

LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

SAFETY IN ELECTRONIC COMMERCE

Fidel Romero Zegarra*

RESUMEN

En el presente trabajo se brinda una visión general acerca del Comercio Electrónico, sus implicancias en el desarrollo, crecimiento y generación de ventaja competitiva para las empresas. Se describe brevemente el crecimiento en el uso de Tecnologías de Información por parte de las empresas, principalmente en aquellas soportadas por Internet para lograr alcanzar nuevos mercados e incrementar sus niveles de ventas.

Además se presenta una descripción de las principales amenazas que afectan el normal desarrollo de los procesos del Comercio Electrónico y que devienen en una pérdida de confianza por parte de los usuarios y muchos riesgos y pérdidas en las empresas que han visto vulnerada su seguridad.

Finalmente se muestran alternativas para minimizar los riesgos tanto para los usuarios, como para las empresas que están apostando hoy en día por utilizar este tipo de medios para hacer negocios, aprovechando el desarrollo tecnológico que estamos viviendo.

Palabras Clave: Comercio Electrónico, B2B, C2C, B2C, Seguridad Informática, Seguridad Tecnológica

ABSTRACT

In this paper is provided an overview of electronic commerce (e-commerce), its implications for the development, growth and creation of competitive advantage for companies. The growth in the use of Information Technology by the companies is briefly described, mainly those supported by Internet to achieve reach new markets and increase their sales levels.

Besides a description of the main threats that affect the normal development of e-business processes and become a loss of confidence on the part of users and many risks and losses in companies that have been compromised their security features.

Finally it shows some alternatives to minimize the risks to both users and companies that are betting today by using such means to do business, taking advantage of technological development we are experiencing.

Keywords: e-commerce, B2B, C2C, B2C, Informatic Security, Security Technology

* Maestrante de la Maestría en Dirección Estratégica de Ingeniería de Software – Universidad Científica del Sur – FUNIBER. Ingeniero de Sistemas de la Universidad Nacional de Cajamarca. Docente de la Universidad Privada Antonio Guillermo Urrelo. Email: fidel.romero@upagu.edu.pe

Recibido: 12/10/2014

Aprobado: 15/12/2014

Citar como: Romero-F. La seguridad en el comercio electrónico. Rev. Experti. 2014, 1(2): 11-19. Recuperado del link OSS

INTRODUCCIÓN

El uso de las Tecnologías de Información en nuestros días es un evento generalizado, podemos ver como se han creado, producido, distribuido y masificado, muchos nuevos dispositivos que facilitan no sólo el acceso a las redes sociales por medio del uso de Internet, que de acuerdo a la ITU (**Unión Internacional de Telecomunicaciones**), llega a casi tres mil millones de usuarios hasta finales del 2014 [1]; sino que han permitido la automatización de procesos para las empresas, dándose un gran incremento en dos operaciones principales como son las adquisiciones o compras y la venta de productos.

Podemos notar sin dificultad el crecimiento del número de empresas que han optado por llevar a la red (Internet), muchos procesos, sobre todo el de ventas. Generándose una “nueva tendencia” llamada e-Commerce o Comercio Electrónico, presentándose muchos modelos que permiten acceder, por parte de los clientes, a los productos ofertados por las empresas. Dentro de estos nuevos modelos podemos destacar los Escaparates Virtuales, Agentes de Transacciones y Mercados en Línea.

Podemos entender al Comercio Electrónico como el conjunto de aquellas transacciones comerciales y financieras realizadas a través de redes informáticas, principalmente Internet. También podría verse como una aplicación informática dirigida a realizar transacciones comerciales.

Pero, a pesar de los avances que se han tenido en los últimos años en temas de Tecnología, el Comercio Electrónico ha sufrido siempre de una gran dolencia: La Seguridad. Es en este contexto en el que se plantea el presente trabajo, en el cual se pretende establecer si el Comercio Electrónico cumple con garantizar la seguridad tanto a las empresas como a los usuarios.

Es muy conocido que para las transacciones comerciales, ya sean físicas o virtuales, el aspecto

más crítico es la confianza, en este sentido, las empresas deben brindar herramientas suficientes para garantizar que de alguna manera el Comercio Electrónico brinde la de seguridad para los usuarios o compradores.

El objetivo principal es determinar si son suficientes los medios utilizados por las empresas que tienen implementadas soluciones de Comercio Electrónico para generar confianza en los usuarios. Es decir, si las herramientas implementadas cumplen con dar al usuario la seguridad necesaria para la realización de la transacción vía virtual o por medios electrónicos.

