

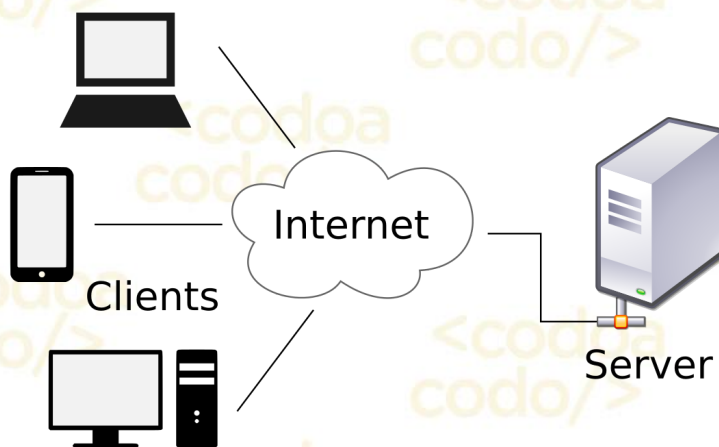
Contenidos a Trabajar

1. Modelo Cliente/Servidor
2. ¿Cómo funciona Internet?
 - a. ¿Cómo se comunican las redes de Internet?
 - b. ¿Qué es un protocolo TCP/IP y cómo funciona?
3. Protocolo HTTP y HTTPS

Modelo Cliente/Servidor

El flujo cliente/servidor es un modelo de comunicación en el que dos o más dispositivos se conectan entre sí para intercambiar información y recursos. En este modelo, uno de los dispositivos actúa como cliente y el otro como servidor.

El cliente es el dispositivo que solicita información o servicios al servidor, mientras que el servidor es el dispositivo que responde a las solicitudes del cliente proporcionando los recursos o servicios solicitados. Esta interacción se basa en un protocolo de comunicación en el que se definen las reglas para el intercambio de datos entre el cliente y el servidor.



Por ejemplo, en la navegación web, el usuario utiliza un navegador (cliente) para solicitar información a través de Internet, como cargar una página web. El

servidor web recibe la solicitud del navegador, procesa la solicitud y envía la respuesta al navegador.

El modelo cliente/servidor se utiliza en muchas aplicaciones y sistemas, como correo electrónico, bases de datos, juegos en línea, servicios en la nube y muchas otras aplicaciones en línea. Este modelo es escalable, ya que múltiples clientes pueden conectarse a un solo servidor y solicitar información o servicios simultáneamente. Además, el uso del modelo cliente/servidor puede mejorar la seguridad, ya que los servidores pueden controlar y proteger el acceso a los recursos y servicios que ofrecen.

Este proceso se realiza a través de un conjunto de protocolos y tecnologías que permiten la comunicación entre los clientes y los servidores. En la mayoría de los casos, la comunicación se realiza a través de Internet utilizando el protocolo TCP/IP.

Para establecer la comunicación, el cliente envía una solicitud al servidor a través de un protocolo de aplicación específico, como HTTP para solicitar páginas web o SMTP para enviar correo electrónico. El servidor recibe la solicitud, procesa la solicitud y envía una respuesta al cliente. La respuesta puede ser una página web, un archivo descargable, un mensaje de correo electrónico o cualquier otro tipo de información que el cliente haya solicitado.

¿Cómo funciona Internet?



Muchos ven a Internet como una “nube” de tecnología o alguna suerte de repositorio de aplicaciones y datos a los que se puede acceder, trabajar o simplemente consultar. Sin embargo, el uso cotidiano hace que muy pocas veces nos preguntemos qué es realmente.

Internet se define como una gran “red de redes”, es decir, una red conectada a otra de manera continua y simultánea, pero para entenderlo mejor veamos primero qué es una red:

Cada uno de estos gráficos representa una especie de red: de computadoras, de puntos o de pesca. Lo que define a estas redes como tales es que existe “interconexión” entre sus componentes, aún cuando no se encuentren la

totalidad de los puntos conectados entre sí. Desde cualquier punto de la red podremos llegar a otro, con más o menos vueltas, pero todos los destinos son alcanzables. Internet es justamente eso: una gran red donde todos los dispositivos están conectados entre sí.

¿Cómo se comunican las redes de Internet?

