“Certificación SSL”

Integrantes: Amairanis Saldaña
Agbert Pitty
Onesimo Arcia

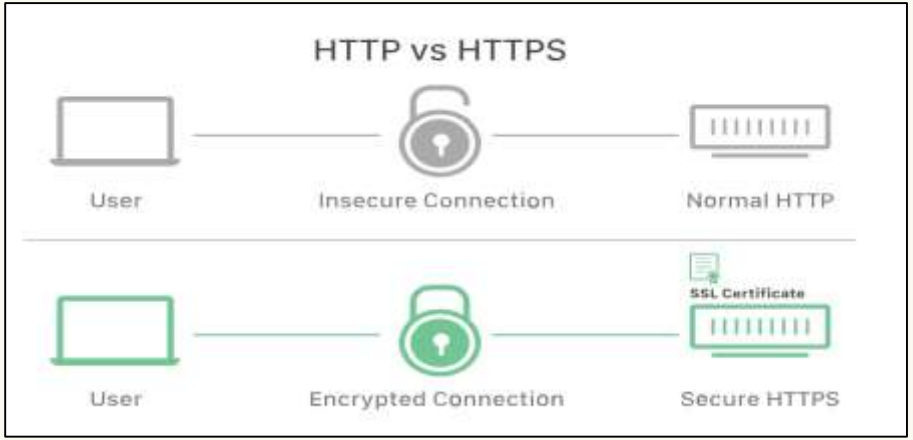
Taher Egmal

Historia

En el año 1994 Netscape, la compañía detrás del conocido navegador web Netscape, desarrolló SSL v2, un protocolo de cifrado diseñado específicamente para proteger las comunicaciones web. En marzo de 1995 este protocolo fue incorporado en el navegador Netscape Navigator 1.1. Esta fue la primera vez que se utiliza un protocolo de cifrado en un navegador.

¿Qué es un certificado SSL?

Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.



Características

Cifrado de Datos

SSL cifra la información transmitida entre el servidor y el cliente, lo que protege los datos sensibles de ser interceptados por terceros.

Autenticación:

SSL proporciona autenticación del servidor, asegurando que los usuarios se conecten al servidor correcto y no a un impostor.

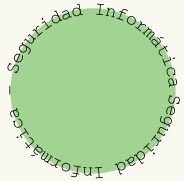
Integridad de los Datos:

SSL garantiza que los datos no sean alterados durante la transmisión. Esto se logra mediante el uso de códigos de autenticación de mensajes (MAC).

Compatibilidad

SSL es compatible con la mayoría de los navegadores y sistemas operativos, lo que facilita su implementación en diversas plataformas.

Proceso de Certificación SSL



- Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL.
- El navegador o servidor solicita que el servidor web se identifique.
- En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL.
- El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web.
- A continuación, el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL.
- Los datos cifrados se comparten entre el navegador o servidor y el servidor web.

¿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.

Ventajas de los certificados SSL

Protegen la información a través del encriptado

Los certificados SSL encriptan la información compartida entre sitios web y sus visitantes.

Elevan la confianza de los usuarios

Cualquier sitio web que recopile información personal debe tener un certificado SSL de forma obligatoria.

Elevan la confianza de los usuarios

Al adquirir un certificado SSL, automáticamente recibes un certificado de servidor que verifica la identidad de tu sitio web.

Ventajas de los certificados SSL

Ayudan al posicionamiento de tu sitio: los certificados SSL ayudan a aumentar la autoridad de un sitio web, por lo que es más probable que buscadores como Google ubiquen en una mejor posición a los sitios web cifrados en los resultados de búsquedas de usuarios.

Permiten aceptar pagos: el certificado de servidor es un requisito obligatorio para los servicios que utilizan datos personales y comerciales en internet, por lo que se deberá tener, uno si planeas aceptar tarjetas de crédito en tu sitio web o tienda en línea.

Protegen a los usuarios ante el robo de identidad: Cuando los usuarios visitan tu sitio no cifrado y ven la advertencia de “sitio no seguro o peligroso”.. ¡no es raro que inmediatamente se alejen de él!, con la protección de un Certificado SSL y el candado verde, tus visitantes y clientes potenciales se podrán sentir seguros de que la información que ingresen en cualquiera de tus páginas es privada y los estafadores cibernéticos no podrán verla.

