



# EL VALOR COMERCIAL DE LA CONFIANZA

ESTRATEGIAS DE LAS EMPRESAS PARA AUMENTAR AL MÁXIMO LAS  
VENTAS POR INTERNET MEDIANTE EL FOMENTO DE LA CONFIANZA  
ENTRE LOS CLIENTES




# EL VALOR COMERCIAL DE LA CONFIANZA

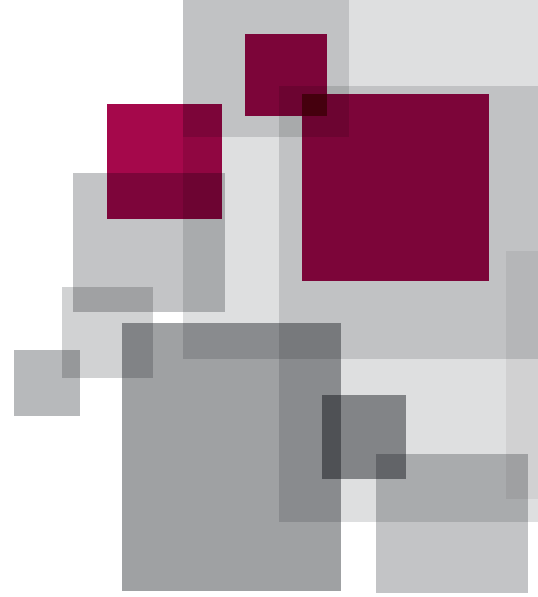
¿Desea aumentar las conversiones, incrementar las ventas y reducir la cantidad de transacciones que se abandonan a medias? En VeriSign, pensamos que la clave para conseguirlo está en el nivel de confianza del cliente. Descubra las medidas que están tomando los gerentes informáticos de varias empresas para que sus clientes se sientan más seguros en Internet.

Los sitios web de comercio electrónico no son fáciles de gestionar. En estos negocios, no basta con cubrir las necesidades normales (nuevos productos, material gráfico y funciones), sino que también hay que mantener el sitio web a pleno rendimiento y batallar con constantes revisiones o fallos. Pero ¿cuál es el objetivo real del sitio web? La respuesta a esta cuestión es tan evidente como trascendental: vender.

Si el cliente confía en la tienda en línea, las probabilidades de compra aumentan. Durante el estudio previo a la elaboración de este informe, cuatro de cada cinco gerentes informáticos afirmaron que consideraban muy importante aumentar el nivel de confianza del cliente. Sin embargo, muchos comercios por Internet pasan por alto técnicas sencillas, probadas y económicas para fomentar la confianza.

Este informe examina la importancia de esa confianza en el comercio electrónico y las estrategias que han adoptado distintas empresas para favorecerla, con mejor o peor resultado. Además, conocerá los métodos rápidos y económicos que VeriSign pone a su disposición para aumentar sus probabilidades de venta.





# EL PESO DE LA CONFIANZA

65%

de los ciudadanos europeos le preocupa que su información privada pueda distribuirse sin control por Internet.

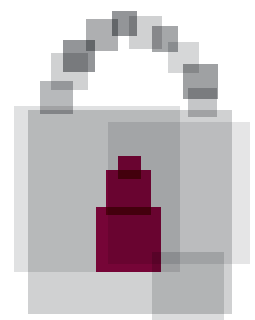
La confianza es importante porque el uso de Internet puede dar lugar a experiencias negativas. Según la campaña Get Safe Online que llevó a cabo el gobierno del Reino Unido, durante el año 2008 un tercio de la población (34%) sufrió el ataque de algún virus, un quinto (22%) fue víctima del phishing y una de cada cinco personas (21%) tuvo problemas de robo de identidad. Como consecuencia de esto, casi un tercio de los usuarios de Internet no realiza compras a través de este medio, bien porque le preocupa su seguridad personal o bien porque no se fía del vendedor<sup>ii</sup>.