Para que una interconexión sea realmente global, todas las redes que se conectan a la gran red de redes deben hacerlo a través de un mismo protocolo o “lenguaje en común”. Es decir, el protocolo de comunicación de Internet debe ser una implementación estándar que garantice la conexión desde cualquier origen hasta cualquier destino.

Durante la década del '70, un grupo de investigadores de Estados Unidos creó un protocolo de comunicación que denominaron TCP/IP, y conectaron entre sí a un conjunto de redes de computadoras a pedido del gobierno de ese país, sin saber que el proyecto resultaría tan exitoso y tendría alcance global. De esta forma, TCP/IP se convirtió en el modelo de comunicación de las redes que componen Internet.

Interconexión

Probablemente la computadora que utilizamos a diario en la oficina esté conectada a una red de computadoras. En nuestra casa, la computadora portátil, tablet y celulares los vinculamos a un dispositivo inalámbrico que luego se conecta a la red de fibra óptica de la empresa que nos brinda servicio de

Internet y de televisión por cable o telefonía. Éste se comunica a la red de otro Proveedor de Servicios de Internet o ISP (por sus siglas en inglés) más grande, que llega a un número mayor de hogares y empresas, y así sucesivamente. A su vez, estos proveedores de acceso internacional se interconectan con otros más grandes, denominados Carriers, a través de fibras ópticas transcontinentales y satélites, entre otros.

Con el correr de los años, esta gran red de redes ha pasado a ocupar un lugar relevante en múltiples niveles ya que es transversal a cuestiones sociales, políticas y económicas, y ya no excluyente de ámbitos tecnológicos. El impacto de Internet es tal que ha modificado paradigmas y continúa estableciendo nuevos desafíos en torno a la educación, la industria, la seguridad, los derechos humanos, las políticas públicas y las nuevas tecnologías, entre otros.

De lo anterior se hace evidente que Internet no es algo dado y que es producto de un proceso histórico e interdisciplinario que continúa en constante movimiento y en donde la participación de diversas partes interesadas ha sido determinante para su desarrollo. Es por esto que resulta fundamental comprender que la participación de diversos sectores, y más aun de nuevas generaciones, en la Gobernanza de Internet, es indispensable en las definiciones del futuro de Internet, contemplando intereses y derechos de todos los sectores de la comunidad.

¿Qué es un protocolo TCP/IP y cómo funciona?

Como sucede con las personas, es importante que los equipos tengan un modo común de comunicarse entre ellos. Para la mayoría de los equipos actuales, este modo es TCP/IP. TCP/IP suele venir integrado en los equipos y está automatizado en buena medida, aunque puede ser útil comprender el modelo TCP/IP, en especial si va a configurar un equipo para conectarlo a otro sistema.

¿Qué significa TCP/IP?

TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP es un conjunto de reglas estandarizadas que permiten a los equipos comunicarse en una red como Internet.

¿Qué hace exactamente TCP/IP? ¿Y cómo funciona?

Por sí mismo, un equipo puede realizar determinadas tareas. Pero su potencia se multiplica cuando es capaz de comunicarse con otros. Muchas de las cosas para las que utilizamos los equipos (enviar mensajes de correo electrónico, ver Netflix u obtener indicaciones para llegar a un sitio) dependen de la comunicación entre ellos. Pueden ser equipos de distintas marcas o incluso encontrarse en zonas del mundo diferentes. Y las personas y programas que los utilizan pueden hablar distintos lenguajes humanos e informáticos.

Una interacción determinada puede darse entre dos sistemas informáticos o involucrar cientos de sistemas. Sin embargo, como sucede al pasar una carta o un paquete de mano en mano, cada transacción se produce entre solo dos equipos cada vez.

Para que esto suceda, los dos equipos deben saber, por adelantado, cómo se espera que se comuniquen.

- ¿Cómo inician la conversación?
- ¿A quién le toca comunicarse?
- ¿Cómo sabe un equipo si su mensaje se ha transmitido correctamente?
- ¿Cómo terminan la conversación?

Los equipos lo resuelven mediante protocolos. Un protocolo es un conjunto de reglas convenido. En términos humanos, utilizamos protocolos sociales para saber cómo comportarnos y comunicarnos con otras personas. Las tecnologías tienen su propia forma de establecer reglas de comunicación, como el telégrafo cuando empleaba el código Morse o una radio CB en la que se utilizan códigos como “10-4”.

