

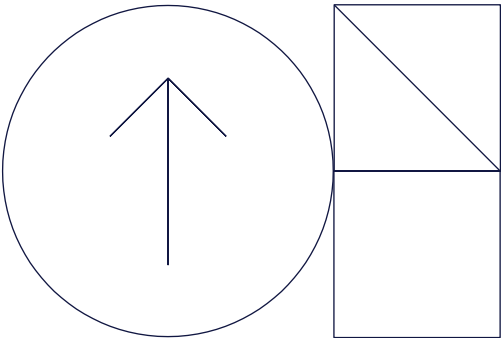
# Fundamentos de Internet

¿Qué es HTTP?



# Índice

Introducción	3
¿Qué hay en una solicitud HTTP?	4
¿Qué es un método HTTP?	5
¿Qué son los encabezados de solicitud HTTP?	5
¿Qué hay en el cuerpo de una solicitud HTTP?	5
¿Qué hay en una respuesta HTTP?	5
¿Se pueden lanzar ataques DDoS a través de HTTP?	7
¿Cuál es la diferencia entre http y https?	7
¿Por qué necesito usar el protocolo HTTPS?	7
¿Qué son IP y TCP?	7



# Introducción

Seguro que has escuchado o visto en muchas ocasiones las letras HTTP. Son uno de los puntos básicos de Internet. De hecho, han sido las cuatro primeras letras con las que empezaba cada enlace. Según sus siglas en inglés, HyperText Transfer Protocol (Protocolo de transferencia de hipertexto) es el método más común de intercambio de información de la World Wide Web. Es un protocolo que define cómo se deben formatear y transmitir los datos a través de Internet. Se utiliza para cargar páginas web con enlaces de hipertexto. Este protocolo de transferencia de hipertexto fue diseñado por Tim Berners-Lee en 1989. Aunque, desde entonces, se ha ido actualizando en diferentes ocasiones.

La clave es que los usuarios pueden acceder a estos contenidos desde cualquier sitio web, incluso desde el ordenador de un amigo, sin necesidad de instalar ningún complemento. Puesto que un flujo típico implica que una máquina cliente realice una solicitud a un servidor, que luego envía un mensaje de respuesta.

## ¿Qué hay en una solicitud HTTP?

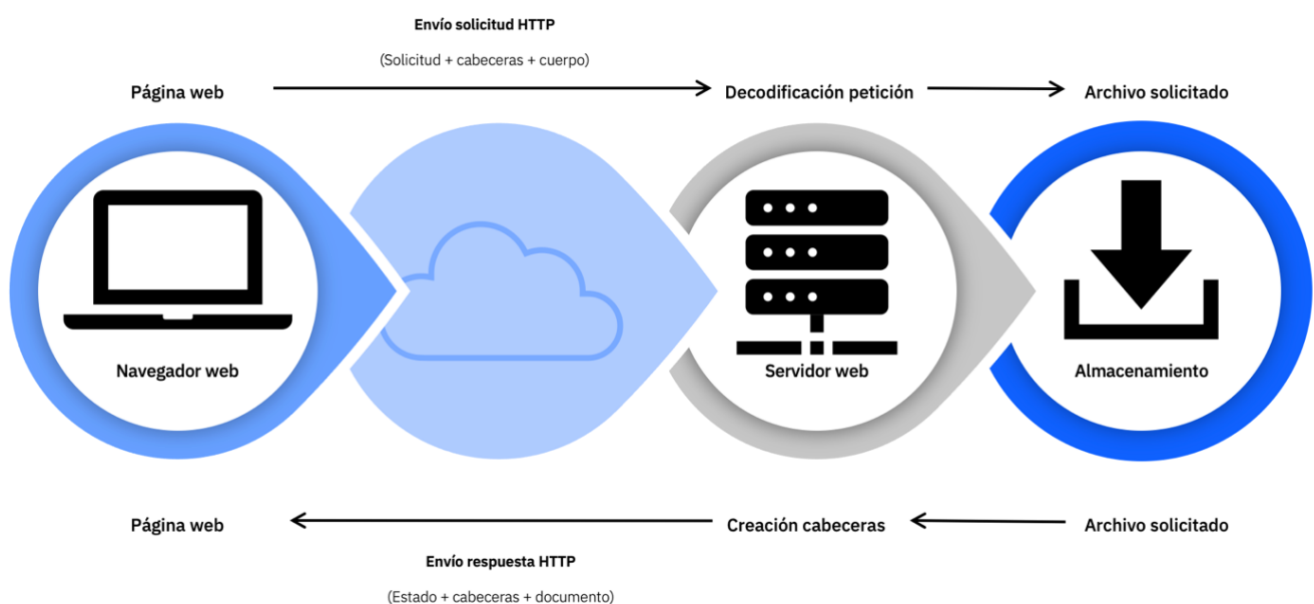
Una solicitud HTTP es la forma en que las plataformas de comunicación de Internet, como los navegadores web, piden la información que necesitan para cargar un sitio web.