Por cada persona que sufre un delito por Internet, otras muchas desarrollan desconfianza hacia este medio. Según un estudio reciente, al 65 por ciento de los ciudadanos europeos le preocupa que su información privada pueda distribuirse sin control por Internet<sup>iii</sup>. Para hacer frente a esos miedos, es preciso que los sitios web inspiren confianza en la seguridad de las transacciones<sup>iv</sup>.

Por suerte, los compradores están cada vez más familiarizados con la seguridad en la Red. Un estudio de VeriSign ha revelado que la mayoría de ellos reconoce las características que indican la seguridad de un sitio web, como

el protocolo HTTPS, el símbolo del candado, la barra de direcciones verde y distintivos de confianza como el sello VeriSign Secured<sup>®</sup> Seal. Así, un certificado caducado puede suponer un gran obstáculo a la hora de ganarse la confianza del cliente. Además, el comprador espera ver consejos sobre cómo protegerse y signos de que el vendedor se toma en serio todo lo relacionado con la seguridad y la confidencialidad, de modo que desconfía de aquellos sitios web que no ofrecen estos elementos.

El comercio electrónico tiene un gran peso. En Europa, las ventas por Internet van camino de alcanzar los 275 mil millones de libras esterlinas para el año 2011<sup>v</sup> y más de dos tercios de la población británica (70%) realiza compras en Internet<sup>vi</sup>. Durante los períodos más comerciales, como la Navidad, hasta un 93 por ciento de la población compra en la Red.<sup>vii</sup>





# AMENAZAS CRECIENTES CONTRA EL COMERCIO ELECTRÓNICO

El miedo de los clientes parte de una base real: los ciberdelincuentes son ingeniosos y pertinaces. En cierto sentido, los delitos por Internet son de mayor envergadura que el narcotráfico mundial, además de que conllevan menos riesgos de caer en manos de la justicia o sufrir una muerte violenta. Una compleja economía sumergida fomenta la especialización y la innovación constante en este campo. Así, los hackers venden sus productos y conocimientos a intermediarios que, a su vez, subcontratan la venta de los productos robados, el blanqueo del dinero o la clonación de tarjetas.

Los delitos en la Red no hacen más que aumentar. Por ejemplo, los fraudes con tarjeta por Internet y por teléfono crecieron un 13 % entre

2007 y 2008, según la asociación británica de pagos APACS. Durante el primer semestre de 2009, se calculó un fraude total de 134 millones de libras esterlinas en el Reino Unido<sup>viii</sup>, una cantidad que triplica las cifras del año 2000 a pesar de que el importe total de las transacciones por Internet sólo se ha duplicado<sup>ix</sup>.

Sin embargo, el cliente no es el único que está expuesto. Las empresas también sufren los efectos del intrusismo, la suplantación de dirección (spoofing), los ataques de denegación de servicio, los programas espía (spyware) y el robo de datos. En el reciente estudio titulado *Information Security Breaches Survey*<sup>x</sup> del Ministerio de Negocios, Innovación y Capacitación del Reino Unido, se indica que casi la mitad (45%) de las empresas pequeñas sufrieron atentados contra su seguridad durante 2008 y que esos ataques les acarrearán pérdidas de entre 10.000 y 20.000 GBP de media. Por su parte, las grandes empresas mostraron una mayor cantidad de problemas (72%) y de más gravedad, dado que las pérdidas ascendían a entre 90.000 y 170.000 GBP de media. De entre las amenazas que afectan a las empresas, hay dos que influyen directamente en la confianza del cliente: el robo de datos y el

spoofing. Si se produce algún fallo en cualquiera de estos dos aspectos, la reputación de la empresa podría verse gravemente afectada.

Los encuestados compartían esta opinión y afirmaron tener muy en cuenta los temores de los clientes (71%). Un gran porcentaje de ellos calificó las siguientes amenazas de muy importantes:

- Spoofing (44%)
- Phishing (40%)
- Robo de identidad (63%)

Los encuestados también expresaron su inquietud por la gestión de certificados en sí misma y los riesgos derivados de que los certificados caducaran antes de tiempo o contuvieran datos anticuados. La gestión de varios certificados ya suponía un problema importante para un 36 por ciento y el 53 por ciento manifestó su preocupación por evitar que los certificados caducaran de forma inesperada.

