## ¿Qué es SSL?

**SSL (Secure Sockets Layer, capa** de sockets seguros), es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente.

## ¿Qué es TLS?

El protocolo **TLS (Transport Layer Security, seguridad de la capa de transporte)** es solo una versión actualizada y más segura de SSL. Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

*“Los dos términos se utilizan con frecuencia indistintamente en la industria, aunque el término SSL sigue siendo el término mayoritario.”*

# ¿Cómo funciona protocolo de enlace de SSL/TLS?

Los protocolos SSL/TLS se utilizan para cifrar información entre dos puntos. Dichos puntos suelen ser el servidor y el cliente, pero en ocasiones es necesario cifrar entre dos servidores o entre dos clientes.

Un certificado **SSL se instala en el servidor** pero muestra indicaciones visuales en el navegador, lo que indica a los usuarios que se encuentran protegidos con SSL. Para empezar, **si en el sitio está presente SSL, los usuarios verán https://** al principio de la dirección web en lugar de http:// **(la "s" extra significa "seguro").**

## ¿Qué es HTTPS?

**HTTPS (Hyper Text Transfer Protocol Secure** o protocolo seguro de transferencia de hipertexto) aparece en la dirección URL cuando un sitio web está protegido por un certificado SSL. Los detalles del certificado, por ejemplo la entidad emisora y el nombre corporativo del propietario del sitio web, se pueden ver haciendo clic en el símbolo de candado de la barra del navegador.

Cuando se instala un certificado SSL en el servidor y un navegador se conecta a él, **la presencia del certificado SSL activa el protocolo SSL (o TLS),** que cifrará la información que se envía entre el servidor y el navegador (o entre servidores). El protocolo SSL funciona directamente encima del protocolo de control de transmisión (TCP) y actúa como una especie de capa de seguridad. Permite que las capas de protocolo superiores se mantengan sin cambios y, al mismo tiempo, se proporciona una conexión segura. Así, debajo de la capa de SSL, las demás capas de protocolo pueden funcionar con normalidad.

## Autoridades de certificación

*Las****autoridad de certificación****, o****certificadoras****, o las siglas****CA****(Certification Authority), señalan a una entidad de confianza, responsable de emitir y revocar los*[*certificados*](https://es.wikipedia.org/wiki/Certificado_digital)*, utilizando en ellos la*[*firma electrónica*](https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica)*, para lo cual se emplea la*[*criptografía*](https://es.wikipedia.org/wiki/Criptograf%C3%ADa)*de*[*clave pública*](https://es.wikipedia.org/wiki/Clave_p%C3%BAblica)*.*

*Jurídicamente, se trata de un caso particular de*[*Prestador de Servicios de Certificación*](https://es.wikipedia.org/wiki/Prestador_de_Servicios_de_Certificaci%C3%B3n)*. Una autoridad de certificación expide los certificados digitales, que ya contienen las identificaciones numéricas y las contraseñas que se necesitan, poniendo a disposición el procedimiento de verificación para validar el certificado proporcionado.*

Dicho **certificado es un documento electrónico** que contiene toda la información esencial: nombre del sitio web, dirección de correo electrónico de contacto e información de la empresa.

En la práctica**, un operador de sitios web obtiene un certificado pidiendo una solicitud de firma de certificado a un proveedor de certificados**.

## Negociación entre el servidor y el sistema cliente

Para que tenga lugar la negociación de SSL/TLS, el administrador del sistema debe preparar al menos dos archivos: la clave privada y el certificado Cuando se solicita a una autoridad de certificación, se debe crear un archivo adicional. Este archivo se denomina solicitud de firma de certificado, que se genera de la clave privada.

## Pasos de ejecución

1. El protocolo SSL comienza a actuar después de establecerse la conexión TCP e inicia lo que se denomina el protocolo de enlace de SSL.
2. El servidor envía su certificado al usuario junto con una serie de especificaciones, como la versión de SSL/TLS y los métodos de cifrado que se utilizarán.
3. A continuación, el usuario comprueba la validez del certificado, selecciona el nivel de cifrado más alto admitido por ambas partes e inicia una sesión segura con estos métodos. Hay una amplia variedad de series de métodos, denominados conjuntos de cifrado, con diferentes puntos fuertes.
4. Todo esto parece largo y complicado, pero en realidad se efectúa casi de manera instantánea.

