Symantec. Website Security.
We go beyond

WHITE PAPER

2017: el año de los sitios web seguros

UN NUEVO CONCEPTO DE CONFIANZA

2017: el año de los sitios web seguros

En 2017, los navegadores harán cambios que afectarán la seguridad de los sitios web. En este artículo, le indicamos cómo prepararse y qué medidas tomar.

En 2014, la facturación global del comercio electrónico de la empresa al consumidor aumentó en un 24 %, hasta alcanzar la cifra de 1 943 000 USD, y se prevé que el comercio electrónico entre empresas alcance los 6,7 billones de dólares en 2020, según Ecommerce Europe[1]. Aunque no se dedique al comercio electrónico, hay otro dato importante: en el ámbito de los negocios B2B, el 83,4 % de las empresas consultan el sitio web de un proveedor antes de decidir si harán alguna compra.[2]

Los cambios normativos y su efecto en la confianza

La seguridad de los sitios web es más importante que nunca. En 2017, se impondrán normas más exigentes a las empresas. Si su sitio web provoca algún incidente de seguridad y llegaran a perderse datos de clientes, es posible que le culpen de ello. Todas las empresas, grandes o pequeñas, están obligadas a cumplir la normativa que protege la información personal identificable[3] y la aplicable al procesamiento de pagos con tarjeta de crédito[4]. Además, las que operan en la Unión Europea también estarán sujetas al reglamento general de protección de datos[5], que entrará en vigor el 25 de mayo de 2018.

En todos los sectores, el sitio web influye cada vez más en la imagen de la empresa, la interacción con los clientes y las transacciones que realizan. Para que inspire confianza y cause una buena impresión, es fundamental que quienes lo visitan sepan en todo momento que es seguro. Si un cliente recibe alguna advertencia que le haga sospechar que corre peligro, saldrá de inmediato del sitio web y la inversión que haya hecho su empresa para atraerlo habrá sido inútil.

Hoy en día, es más importante que nunca entender cómo están cambiando los navegadores y la seguridad en general, y cómo afecta todo esto a los sitios web, la normativa, la seguridad de los clientes y la confidencialidad de sus datos.

Por ejemplo, Google Chrome ya es el navegador mayoritario. Lo usan entre el 50 y el 65 %[6] de los equipos de sobremesa (el porcentaje varía según la fuente), por lo que el más mínimo cambio que haga Google puede tener una repercusión enorme en el funcionamiento de su sitio web.

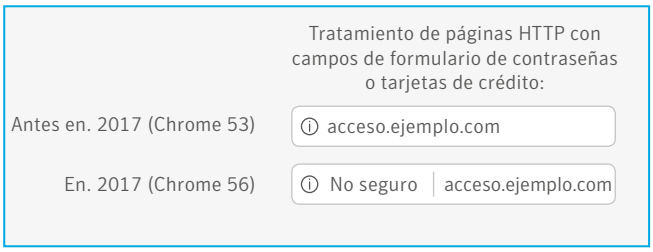
Chrome 56 (la última actualización de Google, disponible desde enero de 2017) cambia las reglas del juego.

Por qué afectarán a su sitio web los cambios de Chrome

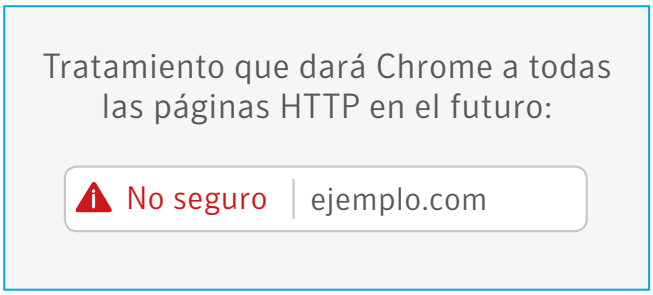
Google ha anunciado recientemente que Chrome 56, la última versión del conocidísimo navegador, contiene un cambio importante:

«A partir de enero de 2017 (en Chrome 56), marcaremos las páginas HTTP que recopilen contraseñas o tarjetas de crédito como no seguras, como parte de un plan a largo plazo que pretende calificar todos los sitios HTTP como no seguros»[7].

