¿Para qué instalar un certificado SSL?

escrito por Andy Garcia | 17/03/2016

Instalar un certificado SSL en tu web es fácil y gratis, pero… ¿cuándo es necesario o recomendable y cuál es la forma óptima de hacerlo?

El certificado de seguridad, más conocido como **certificado SSL**, permite que tu web encripte los datos que los usuarios envían o reciben, añadiendo una capa de seguridad, para evitar que esos datos pudieran ser interceptados.

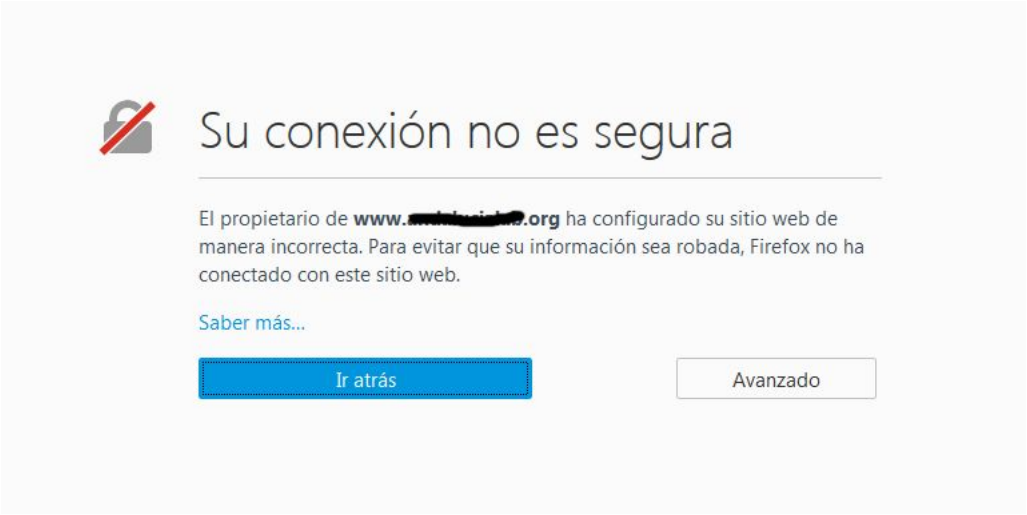
> *Si tu web tiene certificado SSL será visible a través del protocolo **HTTPS** (puerto 443), en lugar del protocolo **HTTP** (puerto 80).*

¿Cuáles son los tipos de certificados SSL?

1. Los autofirmados.
2. Los firmados por una autoridad de certificación, con validación de dominio(s) o subdominios wildcard.
3. Los firmados por una autoridad de certificación, con validación de empresa o validación ampliada.

> ***Casi todas las webs tienen un certificado SSL autofirmado instalado**, aunque el propietario ni siquiera lo sepa.*

Si entras en una web con certificado autofirmado, usando HTTPS, el navegador te avisará que la web no es segura, de la siguiente forma:



NOTA: En el caso anterior el usuario puede «*Añadir una excepción…*» y seguir navegando obviando la advertencia, pulsando el botón «*Avanzado*«.

Si entras en una web con certificado firmado por una autoridad de certificación, no recibirás la advertencia anterior, sin embargo, a la izquierda de la dirección de la web, podrás ver un candado que te indica su situación, en Firefox puede ser uno de los siguientes:

1. **Candado verde** indica que todo está configurado correctamente y todo el contenido de la web es seguro.
2. **Candado verde o gris con triangulo de advertencia** de color gris o amarillo, indica que el certificado SSL no ha sido instalado de forma optima en la web que estás visitando, la mayoría de las veces esta situación es debida a que hay elementos inseguros mezclados con los seguros, el responsable de la web debería corregir la situación.
3. **Candado gris** tachado con una línea roja, indica que has desactivado manualmente los avisos anteriores.

> *Tienes más información sobre el significado exacto de cada icono en la web de MOZILLA: https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure pero la regla general es que si el candado no es verde la web no es segura y no deberías enviar información sensible.*

Si tu web es WordPress, es posible que muchas imágenes usen el protocolo HTTP cuando el resto de la web usa el HTTPS, esto es debido a que WordPress por defecto usa URLs absolutas cuando insertas una imagen, para corregir esta situación sin modificar las URLs de todas las imágenes puedes usar el plugin: SSL Insecure Content Fixer y así evitar los triángulos de advertencias.

¿Cuándo deberías instalar un certificado SSL?

