Guía para principiantes sobre los certificados TLS/SSL

Cómo elegir la mejor opción para garantizar la seguridad en Internet

digicert®

Índice

Introducción

Tanto cuando actúa a título personal como cuando lo hace en nombre de su negocio, debería considerar la seguridad electrónica de forma análoga a la seguridad física de su casa o empresa. No solo sirve para hacer que se sienta más seguro; también protege a las personas que visitan su casa, su oficina o su sitio web. Es esencial conocer los riesgos que existen e implementar un sistema que lo mantenga totalmente a salvo. En este mundo tecnológico en que todo cambia con tanta rapidez, a veces no es fácil estar al día de los últimos avances, así que conviene dirigirse a una empresa de seguridad en Internet digna de confianza.

Esta guía aclara los aspectos tecnológicos de la seguridad electrónica y aporta la información necesaria para elegir la mejor solución a la hora de protegerse en Internet. Si desea consultar un glosario, vaya a la sección «Aclaración de tecnicismos» que aparece al final de este documento.

¿Qué es un certificado TLS/SSL?

Los protocolos de seguridad Transport Layer Security (TLS) y su antecesor Secure Sockets Layer (SSL) son los más utilizados hoy en día, principalmente con estos dos fines:

1. **Autenticación y verificación:** El certificado TLS/SSL contiene ciertos datos sobre la identidad de una persona, empresa o sitio web. Si una persona que está visitando su sitio web desea ver dicha información, solo tiene que hacer clic en el símbolo del candado o en la marca de confianza que aparece en el navegador (por ejemplo, el sello DigiCert® Secured o el sello Norton seguido del texto «powered by DigiCert»). La autoridad de certificación que emite el certificado es quien valida toda la información (con mecanismos más o menos estrictos que veremos después).
2. **Cifrado de datos:** El certificado TLS/SSL también permite cifrar los datos, lo que significa que la información confidencial que se intercambie mediante el sitio web solo será accesible por su legítimo destinatario.

Al igual que un pasaporte o un documento de identidad físico debe ser emitido por las autoridades competentes de cada país, los certificados TLS/SSL son más confiables si proceden de una autoridad de certificación (CA) de confianza. Dichas CA siguen normas muy estrictas a la hora de decidir si un solicitante puede obtener un certificado TLS/SSL o no. Así, cuando una empresa tiene un certificado TLS/SSL emitido por una CA con buena reputación, inspirará más confianza a sus clientes y socios.

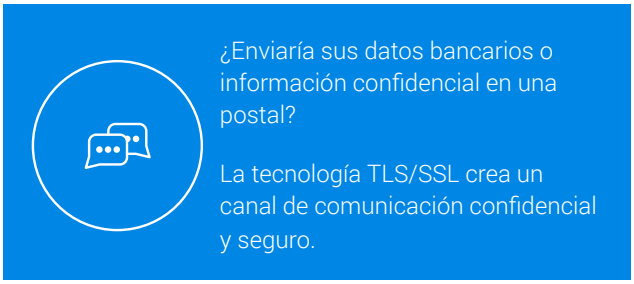
¿Cómo funciona el cifrado TLS/SSL?

Al igual que no se puede abrir una puerta sin la llave correspondiente, con el cifrado se usan claves para bloquear y desbloquear la información. Sin la clave necesaria, no se puede acceder a los datos.

Cada sesión TLS/SSL consta de dos claves:

- La clave pública, que permite cifrar los datos de forma que se vuelvan ininteligibles.
- La clave privada, que descifra la información y restablece su formato original para que se pueda leer.

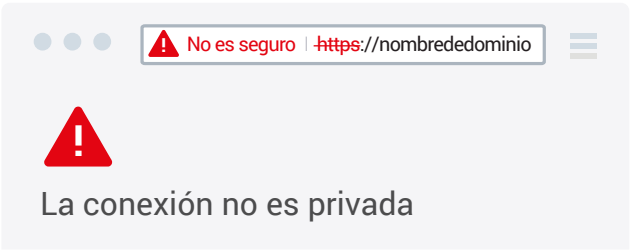
TLS/SSL hace referencia a los protocolos «Transport Layer Security» (seguridad de la capa de transporte) y «Secure Socket Layer» (capa de sockets seguros). Se trata de una tecnología que establece una conexión segura entre el sitio web y el navegador de la persona que lo visita, de forma que toda la información que se transmita se cifre y, por lo tanto, esté bien protegida.