Esto significa que, ahora, las páginas HTTP del sitio web en las que se introducen contraseñas o datos de tarjeta de crédito tienen este aspecto:



Y eso no es todo. Como lo explica Google en su blog de seguridad[8], esta es solo la primera fase de un plan a largo plazo. En futuras versiones, el navegador mostrará estas advertencias en cada vez más páginas web. Más adelante, su intención es cambiar el icono por un llamativo símbolo de advertencia rojo.



¿Servirá esto para algo? Según las investigaciones de Google, en las que se basa su decisión, la respuesta es un «sí» rotundo. El estudio «Rethinking Connection Security Indicators» patrocinado por Usenix [9] recabó la opinión de 1329 personas a las que se formularon preguntas sobre el diseño de varias advertencias de seguridad. Se descubrió que, al ver un signo de exclamación en blanco y negro acompañado de la advertencia «No seguro» en la barra de direcciones de una página web:

- el 58 % de los encuestados no se sentían nada seguros en dicha página;
- al 51 % de los encuestados les preocupaba que alguien instalara malware en su PC, y el 37 % temían que les robaran lo que leían o escribían;
- el 58 % de los encuestados manifestaron que probablemente abandonarían el sitio web. Del 42 % restante que no abandonaría el sitio, el 16 % probablemente no introduciría los datos de su tarjeta de crédito.

Los resultados muestran claramente que ignorar la última actualización de Chrome podría perjudicar la reputación de su sitio web y el volumen de ventas.

Si su empresa se dedica al comercio electrónico, seguramente ya sepa que alrededor del 73,9 % de quienes compran por Internet abandonan el carrito de compras[10] antes de hacer el pago. Lo sorprendente es que, de este porcentaje, el 18 % lo hace porque desconfía del sitio web, según un estudio del Baymard Institute.[11] Este nivel de abandono y el consecuente deterioro de la confianza aumentarán cuando los navegadores empiecen a mostrar la advertencia «No seguro». Si se extrapola este efecto a todos los sitios web y operaciones de la empresa, las consecuencias podrían ser desastrosas.

Cómo mejorar la seguridad e inspirar más confianza

¿Qué significa todo esto para el sitio web de su empresa? Lo primero que debería hacer es trasladar todas las páginas en las que se recopile información de carácter personal (como contraseñas o datos de tarjetas de crédito) a una conexión cifrada y segura protegida con un certificado SSL/TLS emitido por una autoridad de certificación fiable.

Desde la perspectiva del usuario, una página en la que se utilice el protocolo seguro de transferencia de hipertexto (HTTPS) es idéntica a otra protegida con el protocolo de transferencia de hipertexto estándar (HTTP). Pero hay una diferencia fundamental: en una página HTTPS, toda la información intercambiada entre el emisor y el destinatario se cifra mediante un código acordado por el equipo local y el servidor del sitio web. Con este sistema, aunque un atacante logre acceder a la información que se transmite entre el sitio web y el usuario (por ejemplo, una contraseña o los datos de una tarjeta de crédito), no podrá descifrarla.

El proceso utilizado para crear el código, en el que profundizaremos más adelante, se conoce como «cifrado SSL». Al habilitarlo, la URL empezará por HTTPS en lugar de HTTP, y no aparecerá ninguna advertencia de seguridad. Además, en navegadores como Google Chrome o Mozilla Firefox, entre otros, los internautas sabrán que el sitio web es seguro porque aparecerá un candado verde a la izquierda de la dirección.

Cifrado Always-on

No solo es necesario cifrar las páginas del sitio web en las que haya formularios de introducción de contraseñas o datos de tarjetas de crédito. Para Google —como lo mencionábamos antes—, Chrome 56 es la primera fase de un «plan a largo plazo para marcar todos los sitios HTTP como no seguros».

