La importancia del sistema de gestión de la seguridad de la Información en el comercio electrónico empresarial

The importance of the Information Security management system in the Electronic Business commerce

Alexander Lozano
alexander.lozano00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de sistemas

Resumen

La apertura económica generada por los procesos globalizadores ha permitido que la tecnología de los sistemas de información agilice los procesos comerciales, administrativos y financieros de las empresas, facilitando los sistemas de pago y las gestiones de comunicación con los clientes, proveedores y empleados. Sin embargo, en la medida en que se ha ido desarrollando el comercio de las empresas por internet, se apuesto en escena la seguridad de la información como un elemento de mucha importancia para los clientes.
Es por ello que los sistemas de gestión de seguridad de la información en el comercio electrónico, se convierte en una herramienta de vital importancia para aquellas empresas que realizan negocios por este medio, dado que allí se diseñan políticas y estrategias que permiten planificar sistemas comerciales confiables para los usuarios e internautas.
En este orden de ideas, el presente trabajo busca identificar los argumentos que permitan demostrar la necesidad de implementar sistemas de seguridad de la información en las empresas que realizan comercio electrónico, puesto que todavía existen compañías colombianas que, en esta materia se encuentran haciendo negocios en medio de la informalidad informática, sin considerar aspectos que son indispensables para su seguridad y la de sus clientes.
De acuerdo a lo anterior, el presente trabajo se desarrolló en tres secciones, la cual inicia con una descripción general de la importancia que tiene el comercio electrónico en las empresas, dado que aquí se busca contextualizar el tema para hacerlo comprensible a la hora de abordar los principales riesgos que enfrenta el sector, aspecto que se muestra en la siguiente sección, donde se intenta poner en contexto las principales amenazas informáticas que se vislumbra en este tipo de comercio. Posteriormente se finaliza con una sección que relata la importancia de implementar los Sistemas de Gestión de Seguridad de la Información SGSI en dichas organizaciones para ofrecer una mayor confianza a sus clientes y partes interesadas en las actividades comerciales que se desarrollan en estos modelos de negocio.

Palabras Clave: Comercio electrónico, seguridad de la información, sistema de gestión, internauta, ciberserguridad.

Abstract

The economic opening generated by the globalizing processes has allowed the information systems technology to speed up the commercial, administrative and financial processes of the companies, facilitating payment systems and communication processes with customers, suppliers and employees. However, it is wagered on stage information security as an element of great importance for customers.
That is why the information security management systems in electronic commerce, becomes a vital tool for those companies that carry out business by this means, since there are designed policies and strategies that allow to plan reliable commercial systems for users and Internet users
In this order of ideas, this paper seeks to identify the arguments that allow demonstrating the need to implement information security systems in companies that conduct electronic commerce, since there are still Colombian companies that in this area are doing business in means of informatic informality, without

considering aspects that are essential for their safety and that of their clients.
According to the above, the present work was developed in three sections, which begins with a general description of the importance of electronic commerce in companies, since here we seek to contextualize the issue to make it understandable when addressing the main risks facing the sector, an aspect shown in the following section, where the main computer threats that are envisaged in this type of trade are attempted to be put in context. Subsequently, it concludes with a section that recounts the importance of implementing the Information Security Management System in these organizations to offer greater confidence to their clients and interested parties in the commercial activities that are developed in these business models.

Keywords: Electronic commerce, information security, management system, Internet user, cyber security.

1. INTRODUCCIÓN

El desarrollo del internet a nivel mundial se ha convertido en la plataforma ideal para fortalecer el crecimiento de los negocios, pues allí es donde las empresas están concentrando sus esfuerzos para realizar la compra y venta de bienes y servicios (Chiriguayo Lozano, 2015).

En el entorno colombiano, también se evidencia que no ha sido ajeno a este importante crecimiento con un 64% y unas ventas de US$26.700 millones para el año 2016, gracias a que los consumidores ven en el comercio electrónico un sistema cómodo, fácil y rápido para realizar sus transacciones (BlackSip, 2017).

En este sentido, se observa que hay una buena dinámica de crecimiento del comercio electrónico, tanto para el empresario como para el consumidor, lo cual genera mayores riesgos en la seguridad de información para ellos, al presentarse estafas, robo de información, hackeos, entre otras modalidades de delitos informáticos que los perjudican (Chiriguayo Lozano, 2015).

Sin embargo, gran parte de las empresas colombianas no se encuentran preparadas para enfrentar los problemas de seguridad informática que surgen con el auge del comercio electrónico, dado que en el empresariado colombiano la mayoría de empresas son micros, pequeñas y medianas donde se concentra más del 95% de ellas, la cual se caracteriza por una alta informalidad administrativa (Ministerio de Industria, Comercio y Turismo, 2016) que se vislumbra en la falta de politicas y procesos que proporcionen controles preventivos y correctivos que permita la reducción de riesgos.