En el presente trabajo se mostrarán las características principales del Comercio Electrónico, así como los modelos más resaltantes y las ventajas y desventajas que esta forma de hacer negocios genera tanto para la empresa como para los usuarios, además de los medios que se han venido utilizando para garantizar la seguridad. Y considerando que estamos viviendo una Era Digital, en la que muchas de las empresas están apostando por el uso, cada vez más necesario, de Tecnologías de Información es necesario dar un alcance de los riesgos que se pueden presentar al tratar de implementar una estrategia de Comercio Electrónico.

LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

La ejecución de transacciones comerciales utilizando medios virtuales, se ha extendido en esta era, y el uso de la TIC's ha jugado y juega un papel protagónico para el desarrollo de estas actividades. Las empresas apuestan por acceder a un mercado globalizado y la mejor manera es utilizando las redes de comunicaciones, sobre todo Internet.

Existen muchos modelos de negocios entre los que se destacan los **Escaparates Virtuales**, que son páginas web en las que las empresas pueden vender directamente sus productos a consumi-

dores. Un ejemplo es www.amazon.com. Otro modelo es el **Agente de Transacciones**, estas son páginas web que permiten el procesamiento de transacciones de ventas en línea. Un ejemplo es www.lan.com. También tenemos el **Mercado en Línea**, el cuales un entorno digital en el que se pueden reunir compradores y vendedores, con el propósito de buscar, mostrar y establecer precios de productos. Un ejemplo es www.olx.com

Por otro lado tenemos modelos del comercio electrónico, los principales son el **Business to Business (B2B)**, este es un modelo en el que participan dos empresas para hacer negocios. Principalmente se da a partir de alianzas estratégicas entre una empresa y sus proveedores. Otro es el **Business to Customer (B2C)**, es el modelo más común. Se da entre una empresa y un consumidor final, quien es una persona natural. Este modelo se implementa por medio de un Escaparate Virtual o un Agente de Transacciones. Además tenemos el modelo **Customer to Customer (C2C)**, en este modelo quienes participan son dos personas naturales. La forma de implementar este modelo es por medio de un Mercado en Línea.

Estas nuevas formas de negocio tienen muchas ventajas tanto para la empresa como para los consumidores, principalmente podemos referirnos a la disminución de costos, sin embargo también presenta muchos problemas. Uno de los principales inconvenientes que se muestra en el Comercio Electrónico es la inseguridad que se presenta con el uso de la TIC's. A pesar del gran esfuerzo dedicado por muchas organizaciones

para, al menos, reducir el riesgo al que están los usuarios expuestos en las transacciones virtuales, todavía existen muchas vulnerabilidades que crean desconfianza en el uso de estos medios para la realización de negocios.

Los esfuerzos que ponen las diversas organizaciones se ven reflejados en las nuevas formas de garantizar la seguridad. Así tenemos que Visa y Mastercard desarrollan un protocolo de seguridad (SET), el cual permite realizar transacciones electrónicas seguras. También se pueden utilizar Cortafuegos (Firewall), los que permiten llevar un control adecuado del acceso por la red (Internet). La criptografía es una forma de proteger la información que viaja por la red, consiste en codificar por medio de una clave un mensaje que solamente puede ser descifrado si se conoce la clave. Otra forma de dar seguridad es el uso de firmas **digitales y certificados electrónicos**. Muchas empresas utilizan estos medios para garantizar la autenticidad de las personas, para manejar la confidencialidad entre las partes que están tranzando, para mantener la integridad de la información que se intercambia y además garantizar el no repudio; es decir, imposibilitar que alguien niegue su titularidad en un mensaje enviado. Adicional a esto se han desarrollado otros protocolos de comunicación como el SSL (Secure Socket Layer), que también garantiza una transacción segura. [2]

El Comercio Electrónico se ha incrementado indudablemente en los últimos años, así se reporta en un estudio realizado hasta el 2012. [3]

Volumen de comercio electrónico (B2C)