No cabe duda de que, en el futuro, si alguien visita una página de su sitio web en la que se utilice una conexión HTTP, verá llamativas advertencias que le indicarán claramente el peligro que corre.

La importancia de la interactividad irá en aumento, y cada vez habrá más páginas en las que se pidan datos personales a los visitantes. Por ejemplo, en un sitio web de comercio electrónico podría haber reseñas de usuarios en todas las páginas de información sobre productos, y en el sitio web de una empresa habrá diversos formularios de consulta y contenidos de acceso restringido para cuya consulta se requieran determinados datos. En situaciones así, es más lógico usar el cifrado Always-on, que protege todas las páginas, que cifrar solo algunas y dejar otras desprotegidas.

Como lo mencionábamos antes, el cifrado SSL Always-on es mejor para los usuarios, ayuda a cumplir los requisitos de Chrome 56 y, presumiblemente, es más fácil de adoptar. Dado que todas las páginas estarán cifradas, los visitantes siempre se conectarán a los servidores a través de una conexión HTTPS segura. De este modo, ni Chrome 56 ni otras actualizaciones de Chrome que Google realice en un futuro inmediato afectarán negativamente a su sitio web.

Seis razones más para cifrar todo el sitio web

Chrome 56 es un motivo de peso para cifrar su sitio web, pero no el único. He aquí otras razones:

1. El cifrado facilita el cumplimiento de la normativa

Como bien saben los directivos de cualquier empresa, hoy en día un sitio web solo es seguro si cumple la normativa del sector y la legislación aplicable (por ejemplo, las leyes de protección de datos personales identificables, la normativa aplicable al procesamiento de pagos con tarjeta o el reglamento general europeo de protección de datos). Cada vez es más habitual que las infracciones y fugas de datos se sancionen con cuantiosas multas o acarreen responsabilidades civiles. Si se cifran las transferencias de datos, será mucho más difícil que alguien logre robarlos y, por lo tanto, la empresa correrá menos riesgos de recibir una multa.

2. El cifrado es más seguro para usted y para los clientes

Google quiere que la tecnología Always-on SSL se use en más sitios web por una razón muy simple: se trata de una opción mucho más segura tanto para el servidor en el que se alojan como para los navegadores de acceso. El cifrado Always-on SSL protege el sitio web frente a todo tipo de ataques de interposición «Man-in-the-Middle»[12]. Aplicarlo a todas las páginas no tiene por qué ser complicado; es falso que el rendimiento disminuya[13] y, además, si ya ha cifrado algunas páginas (p. ej., los formularios de contacto o de pago), solo tendrá que seguir el mismo procedimiento para ampliar la cobertura SSL a todas las demás.

Según las últimas investigaciones de IBM y el Ponemon Institute, el costo promedio por registro perdido o robado es de 158 USD[14], lo que puede tener graves consecuencias económicas para las empresas que almacenan grandes cantidades de datos importantes o personales. Según el mismo informe, una sola fuga de datos cuesta, en promedio, cuatro millones de dólares. Un sitio web mal protegido puede dar vía libre a un atacante para robar credenciales u otros datos, para infectar con malware los dispositivos y sistemas de los internautas o para sustraer datos confidenciales, como las contraseñas o los datos de tarjetas de crédito guardadas en los servidores web.

3. El cifrado da a los clientes una mayor sensación de seguridad

Si no cifra la conexión, cualquiera podrá interceptar la información transmitida a través del sitio web y cambiar los anuncios de la empresa por cualquier otro contenido publicitario o incluir enlaces infectados. Usted no se dará cuenta antes de que se lo adviertan los usuarios y, mientras tanto, es posible que su sitio web esté plagado de anuncios molestos o incluso ofensivos. En la mayoría de los casos, los internautas no acusarán al verdadero culpable, sino a su empresa. Si protege el sitio web con un sistema más completo que combine los certificados SSL/TLS con análisis periódicos, será más difícil que la publicidad dañina afecte a su sitio web.

