Impacto del comercio electrónico en la actualidad

J. M. Torres, & M. F. Trujillo

***Abstract*— El presente artículo examina el impacto que el comercio electrónico ha tenido en la sociedad actual, fundamentalmente en la sociedad colombiana, y con ello, trata las ventajas que ofrece esta modalidad de negocio. Es así que cuando se habla de comercio electrónico se entiende como un conjunto de operaciones virtuales totalmente diferentes al comercio convencional como comprar, vender o solicitar productos o servicios a través de un medio electrónico. Del mismo modo, estas operaciones necesitan garantizar una seguridad técnica y normativa que genere confianza entre las partes (emisor y receptor), previniendo que los invasores logren objetivos ilícitos a través de accesos no autorizados, por lo tanto, en el presente también se explora una serie de soluciones que pueden garantizar la seguridad y fiabilidad de cualquier transacción de comercio electrónico.**

Palabras Claves*— *Certificados de seguridad, transacciones digitales, seguridad y privacidad de datos.

I. INTRODUCCIÓN

El papel que toma el comercio electrónico en la actualidad genera una importancia enorme debido a las facilidades comerciales que el mismo ofrece, en los últimos años las tecnologías de la información y las comunicaciones (TIC), han realizado grandes avances en el campo de los sistemas informáticos, pues han sido introducidos rápidamente en el campo comercial, bancario, industrial, administrativo, investigativo, entre otros. Son pocos los sectores que no se han incorporado al mundo digital, la aparición y expansión de internet junto los sistemas informáticos, han hecho posible la realización de tareas impensables años atrás, como: transacciones bancarias, resolución de problemas legales, control, docencia y sobre todo el comercio electrónico.

Se define comercio electrónico como "cualquier actividad que involucre a empresas que interactúan y hacen negocios por medios electrónicos, bien con clientes, bien entre ellas o bien con la administración. Se incluye el pedido y pago electrónico y on-line de bienes que se envían por correo u otro servicio de mensajería, así como el envío on-line de servicios como publicaciones, software e información. Así mismo, se incluyen actividades como diseño e ingeniería cooperativa, marketing, comercio compartido, (subastas y servicios posventa)" (Comisión Europea, 1997). De acuerdo con lo anterior, puede entenderse que el comercio electrónico comprende todo tipo de transacciones en las que hay un medio electrónico para el perfeccionamiento de la compraventa, ya sea un bien o un servicio, aclarando que el carácter electrónico no hace referencia exclusivamente al internet, sino a todo tipo de intercambio electrónico.

J. M. Torres. Universidad Libre de Colombia, Bogotá – Colombia johanam.torresl@unilibrebog.edu.co
M. F. Trujillo. Universidad Libre de Colombia, Bogotá – Colombia. mariof.trujilloa@unilibrebog.edu.co
Corresponding author: F.A. Simanca

El comercio electrónico se basa en cinco principios según el 'Information Technology Security Evaluation Cteria (ITSEC)', los cuales son: el principio de autenticidad el cual implica que la persona o empresa que dice de estar del otro lado de la red es quien dice ser, asegurando el origen y el destino de la información; el principio de integridad se basa en que lo transmitido por la red no haya sido modificado, la información no se puede falsificar, los datos recibidos serán los mismos que fueron enviados o almacenados; el principio de intimidad consiste en que los datos enviados no hayan sido vistos durante el traslado telemático pues solo estarán disponibles para aquellos usuarios autorizados a usarla; el principio de accesibilidad o disponibilidad el cual debe impedir el acceso a la información a personas no autorizadas, comprendiendo quien y cuando puede acceder a la información, se debe tener en cuenta que la falta de accesibilidad produce una 'denegación de servicios', que es uno de los ataques más frecuentes en internet y por último el principio de no repudio, el cual no permite que los datos transmitidos puedan ser rechazados o repudiado, entendiendo que cualquier entidad que envía o recibe datos no puede alegar desconocer el hecho.

El comercio electrónico comprende otros criterios de seguridad secundarios como lo son: El criterio de consistencia, la cual asegura que el sistema se comporta como debe ante los usuarios autorizados; el criterio de aislamiento que impide que personas sin permisos ingresen al sistema; el criterio de auditoría se basa en la capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema y quien y cuando lo ha llevado a cabo; el criterio de prevención donde los usuarios deben comprender que todas las actividades que realicen dentro del sistema quedaran registradas y el criterio de información el cual realiza el seguimiento de la misma para detectar comportamientos sospechosos, si los hay.

