

SSL (Secure Sockets Layer) es un **protocolo de seguridad** que establece una **conexión cifrada** entre un **servidor web** y un **navegador web**. Su función principal es **proteger la privacidad y seguridad de la información** transferida entre estos dos sistemas.

Aquí tienes más detalles sobre los certificados SSL:

Autenticación de identidad: Un **certificado SSL** es un **certificado digital** que **autentica la identidad de un sitio web**. Esto significa que verifica que el sitio web es legítimo y pertenece a la entidad que dice ser.

Enlace cifrado: Cuando visitas un sitio web con un certificado SSL, se crea un **enlace cifrado** entre tu navegador y el servidor web. Esto garantiza que los datos transferidos entre ellos sean **imposibles de leer** para terceros malintencionados.

Protección de transacciones en línea: Las empresas y organizaciones deben agregar certificados SSL a sus sitios web para **proteger las transacciones en línea**. Esto incluye información como nombres, direcciones, números de tarjetas de crédito y otros detalles financieros.

Indicadores visuales: Cuando ves un **ícono de candado** junto a la **URL en la barra de direcciones**, significa que el sitio web está protegido por un certificado SSL. Además, la URL comienza con **"https"** en lugar de **"http"**. La **"S"** en **"https"** representa **"seguro"**.

En resumen, el certificado SSL mantiene seguras las conexiones a Internet y evita que los delincuentes lean o modifiquen la información transferida entre dos sistemas. [Aunque el término SSL se ha mantenido, la versión actualizada y en uso se llama TLS \(Transport Layer Security, Seguridad de capa de transporte\) 1234](#). ¡Así que la próxima vez que veas **"https"** y un candado, sabrás que estás navegando de manera segura!