4. El cifrado mejora el posicionamiento en los motores de búsqueda

Desde 2014, Google da un mejor posicionamiento[15] a las páginas web cifradas. La empresa no suele hacer públicas las variables utilizadas en sus algoritmos de posicionamiento, así que tome nota y aproveche esta información para aparecer antes que sus competidores en los resultados de las búsquedas de Google.

5. El cifrado ayuda a prepararse para el futuro

En 2015, el Internet Engineering Task Force o IETF (grupo de trabajo de ingeniería de Internet) publicó una nueva versión del protocolo de transferencia de hipertexto conocido como HTTP/2. Según el IETF[16], el protocolo HTTP/2 hace posible «un uso más eficiente de los recursos de la red», lo que significa que está diseñado para mejorar la rapidez y la capacidad de respuesta de los sitios web que lo utilizan. Pero, por el momento, los principales navegadores solo admitirán HTTP/2 en conexiones SSL/TLS[17], así que solo podrá sacar partido al nuevo protocolo si todo el sitio web está protegido con HTTPS.

Seis razones más para cifrar todo el sitio web

A menudo, tras la negativa de adoptar el cifrado SSL se esconde el miedo a que empeore el rendimiento del sitio web. Sin embargo, si se combina con el protocolo HTTP/2 y un servidor web moderno, una conexión HTTPS es mucho más rápida que una página web HTTP estándar, como lo demuestran las pruebas publicadas en Internet[18]. Dado que HTTP/2 solo puede utilizarse con el cifrado Always-on, observará una diferencia de velocidad notable.

Además, según Google[19] , Chrome ya solo permite usar las siguientes funciones web con una conexión HTTPS (o bien lo hará pronto):

- Geolocalización
- getUserMedia()
- HTTP/2
- Notificaciones Push

} Solo disponible en Chrome con HTTPS

- AppCache
- Extensiones multimedia cifradas

} Incompatibles con HTTP próximamente

A la hora de adoptar el protocolo HTTP/2, Smashing Magazine[20] recomienda lo siguiente:

- usar la tecnología Always-on en el sitio web de la empresa para que las conexiones sean seguras;
- reducir el número de solicitudes HTTP (por ejemplo, convirtiendo en stripes varios archivos de imagen y concatenando archivos CSS y de JavaScript);
- repartir los recursos entre los hosts (lo que se conoce como particionado o sharding);
- actualizar el diseño del sitio web de manera que incorpore el protocolo HTTP/2;
- someter a examen el alojamiento (incluidos los certificados SSL que utiliza);
- hacer un seguimiento de las estadísticas para saber a cuántos visitantes beneficiaría el cambio.

6. El cifrado puede hacer más competitiva a su empresa

Según Google, en la actualidad más del 50 % de todas las páginas cargadas en Chrome desde equipos de escritorio usan HTTPS[21], un número que aumentará con la llegada de Chrome 56 en enero.

Si aún no usa el cifrado SSL en su sitio web, ahora es el momento de solucionarlo. Cifrar sus páginas web le ayudará a ponerse al día y a ganar terreno a empresas más rezagadas que aún no hayan dado el paso.

Cómo cifrar su sitio web

Según un estudio de Sandvine, casi el 40 % del tráfico de bajada de Internet en Estados Unidos está cifrado[22]. Ahora le ha llegado el turno a su sitio web.

Antes que nada, adquiera un certificado SSL/TLS con Extended Validation (EV) o con validación de empresa (OV) de un proveedor fiable. Los certificados SSL con validación de dominio (DV) suelen ser más baratos que los certificados SSL con Extended Validation (EV), pero no son seguros porque los ciberdelincuentes pueden adquirirlos fácilmente.[23] Los internautas más experimentados ya lo saben, y por eso prefieren navegar en sitios web que, al estar protegidos con certificados SSL con EV, se han sometido a procesos de validación y autenticación más rigurosos.

En su sitio web, Symantec ofrece varias opciones de certificación SSL, para que clientes como usted elijan la que mejor se adapte a sus necesidades[24]. Por ejemplo, los certificados con criptografía de curva elíptica (ECC) son adecuados para empresas que, bien por preferencia propia o por imperativo legal, necesitan un nivel de seguridad más elevado[25].

