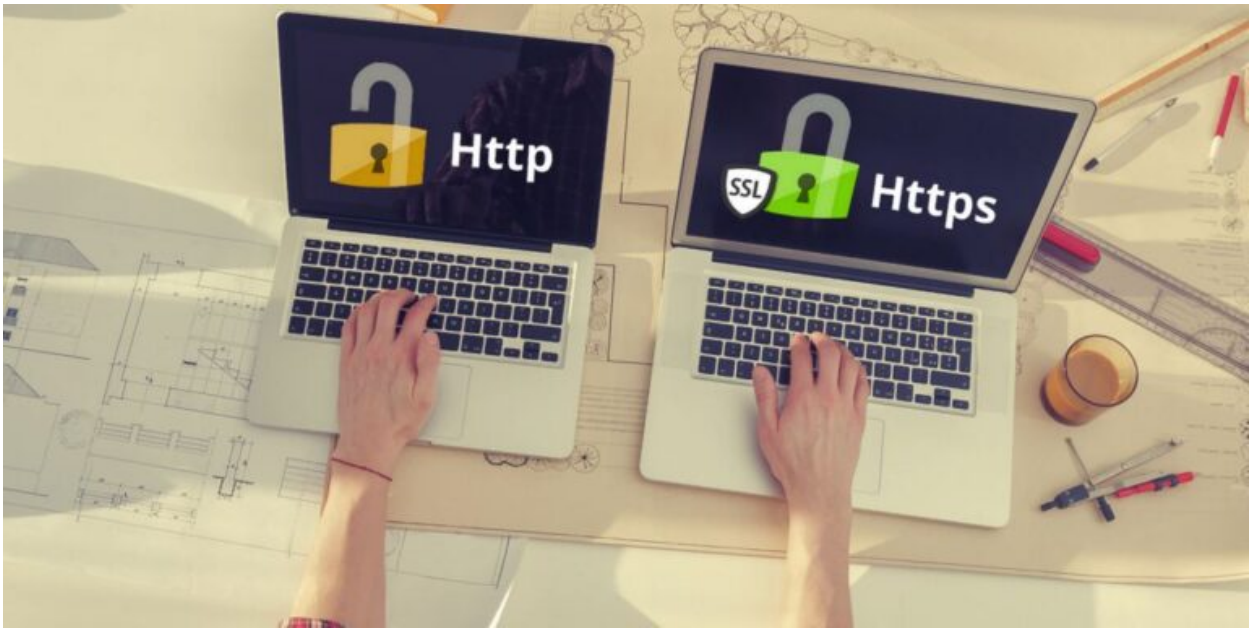
Mitos sobre las webs no seguras

escrito por Andy Garcia | 31/01/2017



Hoy es la fecha que Google anunció para marcar como «*no seguras*» las webs que no tuvieran el protocolo de seguridad HTTPS, mediante un certificado SSL…

- En realidad no es Google sino Chrome (que pertenece a Google) el que marca las webs como «*no seguras*«.
- En realidad no es a partir de una fecha sino a partir de una versión, la 56 de Chrome, disponible desde hace días.