De acuerdo a lo anterior, el escenario actual de seguridad de la información que se presenta entre las empresas colombianas y el comercio electrónico, revela una necesidad apremiante de generar procesos formalizados que blinden las relaciones comerciales por internet, mediante sistemas de gestión que ofrezcan garantías a los clientes y grupos de interés en la confidencialidad, integridad y disponibilidad de la información que se mueven en estos medios de comunicación. Es por ello, que el presente trabajo tiene el propósito de analizar la importancia del sistema de gestión de la seguridad de la Información en el comercio electrónico empresarial.

Esta temática ha sido tratada por una variedad de autores de diferentes profesiones, quienes con sus investigaciones aportaron referentes bibliográficos para la realización de este artículo de reflexión. Entre ellos se destaca el trabajo de Chiriguayo (2015) quien elaboró un análisis sobre la importancia de la seguridad en las transacciones electrónicas, donde diseño un estudio de tipo descriptivo para identificar las principales amenazas que enfrenta una empresa en el tema de seguridad electrónica, estableciendo que las empresas deben conocer los principales delitos informáticos que ocurren en su sector, para inducir procesos de mejora que tiendan a reducir estos riesgos.

También se destaca el trabajo del Instituto Nacional de tecnologías de información de España (2017), cuyo objetivo erá describir los procesos de Implantación de un Sistema de Gestión de Seguridad de la Información SGSI en la empresa, la cual orienta de manera objetiva sobre los aspectos que debe tener en cuenta toda organización para el diseño de un SGSI, puesto que ofrece unas fases puntuales que permiten la identificación de riesgos y la formulación de politicas, estándares y estrategias que toda compañía debe tener como minimo para gestionar la seguridad en las actividades de comercio electronico que realice.

De igual manera es necesario considerar los aspectos legales que enmarcan el comercio electrónico en Colombia, dado que el sustento normativo en la materia es necesario para el diseño de un Sistema de Gestión de Seguridad de la Información SGSI en la empresa, la cual se encuentra referenciado de una manera organizada en el trabjo de García (2004) quien describe las normas partiendo de lo general con el ambito constitucional hasta llegar a lo particular, mencionando el aspecto sectorial.

Se realizo una revisión de los elementos generales de las normas ISO 27001 (Asociación española de usuarios de telecomunicaciones y de la sociedad de la información, 2015), la cual define los lineamientos

para el diseño de Sistemas de Gestión de Seguridad de la Información SGSI en las empresas, de tal manera que se pueda obtener una mayor comprensión sobre los recursos y actividades que requieren los empresarios para desarrollar procesos de implementación, además de identificar sus principales ventajas al aplicarlas.

Conforme a este análisis de referencias se procedio en el desarrollo del presente documento que esta estructurado en tres secciones, iniciando con una descripción de la importancia del comercio electronico para las empresas, posteriormente se muestra los principales riesgos en la seguridad de información de comercio electronico que enfrentan las empresas, para finalizar con un análisis de la manera como los Sistema de Gestión de Seguridad de la Información SGSI pueden evitar las amenazas informaticas en las actividades comerciales que realizan las empresas en los medios virtuales.

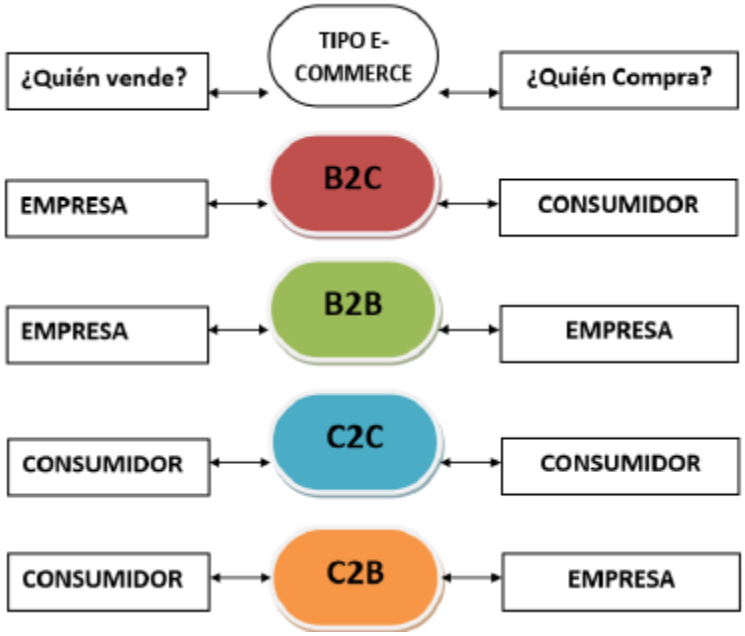
1.1 Importancia del comercio electronico en las empresas

El comercio electrónico en Colombia ha sido determinante para la economía del país, pues ya se ubica con una participación del 4% (BlackSip, 2017) en el PIB (Producto interno bruto), lo que obedece a una serie de factores que remarcan su importancia frente al comercio tradicional.

Como primera medida el empresario que se encuentre inmerso en el comercio electrónico dispone de una plataforma comercial que le permite realizar transacciones las 24 horas al día en cualquier lugar del mundo y a un costo muy reducido (Anteportamlatinam Valero, 2014).