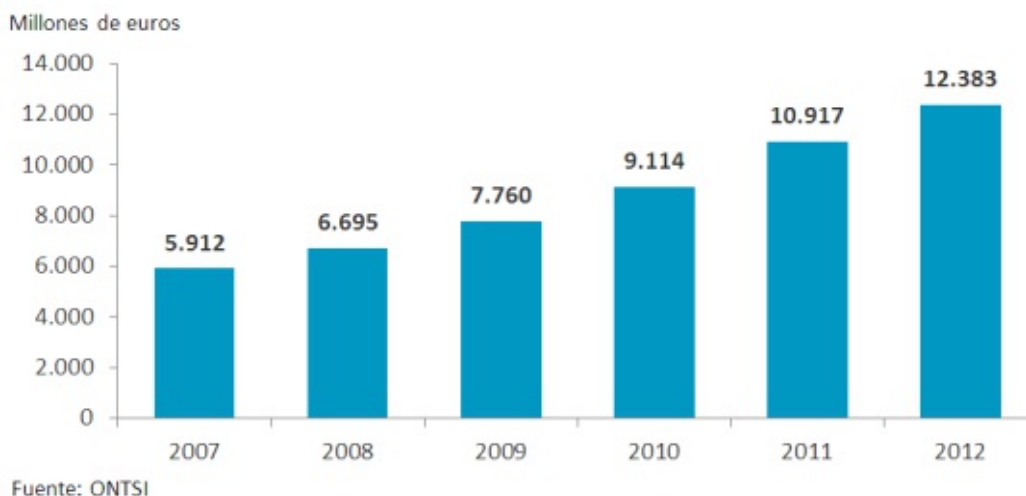


Figura 1: Volumen del comercio electrónico por años en España

Esto demuestra la importancia que ha tomado el uso de las TIC's en la implementación y ejecución del comercio electrónico. Y cómo las empresas y usuarios apuestan con mayor entusiasmo en los procesos virtuales.

De acuerdo al EcommerceFoundation se ha logrado un incremento en el comercio electrónico en todas las regiones, como se evidencia en la Tabla 1.

E-commerce turnover per region
E-commerce turnover of the global regions, 2012-2013

Region	2012	2013	Growth*
World	\$1,255.5bn	\$1,552.0bn	23.6%
Asia-Pacific	\$392.6bn	\$567.3bn	44.5%
Europe	\$411.7bn	\$482.3bn	17.1%
North America	\$411.1bn	\$452.4bn	10.0%
Latin America	\$27.3bn	\$33.2bn	21.4%
MENA	\$11.1bn	\$14.7bn	32.6%

* Growth rate based upon national currencies

Tabla 1: Crecimiento del comercio electrónico por región [4]

Además según un pronóstico realizado por especialistas, tenemos que el comercio electrónico seguirá creciendo en una escala bastante

importante, llegando al año 2017 ha generar movimientos hasta por \$2.357 MM



Figura 2: Evolución de las ventas B2c [5]

De ésta manera, se refuerza la hipótesis de que le comercio electrónico generará mayor desarrollo a pesar de los problemas de seguridad que se pueden presentar en la red. Por otro lado los usuarios empezarán a tener mayor confianza al momento de realizar transacciones por medio del uso de las TIC's.

Sin embargo y a pesar de los avances en temas de seguridad, existen muchas amenazas, entre las más comunes en el comercio electrónico tenemos el Phishing, este término se refiere a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. Otro problema es el Spoofing,

este término se refiere a la falsificación de unos datos, modificándolos de algún modo para obtener por ello un beneficio. Otra forma común es el Pharming, en este tipo de ataque, los delincuentes redireccionan a sus víctimas a páginas web falsas utilizando varios métodos, como por ejemplo correos electrónicos con asuntos llamativos para que las víctimas los abran y sean atacadas; poniendo en peligro información privada.

De acuerdo a la ONTSI, existen usuarios que han tenido problemas o incidentes al momento de realizar una compra por Internet, pero el porcentaje de situaciones negativas es bastante bajo, sin embargo los problema que se presentan son aspectos críticos que pueden generar desconfianza e inseguridad en los usuarios.

Internautas que han tenido problemas en compras por Internet (Año 2011)

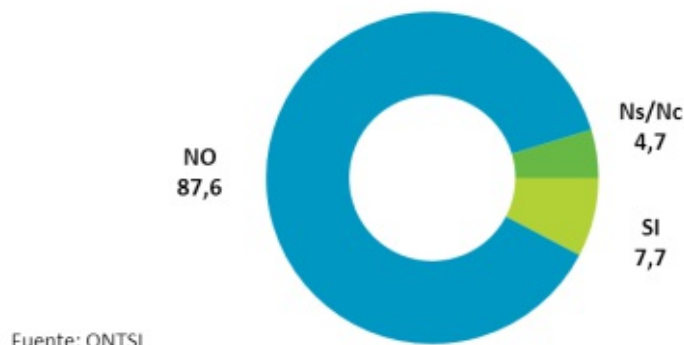


Figura 3: Usuario con problemas en compras por internet

Detalles de problemas en las compras realizadas por Internet
 % sobre internautas compradores que han tenido problemas en la compra
 (Año 2011)



Figura 4: Problemas en las compras por internet

Las empresas deben comprometerse a asegurar la privacidad de la información personal utilizada en las transacciones, principalmente acerca de la información que se requiere para realizar los pagos; existen muchos medios que dan al usuario confianza de que la transacción que realiza es fiable y de que sus datos no son interceptados por agentes externos.

