



Seguramente en más de una oportunidad hemos oído hablar de “HTTPS”, pero no estamos realmente seguros de lo que significa, y tampoco nos importa demasiado. Esta actitud puede ocasionarnos una gran cantidad de serios problemas relacionados con la seguridad de nuestros datos cuando navegamos en Internet, aunque siempre lo hagamos en sitios seguros y de buena reputación. **En este artículo conoceremos qué significa HTTPS y porque ese término es tan importante.**

Antes que nada, tenemos que saber que HTTPS es la forma más segura de navegar por Internet, ya que cualquier dato que introduzcamos en el navegador viajará cifrado y por lo tanto no podrá ser analizado para su uso, tanto con fines comerciales o delincuenciales.

Principales diferencias entre HTTP y HTTPS

El Hypertext Transfer Protocol (HTTP), más conocido en español como Protocolo de Transferencia de Hipertexto, es un sistema utilizado en sistemas de redes, diseñado con el propósito de definir y estandarizar la sintaxis y la semántica de las transacciones que se llevan a cabo entre los distintos equipos que conforman una red.

La principal característica de este protocolo es que es un sistema orientado al funcionamiento del tipo “petición-respuesta”, lo que significa que en la estructura debe existir un cliente y un servidor, siendo el cliente el que efectúe las peticiones y el servidor el que las responde. Las respuestas del servidor pueden ser la descarga de un archivo o la apertura de una página web, dependiendo del tipo de petición solicitada.

Básicamente, una vez que en el navegador escribimos una dirección web y presionamos

la tecla “Enter”, el servidor nos responderá devolviéndonos lo deseado.

HTTP seguro

En el caso del Hypertext Transfer Protocol Secure (HTTPS) o Protocolo de Transferencia de Hipertexto Seguro, el sistema se basa en una combinación de **dos protocolos diferentes, HTTPS y SSL/TLS**.

Que los datos sean transmitidos en forma cifrada garantiza que no podrá ser vista por nadie más que el cliente y el servidor, anulando de esta forma la posibilidad de que pueda ser utilizada, ya que el ciberdelincuente sólo tendrá en sus manos datos cifrados que no podrá descifrar.

Cómo podemos ver, la utilización del protocolo HTTPS es de vital importancia para cualquier actividad que involucre el uso de datos personales como los utilizados en entidades bancarias, tiendas en línea, correos electrónicos y en cualquier otro sitio en el cual debemos introducir passwords, números de tarjeta de crédito u otra información personal.