De igual forma con este modelo de negocio los empresarios pueden reducir sus cadenas de distribución, dado que se genera una relación directa entre cliente – empresa y empresa – proveedor, permitiendo una reducció sustancial de costos y de tiempos de respuesta entre las partes. Estas relaciones mencionadas tienen una descripción técnica que se conocen como tipos de comercio electrónico, las cuales se pueden evidenciar en la figura 1 que se muestra a continuación.

Figura 1. Tipos de comercio electrónico



Fuente: Adaptado de (Asociación Española de la Economía Digital, 2013)

De acuerdo a la figura 1, el comercio electrónico puede darse en la categoría B2C que es la que se produce entre empresa y consumidor; en la categoría B2B que es cuando se produce de empresa a

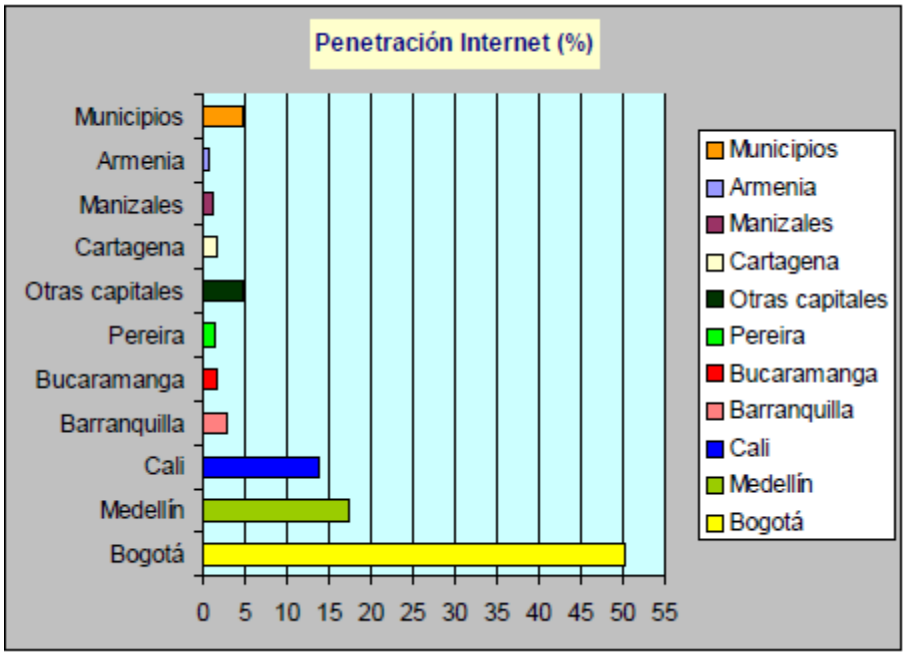
empresa, en la categoría C2C que se da de consumidor a consumidor y la categoría C2B que se da de consumidor a empresa. Todas ellas con la facilidad que tienen las empresas de establecer relaciones directas entre las partes, teniendo la oportunidad de generar estrategias de fidelización con sus clientes a un menor costo y un mejor control para medir la efectividad de sus acciones de mercadeo.

En este aspecto Ferrari (2017) afirma que el empresario tiene importantes ventajas, dado que en el comercio tradional no es posible conocer en detalle la información de los clientes que llegan al establecimiento, mientras que en el comercio electrónico es posible rastrear el tipo de cliente que compra, especialmente en el lugar que vive, la edad que tiene, sus gustos, entre otras variables que sirven de referentes para la realización de investigaciones de mercado. Dado que dicha información obtenida de los consumidores es posible administrarlas en bases de datos que permiten analizarla mediante indicadores estadisticos que determinan el comportamiento de compra de estas personas, tales como: "sitios Web visitados, duración de las visitas en un sitio, páginas visitadas en un sitio, contenido de listas de deseos y carritos de compras, adquisiciones, comportamiento en compras repetidas, número de visitantes que completan el proceso de compra, entre otras mediciones (Anteportamlatinam Valero, 2014).

Por otro lado, los empresarios tienen la facilidad de ofrecer una gran variedad de productos en las plataformas virtuales sin necesidad de tener amplias estanterias y bodegas con inventario. Además de permitir que los clientes puedan realizar sus pagos de una manera facil y comoda desde cualquier lugar del mundo.

En el caso colombiano, el comercio electrónico se desarrollado de manera rapida en las ciudades más grandes, dada por las facilidades logisticas que estas grandes urbes ofrecen para la implementación de infraestructura tecnologica, donde existe una alta penetración de internet (Ver figura 2) en la población, además de que allí se concentra la mayor cantidad de empresas (García Santiago, 2004, p. 36).

