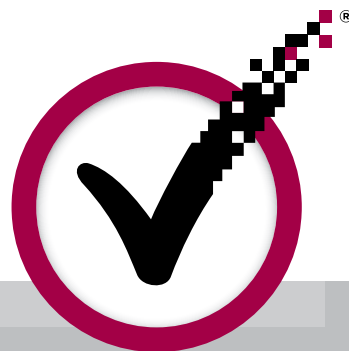




INFORME



# ❑ **CÓMO CONSEGUIR CLIENTES Y FOMENTAR LA CONFIANZA EN INTERNET**

QUÉ HACEN LAS EMPRESAS  
INTELIGENTES PARA FOMENTAR LA  
CONFIANZA Y CONSEGUIR UNA VENTAJA  
COMPETITIVA EN INTERNET

# ➤ CÓMO CONSEGUIR CLIENTES Y FOMENTAR LA CONFIANZA EN INTERNET

Qué hacen las empresas inteligentes para fomentar la confianza y conseguir una ventaja competitiva en Internet

Para las empresas que tienen sitios web, es imprescindible contar con la confianza de sus clientes. Cuesta mucho dinero construir un buen sitio web, y aún más crear una marca y publicitarla, así que sale muy caro perder un cliente justo cuando está a punto de hacer una compra sólo porque el sistema no le inspira confianza. Es un fracaso comercial en toda regla: sería como correr una maratón y pararse justo antes de la meta.

## LA PERCEPCIÓN DEL RIESGO

En los medios de comunicación se habla mucho de los problemas relacionados con Internet, lo cual hace que los consumidores se preocupen, hasta el punto de que algunos no hacen nunca transacciones por este medio. Hay personas muy selectivas a la hora de comprar en línea que evitan usar los sitios web que no les inspiran confianza. Otras inician el proceso de compra pero lo interrumpen justo al final si tienen la impresión de que sus datos personales no están bien protegidos.

Get Safe Online, un sitio web del gobierno del Reino Unido patrocinado por VeriSign, muestra gran cantidad de datos estadísticos sobre la disposición de la gente para comprar por Internet. Aunque muchos consumidores no tienen inconveniente en hacer compras, realizar transacciones bancarias o reservar unas vacaciones en Internet, también hay muchos que no se fían. De hecho, un tercio de la población evita usar este

medio.<sup>1</sup> Son muchas las personas que han sido víctimas de virus informáticos (34%), phishing (22%), estafas en línea (15%) y robos de identidades (21%).

## LA CONFIANZA ES UNA VENTAJA COMPETITIVA

Todos los objetivos que persiguen los responsables del comercio electrónico (reducir el número de abandonos de cestas de la compra, aumentar el valor de los pedidos, proteger los márgenes de beneficios, mejorar la rentabilidad de la inversión en publicidad o competir con grandes marcas) dependen de la confianza de los consumidores. Fuera del ámbito de las compras por Internet, la confianza es aún más importante. Por ejemplo, para realizar transacciones financieras o relacionadas con seguros, los clientes tienen que revelar más datos que al comprar en línea, y las aplicaciones del sector público exigen un grado de confianza aún mayor. ¿Haría la declaración de la renta o accedería a su historial médico en un sitio web del que no se fía?

Si consigue que su sitio web parezca más fiable, este tipo de preocupaciones jugarán a su favor, pues la confianza puede ser una ventaja competitiva.

34%

de las personas han sido víctimas de virus informáticos

<sup>1</sup> Informe de Get Safe Online del año 2009: [http://www.getsafeonline.org/nqcontent.cfm?a\\_id=1517](http://www.getsafeonline.org/nqcontent.cfm?a_id=1517).

# EMPRESAS REALES, DATOS INCUESTIONABLES

Hemos llevado a cabo una encuesta entre 719 gerentes informáticos europeos para descubrir qué preocupa a las empresas y qué hacen éstas para conseguir clientes y fomentar la confianza en Internet.

En primer lugar, les preguntamos qué creían que preocupaba a los clientes, para así descubrir el tipo de amenazas que las empresas intentan evitar.