Durante la popularización del comercio electrónico se han ido implementando diferentes protocolos de seguridad de uso específico como lo son IPSEC (IP Security Protocol), SSH (Secure Shell), PPTP (Point-to-pointTunnelingProtocol) entre otros; sin embargo, solo dos protocolos se han implementado con la intención de proporcionar esquemas de seguridad para las partes que participan en realizar el comercio electrónico como lo son el protocolo SET (Secure Electronic Transactions) y SSL (Secure Sockets Layer), estos protocolos comparten una cualidad la cual es el uso de la criptografía publica de RSA Data Security Inc. Empresa que permite alcanzar distintos objetivos de seguridad.

El protocolo SSL es el protocolo más extendido de la red (Chou, 2002) ya que proporciona un complejo cifrado de datos, consiguiendo un sistema de intercambio de información seguro tanto en el transporte de la información como en la autenticación, el protocolo fue desarrollado por Netscape Communicactions Corporation, con la intención de

proporcionar seguridad y privacidad en internet (Digicert, 2008). El intercambio de información de este protocolo se basa en dos fases en la primera se negocia entre el cliente y el servidor con un certificado digital sólo válido para esa transacción y en la segunda fase se transfieren los datos cifrados con dicho certificado, teniendo en cuenta que estos

pasos son transparentes para el usuario ya que ellos solo saben que el canal de transmisión de información es seguro y proporciona un nivel de confidencialidad entre ambas partes.

Aunque este protocolo sea practico y de fácil uso, no es considerado la solución definitiva puesto que solo protege transacciones entre dos puntos, como lo es el vendedor y cliente, pero adquirir un producto mediante tarjeta de crédito solicita un emisor más que viene a ser la entidad bancaria, además de que los comerciantes corren riesgo de una tarjeta sin fondos o fraudulento.

En cambio, el protocolo SET consiste en 'un conjunto de normas o especificaciones de seguridad que constituyen una forma estándar para la realización de transacciones de pago a través de internet' (Jiménez, 2014). Este protocolo fue desarrollado durante el año 1996 bajo la gestión de empresas como Mastercard, Visa, IBM, Microsoft y empresas de la industria tecnológica como SEPP (Secure Electronic PaymentProtocol) y STT (SecureTransactionTechnology). El protocolo SET busca principalmente proteger el sistema de tarjetas de crédito usado en internet, generando un ambiente de confianza en el mercado virtual, además de aplicar nuevas transacciones financieras seguras para este mercado que está en alza; con esto evitamos el pago de compras con tarjetas de crédito no autorizadas y el robo de información financiera del mismo comprador.

Los certificados digitales mencionados anteriormente (SET y SSL) son una clase de archivos electrónicos que actúan como un tipo de pasaporte en línea. Son proporcionados por una autoridad certificadora confiable, la cual verifica la identidad del poseedor del certificado (Netscape, 1999), el protocolo SSL otorga dos tipos de certificados, uno privado y otro público, el certificado privado se mantiene en un sitio seguro, por ejemplo, cifrado en el disco duro de un sistema, en cambio el certificado público, también llamado certificado asimétrico, es el que se comparte para que puedan

ponerse en contacto con el usuario. Estos certificados son usados por SSL ya que permite cifrar la información con una clave y descifrarla con una clave complementaria desde un par de claves pública-privada determinada. Por su parte los certificados digitales en SET son utilizados para poseedores de tarjetas (tarjetas de crédito electrónicas) y comerciantes, estos certificados permiten las conexiones seguras y privadas entre poseedores de tarjetas, comerciantes y bancos. Las transacciones creadas son seguras e indiscutibles y no se pueden falsificar. Los comerciantes no reciben información sobre tarjetas de crédito que se pueda robar o de la que se pueda hacer un mal uso, siguiendo los principios del comercio electrónico (IBM, 2002).

II. REFLEXIÓN

Según un estudio de transacciones digitales: e-Commerce, realizado en el segundo semestre del año 2017 por una alianza público-privada entre el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Cámara Colombiana de Comercio Electrónico (CCCE) y la Red Nacional Académica de Tecnología Avanzada (RENATA), el total de transacciones digitales entre enero y junio del año 2017, $7,1 billones corresponden a comercio electrónico. Esto representa un incremento de 17 % en comparación a las transacciones digitales hechas en el primer

semestre del 2016. (Observatorio eCommerce, 2018)

En consecuencia, Rivier Gómez, subdirector de Comercio Electrónico del MinTIC,aseguró que Colombia ocupa el cuarto puesto en América Latinaen relación con el valor de las transacciones de comercio electrónico realizadas en cada país (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017), lo cual indica que, en Colombia diversas pequeñas y medianas empresas (PYME) han decidido trasladar sus actividades comerciales a la Red y han aprovechado las ventajas de este medio para beneficiarse considerablemente. Adicionalmente, se ha incrementado el número de tiendas virtuales o que requieren utilizar un medio de pago digital para recibir sus ingresos por los

productos o servicios ofrecidos. Sin embargo y lastimosamente, en este medio de trasferencia de pagos la economía mundial pierde hasta 575,000 millones de dólares al año a causa de la ciberdelincuencia, comprensiblemente es un delito del que no se exenta Colombia, según lo indica un estudio conjunto de la compañía de software McAfee y el Centro de Estudios Estratégicos e Internacionales (López, 2015).