Figura 2. Penetración de internet en las ciudades colombianas



Fuente: Adaptado de (García Santiago, 2004, p. 36)

Esta dinámica ha favorecido el crecimiento del comercio electronico en Colombia, dado que el mercado ya se encuentra más conectado electrónicamente con diversos medios de comunicación como equipos de computo y equipos moviles. Sin embargo, es preciso señalar que los empresarios que laboran

en este medio presten una mayor atención en sus sitemas de seguridad cibernetica y más cuando se encuentran en las grandes ciudades que por su alta actividad comercial y su mayor penetración a internet, es donde existe un mayor riesgo, debido al volumen de negocios que se manejan allí, donde se evidencia que Bogotá con un 80% y Medellin con un 72% son los que mayor comportamiento de acceso y consulta en línea tienen en la compra de bienes y servicios (Ministerio de la Tecnología de Información y Comunicaciones, 2019).

En este sentido, se puede concluir que definitivamente el comercio electrónico se esta constituyendo en la herramienta de venta más importante para las empresas, pues estar fuera de ella, se convierte en un riesgo de perdida de mercado en crecimiento que puede potenciar su sostenibilidad financiera en el mediano y largo plazo.

1.2 Riesgos en la seguridad de información de comercio electrónico que enfrentan las empresas

Es necesario que los empresarios que desarrollan actividades de comercio electrónico comprendan la importancia de identificar los principales riesgos que generan delitos informaticos, dado que este conocimiento fomenta las bases para establecer estrategias de cyberserguridad en sus organizaciones, además de generar un entorno confiable para los compradores y actores interesados.

De acuerdo a Benitez (2016), el aspecto economico es el mayor motivador de los delitos informaticos, los cuales pueden estar relacionados con el robo de información de la empresa, hasta el robo de los datos bancarios de los clientes, donde pueden utilizar esta información para vendersela a otras compañias competidoras o para realizar estafas financieras con las cuentas bancarias.(p. 8).

Adicionalmente, pueden existir motivaciones de tipo organizacional las cuales están representadas en:

- Daños a la imagen de la empresa: donde tienden a modificar las paginas web de las empresas con información falsa o para degradar su presentación, de tal manera que se logre la desconfianza de los consumidores y su good will en el mercado se vea afectado. (Benitez, 2016).
- Ataque a terceros con la técnologia de las empresas: En este escenario los ciberdelincuentes utilizan las web de las empresas que son inseguras para enviar malware, alojar un phishing, infectar los servidores web con el proposito de realizar estafas economicas en nombre de la compañía. (Benitez, 2016).

Para Chiriguayo (2015), en el comercio electrónico pueden darse de dos maneras: una que es a nivel interno, es decir que se produce dentro de la organización, por medio del robo de información o en la falsedad de documentos electrónicos para realizar estafas utilizando el nombre de la empresa. Existe otras amenazas a nivel externos, siendo las más comunes: “Virus, gusanos y caballos de Troya, Spyware y adware, Ataques de día cero, también llamados “ataques de hora cero”, ataques de piratas informáticos, ataques por denegación de servicio, interceptación y robo de datos, robo de identidad”(p, 11). En efecto, cada ataque pone en riesgo la seguridad de la información ocasionando perdidas economicas como consecuencia de las denegaciones de servicios, secuestros de información valiosa para las empresas o puede llegar a ser mucho peor como lo es la reputación corporativa.

Hay autores como Font (2000) que agrupan por categorizan las amenazas informáticas para darle una mejora identificación a los empresarios que promueven estrategias de seguridad:

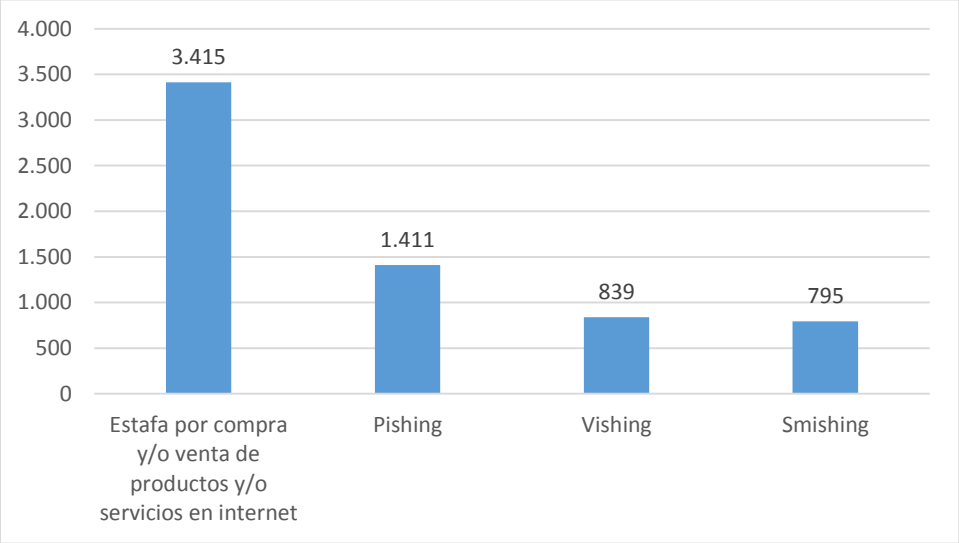
- “Ataques de red: Estas se generan en las redes de internet, las cuales tienden a poner lentos los equipos, afectando los correos electrónicos de las empresas y las redes internas sin ocasionar daños definitivos en los sistemas operativos.
- Las infiltraciones: Este tipo de ataques informaticos se producen dentro de los sistemas operativos, en el cual se busca conocer las claves de los empleados, de los distintos sistemas

de información y areás claves con el proposito de robar información de tipo economico o para generar caos interno dentro de la organización para afectar su imagen ante los clientes.

