INFORME SSL.

APRENDICES:

Eduin Quintero

Jhoan Mena

Sebastián González

Sneyder Vergel

Sergio Calderon

Centro Electricidad, Electrónica y Telecomunicaciones.

ADSO

Instructora: Isaura Martínez Novoa.

2023

**¿Qué Es SSL?**

El Nivel de Conectores Seguros (Secure Sockets Layer o SSL) fue el protocolo de cifrado más ampliamente utilizado para garantizar la seguridad de las comunicaciones a través de Internet antes de ser sustituido por el TLS (inglés) (Seguridad de la Capa de Transporte, o Transport Layer Security) en 1999. Aunque el desuso del protocolo SSL dio paso a la adopción del TLS, la mayoría de las personas sigue refiriéndose a este tipo de tecnología como «SSL».

EL SSL proporciona un canal seguro entre dos computadoras o dispositivos que operan a través de Internet o de una red interna. Un ejemplo frecuente es el uso de SSL para proteger las comunicaciones entre un navegador web y un servidor web. Este protocolo cambia la dirección del sitio web de HTTP a HTTPS, donde «S» significa «seguridad».

El protocolo HTTP no es seguro, por lo que es susceptible de sufrir interceptaciones de intrusos, ya que los datos transferidos desde el navegador web al servidor web o entre dos terminales se transmiten como texto plano. De esta forma, los intrusos pueden interceptar y visualizar datos sensibles, como datos de tarjetas de crédito o de acceso a cuentas. Al enviar o publicar datos en un navegador que emplea HTTPS, el SSL garantiza que la información está cifrada y protegida frente a interceptaciones.

¿Cómo sé si un sitio web está protegido mediante SSL?

Desde el punto de vista técnico, el protocolo SSL es un método transparente para establecer una sesión segura que requiere una intervención mínima por parte del usuario final. En el caso de los navegadores, es posible determinar si un sitio web usa SSL cuando se muestra el candado o la barra de direcciones presenta la URL como HTTPS, en lugar de HTTP.

A continuación, se muestra un ejemplo de sitio web protegido mediante SSL en Chrome 56 y otro ejemplo de sitio web no protegido.



**¿Por qué necesito la seguridad SSL?**

Son muchas las transacciones y comunicaciones que realizamos cada día a través de Internet, por lo que usar SSL es en realidad lo más lógico. El SSL es compatible con los siguientes principios de seguridad de la información:

* Cifrado: protege la transmisión de datos (p. ej., de navegador a servidor, de servidor a servidor, de aplicación a aplicación, etc.).
* Autenticación: garantiza que el servidor al que se conecta es, en efecto, el servidor correcto.
* Integridad de los datos: garantiza que los datos solicitados o enviados son realmente los datos legítimos.

El SSL puede utilizarse para proteger:

* Las transacciones mediante tarjeta de crédito a través de Internet u otros pagos a través de Internet.
* El tráfico a través de una intranet, por ejemplo, una red interna, la función de compartir archivos, las extranets o las conexiones con bases de datos.
* Los servidores de correo web, como el acceso web a Outlook o los servidores Exchange y Office Communications.
* La conexión entre un cliente de correo electrónico como Microsoft Outlook y un servidor de correo electrónico como Microsoft Exchange.
* La transferencia de archivos mediante HTTPS y los servicios de FTP, como las actualizaciones de nuevas páginas por parte del responsable del sitio web o la transferencia de archivos de gran tamaño.
* Los accesos al sistema en aplicaciones y paneles de control como Parallels, cPanel y muchos otros.
* Los procesos de trabajo y la virtualización de aplicaciones como las plataformas Citrix Delivery o las plataformas de computación basadas en la nube.
* Los accesos y la actividad en paneles de control de hosting, como Parallels o cPanel, entre otros.

**¿Cómo funcionan los certificados SSL?**

Los certificados SSL funcionan garantizando que los datos transferidos entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita que los hackers la información que se envía a través de la conexión. Estos datos incluyen información potencialmente confidencial, como nombres, direcciones, números de tarjetas de crédito u otros detalles financieros.

El proceso funciona de la siguiente manera:

1. Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL.
2. El navegador o servidor solicita que el servidor web se identifique.
3. En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL.
4. El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web.
5. A continuación, el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL.
6. Los datos cifrados se comparten entre el navegador o servidor y el servidor web.
7. Este proceso a veces se conoce como “enlace SSL”. Aunque parece ser un proceso largo, se lleva a cabo en milisegundos.

Cuando un sitio web está protegido mediante un certificado SSL, en la URL aparece la sigla HTTPS (que significa HyperText Transfer Protocol Secure, protocolo de transferencia de hipertexto seguro). Sin un certificado SSL, solo aparecerán las letras HTTP, es decir, sin la S de “seguro”. También se mostrará un ícono de candado en la barra de dirección URL. Esto indica que se trata de un sitio web confiable y brinda tranquilidad a quienes lo visitan.

Para ver los detalles de un certificado SSL, puedes hacer clic en el símbolo de candado ubicado en la barra del navegador. Estos son algunos de los detalles que generalmente se incluyen en los certificados SSL:

* El nombre de dominio asociado al certificado emitido
* A qué persona, organización o dispositivo se emitió
* Qué autoridad de certificación lo emitió
* La firma digital de la autoridad de certificación
* Subdominios asociados
* Fecha de emisión del certificado
* La fecha de vencimiento del certificado
* La clave pública (no se revela la clave privada)