1. Si tu web es de comercio electrónico y tus usuarios te envían los datos de su tarjeta de crédito es **practicamente obligatorio** usar SSL y HTTPS.
2. Si tu web no es de comercio electrónico pero los usuarios se registran y posteriormente hacen login con su contraseña, es **muy recomendable** usar SSL y HTTPS.
3. Si tu web no es de comercio electrónico pero los usuarios envían datos a través de formularios de contacto, es **recomendable** usar SSL y HTTPS.

> *Desde un punto de vista SEO, ¿basta con instalar el certificado SSL y asegurarse de que luce el candado verde en todas las páginas de tu web? -la respuesta es un **NO** rotundo-*

Antes de instalar el certificado SSL, todas las URLs de tu web comenzaban por «*HTTP://*» y sin embargo ahora comenzarán por «*HTTPS://*«, es decir, trás la instalación del certificado SSL todas las URLs de tu web serán ahora diferentes, Google ya tenía indexadas todas las URLs con el protocolo «*HTTP*» y si no haces las redireciones 301 de todas las URLs de forma correcta **el posicionamiento y tráfico de tu web podría verse muy resentido durante un**

tiempo.

De la misma forma que todas las URLs de tu web han podido ser indexadas con www. al principio o sin www. al principio y tú puedes estar redirigiendo las URLs para que sólo una de las versiones sea visible y así evitar la percepción de contenido duplicado por parte de Google, ahora deberás hacer algo similar con HTTP o HTTPS.

Antes de hablarte de la forma correcta de redirigir las URLS HTTP a las correspondientes HTTPS para no perder visitas ni posicionamiento **conviene que te pares a pensar en la trascendencia del cambio que vas a hacer**, será más profunda mientras más antiguedad y cantidad de contenidos tenga tu web, por ese motivo es recomendable que hagas lo que sea necesario para que tu web funcione correctamente tanto en HTTP como en HTTPS, en el segundo caso con el candado verde limpio y también es conveniente asegurarse de que cada vez que haces un clic no salte de una versión a otra sino que si entras por HTTP permanezcas en HTTP en todas las páginas que visites y lo mismo con HTTPS.

Una vez conseguido esto, te estarás asegurando que si algo fallara con tu certificado SSL en el futuro, en cualquier momento podrías volver a mostrar tu web mediante HTTP, aunque en ese caso poco podrías hacer para evitar la pérdida de posicionamiento, así que **si tu web no necesita HTTPS piénsalo dos veces antes de dar ese paso**.

Si has llegado a este punto, estás seguro de que tu web necesita SSL o tú lo quieres instalar porque si, has instalado el certificado SSL gratis o no y todas las páginas de tu web lucen un bonito candado verde, puedes navegar sin saltar de una versión a otra, ahora te queda el último paso, que es **convertir la versión HTTPS en la versión canónica de tu web**, redirigiendo cualquier petición HTTP a la correspondiente HTTPS, ya será cuestión de tiempo

que Google actualice sus índices para indexar tus páginas HTTPS sin perder posicionamiento.

Si tu web es WordPress, desde el backend («*Ajustes/Generales*«) debes indicar cual es ahora la URL correcta de la raiz de tu sitio web, añadiendo la «S» al protocolo, como muestra la siguiente imagen:

El siguiente y último paso será añadir al archivo .htaccess, en la raiz de tu sitio web, las siguientes líneas de código para redirigir las páginas de HTTP a HTTPS y de «*sin www*» a «*con www*» (esto último en tu caso puede ser alrevés, es una decisión personal):

> *Hay más información disponible sobre redirecciones 301 en la guía definitiva de redirecciones 301 de* ***Tomas de Teresa***

Para terminar, piensa en los posibles servicios que pudieras estar usando en tu web, por ejemplo Google Analytics o Search Console, y dedícale unos minutos a revisar la configuración para modificar la propiedad de la URL añadiendo el protocolo HTTPS si fuera necesario.

No estaría de más poder comprobar la fecha de expiración, tipo de cifrado, posibles vulnerabilidades y otros detalles técnicos de cualquier certificado SSL instalado en cualquier dominio (por ejemplo puedes probar con el tuyo o incluso con el de tu competencia), usando alguno de los siguientes servicios web:

- https://certlogik.com/ssl-checker/
- https://www.digicert.com/help/

Y si quieres poder comprobar los certificados SSL de cualquier web mientras navegas por ella, te puede ser útil la siguiente extensión de firefox:

- Calomel SSL Validation