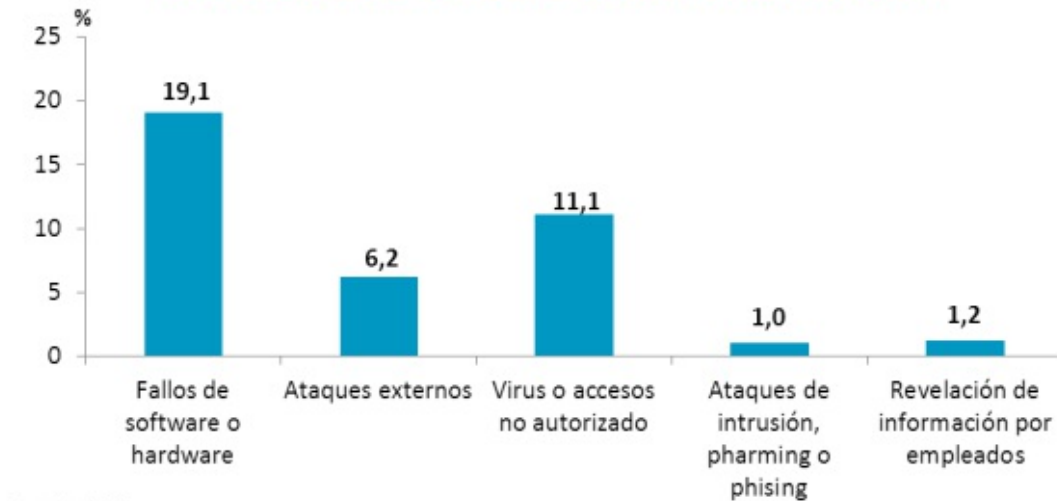
De acuerdo a la información brindada por Deloitte “Las cifras de fraudes en el comercio electrónico alcanzan millones de dólares anualmente y siguen en aumento”[6] y si bien es cierto hay evidencia de muchos fraudes e inseguridad en el comercio electrónico, también podemos atribuir éstos a la falta de información o descuido por parte de los usuarios en el uso de las TIC’s. Se puede evidenciar el esfuerzo de muchas

organizaciones para establecer procesos seguros y brindar un entorno confiable en el cual se puedan llevar a cabo las operaciones y transacciones minimizando y en algunos casos hasta eliminando riesgos de ataques o intrusiones en los sistemas por parte de agentes extraños. Pero también se puede observar en muchos casos la poca importancia o relevancia que los usuarios le prestan a los intentos de vulnerar la seguridad de las empresas que apuestan por el uso de las TIC’s para el Comercio Electrónico.

De acuerdo a un estudio realizado en el 2010 por INE, se establece que los incidentes más críticos son los fallos de software o hardware con un 19,1%, mientras que entre ataques externos y ataques de intrusión sólo llega a un nivel de 7,2% [7]

Empresas que sufrieron incidentes relacionados con los sistemas TIC

% sobre el total de empresas con acceso a Internet (Enero 2010)