Desventajas de los Certificados SSL

Costo: Cuando se hace negocios en línea, se es responsable por los datos financieros y personales de tus clientes, por lo que bien vale la pena invertir en un paquete de seguridad como los certificados SSL. Además, el costo de no hacerlo puede ser mucho mayor.

Difícil Instalación: Cuando estás iniciando tu camino en internet y no tienes conocimientos de programación, la tarea de instalar un certificado SSL puede ser un poco abrumadora.

Menor Rendimiento: Cuando se está iniciando el camino en internet y no se tiene conocimientos de programación, la tarea de instalar un certificado SSL puede ser un poco abrumadora.

Costos de Implementación y Asesoria

El costo de los certificados SSL puede ser un tema complejo. Los certificados SSL deben proteger toda la web, pero no todos los sitios web tienen las mismas necesidades. Por ejemplo, un blog personal no requiere el mismo nivel de seguridad que una gran tienda en línea.

Muchas personas nuevas en este tema creen equivocadamente que los certificados más caros brindan un mejor cifrado. Sin embargo, el precio no está relacionado con el nivel de cifrado, ya que todos los certificados SSL siguen el mismo protocolo universal, TLS (Transport Layer Security), para proteger la información sensible.

Por lo tanto, tanto los certificados SSL más económicos como los más costosos ofrecen el mismo nivel de protección, que en la actualidad es invulnerable con la tecnología disponible.

Factores que Influyen en el Precio de un Certificado SSL

•Tipo de validación

•Qué puede asegurar

•Funciones adicionales como sellos de sitio y garantías SSL

•Imagen de marca de las autoridades de certificación y del propio vendedor.

•Además, el mismo producto SSL le costará más si lo compra directamente a la autoridad de certificación en lugar de

El precio del certificado SSL varía en función de varios factores, entre ellos:

¿Cuánto cuesta un certificado SSL?

Coste del certificado SSL por validación

La validación SSL es lo primero que hay que tener en cuenta al elegir un certificado. También es uno de los principales factores que determinan el coste del SSL.

1. Certificados SSL DV (Validación de dominio) – *precios a partir* de 7,66 $ al año .
La Validación de Dominio sólo verifica la propiedad del dominio y proporciona confianza y características esenciales para el cliente. De ahí que sea la opción más común y barata. Es la elección perfecta para blogs, portafolios en línea y sitios informativos.

2.Certificados SSL BV (Business Validation) – *precios a partir* de 37,33 $ al año .
La validación empresarial verifica la situación jurídica de su empresa además de la titularidad del dominio. Proporciona una mayor garantía de que el sitio web es seguro y pertenece a una organización auténtica.

3.Certificados SSL con EV (Extended Validation) – *precios a partir* de 75 $ al año .
La Validación Ampliada comprueba la existencia física y jurídica de la organización, además de la VD y la VO. Es el nivel más riguroso de validación y, por tanto, conlleva el mayor grado de confianza, credibilidad y coste.

1.Los certificados SSL de dominio único son los más asequibles porque sólo cifran un dominio o subdominio.

2.Certificados SSL multidominio – precios desde sólo 21,66 $ al año .
Pueden asegurar hasta 250 SAN (Subject Alternative Names) adicionales bajo un mismo certificado. Su precio depende del nivel de validación y de la Autoridad de Certificación (marca).

3.Certificados comodín – precios a partir de 56,33 $ al año .
Son más caros porque codifican subdominios ilimitados junto con el dominio principal.

4.Certificados Wildcard multidominio – precios a partir de 150 $ al año .
Es un certificado híbrido que puede asegurar todos sus subdominios en múltiples dominios. Es más caro que los certificados Wildcard o Multidominio normales.

Precio del certificado SSL por dominio

Es un certificado híbrido que puede asegurar todos sus subdominios en múltiples dominios. Es más caro que los certificados Wildcard o Multidominio normales.

Coste del certificado SSL por firma

1.Certificados SSL para correo electrónico – precios a partir de 23,33 $ al-año .
Los certificados de correo electrónico firman digitalmente y cifran los mensajes de correo electrónico y sus archivos adjuntos, y tienen distintos precios para particulares, pequeñas y medianas empresas y empresas.

