¿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.

¿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.

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").**

Niveles de autenticación de negocios

Las Autoridades de Certificación (CA) pueden autenticar la identidad del propietario de un sitio web, al igual que el cifrado, lo que añade otra capa de seguridad. El certificado SSL se utiliza luego como prueba de la identidad de una empresa**.**

## Los certificados pueden dividirse en tres grupos según el nivel de autenticación:

### 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

El certificado SSL de validación extendida ayuda a proteger a los usuarios de proporcionar sus datos a sitios web falsos que pueden ser posteriormente usados por delincuentes para estafas. **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. Al visitar un sitio con EV SSL, la mayoría de navegadores presentan una barra de direcciones de color verde como señal altamente visual de confianza de un sitio y empresa para gestionar la información personal**. Este tipo de certificados solo están disponibles para organizaciones y empresas.**

¿Cómo funciona un certificado SSL?

El principio básico es que, cuando 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); por supuesto, los detalles son un poco más complejos.

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.

**Si un certificado SSL se utiliza correctamente**, lo único que podrá ver un atacante será el puerto y las direcciones IP que están conectadas, y la cantidad aproximada de datos que se envían. Quizá sean capaces de cortar la conexión, pero el servidor y el usuario podrán percatarse de que esto se debe a un tercero. Sin embargo, como **el atacante no puede interceptar ningún dato,** esta acción no tiene prácticamente ninguna utilidad. Como la conexión está cifrada, la información importante queda a salvo.

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 Para garantizar la integridad y la autenticidad de todos los mensajes que se transfieren, los protocolos SSL y TLS también incluyen un proceso de autenticación que utiliza códigos de autenticación de mensajes (MAC, Message Authentication Code). Todo esto parece largo y complicado, pero en realidad se efectúa casi de manera instantánea.

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. Y, tal y como hemos dicho, hace que la gente esté más dispuesta a completar una transacción.

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

Gracias al modo en que funciona SSL, los servidores no necesitan tener certificados raíz integrados, pero sí que necesitará instalar el(los) certificado(s) intermedio(s) correspondiente(s). 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.”*

## ¿Qué es un error de conexión SSL?

Un error de conexión SSL ocurre cuando la página a la que se accede tiene problemas de seguridad. Estos errores ocurren para la protección de los usuarios, interrumpiendo el acceso para informar de que pueden producirse incidencias en la seguridad si continúan.

Pueden tomar varias formas, normalmente distintas en función del navegador elegido. En algunos casos, la página puede volverse roja con la introducción https:// también resaltada en rojo. Si se usa Google Chrome, hay varios mensajes que los usuarios pueden ver aparecer en su pantalla. Estos incluyen "su conexión no es privada" o simplemente, "esta página web no está disponible".

Pueden ocurrir como resultado de un código de seguridad caducado en el sitio web y no significan necesariamente que el sitio web accedido sea sospechoso.

Si durante las pruebas de desarrollo del sitio web se detecta que el sitio presenta errores de conexión SSL, entonces es imprescindible hacer algo al respecto. Esto puede incluir la actualización de la configuración de seguridad o simplemente adquirir un certificado SSL más adaptado. Esto ayudará a los navegadores a establecer que el sitio es seguro y permitirá a los usuarios el acceso sin avisos de seguridad.

## ¿SSL funciona con el correo electrónico?

La mayoría de los grandes proveedores de correo electrónico utilizan el cifrado SSL para cifrar los correos de los usuarios.

## Cómo implementar un certificado SSL en un sitio:

En función de cómo y dónde se hospeda un sitio, hay varias maneras de añadir un certificado SSL. En algunos casos, **si hay un elemento de comercio electrónico en el sitio, será obligatorio tener un certificado.** Los grandes proveedores de alojamiento ofrecen a menudo paquetes que incluyen certificados SSL.

## Autoridad de certificación (CA)

Entidad autorizada para emitir, suspender, renovar o revocar certificados bajo un CPS (Certification Practice Statement, Declaración de Prácticas con Certificados). Las CAs se identifican con un nombre distinguido en todos los certificados y CRLs que emiten. Una autoridad de certificación debe publicar su clave pública, o proporcionar un certificado de una CA de nivel mayor que testifique la validez de su clave pública si es subordinada a una autoridad de certificación primaria. DigiCert es una autoridad de certificación primaria (PCA).

## Wildcard SSL certificates

Tipo de certificado utilizado para que múltiples subdominos sean seguros.