Estudiante: Jorge Isaac Vásquez Valenciano

Taller: Usos de funciones Hash en protocolos SSL, TLS y HTTPS.

Abordando el tema del HTTPS, SSL y TLS, se basará en responder la pregunta general que nos ayude a explicar rápidamente los términos importantes a conocer y la pregunta generadora:

- ¿Qué es SSL, TLS & ¿HTTPS?
- ¿Cómo funciona la tecnología SSL para proteger la información online e incrementar la confianza en los sitios web?

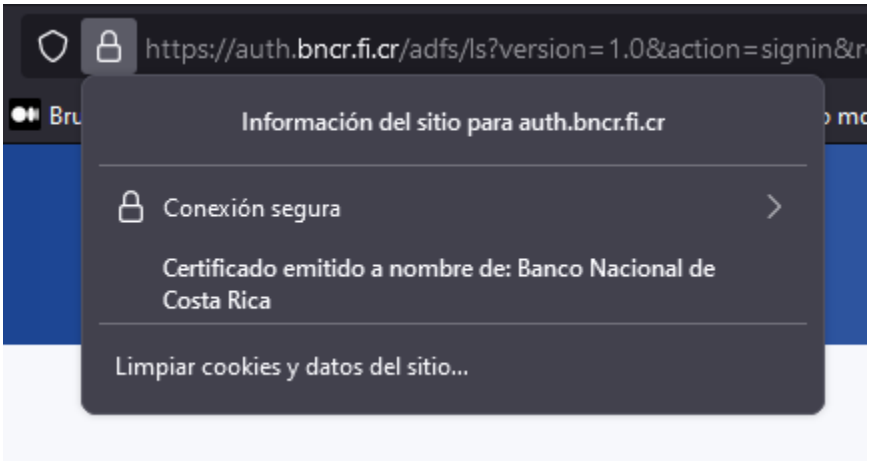


*Ilustración 1HTTPS, Asegurando la conexión*

Como Informático, El protocolo de transferencia de hipertexto seguro (de sus siglas en inglés, HTTPS), es algo del día a día, entramos a los bancos y lo primero que hacemos es verificar que sea una conexión segura, que esté vigente, que el firmante sea válido, etc. Desarrolladores de software, al crear una página web expuesta al internet, los primeros pasos en materia de seguridad es adquirir e instalar los certificados en los servidores para asegurar conexiones seguras.

Sin embargo, muchas veces, no entendemos la importancia de este certificado y la correcta implementación:

**SSL**: Capa de Conexión Segura, “es una tecnología estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web” (digicert, 2023). Cifrar el tráfico de datos

nos provee de una capa de seguridad de navegación para el usuario final, evitando que un tercero intercepte información que pueda ser sensible y robarla.

**SSL/TLS**: TLS, Capa de transporte seguro, es el sucesor del SSL, sin embargo, es más común escuchar o referirse como SSL.

Cuando se establece una conexión segura mediante SSL/TLS, el servidor web presenta un "certificado SSL" emitido por una autoridad de certificación confiable, “una entidad de confianza responsable de emitir y revocar los certificados digitales utilizados en las transacciones y firmas electrónicas” (Estudillo, 2022).

Este certificado contiene la clave pública del servidor y permite que el navegador establezca una conexión segura con el servidor mediante criptografía de clave pública y privada.

Para entender mejor el proceso podemos ver la siguiente imagen:


*Ilustración 2Modelo de ejemplo del SSL*

Como se puede notar, cuando el usuario entra a una página web, se realiza una petición de conexión por SSL al servidor, este responde con el certificado o llave pública para que se pueda establecer una comunicación segura. En el servidor se encuentra otra llave privada que se encargará de desencriptar la información para realizar las diversas transacciones correspondientes. Estas claves son normalmente encontradas en archivos PEM (*Privacy Enhanced Mail*) los cuales presentan encriptación en formato Base64 y están delimitados por "-----BEGIN" y "-----END" para identificar los diferentes componentes. Los archivos. PEM pueden contener tanto la clave privada como el certificado, o solo la clave privada, dependiendo si será transportada al usuario o no.

Es esencial proteger adecuadamente la clave privada del servidor, ya que su compromiso podría permitir a los atacantes interceptar y leer información sensible o incluso suplantar el servidor legítimo para llevar a cabo ataques de tipo "man-in-the-middle". Por esta razón, se aplican fuertes medidas de seguridad para salvaguardar la clave privada en un entorno seguro.

**HTTPS**: El HTTPS, es el indicador de que un sitio está protegido por un certificado SSL o SSL/TLS y sobre este se puede encontrar más información del certificado como de la entidad certificadora.

Finalmente, es por estos motivos: Encriptación y protección de datos del usuario al servidor y privacidad, que una página certificada y correctamente identificada con HTTPS generar confianza en el sitio y ofrecer una experiencia más segura al interactuar en línea. El uso de HTTPS se ha convertido en una práctica estándar para cualquier sitio web que maneje datos sensibles o realice transacciones, y es un componente clave para proteger la integridad de la información en el entorno en línea actual.

Bibliografía consultada

DigiCert, 2023, ¿Qué es SSL, TLS & ¿HTTPS? https://www.digicert.com/es/what-is-ssl-tls-and-http

Estudillo, M. (2022, 12 de Diciembre). ¿Qué es una Autoridad de Certificación? https://blog.signaturit.com/es/que-es-una-autoridad-de-certificacion