El riesgo que creen que despierta más inquietud es el fraude o las pérdidas financieras, seguido de cerca de los comerciantes deshonestos. Estos resultados parecen guardar relación con el espacio que se dedica en los medios de comunicación a los delitos en línea, así como con las conclusiones de las encuestas realizadas entre usuarios, como el informe anual Get Safe Online del gobierno del Reino Unido. Según esto, los gerentes informáticos deberían preocuparse más por conseguir que su sitio web no sólo sea seguro sino que también lo parezca, de forma que los clientes se sientan tranquilos a la hora de facilitar su número de tarjeta de crédito y no piensen que sus datos podrían acabar en manos de delincuentes.

Cuando preguntamos qué preocupaba a los gerentes informáticos, los resultados fueron un poco distintos. Los expertos piensan menos en aspectos como el robo de identidades o el phishing y se centran, como es comprensible, en conseguir que los clientes se sientan seguros. Pero tampoco dejan de lado aspectos prácticos. Por ejemplo, a muchos gerentes les preocupa que el certificado SSL (Secure Sockets Layer o "capa de sockets seguros") caduque de forma imprevista.

También es comprensible que les preocupen estos aspectos. El spoofing es una amenaza real, pues alrededor de 911 marcas fueron secuestradas sólo en el último trimestre de 2009.<sup>2</sup> El fenómeno del phishing, al crear mensajes de correo electrónico y sitios web falsos que parecen de marcas famosas, puede socavar la reputación de dichas marcas. Según estas conclusiones, las empresas deberían hacer un esfuerzo por demostrar que su sitio web es legítimo y no falso. El miedo al robo de identidad es la principal razón de la desconfianza en Internet,<sup>3</sup> así que los propietarios de sitios web tienen que demostrar que los datos personales se protegen correctamente mediante cifrado o de algún otro modo.

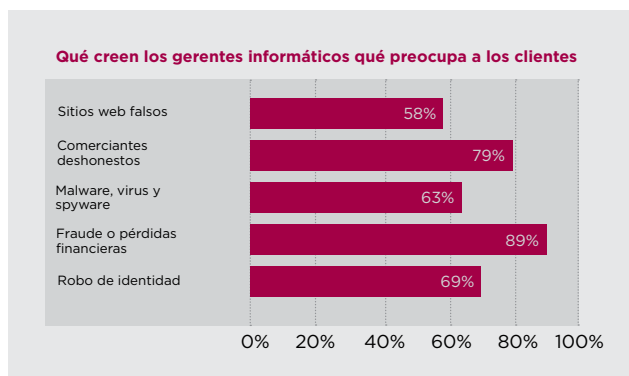
Los certificados SSL caducados ponen en peligro la confianza de los clientes porque hacen que los navegadores web muestren mensajes de error alarmantes (y con un lenguaje muy técnico que

asusta al usuario). Es increíble lo fácil que resulta olvidar las fechas de renovación, sobre todo cuando una empresa cuenta con numerosos certificados SSL, así que es esencial que los gerentes informáticos los gestionen con eficacia para evitar que caduquen sin que se den cuenta.

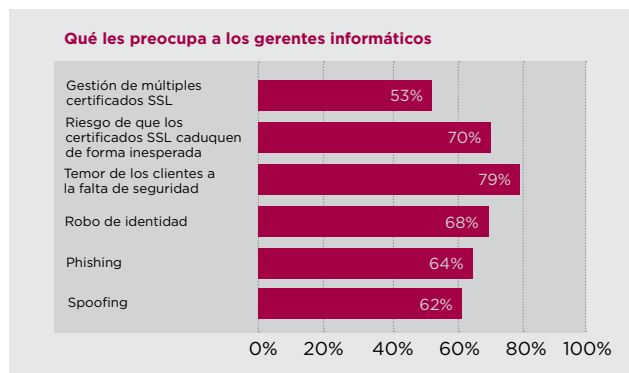
También preguntamos a los encuestados qué medidas tomaban para mejorar la confianza y la seguridad. La solución más habitual es claramente el uso de certificados SSL para cifrar la

información confidencial, pero resulta sorprendente el escaso número de personas que emplean el tipo de certificado más seguro y visible, es decir, los certificados SSL con Extended Validation (EV). Muy pocos usan marcas de confianza como el sello VeriSign Secured® Seal y aún menos explican a los visitantes del sitio web de qué forma los protegen (por ejemplo, mediante una página con consejos sobre seguridad). En definitiva, parece que los gestores de sitios web están dejando de lado aspectos muy importantes.