Fuente: INE

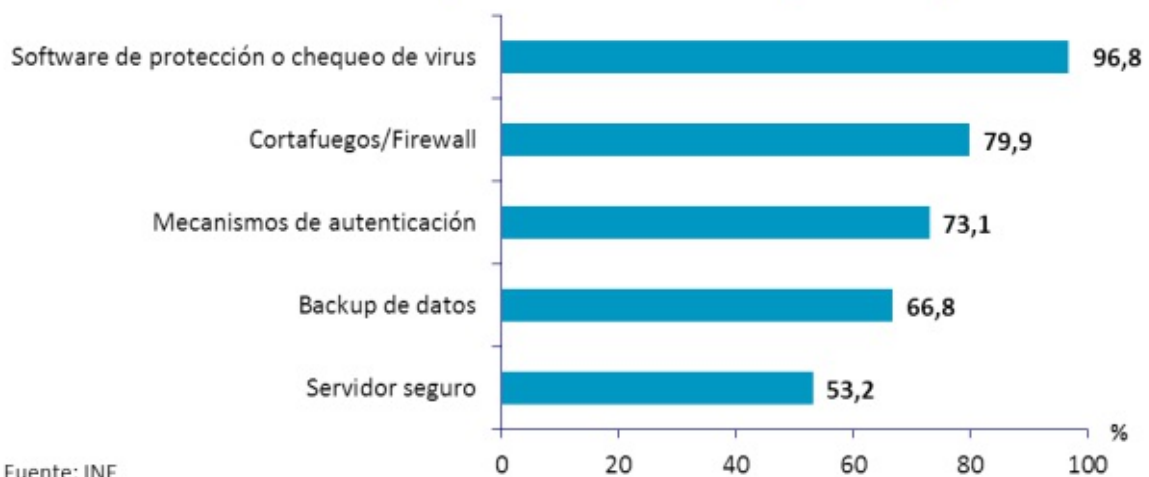
Figura 5: Empresas con problemas relacionados con Tic

Esto nos demuestra que los aspectos de seguridad en la red (Internet) han mejorado, lo que comporta que el Comercio Electrónico sea cada vez más seguro. Por otro lado según la misma organización tenemos que las empresas empie-

zan a utilizar más comprometidamente servicios de seguridad informática, con el propósito de salvaguardar tanto sus intereses como el de sus clientes.

Servicios de seguridad informática utilizados por las empresas

% sobre total de empresas con acceso a internet (Enero 2009)



Fuente: INE

Figura 6: Seguridad informática usada por las empresas

Finalmente los usuarios también deben entender el riesgo que involucra cualquier transacción realizada por Internet, pero los mecanismos

de seguridad que utilizan aún no son los más adecuados.

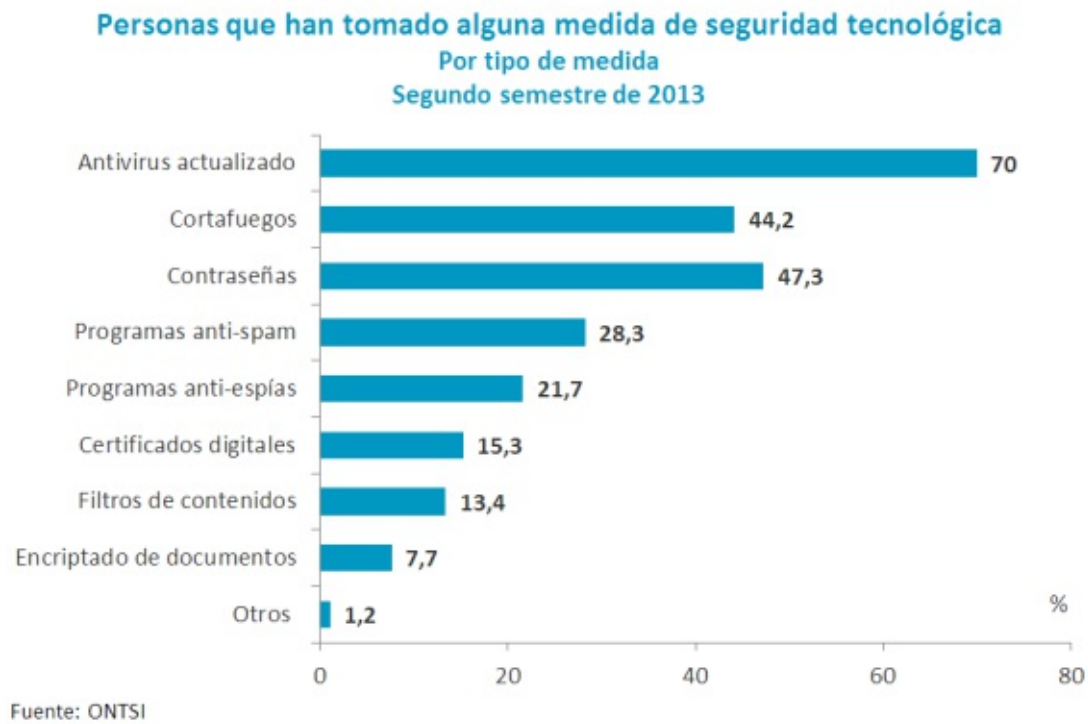


Figura 7: Personas que han tomado medidas de seguridad tecnológica

Los usuarios principalmente se enfocan en ataques por virus, acceso a sus computadoras y seguridad de sus cuentas, pero dejan de lado otros aspectos críticos, como los certificados digitales o la encriptación de datos, los cuales son procesos necesarios para realizar operaciones por Internet con mayor seguridad.

