



UEA

UNIVERSIDAD
ESTATAL AMAZÓNICA

UNIVERSIDAD ESTATAL AMAZÓNICA

TIPO DE PRÁCTICA:

Entendiendo HTTP y HTTPS

MATERIA:

1. DESARROLLO DE APLICACIONES WEB (A)

ESTUDIANTE/S:

Marvin Alban

PERIODO

2025– 2025



"Entendiendo HTTP y HTTPS: Seguridad y Confianza en la Web"

1. Introducción

En el entorno digital actual, la transmisión segura de información es crucial para garantizar la privacidad y confianza de los usuarios. Los protocolos HTTP y HTTPS son fundamentales para la comunicación entre navegadores y servidores web. Este informe explora las diferencias entre ambos, su funcionamiento, y la importancia de emplear HTTPS en aplicaciones modernas.

2. Definiciones

HTTP (Protocolo de Transferencia de Hipertexto): Es un protocolo de comunicación que permite la transferencia de datos en la web. Funciona mediante solicitudes y respuestas entre un cliente (navegador) y un servidor, transmitiendo la información en texto plano, lo que puede vulnerar la seguridad de los datos.

HTTPS (Protocolo Seguro de Transferencia de Hipertexto):

Es una versión cifrada de HTTP que incorpora un mecanismo de seguridad mediante el uso de certificados digitales y cifrado SSL/TLS. Esto asegura que la información enviada entre cliente y servidor esté protegida contra interceptaciones y manipulaciones. (Amazonica, s.f.) .

3. Diferencias

El protocolo HTTPS protege la información confidencial que se envía entre el cliente y el servidor web en Internet, evitando que otras personas puedan interceptarla. En términos simples,

HTTPS es la versión más segura de HTTP.



CARECTERISTICAS	HTTP	HTTPS
Seguridad	Transmisión sin cifrado, susceptible a ataques Comunes	Comunicación cifrada, protege datos sensibles.
Certificados	No requiere certificados	Requiere certificados SSL/TLS
Autenticación	No ofrece garantía de identidad.	Verifica identidad del servidor mediante certificados.
Velocidad	Más rápido, menos carga por cifrado.	Ligeramente más lento por el proceso de cifrado.

4. Aplicaciones Prácticas de HTTPS

HTTPS es esencial en situaciones donde la confidencialidad y la integridad de la información son prioritarias, tales como:

- Transacciones financieras en línea: Protección de datos bancarios y pagos con tarjetas.
- Acceso a plataformas educativas: Resguardo de credenciales y calificaciones de estudiantes.
- Gestión de información médica: Protección de datos sensibles relacionados con la salud.



UEA

Comercio electrónico: Garantiza que las compras y datos personales se transmitan de forma segura.



(Banco Pichincha, 2022)

5. Reflexión Personal

Comprender la diferencia entre HTTP y HTTPS ha transformado mi perspectiva sobre el desarrollo web. Reconozco que la seguridad no es un aspecto opcional, sino una necesidad fundamental para proteger mis datos. El uso de HTTPS no solo aumenta la confianza de nosotros los usuarios, sino que también mejora el posicionamiento web y evita vulnerabilidades críticas. Por tanto, en cualquier proyecto de desarrollo, implementar protocolos seguros debe ser una prioridad para garantizar la integridad y confidencialidad de la información transmitida.

Bibliografía

Amazonica, U. E. (s.f.). *eva.pregrado.uea.edu.ec*. Obtenido de *eva.pregrado.uea.edu.ec*:
https://eva.pregrado.uea.edu.ec/eva2525/web/pluginfile.php/530999/mod_resource/content/8/U1_T1.1_Conceptos%20basicos%20de%20desarrollo%20web.pdf

Banco Pichincha. (27 de 06 de 2022). *pichincha.com*. Obtenido de
<https://www.pichincha.com/blog/http-https-que-son-diferencias>