

Instalación y uso de los certificados SSL

Guía para una seguridad sin fisuras





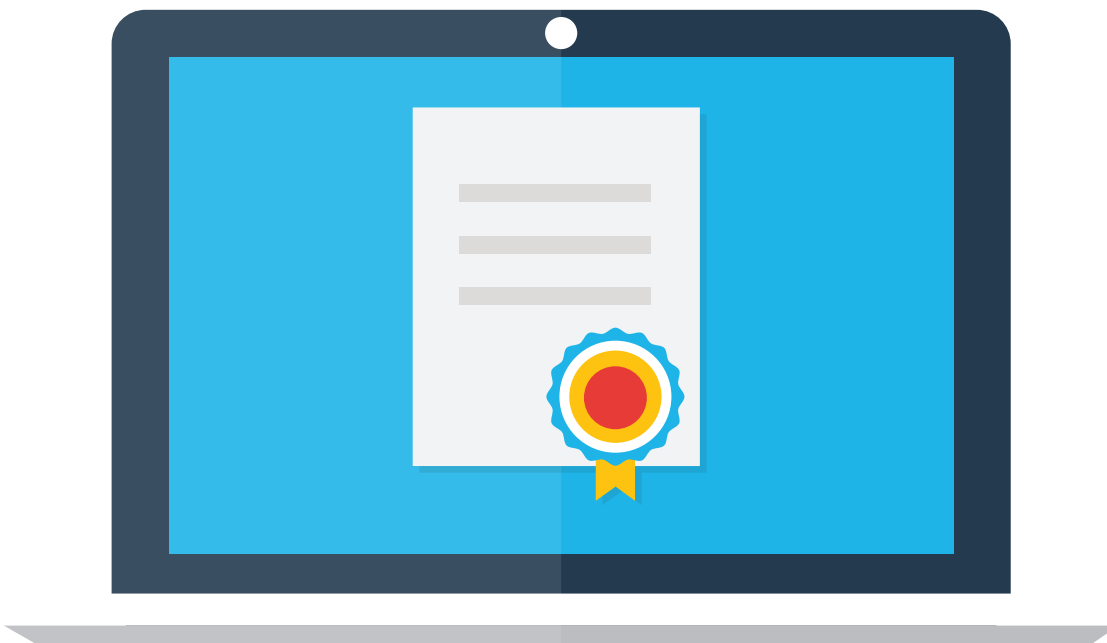
Ya ha dado el primer paso: comprar los certificados SSL.

Para proteger un sitio web, la compra de los certificados debe ir seguida de otros muchos pasos. Con demasiada frecuencia, los certificados no se instalan correctamente, se dejan desprotegidas páginas con información confidencial y no se cifran los datos facilitados en formularios. La consecuencia de estos descuidos es que numerosos sitios web son vulnerables a los ataques.

Por eso Symantec ha recopilado en esta guía una serie de consejos sobre cómo hacer las cosas bien desde el primer momento. En estas páginas le mostramos los peligros de las prácticas y procesos turbulentos que reducen la eficacia de la tecnología SSL y le ayudamos a salir de los terrenos más pantanosos, porque el certificado SSL es el pasaporte necesario para lograr un sitio web más seguro para su empresa, sus empleados y sus clientes.

Solo hay un modo de instalar los certificados SSL: seguir el proceso correcto

Como otras muchas empresas, también la suya es consciente de que es imprescindible comprar un certificado SSL y ha dado este importante paso, pero ahora tiene que asegurarse de que se instale correctamente. Recuerde que si los clientes no se sienten seguros en su sitio web, no querrán hacer ninguna transacción.





CONSEJO 1: Preparación de la clave privada y la solicitud de firma de certificado (CSR)



Antes de instalar un certificado digital, tiene que generar la clave privada y, con ella, la solicitud de firma de certificado (CSR) para el servidor en el que vaya a instalar el certificado. A continuación, se deberá enviar la CSR para firmar el certificado. Veamos cómo se hace.