Cada solicitud HTTP realizada por Internet lleva consigo una serie de datos codificados que contienen diferentes tipos de información. Una solicitud HTTP típica contiene:

- Tipo de versión de HTTP
- Una URL
- Un método HTTP
- Encabezados de solicitud HTTP
- Cuerpo HTTP opcional

Profundicemos en el funcionamiento de estas solicitudes y en cómo se puede utilizar el contenido de una solicitud para compartir información.

En el envío de una solicitud HTTP, podemos encontrar la solicitud, cabeceras y cuerpo, entre otras cosas.



## ¿Qué es un método HTTP?

Un método HTTP, a veces denominado verbo HTTP, indica la acción que la solicitud HTTP espera del servidor consultado. Por ejemplo, dos de los métodos HTTP más comunes son "GET" y "POST"; una solicitud "GET" espera que se le devuelva información (normalmente en forma de página web), mientras que una solicitud "POST" suele indicar que el cliente está enviando información al servidor web (como información de un formulario, por ejemplo, un nombre de usuario y una contraseña enviados).

## ¿Qué son los encabezados de solicitud HTTP?

Los encabezados de HTTP contienen información de texto almacenada en pares clave-valor, y se incluyen en cada solicitud HTTP (y respuesta, más adelante). Estos encabezados comunican información básica, como el navegador que utiliza el cliente y los datos que se solicitan.

Ejemplo de encabezados de solicitud HTTP de la pestaña de red de Google Chrome:

```
▼ Request Headers
:authority: www.google.com
:method: GET
:path: /
:scheme: https
accept: text/html
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0
```

## ¿Qué hay en el cuerpo de una solicitud HTTP?

El cuerpo de una solicitud es la parte que contiene el "cuerpo" de la información que está transfiriendo la solicitud. El cuerpo de una solicitud HTTP contiene toda la información que se envía al servidor web, como un nombre de usuario y una contraseña, o cualquier otro dato introducido en un formulario.

## ¿Qué hay en una respuesta HTTP?

Una respuesta HTTP es lo que los clientes web (normalmente los navegadores) reciben de un servidor de Internet en respuesta a una solicitud HTTP. Estas respuestas comunican información valiosa basada en lo que se pidió en la solicitud HTTP.

Una respuesta HTTP típica contiene:

- un código de estado HTTP
- encabezados de respuesta HTTP
- cuerpo de HTTP opcional

Vamos a desglosarlas:

### ¿Qué es un código de estado HTTP?

Los códigos de estado HTTP son códigos de 3 dígitos que se utilizan con mayor frecuencia para indicar si una solicitud HTTP se ha completado con éxito. Los códigos de estado se dividen en los siguientes 5 bloques:

- 1xx Informativo
- 2xx Éxito
- 3xx Redirección
- Errores de cliente 4xx
- 5xx Error del servidor

Las "xx" hace referencia a diferentes números entre 00 y 99.

Los códigos de estado que empiezan por el número "2" indican que la solicitud se ha realizado correctamente. Por ejemplo, después de que un cliente solicite una página web, las respuestas más habituales tienen un código de estado "200 OK", que indica que la solicitud se ha completado correctamente.

Si la respuesta empieza con un "4" o un "5", significa que ha habido un error y que no se mostrará la página web. Un código de estado que empieza con un '4' indica un error del lado del cliente (es muy común encontrar un código de estado '404 NO ENCONTRADO' cuando escribe mal una URL). Un código de estado que empieza con '5' significa que algo ha ido mal en el lado del servidor.

Los códigos de estado también pueden empezar con un "1" o un "3", que indican una respuesta informativa y una redirección respectivamente.

¿Qué son los encabezados de respuesta HTTP?

Al igual que una solicitud HTTP, una respuesta HTTP viene con encabezados que transmiten información importante, como el idioma y el formato de los datos que se envían en el cuerpo de la respuesta.

Ejemplo de encabezados de respuesta HTTP de la pestaña de red de Google Chrome:

▼ **Response Headers**

```
cache-control: private, max-age=0
content-encoding: br
content-type: text/html; charset=UTF-8
date: Thu, 21 Dec 2017 18:25:08 GMT
status: 200
strict-transport-security: max-age=86400
x-frame-options: SAMEORIGIN
```

¿Qué hay en el cuerpo de una respuesta HTTP?

Las respuestas HTTP satisfactorias a las peticiones "GET" suelen tener un cuerpo con la información solicitada. En la mayoría de las solicitudes web, se trata de datos HTML que el navegador traducirá en una página web.

## ¿Se pueden lanzar ataques DDoS a través de HTTP?

Ten en cuenta que HTTP es un protocolo "sin estado", lo que significa que cada comando se ejecuta independientemente de cualquier otro comando. En la especificación original, las solicitudes HTTP creaban y cerraban cada una conexión TCP. En las versiones más recientes del protocolo HTTP (HTTP 1.1 y superiores), la conexión persistente permite que varias solicitudes HTTP pasen por una conexión TCP persistente, lo cual mejora el consumo de recursos. En el contexto de ataques DoS o DDoS, las solicitudes HTTP en grandes cantidades pueden utilizarse para montar un ataque contra un dispositivo objetivo, y se consideran parte de los ataques a la capa de aplicación o a la capa 7.