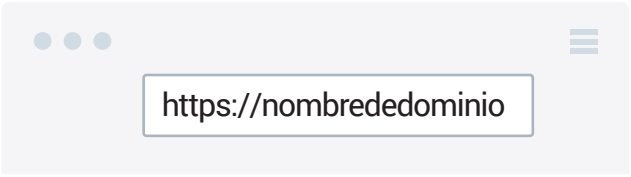
El proceso: Los certificados TLS/SSL se emiten para un servidor y un dominio web concretos (es decir, una dirección de sitio web) pertenecientes a una entidad que haya sido verificada por una CA. Cuando una persona accede a la dirección de un sitio web con un certificado TLS/SSL, el navegador y el servidor «se saludan»: se solicita una serie de datos al servidor que el visitante del sitio web podrá ver en el navegador. Hay una serie de cambios que indican que se ha iniciado una sesión segura. Por ejemplo, las marcas de confianza, en las que se puede hacer clic para ver información adicional, como el periodo de validez del certificado TLS/SSL, el dominio protegido, el tipo de certificado y la CA que lo ha emitido. Se establece una clave de sesión que garantiza la seguridad y, a partir de ese momento, la comunicación se lleva a cabo sin peligro alguno.

¿Cómo se sabe si un sitio web cuenta con un certificado TLS/SSL válido?

1. Cuando estamos en un sitio web estándar sin protección TLS/SSL, en la barra de direcciones del navegador aparece la indicación «http://» delante de la dirección del sitio web. Este acrónimo significa «protocolo de transferencia de hipertexto», una forma de transmitir información en Internet sin garantías de seguridad. En la actualidad, si una página web no tiene un certificado TLS/SSL bien instalado, la mayoría de los navegadores se lo indica a los internautas, que al saberlo pueden dar por terminada su visita.



En cambio, en los sitios web protegidos con un certificado TLS/SSL, la dirección aparece precedida de la indicación «https://», que significa «protocolo de transferencia de hipertexto seguro».



2. También aparece el símbolo de un candado en la parte superior o inferior del navegador (la posición varía en función del navegador que se use).

3. Con frecuencia, el sitio web también tiene una marca de confianza. Los clientes de DigiCert™ utilizan el sello DigiCert® Secured o el sello Norton seguido del texto «powered by DigiCert». Al hacer clic en el símbolo del candado o en cualquiera de las marcas de confianza de DigiCert (o con el texto «powered by DigiCert»), se ve la información del certificado con todos los datos de la empresa que la CA ha verificado y autenticado.

4. Al hacer clic en el candado o en algunas de las marcas de confianza TLS/SSL (p. ej., el sello DigiCert® Secure o el sello Norton Secured) que aparecen en el navegador, se ve el nombre de la empresa autenticada. En navegadores más seguros, dicho nombre se muestra claramente y la barra de direcciones o el texto pueden colorearse de verde cuando se detecta un certificado TLS/SSL con Extended Validation (EV). Si la información no coincide con los valores esperados o el certificado ha caducado, el navegador muestra una advertencia o un mensaje de error.

¿En qué casos resultan útiles los certificados TLS/SSL?

En pocas palabras, los certificados TLS/SSL se usan siempre que se quiera transmitir información de forma segura.

Por ejemplo, en los siguientes casos:

- Para proteger la comunicación entre su sitio web y el navegador de su cliente.
- Para garantizar la seguridad de la comunicación que se establece dentro de la intranet empresarial.
- Para proteger la información que se transmita entre servidores (tanto externos como internos).
- Para garantizar la confidencialidad de la información que se transmita mediante dispositivos móviles.

Tipos de certificados TLS/SSL

Actualmente existen distintos tipos de certificados TLS/SSL en el mercado.

- El primero es el certificado autofirmado. Como su propio nombre indica, se genera para fines internos y no es emitido por una autoridad de certificación. Dado que lo genera el propietario del sitio web, no tiene el mismo peso que un certificado TLS/SSL autenticado y verificado que haya sido emitido por una CA.
- El certificado de validación de dominio es un certificado TLS/SSL de nivel básico que se puede emitir con rapidez. Lo único que se comprueba es que el solicitante sea el propietario del dominio (o «dirección del sitio web») en el que quiera usar el certificado. No se toma ninguna medida más para garantizar que el propietario del dominio sea una entidad empresarial válida.
- El certificado TLS/SSL autenticado constituye el primer paso para garantizar por completo la seguridad en Internet e inspirar confianza. El proceso de emisión es un poco más largo y, para obtenerlo, el solicitante debe superar una serie de comprobaciones y procedimientos de validación que confirmen que la empresa existe, que es la propietaria del dominio y que el usuario está autorizado para solicitar el certificado.

Todos los certificados TLS/SSL de DigiCert son autenticados.