Con los equipos sucede lo mismo, aunque las reglas son más estrictas. Cuando todos los equipos emplean el mismo protocolo, es posible transferir información. Cuando no es así, cunde el caos.

La comunicación era más complicada cuando la gente comenzaba a intercambiar información entre equipos. Cada fabricante tenía un sistema de

comunicación propio entre sus máquinas, pero dichos sistemas no permitían la comunicación con los equipos de los demás fabricantes. Pronto quedó claro que era necesario un estándar convenido que permitiera a los equipos de todos los fabricantes comunicarse entre ellos. Ese estándar es TCP/IP.

¿En qué se diferencian TCP e IP?

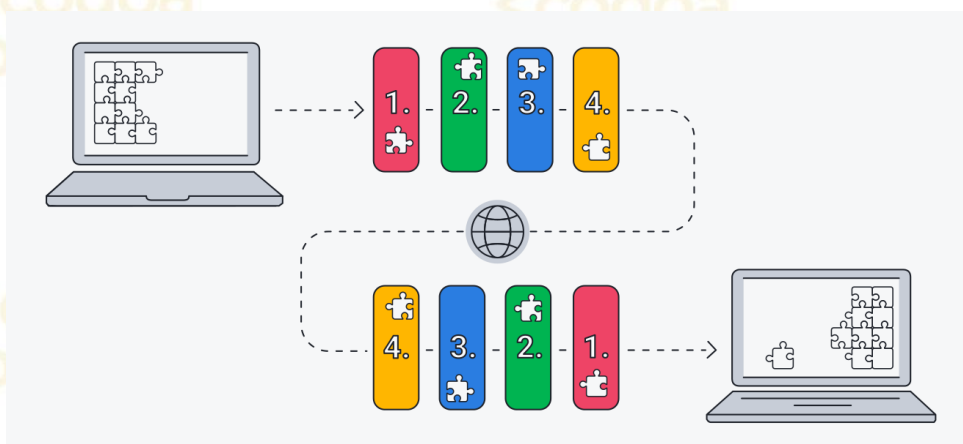
TCP e IP son dos protocolos distintos para redes informáticas. IP es la parte que obtiene la dirección a la que se envían los datos. TCP se encarga de la entrega de los datos una vez hallada dicha dirección IP. Es posible separarlos, pero lo cierto es que no tiene mucho sentido diferenciar entre TCP e IP. Como se usan juntos tan habitualmente, “TCP/IP” y “modelo TCP/IP” son ya terminología reconocida.

Mírelo de esta forma: La dirección IP es como el número de teléfono que se asigna a su smartphone. TCP es toda la tecnología que hace que el teléfono emita un timbre al recibir una llamada y que le permite hablar con alguien al otro lado de la línea. Son cosas diferentes, pero tampoco tienen sentido la una sin la otra.

¿Qué hace exactamente TCP/IP? ¿Y cómo funciona?

TCP/IP fue desarrollado por el Departamento de Defensa de EE. UU. para especificar el modo en que los equipos transfieren datos de un dispositivo a otro. TCP/IP incide mucho en la precisión y dispone de varios pasos para garantizar la correcta transmisión de los datos entre ambos equipos.

Este es uno de los mecanismos que emplea para ello. Si el sistema enviara un mensaje entero en una pieza y se encontrara cualquier problema, sería necesario enviar de nuevo el mensaje completo. Lo que hace TCP/IP es descomponer cada mensaje en paquetes que se vuelven a ensamblar en el otro extremo. De hecho, cada paquete podría tomar una ruta distinta hasta el equipo de destino si la ruta deja de estar disponible o está muy congestionada.



Además, TCP/IP divide las distintas tareas de comunicación en capas. Cada capa tiene una función distinta. Los datos pasan por cuatro capas independientes antes de recibir se en el otro extremo (como se explica en la sección siguiente). A continuación, TCP/IP recorre estas capas en orden inverso para reensamblar los datos y presentárselos al destinatario.

El propósito de las capas es crear un sistema estandarizado, sin que los distintos fabricantes de hardware y software tengan que gestionar la comunicación por su cuenta. Es como conducir un coche: todos los fabricantes convienen en la posición de los pedales, así que no tenemos que tener eso en

cuenta al cambiar de coche. También significa que es posible actualizar determinadas capas, por ejemplo, para mejorar el rendimiento o la seguridad, sin tener que actualizar todo el sistema.