En resumen, los problemas son reales y tanto los gerentes informáticos como los clientes los consideran un obstáculo para el comercio electrónico. Por suerte, existen métodos sencillos y consolidados para que las empresas fomenten la confianza del cliente y protejan sus datos.



# 45%

de las empresas pequeñas sufrieron atentados contra su seguridad durante 2008.

# EL PAPEL DE VERISIGN

VeriSign puede ayudarle en dos aspectos fundamentales. Por un lado, contribuye a la protección del cliente mediante el cifrado de su información personal y ofrece garantías de que el sitio web es auténtico. Por el otro, demuestra sin lugar a dudas que su empresa

se preocupa por la seguridad del cliente y la confidencialidad de sus datos. Nuestro estudio determinó que el uso de la tecnología probada de VeriSign en su tienda puede ayudarle a conseguir sus objetivos comerciales.



Objetivo comercial	Porcentaje de encuestados que lo considera muy importante	Aportación de VeriSign
Fomentar la confianza y la sensación de seguridad del cliente	80%	Como existen distintos proveedores de certificados SSL, lo mejor es escoger aquel que genera el mayor grado de confianza y seguridad en los clientes. Según un estudio reciente, el 81 por ciento de los británicos que realizan compras en la Red reconoce el sello VeriSign Secured Seal, una cifra muy superior a la de cualquier otro distintivo de confianza <sup>xi</sup> , y el 78 por ciento de los compradores europeos consideran que VeriSign es la empresa que transmite más confianza <sup>xii</sup> . Al incluir el sello VeriSign Secured Seal en un sitio web, no sólo permite que el cliente compruebe la validez del certificado SSL, sino que le ofrece una confirmación visual de que sus datos contarán con la protección de una empresa fiable. Por su parte, los certificados SSL con Extended Validation de VeriSign muestran el nombre del propietario del sitio web y colorean de verde la barra de direcciones de los navegadores más actuales a modo de confirmación visual de que el sitio web es auténtico y utiliza el cifrado SSL.
Reforzar la seguridad	64%	Los certificados de VeriSign con criptografía activada por servidor (Server-Gated Cryptography, SGC) permiten ofrecerle a más del 99,9% de los visitantes un cifrado SSL de 128 o 256 bits (según el navegador web, el sistema operativo y el servidor anfitrión), que es el mejor cifrado SSL disponible en el mercado hoy en día <sup>xiii</sup> . Esta tecnología garantiza la protección de los datos del cliente cuando viajan desde el navegador hasta su servidor.
Mejorar el valor de su marca	54%	La inmensa mayoría (84%) de los británicos que compran por Internet reconoce las características que indican la seguridad de un sitio web, como el protocolo HTTPS, el símbolo del candado, la barra de direcciones verde y los distintivos de confianza <sup>xiv</sup> . Por eso, puede aprovechar estos elementos visuales para incorporar un plus de fiabilidad a su marca y su sitio web. Además, VeriSign le permite gestionar todos sus certificados desde un mismo lugar, ya sea el Certificate Center de VeriSign® o el Managed PKI para SSL de VeriSign® para grandes empresas. Gracias a estos sistemas, hay menos probabilidades de que los certificados caduquen sin que se dé cuenta, de forma que se reducen los riesgos para la seguridad y su reputación.
Incrementar las conversiones	44%	Una cosa es atraer al cliente y otra muy distinta, conseguir que compre algo. Aunque el marketing y la publicidad contribuyen a aumentar el tráfico de visitas, el funcionamiento del sitio es un factor clave para las conversiones. De hecho, más de dos tercios de los consultados (68%) afirman que, a la hora de realizar transacciones en línea, tienen más dudas si el vendedor no muestra ningún distintivo de confianza u otro tipo de garantía <sup>xv</sup> . Mediante el uso de certificados SSL con Extended Validation y distintivos de confianza como el sello VeriSign Secured Seal, se logra fomentar la confianza del cliente y animarlo a comprar, sobre todo cuando llega el momento de iniciar la transacción o facilitar datos personales. Para potenciar el efecto, también puede ofrecer información sobre las medidas que toma su empresa para proteger al cliente.
Aumentar el valor de los pedidos	34%	Unos mayores niveles de confianza y seguridad pueden ser un buen complemento a sus técnicas para vender bienes y servicios adicionales. Si el cliente no confía en el sitio web, los enlaces a prolongaciones de garantía o productos relacionados pueden parecer publicidad emergente o no deseada. Por el contrario, cuando el cliente se fía del sitio web, puede sentirse más tentado de estudiar estas ofertas con detenimiento. Este comportamiento se hace más evidente cuando la empresa necesita que sus clientes proporcionen una mayor cantidad de información, como es el caso de las compañías de seguros, que precisan numerosos datos personales para elaborar sus presupuestos. Se ha observado que, cuando los visitantes no se sienten seguros, las tasas de abandono de la cesta de la compra aumentan y las de registro disminuyen.