La influencia de hackers malignos que se encargan del robo de datos confidenciales ya sea una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria, provoca preocupación e inseguridad para que algunas personas y empresas implementen en sus vidas este medio de compra. Es así como la seguridad cibernética dejo de ser una pequeña área en las empresas para convertirse en pieza clave y relacionada con todas las áreas de la empresa.

Para contrarrestar la influencia de los hackers malignos y asegurar la privacidad y seguridad de datos, las empresas han trabajado en numerosas áreas desde la contratación de hackers éticos para que prueben constantemente la seguridad de las páginas, hasta mejoras en la creación de sistemas de codificación de datos para que estos sean indescifrables y así, proteger la confidencialidad de la información, la integridad de la información de pago y la autentificación del comerciante y del poseedor de la tarjeta. Adicionalmente, para asegurar la confiabilidad de las transacciones

comerciales se usan certificados de seguridad, los más conocidos son SSL y SET.

Como ya se ha mencionado, el certificado SSL o Secure Sockets Layer, busca proteger la confidencialidad de la información, la integridad de la información de pago y la autentificación del vendedor y del comprador (Fernández, 2013). Lo cual resulta siendo una ventaja que brinda fiabilidad y se ocupa de garantizar la seguridad del pago mientras

navega por el canal que transcurre entre comprador y vendedor. No obstante, con el certificado SET o Secure electronic transaction, que consiste en una serie de normas estándares que permiten la autenticación, confidencialidad, integridad y no repudio (Castañeda y Morales, 2004), es posible proteger el número de la tarjeta de crédito del titular, autentificar comerciantes y los bancos que intervienen en las operaciones que son necesarias para efectuar una compra por internet y asegurar que solo pueden usarla las personas autorizadas.

Por otro lado, una de las prevenciones que cada uno como usuario puede tomar para evitar el robo de sus datos es principalmente verificar la fiabilidad de la página web en la que se ha decidido realizar la compra. Esto se hace identificando el protocolo de aplicación con el que el sitio web está adaptado, es decir, para proteger la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web se debe adaptar el protocolo seguro de transferencia de hipertexto o más conocido por sus siglas en inglés, HTTPS, que provoca que la página web codifique la sesión con certificado digital, es decir con el certificado SET, que como ya mencionado anteriormente contiene información segura que posibilita la autentificación de la identidad de su propietario y de este modo, el usuario tiene ciertas garantías de que la información que envíe desde dicha página web no podrá ser interceptada ni utilizada por terceros.

Otra manera para conseguir un pago seguro y evitar ataques cibernéticos es contar con aspectos de seguridad básicos como antivirus, antimalware, cortafuegos y evitar ataques de Ingeniería social, es decir, no abrir ligas de personas desconocidas o mensajes extraños de nuestros conocidos ya que son el "blanco perfecto" para un malware.

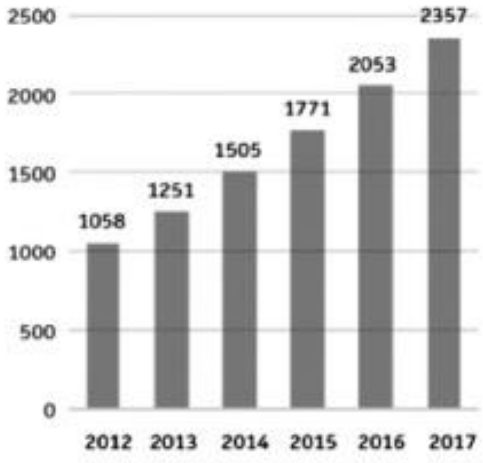
No obstante, el usuario también debe tener precaución para no dejar sus datos en manos de alguien malicioso frente a un keylogger, un tipo de software que se encarga de registrar las pulsaciones que se realizan en el teclado para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

En caso de tener un keylogger en el ordenador se puede engañar al mismo e impedirle que tenga el registro de las contraseñas de las tarjetas de crédito o de cualquier información confidencial bancaria que se esté ingresando para efectuar alguna compra. El keylogger no tiene acceso a la interfaz gráfica del ordenador, así que mientras se ingresa el registro en el sitio web en la que se efectuará la compra o en el que se hará alguna consulta, por ejemplo, para ingresar a un sitio web bancario, se utilizara un editor de texto en el que se ingresará dígitos al azar y que así el keylogger nunca tenga registro de la clave correcta del usuario.