- El código maligno: En esta categoría se encuentran todas aquellas amenazas de caracter externo que se describió anteriormente con Chiringuayo (2015), donde se destacan los virus y los gusanos.

Por otro lado, se debe destacar que en el entorno Colombiano las cifras de delitos informaticos vienen aumentando de manera preocupante, las estadisticas oficiales de la Policia Nacional advierte que para el año 2017 las denuncias por estos crimenes se incrementaron en un 28,3%, respecto al año anterior, afectando a 446 empresas del país (Portafolio, 2019). Dichas estadisticas apuntan que las acciones más delictivas se presentan en el comercio electrónico. Ver figura 3.

Figura 3. Relación de crímenes informáticos más comunes en Colombia año 2017



Fuente: Adaptado de (Policia Nacional de Colombia, 2018, P. 4)

De acuerdo al estudio de la Policia Nacional, estos delitos se producen “por incumplimiento de alguna de las partes, bien sea en el envío o recibo de productos vendidos o comprados en las plataformas, ó en el cambio de las condiciones y calidad de los mismos”. En el pishing es donde ciberdelincuente toma los datos de un usuario legitimo para tomar datos confidenciales como correos, contraseñas y datos bancarios para realizar fraudes Mientras que en los delitos vía vishing y smishing, hace referencia al uso de marcas de empresas e instituciones reconocidas para difundir mensajes y despues el delincuente llama ofreciendo dadivas por parte de operadores de telefonía celular y almacenes de cadena, las falsas ofertas en bolsas de empleo virtuales y la falsa llamada del sobrino retenido” (Policia Nacional de Colombia, 2018).

Pero lo peor, es que se evidencia una falta de conciencia de los empresarios nacionales en la implementación de procesos que permitan la identificación de riesgos informaticos, dado que el 83% de ellas no cuentan con protocolos de respuesta a la violación de politicas de seguridad informatica (Portafolio, 2019). A esto se le suma que las empresas muy poco invierten en capacitación al personal (el 72% de ellas), a pesar de que el 63% considera razonable que sus colaboradores dominen las Tecnologias de Información y Comunicación TIC(Portafolio, 2019). En efecto estos acontecimientos evidencian que son pocas las empresas que cuentan con un sistema de gestión de seguridad informatica que les proporcione politicas, manuales, estrategias y recursos economicos y humanos que les permita enfrentar de manera objetiva los riesgos que se generan en los canales de comercio electronico.

Se puede concluir entonces que son muchos los riesgos ciberneticos que tienen las empresas que se encuentran dentro del comercio eletronico, dado por el mercado en crecimiento que tienen estos modelos de negocios, donde resulta dificil identificar los ciberdelincuentes.

1.3 Validez de los Sistemas de Gestión de Seguridad de la Información SGSI en el comercio electrónico de las empresas

De acuerdo a la Asociación española de usuarios de telecomunicaciones y de la sociedad de la información (2015) que relaciona los elementos de la Norma ISO 27000, define un Sistema de Gestión de Seguridad de la Información SGSI como un "proceso que tiene el proposito de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías"(p. 2).

Algo similar fue descrito por Inteco (2017) cuando afirma que un Sistema de Gestión de Seguridad de la Información SGSI "es una herramienta de gestión que permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en la empresa(p.3).

Esto significa que los Sistemas de Gestión de Seguridad de la Información SGSI es un instrumento que permite reducir los riesgos de delitos informaticos en las empresas, dado que se formula bajo procesos que ayudan a identificarlos y atacarlos con estrategias específicas. Según Montes (2014) la gestión del Riesgo es el "Conjunto de actividades planeadas que sirven para manejar y realizar seguimiento a una empresa en lo que respecta al riesgo" Es, por lo tanto, una función estratégica, transversal e imprescindible de la empresa bien gestionada. También es responsabilidad de toda la empresa y al frente el Consejo de Administración, junto con la finalidad de lograr la consecución de los objetivos estratégicos y la obtención de ventajas competitivas, a través del conocimiento global del riesgo de la organización y su incidencia en el logro de dichos objetivos. (p, 186).

Este concepto pone en evidencia que en estos sistemas se ofrecen una serie de actividades que van conectadas entre si para poder enfrentar los riesgos, pues en el entorno empresarial se encuentran ciertas organizaciones que cuentan con dispositivos de seguridad como lo son cortafuegos o firewall, software de antivirus, actualizaciones de sistemas operativos, renovaciones de equipos entre otros para detectar posibles ataques, pero no se complementan con una serie de medidas integradas objetivamente que procuren realizar un seguimiento para tomar decisiones efectivas en la materia.