Las cuatro capas del modelo TCP/IP

TCP/IP es un protocolo de enlace de datos que se utiliza en Internet. Su modelo se divide en cuatro capas diferenciadas. Cuando se emplean juntas, es posible referirse a ellas como un paquete de protocolos.

Capa de enlace de datos

La capa de enlace de datos (también denominada capa de enlace, capa de interfaz de red o capa física) es la que maneja las partes físicas del envío y recepción de datos mediante el cable Ethernet, la red inalámbrica, la tarjeta de interfaz de red, el controlador del dispositivo en el equipo, etcétera.

Capa de Internet

La capa de Internet (también denominada capa de red) controla el movimiento de los paquetes alrededor de la red.

Capa de transporte

La capa de transporte es la que proporciona una conexión de datos fiable entre dos dispositivos. Divide los datos en paquetes, hace acuse de recibo de los

paquetes que recibe del otro dispositivo y se asegura de que el otro dispositivo haga acuse de recibo de los paquetes que recibe a su vez.

Capa de aplicaciones

La capa de aplicaciones es el grupo de aplicaciones que requiere comunicación de red. Es con lo que el usuario suele interactuar, como el correo electrónico y la mensajería. Como la capa inferior gestiona los detalles de la comunicación, las aplicaciones no tienen que preocuparse por ello.

¿Mis paquetes de datos se mantienen privados?

No. Cuando los paquetes se transmiten entre equipos, son vulnerables y otros pueden verlos. Esa es una de las razones por las que se aconseja evitar las redes Wi-Fi públicas para enviar datos que deban mantenerse privados, así como utilizar cifrado. Si esto es algo que le preocupa (por ejemplo, si va a enviar información de identificación personal o datos financieros), puede cifrar los datos empleando una red privada virtual (VPN) o trabajando con páginas web con seguridad https.

¿TCP/IP funciona con toda clase de direcciones IP?

Hay varios tipos de direcciones IP. No obstante, todas ellas utilizan TCP/IP. Las diferencias entre los tipos de direcciones IP son transparentes para el usuario esporádico, y el hecho de que no necesite saber mucho al respecto es una de las ventajas de TCP/IP. Normalmente, estos asuntos los administra quien haya

configurado el sistema operativo del equipo o el dispositivo móvil. En cualquier caso, a modo de aclaración:

- Las direcciones IP estáticas no cambian en ningún momento. Son como la dirección fija de su domicilio, un dato inalterable.
- Las direcciones IP dinámicas cambian, o al menos están diseñadas para cambiar. Cuando un sistema informático utiliza una dirección IP dinámica, anuncia “¡aquí es donde puedes encontrarme!” a la red local.

Tal vez haya oído hablar de ciudades en las que la población crece tan rápido que se han tenido que crear nuevos códigos de área para que los recién llegados puedan tener número de teléfono. Con el número siempre creciente de dispositivos conectados, TCP/IP ha tenido un problema similar. Básicamente, Internet se estaba quedando sin direcciones IP. Por eso se desarrolló una nueva versión de dirección IP denominada IPv6, una alternativa a las direcciones IPv4 existentes.

De hecho, TCP/IP se incluye como estándar. TCP/IP es el paquete de protocolos más utilizado en la web. Millones de personas lo emplean cada día, aunque no sean conscientes de ello. En la inmensa mayoría de los equipos, TCP/IP se integra como estándar. No tiene que hacer nada para configurarlo de manera manual. En ocasiones, tal vez tenga que decirle a una aplicación cuál es su dirección TCP/IP.

En algunas circunstancias puede querer ocultar su dirección IP, normalmente por motivos de seguridad. ¿Cómo puedo saber cuál es mi dirección TCP/IP?

Cada dispositivo tiene su propia dirección TCP/IP. Por lo general, el dispositivo puede comunicarse automáticamente, pero a veces es necesario proporcionar su dirección TCP/IP de forma manual. El modo de encontrar su dirección IP depende del sistema operativo.

Podés consultar tu IP pública desde una página web como <https://www.cual-es-mi-ip.net/>. Conceptualmente, el número obtenido se puede asemejar a la “dirección” de una habitación de hotel, en la que la gerencia del mismo sabe que puede encontrarlo o el número de teléfono de tu celular.