### 1 CERTIFICADOS DE VALIDACIÓN DE DOMINIOS

Estos certificados solo requieren que los negocios demuestren su control sobre el nombre del dominio. El certificado contiene el nombre de un dominio que se proporcionó a la autoridad emisora como parte de la petición. Debido a que aquí no se comprueba la identidad de la organización, los certificados de validación de dominios son los certificados SSL de nivel más básico, y **son solamente adecuados para los servidores de pruebas y los enlaces internos.**

### 2 CERTIFICADOS DE VALIDACIÓN DE ORGANIZACIONES

Este certificado requiere no solo que el solicitante demuestre que es propietario del nombre del dominio que quiere que sea seguro, sino también **demostrar que su compañía está registrada y es legalmente responsable como negocio**. El certificado emitido es prueba de dominio y de nombre de la empresa. Este nivel de autenticación es adecuado para sitios web de cara al público que recogen datos personales de los usuarios del sitio. Tenga en cuenta que **las personas físicas no pueden obtener tales certificados, solo las organizaciones y empresas.**

### 3 CERTIFICADOS DE VALIDACIÓN EXTENDIDA

**Estos certificados requieren las dos validaciones anteriores, de dominio y empresa**, así como varios pasos de verificación adicionales relacionados con demostrar que el certificado SSL pertenece a una empresa registrada. Esta información extra de la empresa se representa luego en el certificado emitido en la barra de direcciones y puede accederse a él desde varios navegadores Web haciendo clic en el icono de un candado**. Este tipo de certificados solo están disponibles para organizaciones y empresas.**

**Si hay un elemento de comercio electrónico en el sitio, será obligatorio tener un certificado.**

## Wildcard SSL certificates

Tipo de certificado utilizado para que múltiples subdominos sean seguros.

Es posible que se deban instalar en el servidor unos certificados adicionales denominados certificados de autoridad de certificación intermedia y certificados raíz de autoridad de certificación. Eso depende también del software de servidor. En general, no hace falta instalar en los navegadores o las aplicaciones cliente los archivos de certificado de autoridad de certificación intermedia y de certificado raíz de autoridad de certificación (CA).

## Encriptación

## La encriptación de datos o cifrado de archivos es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes. Así, cualquier persona que no disponga de las claves correctas no podrá acceder a la información que contiene.

 Encontramos**dos tipos de encriptación de archivos**: simétrico o asimétricos.

El **sistema de cifrado simétrico** es aquel que utiliza una misma clave para cifrar y descifrar, mientras que, en la **encriptación de datos asimétrica** se usan diferentes claves: una clave pública para cifrar y una de carácter privado para descifrar, de forma que sea imposible deducir la contraseña privada a través de la pública.

Por tanto, encontramos diferentes niveles de seguridad con algoritmos, más o menos complejos.

# Criptografía asimétrica

Se trata de códigos que implican un par de 2 claves durante los procesos de encriptación y des encriptación. En el mundo de SSL y TLS se conocen como clave privada y clave pública.

Ventajas

## Compras seguras

Al igual que ocurre con cualquier compra, online o no, la mayoría de la gente preferirá comprar con un vendedor de confianza. Los certificados que demuestran autenticidad o especialización en un campo determinado contribuyen en gran medida a hacer sentir a los usuarios una mayor seguridad. La presencia del icono del candado en la barra de direcciones es también un gran indicador de seguridad. Proporciona una mayor confianza a los clientes de que su conexión es segura y está cifrada.

## Ofrecer subscripciones

Si un sitio ofrece la subscripción o cualquier otra operación que implique la recopilación de direcciones electrónicas u otra información confidencial, SSL es una buena idea. Siempre es buena idea mantener la información de los clientes de la forma más segura posible.

## Si se utilizan formularios

Lo mismo sucede si se utiliza cualquier tipo de formulario con el que los usuarios enviarán información, documentos o imágenes. Es sorprendente la cantidad de información que se recoge sobre los visitantes de una página web, así que vale la pena protegerla.

**Si se trata simplemente de un blog o un sitio informativo estándar**, HTTPS puede ayudar a proteger la seguridad de los sitios, reduciendo el riesgo de manipulación y de intrusos que añadan anuncios a la página para destruir la experiencia del cliente.

## SSL funciona en todos los dispositivos.

Son compatibles con todos los grandes sistemas operativos para ordenadores, tablets y móviles. Sin embargo, en el caso de los móviles, puede ocurrir que algunos dispositivos antiguos no sean compatibles con los protocolos SSL o TLS más nuevos. Del mismo modo que los sitios son creados para funcionar con todas las plataformas de navegadores, **los SSL/TLS** de un proveedor con buena reputación **funcionarán en el 99 % de los casos**.

## Servidores

Si el certificado está instalado correctamente, será compatible con cualquier servidor. Dependerá del navegador determinar si es de confianza o no durante el proceso del protocolo de enlace.

***“Google aboga ahora porque HTTPS o SSL se usen en toda la red y, desde el año 2014, el motor de búsqueda ha recompensado los sitios web seguros con posiciones mejoradas en la web, otra buena razón para que cualquier sitio instale SSL.”***