Finalmente, el énfasis del presente escrito es el impacto que el comercio electrónico ha provocado sobre la sociedad y el crecimiento exponencial que este ha tenido pero teniendo en cuenta que del mismo modo que aumenta el comercio electrónico también aumenta la ciberdelincuencia y que como consecuencia se deben tomar medidas para evitar o al menos contrarrestar el dominio de un hacker malicioso sobre información personal o confidencial del usuario y en efecto, asegurar la privacidad y seguridad de datos cuando se realizan transacciones digitales o compras vía internet.

A continuación se muestra información en una grafica sobre cuanto ha crecido el comercio electrónico a nivel global y de Latinoamérica en los ultimos 6 años:

Figura 1. Estimaciones de ventas mundiales B2C *e-Commerce* 2012-2017 (Billones de dólares)



Fuente. eMarketer inc., (s.f.).

Se puede observar el crecimiento en ventas global estimado por eMarketer Inc (Figura 1), destacando que para 2017 se alcanzaron ventas alrededor de 2.35 trillones de dólares en comercio electrónico, lo que representa un 56.6% más que en 2014 y un 122.78% de crecimiento desde 2012. (Abad, 2014, p. 9).

3. CONCLUSIONES

Cada año el comercio electrónico en Colombia crece exponencialmente debido al esfuerzo que há realizado la Cámara Colombiana de Comercio Electrónico (CCCE) y la Superintendencia de Industria y comercio (SIC), entidades que arrojan resultados muy positivos pese a la desaceleración económica que vive el país.

Al paso del tiempo diferentes empresas de la industria tecnológica se han ido consolidando en los proyectos de seguridad informática como lo son los protocolos SET y SSL, estas empresas importantes reafirman que el comercio electrónico está en constante crecimiento y, por ende, ellos deben continuar garantizando un espacio seguro.

Los hackers maliciosos seguirán buscando la forma de filtrarse entre los protocolos de seguridad y derribar a los mismos para lograr objetivos ilícitos, entendiendo que por más completo que este un protocolo, seguirá teniendo altas vulnerabilidades. Sin embargo, la seguridad informática seguirá en la búsqueda y actualización de nuevos protocolos para así mantener la confianza de los usuarios y seguir combatiendo a estos hackers maliciosos

Referencias

[1] P. GARCÍA Y F. ÁLVAREZ. El comercio electrónico y la seguridad de sus transacciones. Investigación y Ciencia. 2009, p. 41-47.
[2] L. MARTÍNEZ, F. MATA Y R. RODRÍGUEZ. Sistemas de pago seguro, seguridad en el comercio electrónico, 2009, pp. 63-67.
[3] J. HERNANDEZ (1999, Jun 28) [Online] Avaible: http://www.eltiempo.com/archivo/documento/MAM-915340 [Consultado el: 10 de mayo de 2018].
[4] J. HERNÁNDEZ (2017, Dic. 13) [Online] https://www.elespectador.com/economia/el-boom-del-Comercio-electronico-artículo-728305 [Consultado el: 10 de mayo de 2018].
[5] F. GÓMEZ, E. ISABEL. Las medidas de seguridad del comercio electrónico en las pymes. pp. 23-33, 2003.
[6] IBM (2002, Nov 15) [Online] https://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user276.htm [Consultado el: 10 de mayo de 2018].
[7] Y. JIMÉNEZ, J. VEGA. Que es protocolo SET, Universidad de la Sallé, Bogotá, Colombia, (2014, abril 14)
[8] El comercio electrónico en Colombia [abril, 2017] [Online] https://www.crcom.gov.co/recursos_user/2017/ComElecPtd_0.pdf
[9] COMISIÓN EUROPEA [1999] [Online] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:51997DC0157&from=EN [Consultado el: 2 de mayo de 2018].
[10] M. CASTAÑEDA, M. MORALES. &Quot;Seguridad en las transacciones Electronicas" (Tesis de pregrado).
Universidad javeriana, Colombia. pp 45, 2004.
[11] A. LÓPEZ (2015, mayo 14). Ciberseguridad en los países del MINT. Revista de Tecnologías de la Información. Vol.2 No.3. pp. 155-167.
[12] OBSERVATORIO ECOMMERCE. (2018, abril 5). [Online] https://observatorioecommerce.com/ [Consultado el: 11 de mayo de 2018].
[13] DIGICERT (2008, junio) [Online] https://www.digicert.com/ [Consultado el: 5 de mayo de 2018].
[14] L. ROMERO (2008) [Online] http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf [Consultado el: 1 de mayo de 2018].
[15] ABAD, F. C. (2014). Influencia de las tecnologías de la información y comunicación en el rendimiento de las micro, pequeñas y medianas empresas colombianas. Estudios Gerenciales, 30(133), p. 9.
[16] L. ROMERO (2018) https://ecommerce-news.es/emarketer [Online] [Consultado el: 31 de mayo de 2018].