Si tiene un servidor Redhat Linux o bien IIS 6 (o versiones posteriores), descargue el [asistente SSL de Symantec](#) y siga las sencillas indicaciones que le irá mostrando. En caso contrario, en nuestro sitio web encontrará las instrucciones sobre cómo [crear una solicitud de firma de certificado](#) en otros servidores. Para suscribirse a cualquiera de los servicios de certificados SSL que ofrece Symantec, necesitará la siguiente información:

- El periodo de validez del certificado: 1, 2 o 3 años
- El número de servidores en los que se aloja un solo dominio (hasta 5 servidores)
- La plataforma del servidor
- La empresa, el departamento y la dirección
- Los datos del pago y un contacto para la facturación
- El nombre común, es decir, el nombre del dominio y el host, como `www.midominio.com` o `webmail.midominio.com`
- Una dirección de correo electrónico a la que Symantec pueda escribirle para validar los datos
- Una solicitud de firma de certificado (CSR) generada desde el servidor que quiera proteger

Después, una vez haya recibido el certificado, siga las instrucciones del consejo 3.

Si su servidor no aparece enumerado en nuestras instrucciones o necesita más información, consulte la documentación de su servidor o póngase en contacto con el proveedor de este. Si no sabe qué software usa su servidor, pregunte al personal de TI.

A la hora de llevar a cabo la inscripción, envíe la CSR con el encabezado y pie que se indican a continuación:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



CONSEJO 2: Cómo instalar (bien) un certificado SSL



¿Va a instalar un certificado SSL por primera vez y la idea le asusta un poco? No se preocupe: es mucho más fácil de lo que piensa. Veamos cómo se instala un certificado de Symantec en un servidor.

Independientemente del tipo de servidor, el proceso consta de los siguientes pasos.

Paso 1: Guardar el certificado

Siga las instrucciones indicadas en el mensaje de correo electrónico de confirmación para guardar el certificado SSL en el escritorio desde la URL facilitada. De este modo, obtendrá tanto su certificado como los certificados de las AC intermedias.

Paso 2: Instalar o mover a una carpeta de certificados

Paso 3: Configurar el certificado en el sitio web

Paso 4: Dar un nombre de referencia al certificado

[Haga clic aquí](#) si desea obtener más información o instrucciones detalladas para cada tipo de servidor.

Para aprovechar al máximo el certificado SSL, no olvide colocar el sello Norton Secured en su sitio web. Así, sus clientes se sentirán más seguros al hacer transacciones con su empresa.

Solo tiene que copiar y pegar el texto que se indica en las páginas del sitio web de Symantec relativas al sello Norton Secured. Al final de esta sección encontrará un enlace a una serie de instrucciones muy claras sobre cómo colocar el sello en el sitio web y cómo comprobar que el certificado se haya instalado correctamente: basta escribir el dominio cuando se lo pida nuestra herramienta de validación (Certificate Installation Checker).

Ahora el certificado SSL está instalado y listo para cumplir su misión.

¿Necesita ayuda?

Symantec cuenta con una serie de vídeos tutoriales para diferentes servidores: [vea los tutoriales](#).

Comprobación de la instalación

Solo tiene que escribir la URL del servidor que desee comprobar: [compruebe la instalación](#).

Generación del sello para su sitio web

Siga las instrucciones de instalación del sello Norton Secured: [genere el sello](#).

Solución de problemas

Visite el sitio web de asistencia de Symantec: [acceda al servicio de asistencia](#).



CONSEJO 3: Cómo proteger las claves privadas y elegir las mejores



Las claves públicas y privadas son esenciales en el funcionamiento de la tecnología SSL. La clave privada, que se guarda en el servidor y se mantiene en secreto, permite cifrar toda la información del sitio web. La pública, por su parte, se encuentra dentro del certificado y constituye una parte más de la identidad del sitio web, como el nombre del dominio y los datos de la empresa.