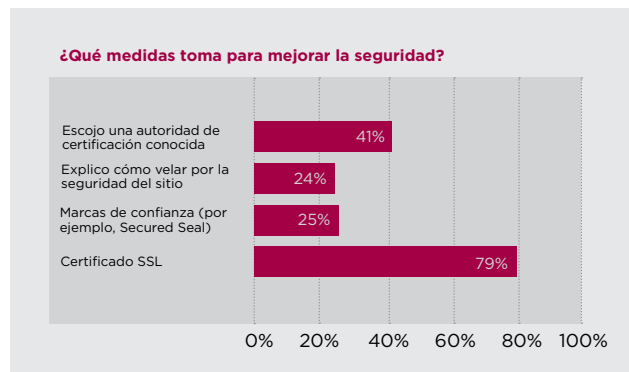
(i)



(ii)



(iii)



<sup>2</sup> Anti-Phishing Working Group, diciembre de 2009, [www.apwg.org](http://www.apwg.org).

<sup>3</sup> Estudio realizado por Synovate y GMI en el año 2009.

# VENTAJAS DE LOS CERTIFICADOS SSL CON EXTENDED VALIDATION

¿Cómo se consigue realmente la confianza y la sensación de seguridad? Por un lado, hay que combatir los delitos en línea, como el robo de identidades; y, por el otro, conviene cambiar la percepción de seguridad de los clientes. Hemos dividido estos aspectos en cuatro categorías:

- Autenticación del vendedor (“somos quien aseguramos ser”)
- Cifrado y protección de datos (“protegemos sus datos”)
- Mejora de la imagen de la marca (“respetamos su confidencialidad”)
- Fomento de la confianza (“puede comprar aquí con toda tranquilidad”)

Los certificados SSL con Extended Validation (EV) constituyen una versión superior de los certificados SSL tradicionales que permite mostrar el nombre de la empresa y un fondo verde en la barra de direcciones de los navegadores compatibles (como Internet Explorer 7 y versiones posteriores o Firefox 3.0 y versiones posteriores) y en los teléfonos inteligentes más avanzados. De este modo, los usuarios disponen de una demostración visible de que el sitio web es digno de confianza.

Este tipo de certificado aborda los cuatro ámbitos citados anteriormente:

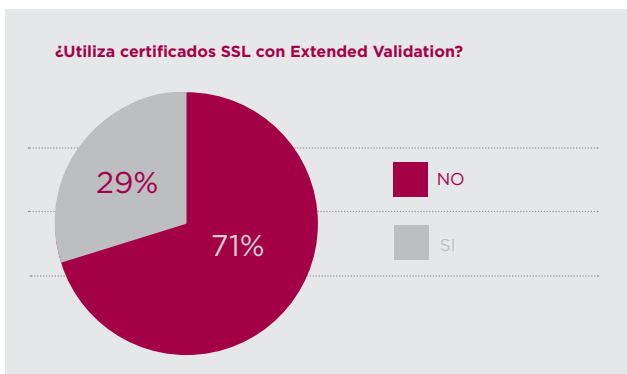
- **Autenticación del vendedor.** VeriSign aplica procesos de autenticación estrictos antes de emitir un certificado, así que los usuarios del sitio web pueden tener la certeza de que no es falso.
- **Cifrado y protección de datos.** Los certificados SSL con EV cifran los datos de los usuarios entre el navegador y el propietario del sitio web con el nivel de cifrado más alto que existe.
- **Mejora de la imagen de la marca.** Los certificados SSL con EV muestran el nombre de la empresa en la barra de direcciones de los navegadores compatibles, con lo que los usuarios pueden comprobar que el sitio web pertenece efectivamente a la empresa con la que quieren realizar la transacción.
- **Fomento de la confianza.** Los sitios web protegidos mediante un certificado SSL con EV se distinguen porque la barra de direcciones aparece de color verde, un signo de alto nivel de seguridad claramente visible que inspira confianza a los usuarios.