Una vez comprado el certificado, solo le quedará instalarlo y activarlo. El procedimiento depende del tipo de alojamiento del sitio y de cómo funcione. El equipo técnico de Symantec le indicará qué pasos seguir, pero también puede consultar las instrucciones detalladas de Google[26] o descargar las versiones beta[27] de Chrome para ensayarlas.

En cuanto active el certificado, el tráfico del sitio web estará cifrado, de acuerdo con los requisitos de Chrome 56. A partir de ese momento, además de redirigir los enlaces de sus páginas a su equivalente HTTPS, tendrá que hacer un seguimiento de los certificados SSL y renovarlos antes de que caduquen. Symantec cuenta con herramientas de detección automática[28] que permiten hacer todo esto de manera sencilla, rápida y eficiente.

No espere más

Si su sitio web puede cumplir ahora los requisitos del nuevo Google Chrome 56, ¿por qué esperar más tiempo? Las ventajas de adoptar el cifrado Always-on en todas sus páginas superan ampliamente los posibles inconvenientes. En un mercado digital cada vez más competitivo y con una mayor dependencia de los datos, las empresas que den prioridad a la seguridad, la confidencialidad y la confianza de los clientes jugarán con ventaja.

[1] https://www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014
[2] https://www.accenture.com/gb-en/insight-state-b2b-procurement-study-uncovering-shifting-landscape
[3] http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information
[4] https://www.pcicomplianceguide.org/pci-faqs-2/
[5] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[6] https://en.wikipedia.org/wiki/Usage_share_of_web_browsers
[7] https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html
[8] https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html
[9] https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf
[10] https://blog.salecycle.com/stats/infographic-remarketing-report-q3-2016/
[11] https://baymard.com/checkout-usability
[12] http://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM
[13] https://www.maxcdn.com/blog/ssl-performance-myth/
[14] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
[15] https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html
[16] https://tools.ietf.org/pdf/draft-ietf-httpbis-http2-17.pdf
[17] https://www.mnot.net/blog/2015/06/15/http2_implementation_status
[18] http://www.httpvshttps.com
[19] https://www.youtube.com/watch?v=e6DUrH56g14
[20] https://www.smashingmagazine.com/2016/02/getting-ready-for-http2/
[21] https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html
[22] https://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html
[23] https://www.symantec.com/connect/blogs/dangers-domain-validated-ssl-certificates
[24] https://www.symantec.com/en/aa/ssl-certificates/
[25] https://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa
[26] https://developers.google.com/web/fundamentals/security/encrypt-in-transit/enable-https?hl=en
[27] https://www.google.co.uk/chrome/browser/beta.html
[28] https://www.symantec.com/page.jsp?id=ent-ssl-automate-discover

Symantec. Website Security.
We go beyond

Symantec™ Complete Website Security

Armonice y refuerce la seguridad de los sitios web

Symantec™ Complete Website Security puede ayudar a reforzar la seguridad de los sitios web; a evitar o minimizar los daños provocados por las amenazas avanzadas, que aumentan constantemente; a liberar recursos para destinarlos a tareas más estratégicas; a simplificar la protección de los sitios web; y a administrar la empresa e impulsar su expansión sin temer por su seguridad.

Para abrir una cuenta o solicitar más información sobre lo que puede hacer Symantec™ Complete Website Security por su empresa, póngase en contacto con nosotros.

Llame al:
América Latina: +1 520 477 3111
Correo electrónico: ssl_info@symantec.com
Si desea los números de teléfono de algún país en particular, consulte nuestro sitio web.

Para recibir información sobre productos, llame al:
América Latina: +1 520 477 3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/complete-website-security

Symantec Mexico
Ciudad de México,
Paseo de Tamarindos #400A P-16, Col.
Bosque de las Lomas,
Cuajimalpa, CP 05120,
México DF, México
www.symantec.com/es/mx/complete-website-security

Vaya siempre un paso por delante con Symantec