**HTTP Y HTTPS**

**Aprendices:**

**Enyeer Manuel Granados Mardinis**

**Jhoan Andrey Ducuara Perdomo**

**Daniel Alberto Rodríguez Pineda**

**Emelyn Yulieth Yepez Ballesteros**

**Katherine Paola Uzgame Fernandez**

**Servicio Nacional de Aprendizaje - SENA**

**Centro de Electricidad, Electrónica y Telecomunicaciones - CEET**

**Ficha 2558104**

**Instructora: Isaura María Novoa**

**ÍNDICE:**

**CONCEPTO DE HTTP**

**¿Qué es HTTP?**

**¿Qué es un protocolo de comunicación?**

**¿Para qué sirve el protocolo HTTP?**

**¿Cómo funciona?**

**¿Qué es HTTPS?**

**DIFERENCIAS ENTRE HTTP Y HTTPS**

**Ventajas y Desventajas de HTTP**

**Evolución HTTP antes de HTTPS**

**¿Qué es un certificado SSL?**

**REFERENCIAS**

**CONCEPTO DE HTTP**

HTTP (Hypertext Transfer Protocol) es un protocolo de comunicación utilizado en la World Wide Web (WWW) para la transferencia de datos entre un cliente (generalmente un navegador web) y un servidor web. HTTP es la base de la comunicación en línea y permite que los usuarios soliciten y reciban recursos, como páginas web, imágenes, videos y otros archivos, a través de Internet.

**¿QUÉ ES UN PROTOCOLO DE COMUNICACIÓN?**

Es un sistema de reglas que permiten que dos o más entidades (computadoras, teléfonos celulares, etc.) de un sistema de comunicación se comuniquen entre ellas para transmitir información, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse.

Los sistemas de comunicación utilizan formatos bien definidos (protocolo) para intercambiar mensajes. Cada mensaje tiene un significado exacto destinado a obtener una respuesta de un rango de posibles respuestas predeterminadas para esa situación en particular.

**Funcionamiento**

El funcionamiento básico de HTTP involucra una serie de solicitudes y respuestas entre un cliente y un servidor:

1. ***Solicitud (Request):*** El cliente envía una solicitud HTTP al servidor para solicitar un recurso específico, como una página web. Esta solicitud contiene información como el método (GET, POST, PUT, DELETE, etc.), la URL del recurso deseado y otras cabeceras opcionales que pueden proporcionar información adicional al servidor.
2. ***Procesamiento en el Servidor:*** El servidor recibe la solicitud, procesa la solicitud y determina cómo responder. Puede ejecutar ciertas acciones, acceder a bases de datos, generar contenido dinámico, etc.
3. ***Respuesta (Response):*** El servidor genera una respuesta HTTP que contiene información sobre el estado de la solicitud y, si corresponde, el recurso solicitado. La respuesta también incluye una línea de estado que indica si la solicitud se procesó correctamente o si ocurrió algún error, además de cabeceras que proporcionan información adicional sobre la respuesta.
4. ***Recuperación por el Cliente:*** El cliente recibe la respuesta del servidor, analiza la línea de estado y las cabeceras para determinar cómo se maneja la respuesta. Si la respuesta incluye el recurso solicitado (como una página web), el cliente lo procesa y muestra al usuario. Si hubo un error, el cliente puede mostrar mensajes de error apropiados.

**Concepto de HTTPS**

El protocolo HTTPS es la evolución del HTTP en una versión segura. Este incluye una capa extra de protección a la hora de operar con datos de los usuarios. El HTTPS utiliza una combinación de dos protocolos (HTTP + SSL) que hace que cualquier información personal que facilites en la web sea cifrada o encriptada y nadie pueda acceder a ella, únicamente el navegador y el servidor web.

**Diferencias entre HTTP y HTTPS**

Los mensajes HTTP son de texto plano en donde las personas no autorizadas pueden acceder a ellos y leerlo fácilmente a través de internet, por otra parte HTTPS lleva todos los datos de forma cifrada.

**Ventajas y Desventajas de HTTP y HTTPS**

**HTTP**

|  |  |
| --- | --- |
| **VENTAJAS** | **DESVENTAJAS** |
| * Mayor velocidad de carga. | * La poca seguridad. |
| * Mejora del posicionamiento web. |  |
| * Priorización automática. |  |
| * Menos consumo de banda ancha. |  |
| * Presentación inmediata. |  |

**HTTPS**

|  |  |
| --- | --- |
| **VENTAJAS** | **DESVENTAJAS** |
| Mayor privacidad para los datos de los usuarios. | * Errores 404. |
| Genera confianza y credibilidad. | * Problemas de migración. |
| Aumenta la protección frente a ataques. | * Rendimiento web. |
| Mejora el SEO y aumenta el tráfico. |  |
| Favorece las ventas |  |

**Certificado SSL**

Un certificado SSL es un pequeño archivo de datos que vincula digitalmente una clave criptográfica con los datos de una organización. Una vez instalado en el servidor web, el certificado activa el candado y el protocolo https y, de esta forma, se habilita una conexión segura desde el servidor web hasta el navegador. Normalmente, el SSL se utiliza para proteger las transacciones con tarjeta de crédito, la transferencia de datos y los inicios de sesión y, más recientemente, se está convirtiendo en el estándar para proteger la navegación por redes sociales.