## ACERCA DE LOS CERTIFICADOS SSL CON EXTENDED VALIDATION

La creación de los certificados SSL con Extended Validation fue una respuesta al aumento del fraude en Internet, que estaba minando la confianza de los consumidores en las transacciones en línea. El estándar SSL con Extended Validation sube el nivel de verificación que ofrecen los certificados SSL tradicionales y muestra marcas visibles en los navegadores de alta seguridad.

En el año 2006, varios proveedores de navegadores y entidades emisoras de certificados SSL aprobaron una serie de prácticas estándar para validar y mostrar los certificados que llamaron “estándar Extended Validation”. Para emitir un certificado SSL que cumpla el estándar, las CA (autoridades de certificación) deben seguir dichas prácticas y superar una auditoría de WebTrust. El proceso de validación exige que la CA autentique la identidad empresarial del solicitante del certificado y su posesión del dominio, así como que compruebe que el encargado de la aprobación sea un empleado de la empresa solicitante y esté autorizado para obtener el certificado SSL con Extended Validation.

Los certificados SSL con Extended Validation proporcionan a los navegadores web de alta seguridad datos que permiten identificar claramente a qué empresa pertenece un sitio web. Por ejemplo, si se usa Microsoft® Internet Explorer 7 o versiones posteriores para visitar un sitio web protegido con un certificado SSL que cumple el estándar Extended Validation, la barra de direcciones aparecerá de color verde y, a su lado, se mostrará de forma alterna el nombre de la empresa indicado en el certificado y el de la autoridad de certificación (por ejemplo, VeriSign). Firefox 3 también es compatible con los certificados SSL con Extended Validation.



# RESULTADOS REALES

Nuestra encuesta ha revelado que las empresas que usan certificados SSL con EV han conseguido aumentar los valores de los pedidos, reducir el número de abandonos de cestas de la compra e impulsar las ventas. Pero la principal ventaja que han obtenido ha sido mejorar la sensación de seguridad de los clientes en el sitio web, pues una abrumadora mayoría de encuestados (el 70%) ha mencionado este aspecto.

Estos resultados se repiten una y otra vez entre nuestros clientes. Las empresas que protegen sus sitios web mediante certificados SSL con EV de VeriSign consiguen un aumento medio de las transacciones de más del 20%.<sup>4</sup> Según varios estudios recientes, los clientes de VeriSign que usan certificados SSL con EV disfrutaban de importantes ventajas:\*

- Misco, un vendedor al detalle de productos de electrónica, redujo un 5% el número de abandonos de cestas de la compra.
- Directline holidays aumentó las conversiones un 8%.
- Las ventas de QuickRooms.com crecieron casi un 7%.
- Papercheck.com prácticamente duplicó las inscripciones en línea (aumentaron un 87%).
- CarInsurance.com aumentó las inscripciones en línea un 18%.
- Fitness Footwear incrementó las conversiones un 16,9% y redujo los abandonos de cestas de la compra un 13,3%.
- CreditKarma.com obtuvo un aumento del 26% en su tasa de conversión.

## CONCLUSIONES DE VERISIGN

Existen cinco medidas sencillas que permiten mejorar la confianza y la sensación de seguridad de los usuarios:

- **Pásese al certificado SSL con EV.** Los certificados SSL constituyen una buena solución, pero los SSL con Extended Validation son aún mejores. Sustituyen por completo a los SSL, cuestan poco más y son prácticamente igual de fáciles de implementar.