2.Certificados SSL de dirección IP – precios desde 44,43 $ al año

Están disponibles tanto para sitios web normales como para organizaciones registradas oficialmente que deben proteger una dirección IP pública. En función de sus necesidades, puede solicitar un certificado DV para proteger varias SAN o un certificado BV para cifrar una dirección IP.

3.Firma de códigos – precios a partir de 219 $ al año .
La firma de código añade una firma digital al software y las aplicaciones y verifica que el código incluido no ha sido alterado después de ser firmado.

Precios SSL por imagen de marca

1.El certificado Sectigo PositiveSSL más asequible de Sectigo(antes Comodo) cuesta 7,66 $ al año, mientras que el certificado Sectigo OV SSL Wildcard más caro cuesta 416,66 $ al año.

Ofrecen una amplia gama de productos SSL para todas las necesidades y presupuestos. Nadie iguala sus precios asequibles, e incluso tienen productos económicos EV y Wildcard multidominio.

2.El certificado SSL DigiCert Standard más asequible cuesta 216,66 dólares al año, mientras que el DigiCert Secure Site PRO Wildcard más caro cuesta 3.333,33 dólares al año.

DigiCert se centra en los mercados de alta seguridad, proporcionando soluciones BV y EV para grandes organizaciones y empresas.

La diferencia de precio entre los certificados de Sectigo y Digicert es enorme, pero ambas empresas prosperan.

Coste de SSL por funciones adicionales

1.Los sellos del sitio pueden ser estáticos o dinámicos; puede colocarlos en cualquier lugar de su sitio, incluidas las páginas de pago, las barras laterales y la zona del pie de página. Cuanto más popular sea la marca, más eficaz será el sello del sitio. Los certificados con sellos dinámicos cuestan más que los productos similares con sellos estáticos.

Por ejemplo, Sectigo Essential SSL**(16,66 $** al año) y Thawte SSL 123**(36,66 $ al año)** son certificados DV. Pero este último cuesta el doble que el primero por su sello de sitio dinámico y su reputación de marca.

2.Garantía SSL protege a los usuarios frente a posibles violaciones de datos. Aunque es muy poco probable que un atacante rompa el cifrado SSL, una CA puede emitir un certificado SSL de forma fraudulenta o por error al destinatario equivocado.

Los certificados de gama básica suelen tener garantías más reducidas que los de gama alta. La garantía SSL puede oscilar entre 10.000 y 2.000.000 de dólares en función del tipo de validación y de la autoridad de certificación.

Precio del certificado SSL por el vendedor

Puede comprar un certificado SSL en diferentes sitios, pero el más barato es un proveedor especializado en SSL como SSL Dragon. También llamado revendedor SSL, una empresa como la nuestra tiene asociaciones platino con las principales CA que nos permiten comprar certificados al por mayor a precios muy rebajados. Trasladamos el ahorro a nuestros clientes y les ofrecemos ofertas periódicas para que gasten lo menos posible.