Considere las claves privadas como recursos valiosísimos: revélelas a la menor cantidad posible de empleados y socios, y solo si son de su máxima confianza. Si usted fuera gerente de un banco, ¿dejaría a cualquiera las llaves de la cámara acorazada? Seguro que no, así que tenga en cuenta los siguientes consejos:

- **Genere las claves privadas en un servidor de confianza.** No deje esta tarea en manos de terceros.
- **Proteja las claves privadas con contraseña** para evitar problemas cuando se guarden en sistemas de copia de seguridad.
- **Renueve los certificados todos los años y**, cada vez que lo haga, cree nuevas claves privadas.

El tamaño de la clave privada influye muchísimo en el *handshake* (o protocolo de enlace) criptográfico que permite establecer conexiones sin riesgos. Si es demasiado corta, el nivel de seguridad será escaso, pero si es demasiado larga es posible que se ralenticen mucho las operaciones.

Cada vez se presta más atención a la criptografía de curva elíptica (ECC), que garantiza un alto nivel de seguridad con claves más cortas. De hecho, Symantec ofrece claves ECC que tienen muchísimos menos bits que las RSA y DSA pero resultan 10 000 veces más difíciles de descifrar (las claves ECC de 256 bits garantizan una eficacia criptográfica equivalente a la de las RSA de 3072 bits). En definitiva, la ECC brinda una mayor seguridad con una carga de trabajo mucho menor para el servidor y ayuda a reducir los ciclos de CPU necesarios para las operaciones de cifrado del servidor.

En la página 7 encontrará más información sobre la ECC.



CONSEJO 4: Eliminación de puntos vulnerables de la cadena



En la mayoría de los entornos de SSL, no basta con instalar un certificado en el servidor: se necesitan al menos tres para crear una cadena de confianza completa. Una cadena de certificados consta de todos los certificados necesarios para certificar el firmante identificado en el certificado final.

En la práctica, esta cadena abarca el certificado de entidad final, los certificados de las AC intermedias y el certificado de la AC raíz.

Para garantizar la autenticidad y validez de un certificado recién recibido, se deben comprobar todos los certificados, desde la AC raíz de confianza universal hasta el certificado nuevo (el «certificado de entidad final»), pasando por las AC intermedias. Un certificado solo será digno de confianza si forma parte de una cadena en la que todos y cada uno de los certificados se hayan emitido y validado correctamente.

Con frecuencia el certificado de entidad final está bien configurado, pero se ha olvidado incluir los certificados de las AC intermedias. Para garantizar que todos los certificados de la cadena se hayan instalado correctamente, utilice nuestra [herramienta de validación](#).



CONSEJO 5: RSA, ECC y por qué es importante la longitud de la clave



La criptografía de curva elíptica (ECC) permite a la empresa gozar de una mayor seguridad y un mejor rendimiento que los sistemas de cifrado actuales.

La ECC, un método de cifrado aprobado por el gobierno de Estados Unidos y avalado por la NSA (agencia de seguridad nacional estadounidense), crea un par de claves (la pública y la privada) definiéndolas como si se tratara de puntos de una curva. Con este sistema, resulta difícil robar las claves mediante los ataques de fuerza bruta que suelen lanzar los *hackers* y, además, es una solución más rápida que consume menos capacidad de procesamiento que el cifrado basado en RSA.

El algoritmo de firma digital y cifrado RSA ha sido la base de la seguridad en Internet durante casi dos décadas y sigue siendo válido, pero con el tiempo ha ido aumentando el tamaño mínimo que deben tener las claves para garantizar la protección frente a ataques criptográficos cada vez más avanzados. Con la tecnología ECC mejora el rendimiento, porque se consigue un nivel de seguridad superior con claves de menor longitud. Por ejemplo, una clave ECC de 256 bits resulta tan eficaz como una RSA de 3072 bits, lo que significa que se obtiene el nivel de protección necesario sin ralentizar el rendimiento.

Además, como las claves ECC son más cortas, también se reduce la dimensión de los certificados, lo que se traduce en un menor consumo de ancho de banda, un aspecto fundamental para mejorar la experiencia del cliente ahora que se está difundiendo el uso de dispositivos más pequeños para las transacciones online. Las raíces ECC de Symantec se usan en los tres principales navegadores desde el año 2007, así que nuestros certificados ECC funcionarán correctamente en su infraestructura actual, siempre que se utilicen navegadores modernos. Además, están disponibles sin coste adicional.