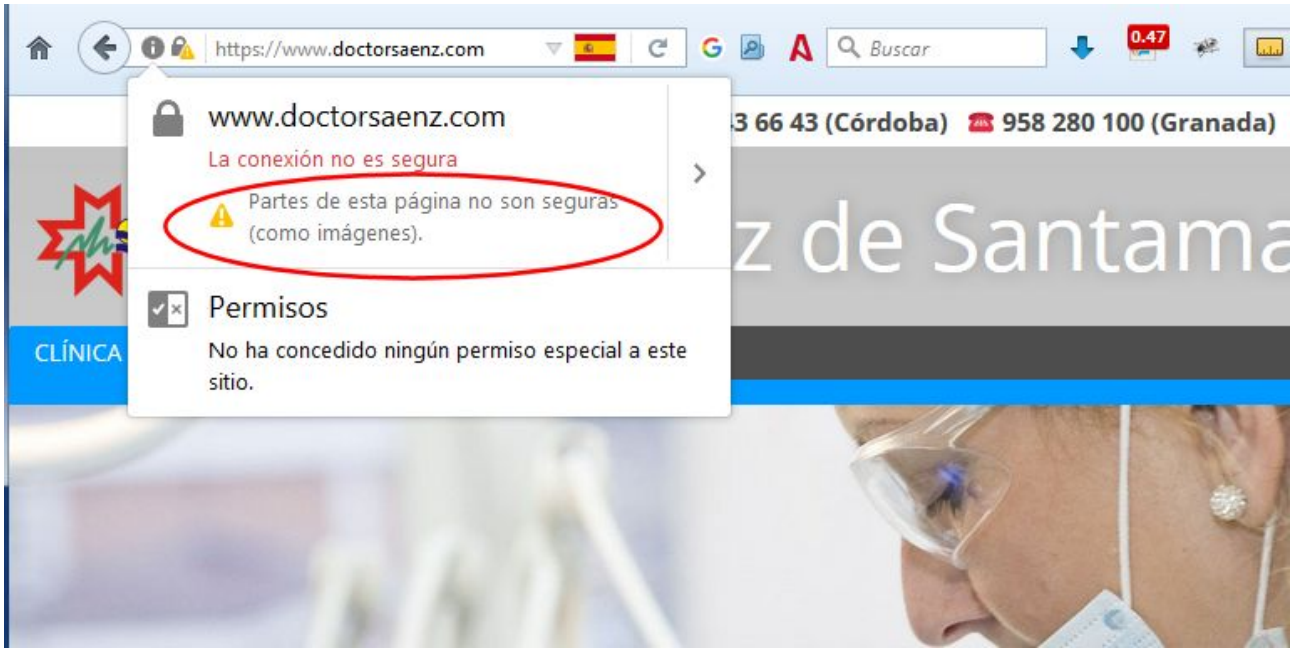
- En realidad no es sólo Chrome ya que Firefox también marca las webs como «no seguras» a partir de la versión 51.

- No basta con tener el certificado SSL instalado sino que hay que visitar la web con el «*protocolo https*«.
- No basta que el webmaster visite la web mediante https, sino que tiene que ser la versión por defecto.
- Si la web se marca como «*segura*» en realidad no significa que lo sea al 100%, sólo que utiliza

encriptación.

- No basta tener un cerficicado SSL instalado y configurado sino que tiene que ser emitido por un tercero.
- No es necesario pagar por un certificado SSL emitido por un tercero (ver SSL gratis en Plesk).
- El certificado SSL no hace la web más segura, tan sólo encripta la información que el usuario envía.
- Sólo si una página tiene un campo para enviar información sensible, por ejemplo una contraseña, será marcada como «*no segura*«.

- Si hay URLs absolutas dentro del código que usan el «*protocolo http*» serán marcadas como no seguras.
- Si ocurre lo anterior verás errores de «*código mixto*» que puedes solucionar convirtiendo las URLs afectadas.
- Para buscar y reemplazar todos los URLs absolutos «*http*» por «*https*» puedes usar el plugin Better Search Replace
- Si prefieres trucar los URL sin hacer cambios en la base de datos puedes usar el plugin SSL Insecure Content Fixer



Una vez instalado el certificado SSL emitido por un tercero y corregido los errores de código mixto, debes convertir tu web con protocolo https en la versión por defecto, para ello basta con añadir estas 2 sencillas líneas de código universal (valido con cualquier dominio o servidor, sin necesidad de adaptar ni modificar nada) en tu «*fichero .htaccess*«:

```
RewriteCond %{HTTPS} off
RewriteRule  ^(.*)$  https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Justo a continuación de esta línea:

```
RewriteEngine on
```

- También puedes activar una redirección permanente de «*http*» a «*https*» usando el plugin Easy HTTPS Redirection

Si tienes tu web con certificado SSL instalado y quieres comprobar que todo funciona correctamente puedes usar alguna de estas herramientas de testeo automático:

- https://www.ssllabs.com/ssltest/

- https://www.whynopadlock.com/

Si después de comprender todas las afirmaciones de este post no consigues desterrar los mitos o tienes alguna dificultad para que todo funcione correctamente, deja un comentario con el URL de tu web y le echamos un vistazo, nos encanta ayudar a los colegas.