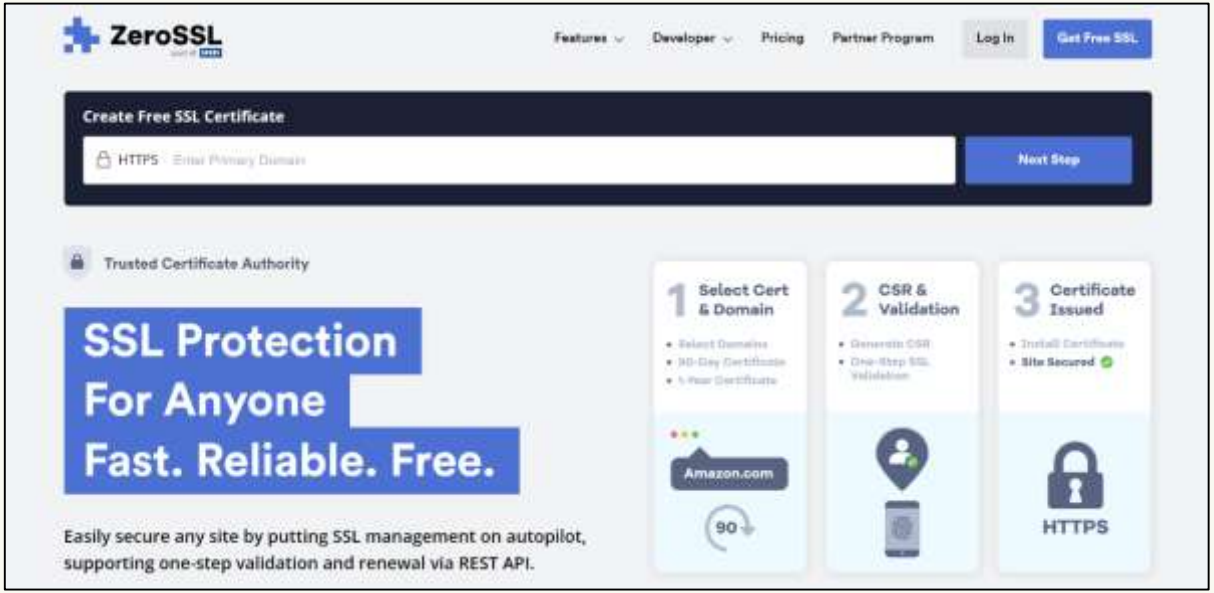
A diferencia de los distribuidores de SSL, las empresas de alojamiento, por ejemplo, venden los certificados SSL como un producto adicional a su producto principal. Ofrecen un precio competitivo para el primer año, pero la renovación del SSL es mucho más cara. Comprar directamente a la AC tampoco es una buena idea, ya que el precio es elevado.

Thawte Web Server EV cuesta sólo 170 dólares al año en SSL Dragon. El mismo certificado cuesta 398 dólares al año en el sitio web oficial de Thawte.

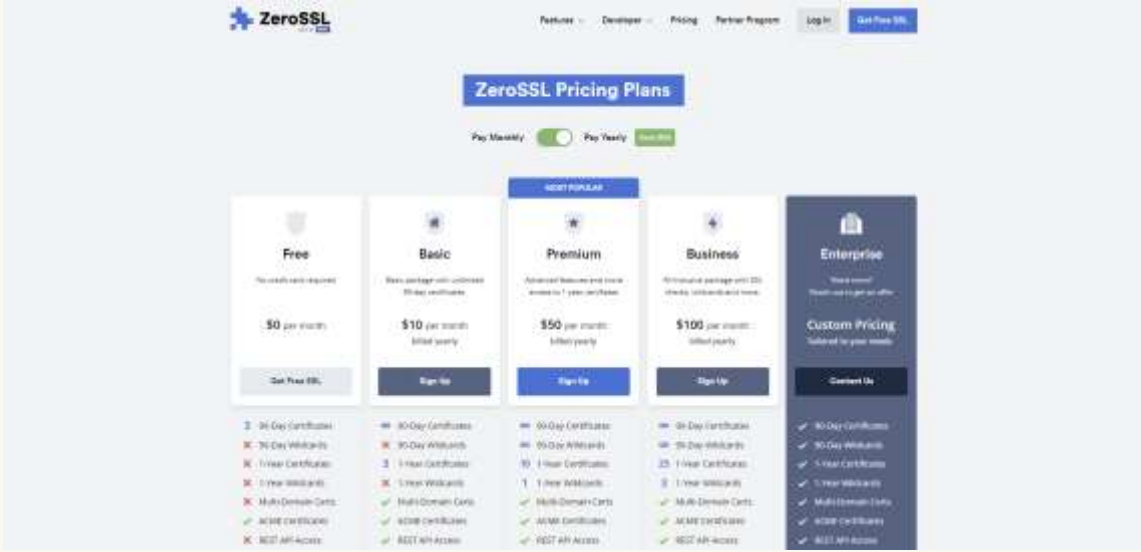
Adiestramiento y Certificaciones

Existen dos formas de conseguir un certificado SSL para tu sitio web, el primero certificarte con una empresa encargada de otorgar las certificaciones entre ellas tenemos:

