. En muchos casos funcionan en clústers para permitir entornos inmensos y grandes cantidades de jugadores. Un ejemplo de esto es el servidor AllDead de Minecraft: mc.alldead.eu

**9. Servidor de virtualización.**

**10. servidor de seguridad (firewall o VPN)**

**11. Servidor FTP (file transfer protocol)**

**12. servidor de backup (respaldo de datos)**