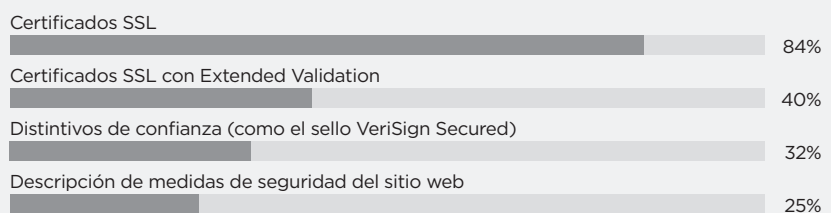
# CÓMO SE PROTEGEN LAS EMPRESAS

Una perspicaz mayoría de empresas ya cumple casi todas nuestras recomendaciones: utiliza certificados SSL con Extended Validation, exhibe distintivos de confianza como el sello VeriSign Secured Seal y ofrece explicaciones e indicadores visuales sobre las medidas de seguridad presentes en el sitio web. No obstante, es sorprendente la cantidad de empresas que no lo hace. De hecho, sólo un 40 por ciento de los encuestados utilizaba Extended Validation, un escaso 32 por ciento mostraba distintivos de confianza y tan sólo un 30 por ciento contaba con un sistema de gestión de certificados centralizado. Estas carencias podrían provocar una pérdida de clientes en favor de otros

vendedores mejor preparados, que se encuentran con esta ventaja competitiva en bandeja.

La aplicación de estas medidas tampoco acarrea mayores problemas, ya que son sencillas y económicas. El cambio de un certificado SSL normal a otro con Extended Validation no entraña ninguna complicación técnica, sobre todo cuando se cuenta con la asistencia de VeriSign. En cuanto al distintivo de confianza y a los consejos sobre seguridad, tan sólo suponen unos ligeros cambios estéticos en el sitio web. Por último, la gestión de certificados centralizada favorece en gran medida que los certificados nunca caduquen de forma accidental.

**Gráfico: Cómo fomentan la confianza las empresas**



Fuente: Encuesta de VeriSign a gestores informáticos, enero de 2010.

# CONCLUSIONES DE VERISIGN

Tras adoptar la tecnología de VeriSign, nuestros clientes afirman haber observado un importante aumento de las conversiones y las ventas, así como un descenso de los abandonos de cestas de la compra. Misco, por ejemplo, experimentó un cinco por ciento menos de abandonos tras incorporar los certificados SSL con Extended Validation.\* Asimismo, directline holidays advirtió un aumento del ocho por ciento en las conversiones\* y QuickRooms.com contabilizó casi un siete por ciento más de ventas tras instalar certificados SSL con Extended Validation y el sello VeriSign Secured\* Seal.

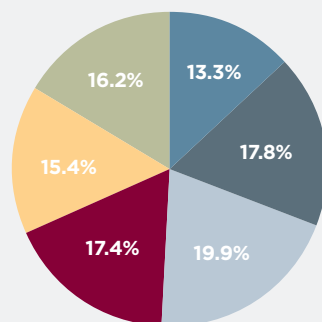
Aunque es posible que otros factores hayan influido en los resultados de estos clientes y su

empresa no tiene por qué seguir la misma tendencia, el gasto es relativamente pequeño para el presupuesto de la mayoría de los sitios web y las posibles ventajas constituirían un porcentaje importante de los ingresos por Internet. En definitiva, se trata de una inversión fácil de justificar.