- ZeroSSL
- Lets Encrypt
- SSL For Free
- SSL.com
- CloudFlare

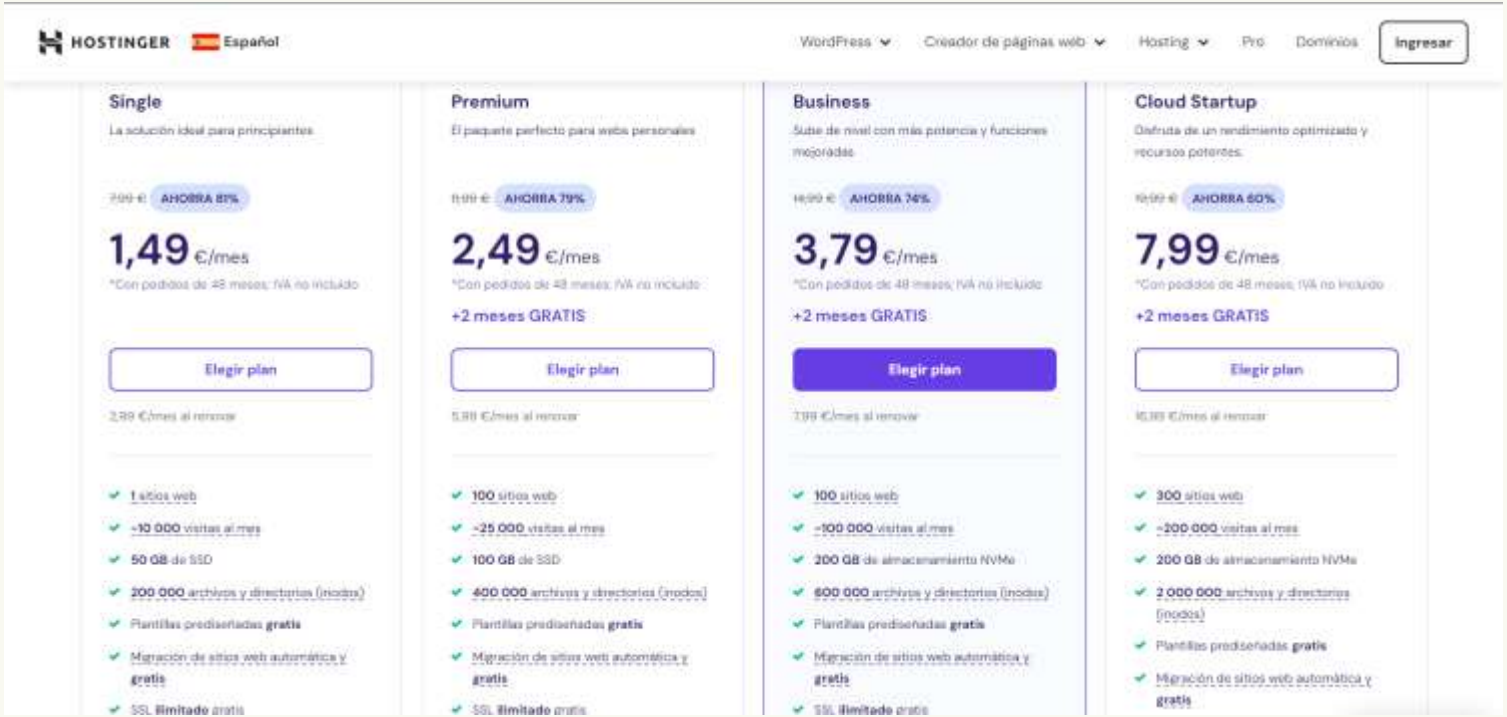


Adiestramiento y Certificaciones



Adiestramiento y Certificaciones

Seguridad Informática - Seguridad Informática



Todas estas empresas otorgan la certificación tras pasar por una estricta evaluación, cabe resaltar que estas certificaciones son gratuitas en cualquiera de estas plataformas.