- **Seleccione una autoridad de certificación (CA) de confianza.** La reputación de la autoridad de certificación (CA), como VeriSign, es muy importante para los usuarios. En un estudio, el 88% de los encuestados aseguró que confiaba en VeriSign, mientras que el segundo proveedor de la clasificación sólo contaba con la confianza del 22%.<sup>5</sup>
- **Utilice una marca de confianza.** Además de los certificados SSL con EV, utilice otros indicadores visuales que demuestren que tiene muy en cuenta la seguridad de sus clientes. Las marcas de confianza de este tipo serán más útiles si son muy conocidas. Por ejemplo, el 68% de las personas que compran en línea en toda Europa conocen el sello VeriSign Secured® Seal<sup>6</sup>, lo que significa un nivel de popularidad muy superior al de cualquier otra marca de confianza.
- **Mejore la forma de gestionar los certificados.** Haga un seguimiento de sus certificados para asegurarse de que recibe un aviso automático cuando se acerque la fecha de expiración. Considere la posibilidad de reunir todos los certificados en una sola cuenta. Gracias al VeriSign Certificate Center, podrá gestionar los certificados de VeriSign en línea desde una ubicación centralizada. Si usa muchos certificados o tiene varios de distintas autoridades de certificación, invierta en una herramienta de gestión como VeriSign Managed PKI (infraestructura de clave pública) para SSL.
- **Explique a los usuarios las medidas que toma para protegerlos.** Los usuarios se sentirán más tranquilos si añade una página en la sección de ayuda o un apartado en el menú inferior que explique lo que hace para protegerlos (por ejemplo, puede comentar para qué sirve un certificado SSL).

Según nuestra encuesta, las empresas gastan por término medio un 14% del presupuesto informático en medidas de seguridad. Sin embargo, a pesar de este elevado porcentaje, muchas de ellas no siguen los sencillos pasos que hemos enumerado para mejorar la confianza y la sensación de seguridad de los usuarios de sus sitios web.

Para poner en práctica estas medidas, hay que dedicar un poco de tiempo (por ejemplo, el necesario para modificar el diseño de una página web de forma que muestre una marca de confianza), pero no son caras ni en términos absolutos ni con relación al presupuesto total dedicado a la seguridad del sitio web.

El uso de la tecnología SSL con EV será cada vez mayor. Las empresas que saben lo que hacen ya usan estos certificados, mientras que los consumidores cada vez conocen mejor sus ventajas y distinguen de inmediato los sitios web que cuentan con este tipo de protección. Sin embargo, sigue habiendo muchas empresas (entre ellas, muchos de sus competidores) que carecen de este sistema y no toman ninguna medida para fomentar la confianza y la sensación de seguridad de los usuarios. En este contexto, si adopta la tecnología SSL con EV y sigue los demás pasos que recomendamos en este informe, su negocio saldrá ganando. Conseguir la confianza de sus clientes y hacer que se sientan seguros le aporta una clara ventaja competitiva y es algo que está a su alcance gracias a VeriSign.

# 68%

de las personas que compran en línea en toda Europa conocen el sello VeriSign Secured® Seal<sup>6</sup>

<sup>4</sup> Según un estudio de diciembre de 2009 basado en pruebas realizadas en decenas de sitios web de todo el mundo, los certificados SSL con EV de VeriSign contribuyeron a un aumento de conversiones de entre el 5 y el 87%, mientras que el incremento medio superó el 20%.

<sup>5</sup> Tec-Ed, enero de 2007.

<sup>6</sup> Estudio realizado por Synovate y GMI en el año 2009.

## ➤ 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 entidad emisora de certificados SSL que protege el comercio electrónico y la comunicación 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).**

\* 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.

---

© 2010 VeriSign Spain, S.L. Todos los derechos reservados. VeriSign, el logotipo de VeriSign, la uve sobre el círculo, VeriSign Secured y otras marcas comerciales, marcas de servicio y logotipos son marcas registradas o no registradas de VeriSign y sus filiales en Estados Unidos y otros países. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios.