## ¿Cuál es la diferencia entre http y https?

HTTP pronto se convirtió en el protocolo mayoritario en la red. Sin embargo, conforme avanzó el tiempo, se demostró que resultaba demasiado vulnerable para determinados sitios web donde los internautas compartían información sensible. Estamos hablando por ejemplo de webs de tiendas online donde los usuarios introducen la información de su tarjeta de crédito.

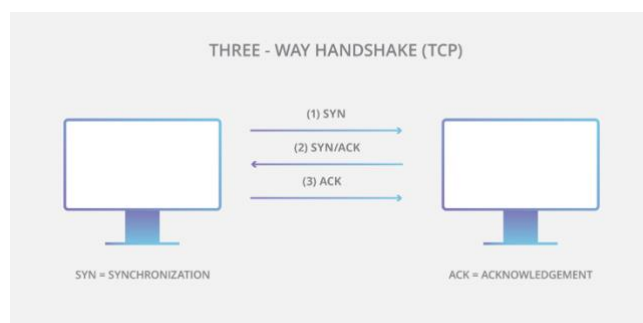
Por eso surgió la necesidad de crear un protocolo más seguro. De ese modo surgió el HTTPS, que cifra la información que circula entre la web y el usuario, para hacerla indescifrable a ojos de los hackers. Todas las webs de venta online adoptaron pronto ese protocolo.

¿Sabrías ver si una web usa http o https? Es mucho más sencillo de lo que te podría parecer en un comienzo, solo tienes que fijarte en su dirección.

Además, **el navegador suele añadir un icono al lado de la URL con https** para certificar que ofrece una conexión segura.

## ¿Por qué necesito usar el protocolo HTTPS?

Hemos dicho que el protocolo es ampliamente utilizado por tiendas online, pero si nuestra página web fuese por ejemplo de una clínica, ¿Deberíamos pasarnos a https? La respuesta es sí. Hoy día casi todas las webs tienen un espacio donde interactuar con las personas que visitan la web. Aunque solo sea un formulario de contacto. Nuestra web podría tener uno para que la gente pueda reservar una cita en nuestra clínica. Datos como el teléfono o el correo electrónico pueden ser considerados sensibles, por lo que **es importante usar el protocolo https para proteger esa información.**



## ¿Qué son IP y TCP?

El protocolo de Internet (IP) es el sistema de direcciones de Internet y tiene la función principal de entregar paquetes de información desde un dispositivo de origen a un dispositivo de destino. Es la forma principal en la que se realizan las conexiones de red y establece la base de Internet, pero no gestiona el orden de los paquetes ni la verificación de errores. Esta funcionalidad requiere otro protocolo, normalmente TCP.

La relación entre los protocolos TCP e IP es similar a enviar a alguien un mensaje escrito en un rompecabezas por correo postal. Se escribe el mensaje y se desmontan las piezas del rompecabezas. Luego, cada pieza puede viajar a través de una ruta postal diferente, algunas de las

cuales requieren más tiempo que otras. Cuando las piezas del rompecabezas llegan después de recorrer diferentes rutas, es posible que estén desordenadas. El protocolo de Internet garantiza que las piezas lleguen a su dirección de destino. Por su parte, el protocolo TCP sería como la persona que ordena las piezas del rompecabezas en el otro lado. Reúne las piezas en el orden correcto, solicita el reenvío de las piezas que faltan e informa al remitente de que se ha recibido el rompecabezas. Además, mantiene la conexión con el remitente antes del envío de la primera pieza del rompecabezas hasta después del envío de la última pieza.

IP es un protocolo sin conexión, lo que **significa que cada unidad de datos se aborda individualmente y se enruta desde el dispositivo de origen al dispositivo de destino**, que no envía una confirmación de vuelta al origen. Ahí es donde entran en juego protocolos como el TCP. Este último se utiliza junto con el protocolo de Internet para mantener una conexión entre el remitente y el destino y para garantizar el orden del paquete.

Por ejemplo, cuando se envía un correo electrónico a través del protocolo TCP, se establece una conexión y se realiza un protocolo de enlace de 3 vías. En primer lugar, el origen envía un paquete de "solicitud inicial" SYN al servidor de destino para iniciar la comunicación. Luego, el servidor de destino envía un paquete SYN-ACK para aceptar el proceso. Por último, el origen envía un paquete ACK al destino para confirmar el proceso, tras lo que se puede enviar el contenido del mensaje. El mensaje de correo electrónico se divide en última instancia en paquetes antes de que cada paquete se envíe a Internet, donde recorre una serie de puertas de enlace antes de llegar al dispositivo de destino donde el TCP reagrupa el conjunto de paquetes en el contenido original del correo electrónico.

La versión principal de IP que se utiliza en Internet hoy en día es la versión 4 (IPv4). Las limitaciones de tamaño en el número total de direcciones posibles en IPv4 propiciaron el desarrollo de un protocolo más nuevo, que se llama IPv6 y permite que haya muchas más direcciones disponibles. Su adopción es cada vez más frecuente.