Protocolo HTTP y HTTPS



Http



Https

HTTP

HTTP (Hypertext Transfer Protocol) es un protocolo utilizado para transferir datos a través de la web. Es el protocolo que permite que los navegadores web soliciten y reciban páginas web, imágenes y otros recursos de los servidores web.

Es el contrato que utilizan los navegadores y servidores web para comunicarse y enviar información a través de Internet. Es como si fuera el idioma común que hablan dos personas que se encuentran en un país extranjero y no hablan el mismo idioma.

Imagina que quieres visitar una página web como Google. Cuando escribes la dirección en tu navegador, éste envía una solicitud al servidor de Google pidiéndole que te muestre la página. El servidor de Google recibe esa solicitud y, gracias a HTTP, puede entender lo que tu navegador está pidiendo. Entonces el servidor envía de vuelta la página web a tu navegador en formato HTML para que lo puedas visualizar.

Pero esta comunicación no sería posible sin el protocolo TCP/IP. TCP/IP es como el sistema de calles o rutas que conecta a todas las computadoras y servidores en Internet. Es el protocolo que permite que la información se mueva de un lugar a otro en la red.

HTTP, por su parte, utiliza el protocolo TCP/IP para transmitir la información de la solicitud y la respuesta entre el navegador y el servidor. Es como si HTTP fuera el contenido de los camiones que se mueven por la red de rutas de TCP/IP.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) es una variante segura de HTTP que utiliza criptografía para proteger los datos transferidos entre el navegador y el servidor web. A diferencia de HTTP, que transfiere datos en texto plano, HTTPS utiliza una capa adicional de seguridad para encriptar los datos en tránsito, lo que los hace más seguros y protege la privacidad del usuario.

Cuando visitas un sitio web que utiliza HTTPS, se establece una conexión segura entre el navegador y el servidor web. El servidor web envía al navegador un certificado digital que verifica la identidad del sitio web y su autenticidad. A partir de ese momento, cualquier dato que se transmita entre el navegador y el servidor web estará encriptado, lo que reduce el riesgo de que alguien pueda interceptar o manipular los datos en tránsito.

Los certificados digitales son emitidos por Autoridades de Certificación (AC), que son entidades de confianza que verifican la identidad de los solicitantes de certificados. Cuando se solicita un certificado, se debe proporcionar información que verifique la identidad del solicitante, como el nombre, la dirección y la organización a la que pertenece. La AC verifica esta información y emite el certificado digital correspondiente.

En general, los certificados para sitios web se pueden obtener a través de proveedores de servicios de certificación, quienes se encargan de verificar la identidad del solicitante y emitir el certificado correspondiente. Algunos proveedores de servicios de alojamiento web también ofrecen certificados gratuitos, como Let's Encrypt.

Para obtener un certificado digital, normalmente se deben proporcionar detalles como el nombre de dominio, la dirección de correo electrónico y la ubicación geográfica de la entidad que solicita el certificado. También es necesario generar una clave privada que se utilizará para cifrar los datos que se transmiten en la conexión segura. Una vez que se ha completado el proceso de solicitud y verificación, la AC emite el certificado digital, que se puede

instalar en el sitio web o en el equipo personal del usuario, según sea necesario.



Se los conoce como certificados SSL (Secure Sockets Layer) ya que este es el protocolo que se utiliza para la transferencia segura de datos en internet, mientras que TLS (Transport Layer Security) es su sucesor y versión actual. Sin embargo, el término SSL se ha popularizado y a menudo se utiliza indistintamente con TLS.

Un certificado SSL/TLS es un tipo de certificado digital que se utiliza para autenticar la identidad de un sitio web y proteger la comunicación entre el navegador web del usuario y el servidor del sitio web. Cuando se utiliza un certificado SSL/TLS, la información que se transfiere entre el navegador y el servidor se cifra y se verifica que el servidor es quien dice ser.

En resumen, un certificado SSL/TLS es un documento digital que verifica la identidad de un sitio web y proporciona una capa adicional de seguridad para la comunicación entre el usuario y el sitio web. Los certificados SSL/TLS son emitidos por Autoridades de Certificación (CA) confiables y pueden ser adquiridos a través de ellas o de proveedores de hosting que ofrezcan certificados SSL/TLS.