- Con frecuencia, se usa un nombre de dominio con varios sufijos de host distintos, así que se puede emplear un certificado con caracteres comodín que permite proteger con la tecnología TLS/SSL cualquier host de un dominio determinado: por ejemplo, host.su_dominio.com («host» varía, pero el nombre de dominio permanece constante).
- El certificado TLS/SSL SAN (nombre alternativo del sujeto) es similar al certificado con caracteres comodín, pero un poco más versátil, pues permite agregar más de un dominio en un solo certificado TLS/SSL.
- El certificado TLS/SSL con Extended Validation (EV) ofrece el nivel de autenticación más alto del sector y constituye la solución más eficaz para ganarse la confianza de los clientes. Al visitar un sitio web protegido con un certificado TLS/SSL con EV, la barra de direcciones de algunos navegadores se muestra de color verde y aparece un campo especial donde se indican los nombres del propietario del sitio web y del proveedor de seguridad que emitió el certificado. En la barra de direcciones también se indica el nombre del propietario del certificado y la autoridad de certificación que lo ha emitido. Gracias a estos distintivos visuales, los consumidores confían más en el comercio electrónico.

Aclaración de tecnicismos

Cifrado: Proceso que «desordena» la información de forma que solo pueda consultarla el legítimo destinatario.

Descifrado: Proceso que restablece el formato original de la información.

Clave: Algoritmo o fórmula matemática que se usa para cifrar y descifrar la información. Al igual que un candado resulta más difícil de abrir si tiene muchas combinaciones posibles, la clave de cifrado será más eficaz cuanto más larga sea, es decir, cuanto mayor sea el número de bits.

Navegador: Programa que permite acceder a Internet, como Microsoft Edge, Mozilla Firefox, Apple Safari y Google Chrome.

Conclusión

La confianza marca la diferencia en el mundo del comercio electrónico. Para que un sitio web tenga éxito —ya se trate de una tienda virtual o de una empresa que ofrece sus servicios por Internet—, es esencial invertir en tecnologías que protejan a los clientes y permitan ganarse su confianza. En este sentido, hay dos medidas de eficacia probada: implementar correctamente certificados TLS/SSL y colocar marcas de confianza en los lugares más indicados.

DigiCert, principal proveedor de certificados TLS/SSL del mundo en la actualidad, garantiza la seguridad de los clientes a la hora de hacer búsquedas, navegar, comprar o iniciar sesión en sitios web*. Protege más de un millón de servidores web en todo el mundo, más que ninguna otra autoridad de certificación*, y dos tercios de los certificados TLS/SSL con Extended Validation utilizados para proteger sitios web son suyos, incluidos los de las principales empresas de comercio electrónico y servicios bancarios.* Además, goza de un historial intachable como autoridad de certificación y cuenta con la marca de confianza más reconocida en Internet, dos ventajas importantísimas a la hora de proteger su sitio web y su reputación.

Si desea más información, visite https://resources.digicert.com/ssl-tls.

* Se incluyen las empresas subsidiarias de DigiCert o afiliadas a esta, así como sus distribuidores.

Si desea más información, envíe un mensaje a nuestros expertos en seguridad a contactus@digicert.com

América

Lehi, Utah (Estados Unidos)
2801 North Thanksgiving Way, Lehi, Utah 84043, Estados Unidos

Mountain View, California (Estados Unidos)
485 Clyde Ave., Mountain View, California 94043, Estados Unidos

Asia-Pacífico y Japón

Bangalore (India)
RMZ Eco World, 10th Floor, 8B Campus, Marathalli Outer Ring Road, Bangalore - 560103, India

Melbourne (Australia)
437 St Kilda Road, Melbourne, 3004, Australia

Tokio (Japón)
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokio 104-0061, Japón

Europa, Oriente Medio y África

Nieuwegein (Países Bajos)
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein, Países Bajos

Ciudad del Cabo (Sudáfrica)
Gateway Building, Century Blvd & Century Way 1, Century City, 7441, Ciudad del Cabo, Sudáfrica

Dublín (Irlanda)
Block 21 Beckett Way, Park West Business Park, Dublin 12, D12 C9YE, Irlanda

San Galo (Suiza)
Poststrasse 17, San Galo, Suiza, 9000

Londres (Inglaterra)
7th Floor, Exchange Tower, 2 Harbour Exchange Square, Londres, E14 9GE, Reino Unido

Malinas (Bélgica)
Schaliënhoevedreef 20T, 2800 Malinas, Bélgica

Múnich (Alemania)
Ismaninger Strasse 52, 81675 Múnich, Alemania

digicert®