La validez de los Sistemas de Gestión de Seguridad de la Información SGSI es una necesidad apremiante para enfrentar el fraude en el comercio electrónico, dado que estos sistemas plantean soluciones a una problemática que es multidisciplinar (Cano, 2016), es decir que es necesario combatirla desde las distintas disciplinas y procesos que desarrollan las empresas, puesto que el fraude no solo se genera desde el ambito comercial, sino que puede estar produciendose desde el ambito administrativo, operativo o financiero. Esto quiere decir que los SGSI debe ser un complemento de otros sistemas de gestión que tengan las organizaciones, como es el caso de los Sistemas de Gestión de Calidad, entre otros.

Lo anterior indica que los Sistemas de Gestión de Seguridad de la Información SGSI se convierten en un instrumento que incentiva el compromiso de todos los miembros de la organización, dado que este fomenta el desarrollo de una cultura de seguridad informatica, en la cual es necesario formalizar todos los procesos de la empresa, mediante la documentación y el diseño de indicadores que midan la efectividad del sistema (Asociación española de usuarios de telecomunicaciones y de la sociedad de la información, 2015).

De tal manera que un Sistemas de Gestión de Seguridad de la Información SGSI no solo se convierte

en una herramienta que sirve para minimizar riesgos en el comercio electrónico, sino que es un modelo de mejoramiento que trae beneficios de gestión en toda la organización, dado que estos se sustentan en modelos sistemicos de procesos de mejora continua que de acuerdo a Chase, R., Aquilino, N., & Jacobs, F (2006), el mejoramiento de Deming fomenta el pensamiento orientado a procesos, “ya que los procesos deben perfeccionarse para que mejoren los resultados. El hecho de no lograr los resultados planeados indica una falla en el proceso. La gerencia debe identificar y corregir tales errores debidos al proceso”. (p,187).

El “Mejoramiento de procesos se presenta en un ciclo de mejora continua que cuenta con las siguientes fases Chase (2006):

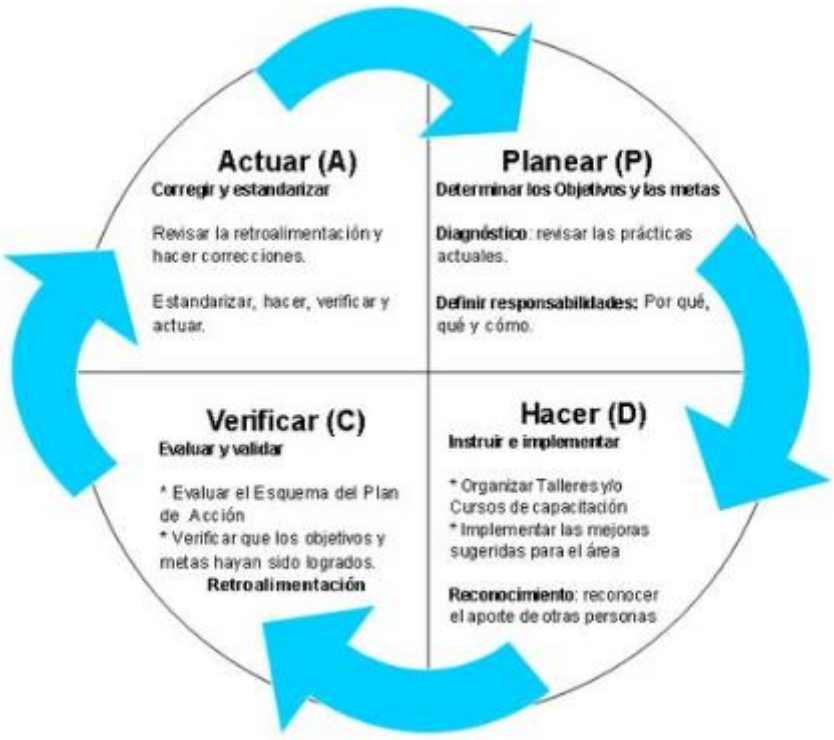
Planeación: En esta fase se determinan las actividades que se van a desarrollar para llevar a cabo la mejora, en ellas se establecen objetivos medibles a traves de indicadores que permiten hacerle seguimiento al plan.

Ejecución: Despues de haberse planeado se procede a ejecutar las acciones propuestas, teniendo en cuenta la recolección de información requerida para realizar el respectivo proceso de verificación.

Verificación: Es el proceso mediante el cual se realiza un análisis comparativo entre los resultados obtenidos en la ejecución frente a las metas definidas en la planeación, pues la idea es identificar si realmente se esta cumpliendo con lo presupuestado y si el plan va dar los resultados deseados.

Actuar: En esta etapa se procede a desarrollar las acciones de mejora que se requieren para corregir las fallas encontradas en el proceso de verificación. Ver figura 4.

