El futuro digital es de todos | MinTIC

UNIVERSIDAD EL BOSQUE | MisiónTIC 2022

Ciclo 4A

Semana 2

Lenguajes Web.

Lectura 1 - El protocolo HTTP Seguro.

Convenio de asociación no. 777 de 2021 suscrito entre el Fondo Único de Tecnologías de la Información y las Comunicaciones y la Universidad el Bosque.

El protocolo HTTP Seguro

El protocolo Transport Layer Security (TLS) añade una capa de seguridad sobre los protocolos de transporte TCP/IP -ver figura 3-. TLS utiliza métodos de encriptación para enviar datos privados de forma segura, y añade características de seguridad adicionales, como autenticación y detección de manipulación de mensajes. El protocolo HTTP seguro utiliza TLS para transportar de forma segura los mensajes entre el cliente y el servidor.

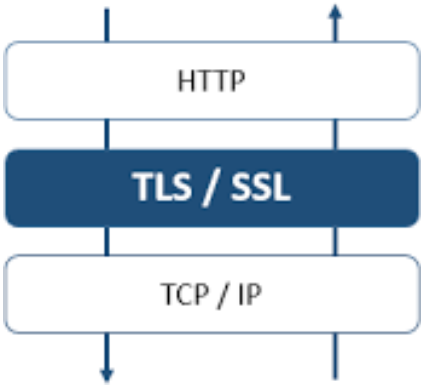

Figura 1. Protocolo TLS

Para utilizar HTTP seguro, es necesario adquirir un certificado de seguridad, el cual debe comprarse a una entidad debidamente autorizada para emitir este tipo de certificados. Cuando el cliente carga una URL que comienza con "https", inicia el proceso de establecer una conexión segura a través de TLS. Al principio de ese proceso, el navegador debe verificar el certificado digital del dominio. Hay muchas maneras en que un certificado puede ser inválido, lo cual se traduce en un error en la conexión. Si el certificado es válido, el mismo es utilizado para cifrar los mensajes enviados entre el cliente y el servidor.

Una conexión HTTPS asegura que sólo el cliente y el dominio seguro vean los datos en solicitudes y respuestas HTTP. Por otra parte, también previene la manipulación del contenido del sitio web, evitando que los paquetes sean interceptados y manipulados.