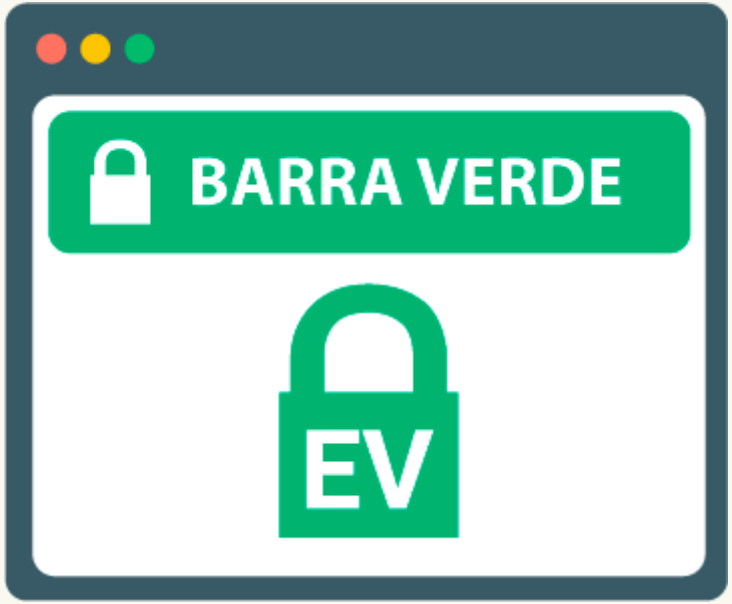
La otra forma de obtener una certificación SSL al comprar un hosting muchas de estas empresas ahorran el trámite de certificación y lo incluyen dentro del paquete al comprar el espacio de hosting.

Adiestramiento y Certificaciones

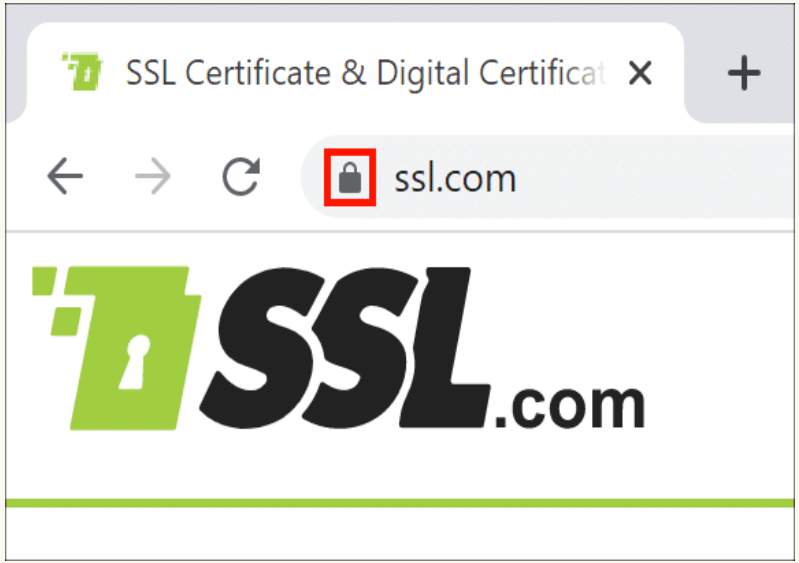
Seguridad Informática - Seguridad Informática

Tipos de Certificaciones de SSL

Existen diferentes tipos de certificados SSL con diferentes niveles de validación. Estos son los tipos principales:



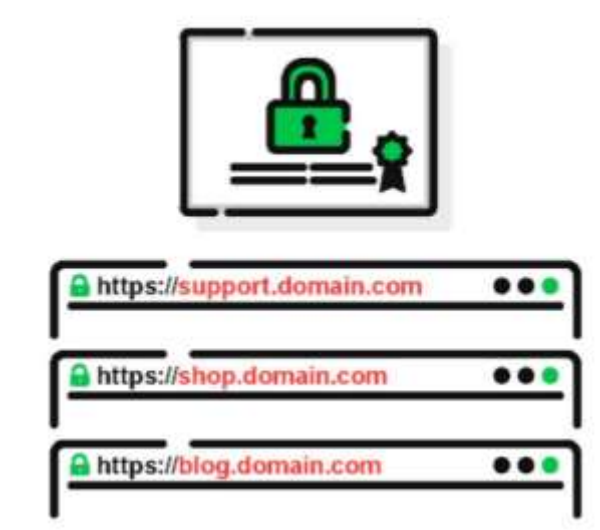
1. Certificados de validación extendida (EV SSL): Este es el tipo de certificado SSL de clasificación más alta y más costoso. Tiende a utilizarse en sitios web de alto perfil que recopilan datos e involucran pagos en línea. Cuando está instalado, este certificado SSL muestra el candado, la sigla HTTPS, el nombre de la empresa y el país en la barra de direcciones del navegador.