Figura 4. Ciclo de mejora de un Sistema de Gestión de Seguridad de la Información SGSI



Fuente: Adaptado de (Chase, Aquilino, & Jacobs, 2006)

La herramienta PHVA que se explico anteriormente es empleado para mantener las labores de control y seguimiento, mediante indicadores donde se han definido unos estandares aceptables que le dan validez a sus procesos y de un sistema que hace parte de los “procedimientos Operacionales de Estándar

POE" (Chase, Aquilino, & Jacobs, 2006, p. 192).

Este modelo de mejoramiento fue creado por Edward Deming (1986), un prestigioso investigador de Estados Unidos que centraba su atención en el fortalecimiento del capital humano para impulsar la calidad. En esta misma línea contribuyo Jhosep Juran (1980), cuando manifestaba que los equipos de trabajo mejoraban las capacidades para aumentar la calidad. A su vez contribuyo el investigador Phillip Crosby (1979) quien manifestaba que la calidad es un resultado de un compromiso entre la dirección y los empleados.

De acuerdo a este precepto teorico de mejoramiento, las empresas que implementan este instrumento han tenido que incorporar programas de concientización y de capacitación entre los funcionarios de la empresa. En este aspecto Reyes (Reyes, 2016) manifiesta que las capacitaciones a los funcionarios deben enfocarse en modelos de seguridad de la información y en normas internacionales de comercio electronico que sean un referente para la implementación de acciones de ciberseguridad, las cuales están enmarcadas en las "ISO/IEC 27001 (estándar para la implementación de un sistema de gestión de la seguridad de la información), ISO 27017 (estándar para la aplicación de controles de seguridad de información en sistemas o servicios basados en computación en nube) e ISO 27032 (Guía sobre ciberseguridad), entre otras.(p. 13).

De igual manera, estas medidas deben ir acompañadas de una comunicación permanente entre los miembros de las diferentes áreas de la empresa para ir registrando y hacerle seguimiento a las modalides de delitos informaticos más comunes, de esta forma se pueden ir mejorando las politicas o controles de ciberseguridad, además de mejorar los sistemas de información y la infraestructura tecnologica con sus respectivas actualizaciones que requieren los equipos de computo en hardware y software, las cuales deben ser permanentes.

Conforme a estas medidas las empresas que implementan los Sistemas de Gestión de Seguridad de la Información SGSI va lograr en primera instancia minimizar los riesgos en el comercio electrónico, donde se genera un compromiso integral de todos los funcionarios de la organización, la fortalecerá la imagen de la compañía en sus segmentos de mercado. Adicionalmente este sistema le va a proporcionar la información suficiente para realizar inversiones planeadas y efectivas, dado que se enfoca en las necesidades de la organización, generando una mayor eficiencia en el uso de sus recursos financieros para estos propósitos.

Por otro lado, estas medidas pasan a convertirse en un ciclo repetitivo como el planteado en la figura 4, donde participa todos los funcionarios de la organización con el propósito de promover las mejoras correspondientes, existiendo un mayor interés de sus directivas por formalizar todos sus procesos, lo que fortalece a un más, las medidas de ciberseguridad propuestas.

Adicionalmente, las empresas pueden dar cumplimiento al marco legal vigente, evitando posibles sanciones o demandas intempestivas, que en el caso colombiano están consagrados en la ley 527 de 1999, la cual tiene una definición amplia de las actividades que se pueden realizar en el comercio electrónico. Igualmente es necesario resaltar la Ley 1581 de 2012 que hace referencia a la norma que regula la protección de datos, la cual se expone en el artículo 1 de la presente norma: *"Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"* (Ministerio de comercio, industria y turismo, 2013). Esta regulación es muy importante revisarla, dado que las empresas requieren de la implementación de sistemas de seguridad que protejan los datos de sus usuarios, además porque de no aplicarlas se someten a fuertes sanciones que van desde multas economicas hasta la cancelación del uso de las franquicias como Visa, Mastercard, American Express, Diners por citar las mas conocidas. Entre dichos sistemas, se destaca las normas de seguridad de datos de la industria de tarjetas de pago

(Payment Card Industry Data Security Standard) que se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. La PCI DSS proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas.

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Desarrolle y mantenga redes y sistemas seguros.	**1.** Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. **2.** No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	**3.** Proteja los datos del titular de la tarjeta que fueron almacenados **4.** Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	**5.** Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. **6.** Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	**7.** Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. **8.** Identificar y autenticar el acceso a los componentes del sistema. **9.** Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	**10.** Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta **11.** Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	**12.** Mantener una política que aborde la seguridad de la información para todo el personal

Tomado de la guía de requisitos y procedimientos de evaluación de seguridad Versión 3.2 abril de 2016

Estas se aplican a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD). (Consejo sobre Normas de seguridad de la PCI, 2016).

Esto obedece a que los usuarios que realizan transacciones en internet deben de dejar sus datos personales, lo que se constituye en una responsabilidad de las empresas de proteger la información que dejan sus usuarios en sus sistemas de información electronica, de tal manera que se garantice la confidencialidad de sus datos y se reduzcan los riesgos de fraude en el mercado del comercio electrónico.