Consulte más información sobre la tecnología [ECC y la agilidad de los algoritmos](#).



CONSEJO 6: Protección total con Always-On SSL



Es fundamental cifrar con SSL todo el sitio web y, para ello, hay que optar por la tecnología Always-On SSL, un sistema de seguridad rentable que protege al usuario en todo momento, con lo que permite hacer búsquedas, compartir información y comprar online sin correr ningún peligro.

Las empresas que se tomen más en serio el cuidado de su reputación y la protección de los clientes adoptarán certificados con Always-On SSL emitidos por una autoridad de certificación de renombre, como Symantec. Esta medida de seguridad, que resulta muy fácil de implantar, autentica la identidad del sitio web y cifra toda la información que se intercambie entre este y el usuario (incluidas las *cookies*), con lo que impide que alguien no autorizado vea, manipule o utilice los datos.

Resulta significativa la siguiente recomendación de la Online Trust Alliance: «Always-On SSL es una medida de seguridad práctica y de eficacia probada que se debería implantar en todos los sitios web en los que los usuarios compartan o vean información confidencial».

De hecho, muchos de los sitios web con más éxito del mundo son conscientes de que conviene adoptar Always-On SSL para no caer en las redes del *hacking* o sufrir secuestros de sesión (también denominados *sidejacking*), pues esta tecnología protege ante amenazas como Firesheep o la inyección de código dañino.

Con Always-On SSL, le resultará más fácil conservar la confianza que los usuarios han depositado en su sitio web, pues sabrán que su empresa se toma muy en serio la seguridad y la confidencialidad y que adopta todas las medidas posibles para que no corran ningún peligro en Internet.



CONSEJO 7: Fijación de claves públicas, una cuestión de confianza



La fijación de claves públicas (o, más exactamente, la extensión de fijación de claves públicas para HTTP) se ha concebido con el objetivo de permitir a los operadores de sitios web restringir qué autoridades de certificación pueden emitir certificados para sus servidores.

A grandes rasgos, la fijación de claves públicas consiste en asociar un host con su clave pública o certificado previstos. Una vez conocida o vista la clave pública de un host, esta se asocia o «fija» al host en cuestión.

Según el CA Security Council, este sistema permite al propietario del sitio web especificar que su certificado SSL debe cumplir uno o varios de los siguientes requisitos:

- Tener una clave pública concreta
- Haber sido firmado por una AC con dicha clave pública
- Gozar de confianza jerárquica en una AC con dicha clave pública

Si un certificado destinado al dominio del propietario del sitio web es emitido por una AC que no esté enumerada (es decir, «fijada»), en los navegadores compatibles con la fijación de claves públicas aparecerá una advertencia de seguridad. Los propietarios de sitios web también pueden fijar varias claves procedentes de distintas AC, en cuyo caso los navegadores considerarán válidas todas ellas.

El propietario de un sitio web confía en que la AC elegida no emitirá por error un certificado para su dominio. Por lo general, las AC restringen quién puede solicitar la emisión de un certificado para los dominios de un propietario dado, lo que contribuye a evitar que se facilite un certificado a alguien no autorizado.

Por desgracia, el CA Security Council constata que la fijación de claves públicas adoptada por Google en 2011 no es escalable, pues exige añadir al navegador las claves públicas de cada dominio. Actualmente se está documentando una nueva solución escalable mediante una IETF RFC (petición de comentarios del grupo de trabajo de ingeniería de Internet).

Según esta nueva propuesta, las claves públicas fijadas se definirán mediante un encabezado HTTP desde el servidor hasta el navegador. Dicho encabezado puede contener datos como el algoritmo de clave SHA-1 o SHA-256, la edad máxima de la fijación, si admite o no subdominios y el nivel de rigor de la fijación.