Además, el potencial a largo plazo es incluso mayor. A medida que el mercado se amplía y la competencia se recrudece, el fomento de la confianza podría convertirse en el aspecto diferenciador de su sitio web y en una forma de aumentar las conversiones e incrementar el valor de los pedidos. No sólo estará haciendo lo correcto, sino que además eso redundará en beneficios para la empresa.

La sensación de falta de seguridad de los clientes es la principal preocupación de los gerentes informáticos.

Amenazas más importantes



- Gestión de varios certificados SSL
- Riesgo de que los certificados SSL caduquen de forma inesperada
- Temor de los clientes a la falta de seguridad en Internet
- Robo de identidad
- Phishing
- Spoofing

# ACERCA DE VERISIGN

VeriSign (Nasdaq: VRSN) es el proveedor de referencia de servicios para infraestructuras de Internet en la era de la interconexión mundial. Cada día, los servicios de registro, protección de identidad, autenticación y SSL de VeriSign ayudan a empresas y particulares de todo el mundo a establecer miles de millones de comunicaciones y relaciones comerciales con plena confianza.

VeriSign es la principal autoridad de certificación SSL que protege el comercio electrónico y las comunicaciones en sitios web, intranets y extranets. VeriSign lidera el sector de los certificados SSL y forma parte del CA/Browser Forum, una organización voluntaria que ahora se ha centrado en los certificados SSL con EV.

➤ Para obtener más información, visite **[www.verisign.es](http://www.verisign.es)**.

<sup>i</sup> Investigación de VeriSign realizada en Internet del 4 al 13 de enero de 2010.

<sup>ii</sup> El miedo frena las compras por Internet (en inglés), BBC News, mayo de 2009. Disponible en <http://news.bbc.co.uk/2/hi/business/8043717.stm>

<sup>iii</sup> "Un experto de la UE afirma que la pérdida de datos es un problema a escala europea (en inglés), SC Magazine, octubre de 2008. Disponible en <http://www.scmagazineuk.com/Data-loss-is-Europe-wide-problem-says-EU-expert/article/119969/>

<sup>iv</sup> Datos de Get Safe Online: Informe anual de GSO para 2009, [www.getsafeonline.org](http://www.getsafeonline.org)

<sup>v</sup> Informe de eMarketer, mayo de 2008

<sup>vi</sup> Datos de Get Safe Online: Informe anual de GSO para 2009, [www.getsafeonline.org](http://www.getsafeonline.org)

<sup>vii</sup> Estudio de IMRG: <http://www.imrg.org>

<sup>viii</sup> APACS: [http://www.ukpayments.org.uk/media\\_centre/press\\_releases/-/page/732/](http://www.ukpayments.org.uk/media_centre/press_releases/-/page/732/)

<sup>ix</sup> APACS: [http://www.ukpayments.org.uk/resources\\_publications/key\\_facts\\_and\\_figures/card\\_fraud\\_facts\\_and\\_figures/](http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/)

<sup>x</sup> Estudio sobre atentados contra la seguridad de la información (en inglés): [http://www.pwcc.co.uk/eng/publications/berr\\_information\\_security\\_breaches\\_survey\\_2008.html](http://www.pwcc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html)

<sup>xi</sup> Investigación de la marca VeriSign en 2009, Synovate/GMI, mayo de 2009

<sup>xii</sup> Synovate/GMI, ibid.

<sup>xiii</sup> SGC: <http://www.verisign.com/ssl/ssl-information-center/strongest-ssl-encryption/index.html>

<sup>xiv</sup> Investigación de la marca VeriSign en 2009, Synovate/GMI, mayo de 2009

<sup>xv</sup> Synovate/GMI, ibid.

\* Los resultados pueden variar en cada empresa, ya que otros factores podrían haber contribuido al rendimiento final de estos clientes. Póngase en contacto con VeriSign hoy mismo y le recomendaremos la mejor solución de seguridad para su empresa.