Certificados validados por la organización (OV SSL): Esta versión del certificado SSL tiene un nivel de seguridad similar al del certificado EV SSL, ya que para obtener uno el propietario del sitio web debe completar un proceso de validación sustancial. Este tipo de certificado también muestra la información del propietario del sitio web en la barra de direcciones para distinguirlo de los sitios maliciosos.

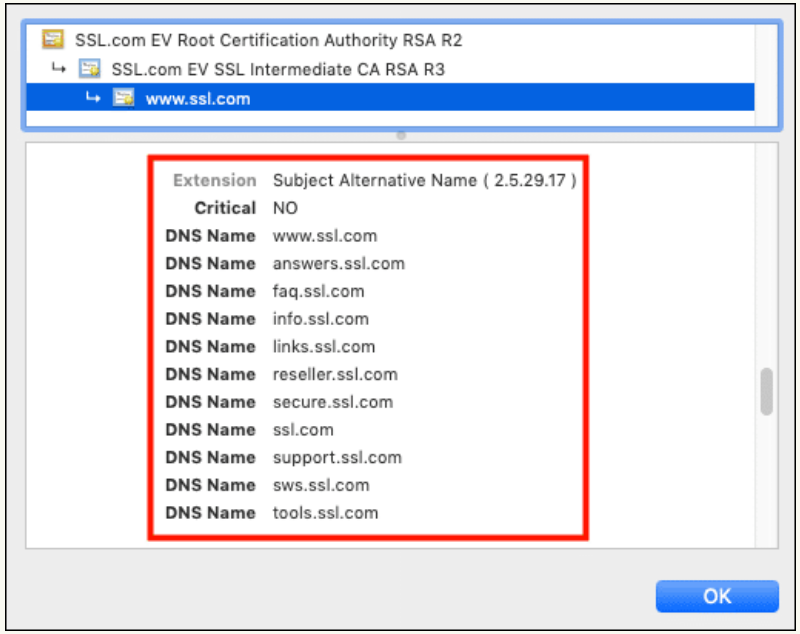
Certificados validados por el dominio (DV SSL):

El proceso de validación para obtener este tipo de certificado SSL es mínimo y, como resultado, los certificados SSL de validación de dominio proporcionan una menor seguridad y un cifrado mínimo. Suelen utilizarse en blogs o sitios web informativos, es decir, que no involucran la recopilación de datos ni pagos en línea.



Certificados SSL comodín: Los certificados SSL comodín te permiten proteger un dominio base y subdominios ilimitados en un solo certificado. Si tienes varios subdominios que proteger, la compra de un certificado SSL comodín es mucho menos costosa que comprar certificados SSL individuales para cada uno de ellos.

Certificados de comunicaciones unificadas (UCC): Los certificados de comunicaciones unificadas (UCC) también se consideran certificados SSL de varios dominios. Inicialmente, los UCC se diseñaron para proteger los servidores de Microsoft Exchange y Live Communications. Hoy, cualquier propietario de sitios web puede utilizar estos certificados para permitir que se protejan varios nombres de dominio con un solo certificado.



Cómo saber si un sitio tiene un certificado SSL

- La manera más fácil de ver si un sitio tiene un certificado SSL es mediante la barra de direcciones de tu navegador:
  - Si la URL comienza con HTTPS en lugar de HTTP, significa que el sitio está protegido mediante un certificado SSL.
  - Los sitios seguros muestran un distintivo de candado cerrado, en el que puedes hacer clic para ver los detalles de seguridad; los sitios más confiables tendrán candados o barras de dirección verdes.
  - Los navegadores también muestran señales de advertencia cuando una conexión no es segura, como un candado rojo, un candado que no está cerrado, una línea que pasa a través de la dirección del sitio web o un triángulo de advertencia en la parte superior del emblema del candado.

Conclusiones

una certificación SSL es esencial para cualquier sitio web que maneja información sensible. Ofrece seguridad, confianza y mejora el SEO. Es importante elegir el tipo de certificado adecuado y un proveedor confiable para garantizar la seguridad de tu sitio web.