CONSEJO 8: Uso de Perfect Forward Secrecy para ahuyentar a los intrusos



Imagínese que en este momento alguien está interceptando el tráfico de su sitio web. ¿Se le ha ocurrido pensar que tal vez un día pudiera descifrar los datos? Inquietante, ¿verdad? Pues quizá su empresa se encuentre precisamente en esa situación, aunque no sea en absoluto consciente del peligro.

Por ejemplo, RSA genera una clave pública y otra privada para cifrar y descodificar los mensajes. Sin embargo, como se usan constantemente claves recuperables, los datos cifrados almacenados corren peligro si alguien roba las claves en el futuro. En muchos casos, si un atacante intercepta tráfico SSL y consigue su clave privada, podrá usarla para descifrar todas las claves de sesión negociadas durante los handshakes SSL y, con ellas, acceder a todos los datos de la sesión. Desde luego, no es la situación ideal para dormir bien por las noches.

Lo bueno es que esta pesadilla se puede evitar: la solución se llama Perfect Forward Secrecy (o PFS) y consiste en generar claves de sesión temporales irrecuperables que se desechan una vez utilizadas. Además, si se implanta correctamente junto con la criptografía de curva elíptica (o ECC: véase Consejo 5), se logra un mayor rendimiento y un nivel de seguridad más alto del que ofrecen los algoritmos RSA.

Cuando se usa PFS, no hay ningún vínculo entre la clave privada del servidor y cada clave de sesión. Si tanto el cliente como el servidor admiten PFS, utilizan una variante de un protocolo llamado Diffie-Hellman (por los nombres de quienes lo inventaron), que consiste en el intercambio seguro de números aleatorios entre ambas partes para llegar al mismo secreto compartido. Con este inteligente algoritmo, aunque un intruso vea todo el tráfico, no tendrá acceso al secreto.

Si desea más información, consulte la siguiente infografía de Symantec:

[Ver infografía](#)



CONSEJO 9: Seguridad garantizada con HTTP Strict Transport Security



Gozar de la máxima seguridad en Internet es vital, y a veces para lograrlo no basta con cumplir unos requisitos mínimos: hay que llegar más lejos.

Los *hackers* en ocasiones usan herramientas como SSLstrip para lanzar ataques de interposición *man-in-the-middle* por redes inalámbricas, que les permiten interceptar solicitudes del navegador a sitios web HTTPS y devolver las páginas requeridas por HTTP. De este modo, la conexión deja de estar cifrada, con lo que el *hacker* puede interceptar los datos que la víctima facilite en el sitio web supuestamente protegido. Es fácil que el usuario no llegue a darse cuenta del cambio, pues no se fijará en la barra de direcciones del navegador cada vez que entre en una nueva página de un mismo sitio web. Los navegadores no saben si un sitio web se debe mostrar de forma segura, así que no avisan cuando se carga mediante una conexión sin cifrar.

Con el sistema HTTP Strict Transport Security (HSTS), este peligro no existe, pues los servidores envían un mensaje al navegador en el que piden que toda conexión sea cifrada. A continuación, el navegador actúa en consecuencia, con lo que todas las páginas que visiten sus clientes estarán cifradas. De este modo, tanto su empresa como los internautas estarán a salvo de los ataques.

Para activar la protección HSTS, hay que especificar en el sitio web un encabezado de respuesta única. A continuación, los navegadores compatibles con HSTS (como Chromium, Google Chrome, Firefox, Opera y Safari) respetarán sus instrucciones. Una vez activado, el sistema HSTS convierte automáticamente todos los enlaces sin cifrar en enlaces seguros, con lo que no permite que se establezcan comunicaciones desprotegidas con su sitio web.

Internet Explorer todavía no es compatible con HSTS, pero Microsoft ha declarado que a partir de la versión 12 sí admitirá esta tecnología.

© 2015 Symantec Corporation. Todos los derechos reservados. Symantec, el logotipo de Symantec, el logotipo de la marca de comprobación y el logotipo de Norton Secured son marcas comerciales o marcas comerciales registradas en los Estados Unidos y en otros países por Symantec Corporation o sus filiales. Los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.