Por otro lado los usuarios deben ser más responsables para no ser víctimas de ataques maliciosos, en este sentido el Instituto Nacional de Tecnologías de la Información (INTECO) de España propone una secuencia de pasos a seguir para tener mayor seguridad al momento de realizar una compra por Internet.

A modo de conclusión podemos decir que el Comercio Electrónico es una actividad estratégica que las empresas deben empezar a implementar y fortalecer con el objetivo de alcanzar ventaja competitiva y desarrollo, no obstante, existen muchos riesgos en la seguridad de la información utilizada en las transacciones, y tanto las empresas que brindan el servicio de comercio electrónico, como los usuarios que acceden a estos servicios son responsables de minimizar los peligros que siempre existirán.

Las empresas que quieran iniciar un proceso de Comercio Electrónico deben establecer políticas de seguridad que garanticen que todo el proceso de comercio que se dé a través de Internet sea fiable.

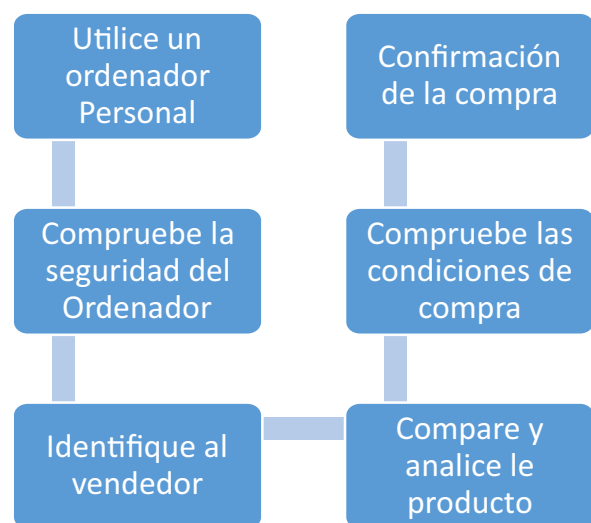


Figura 8: Pasos para realizar una compra segura [8]

REFERENCIAS

- [1] ITU, «ITU,» [En línea]. Available: http://www.itu.int/net/pressoffice/press_releases/2014/23-es.aspx#.VLbd49KG8UN. [Último acceso: 14 Enero 2015].
- [2] M. H. González, «ISACA,» [En línea]. Available: <http://www.isaca.org/Journal/Past-Issues/2000/Volume-6/Pages/Comercio-Electronico.aspx>. [Último acceso: 13 Febrero 2015].
- [3] Observatorio Nacional de Tecnologías y SI, «ONTSI,» [En línea]. Available: <http://www.ontsi.red.es/ontsi/es/indicador/problemas-con-las-compras-realizadas-por-internet>. [Último acceso: 13 Febrero 2015].
- [4] Ecommerce Foundation, «Ecommerce Foundation,» 2014. [En línea]. Available: www.ecommercefoundation.com. [Último acceso: 13 Febrero 2015].
- [5] BrainSINS, «BrainSINS,» 22 12 2014. [En línea]. Available: <http://www.brainsins.com/es/blog/tendencias-ecommerce-2015/111509>. [Último acceso: 13 Febrero 2015].
- [6] Deloitte, «Deloitte,» [En línea]. Available: https://www.deloitte.com/assets/Dcom-Panama/Local%20Assets/Documents/pa_es_comercioelectronico_06_08.pdf. [Último acceso: 13 Febrero 2015].
- [7] Observatorio Nacional de Tecnologías y SI, «ONTSI,» [En línea]. Available: <http://www.ontsi.red.es/ontsi/es/indicador/empresas-que-han-tenido-alg%C3%BAAn-problema-de-seguridad-en-los-%C3%BAAltimos-doce-meses>. [Último acceso: 13 Febrero 2015].
- [8] Instituto Nacional de Tecnologías de la Comunicación, «Guía sobre seguridad y Privacidad en el comercio electrónico,» Madrid, 2010.

Correspondencia:

Autor: Fidel Romero Zegarra

Dirección: Jr. José Sabogal N° 913

Email: fidel.romero@upagu.edu.pe