Por lo tanto, todos los empresarios que trabajan en el comercio electrónico deberian adaptarse a los estándares de pago electrónico del PCI para garantizarle la seguridad de los datos que suministran sus clientes, dado que si no lo hacen y sucede algún fraude en este proceso, la empresa está sujeta a pagar una multa por parte de la asociación de tarjetas, además de asumir la responsabilidad económica y legal que provenga de estos hechos delictivos. Pero en caso de cumplir con estos parámetros la multa podría ser mínima e incluso no ser responsable de las transacciones fraudulentas.

En el cuadro que se muestra a continuación se evidencia las clasificaciones de las empresas que realiza el PCI, de acuerdo al número de transacciones.

Tipo de empresa	Número de transacciones realizadas
Nivel 1	El comerciante acepta / procesa más de 6 millones de transacciones de Visa por año y/o está identificado como Nivel 1 por el Consejo de Normas de Seguridad.
Nivel 2	El comerciante acepta / procesa de 1 a 6 millones de transacciones en línea de Visa (todos los canales) o MasterCard anualmente.
Nivel 3	El comerciante acepta / procesa entre 20,000 y 1 millón de transacciones en línea de Visa o MasterCard anualmente.
Nivel 4	El comerciante acepta / procesa menos de 20,000 transacciones en línea Visa o MasterCard.

Fuente: Autor con base a Consejo sobre Normas de seguridad de la PCI. (Abril de 2016).

De tal manera que estos Sistemas de Gestión de Seguridad de la Información SGSI, a través del PCI son importantes puesto que permite a las empresas que utilizan medios de pago en el comercio electrónico certificarse, abriéndole puertas a nuevos mercados, puesto que mejora la imagen con los clientes, proveedores y socios, facilitando la asociación con otras organizaciones que pueden ser estratégicas para su crecimiento corporativo.

La certificación es una distinción que obtiene una compañía que trabaja en el mejoramiento de sus prácticas y procesos, los cuales buscan ajustarse a estándares mínimos que se exigen en un mercado, quienes generalmente están adaptados a parámetros internacionales. (Zuckerman, 1999). Por lo tanto es un premio para aquellas empresas que siempre intenta mejorar sus procesos y sus productos.

Estas certificaciones son importantes para una empresa facilita la entrada a los mercados por la confianza que genera sus productos, los cuales cumplen con estándares mínimos de seguridad exigidos por las autoridades de un país, además de cumplir con las exigencias del consumidor.

Adicionalmente la certificación permite que la empresa obtenga un producto diferenciado que le permite ser competitivo en un mercado, aspecto que a su vez genera oportunidades para que la empresa participe en el mercado con precios más altos, en coherencia con dicha diferenciación.

2. CONCLUSIONES

De acuerdo al análisis realizado en este artículo de reflexión se pudo determinar que el auge que produce el crecimiento del comercio electrónico a nivel mundial, obliga a todas las compañías que participan en este sector a tomar las medidas necesarias que les permita reducir sus riesgos de seguridad en sus sistemas de información.

En este sentido los Sistemas de Gestión de Seguridad de la Información SGSI se han convertido en una herramienta estratégica para las organizaciones que desean mejorar su imagen en el mercado donde participan, dado que estos modelos de gestión permiten que las empresas formalicen sus procesos de seguridad informática, las cuales son importantes para establecer relaciones de confianza entre sus grupos de interés (Clientes, proveedores, socios, empleados, gobierno y comunidad).

No obstante, la mayoría de empresas y especialmente las colombianas son micros, pequeñas y medianas, quienes se caracterizan por su alta informalidad en sus procesos y donde los resultados de la investigación pudieron constatar que gran parte de ellas (el 83%) no son conscientes de los riesgos generados en la seguridad informática. Por tanto, los Sistemas de Gestión de Seguridad de la Información SGSI se convierten en una oportunidad para que dichas compañías formalicen sus procesos, mediante modelos de gestión que promueven el compromiso de todos los miembros de la organización,

partiendo desde sus esferas más altas de poder, quienes deben de impartir una cultura de seguridad que debe concientizar a todos los equipos de colaboradores para que trabajen en este propósito.

En el análisis realizado se pudo establecer que existen amenazas informáticas de carácter interno que es cuando se presentan dentro de la organización, siendo las más comunes el robo de información, y externo cuando se presenta fuera de ella, siendo las más comunes los virus y los gusanos. En este escenario de delitos informáticos al que se debe enfrentar las empresas, es importante que estén preparadas para asumir este tipo situaciones, la cual no solo le puede generar pérdidas económicas y de imagen, sino conflictos legales que puede impactar en sanciones o demandas inesperadas.

Es por ello, que un modelo de detección de riesgos se convierte en una herramienta valiosa que ayuda a que las organizaciones identifiquen sus principales debilidades de seguridad informática para contrarrestarlas mediante estrategias planeadas y orientadas objetivamente con un Sistema de gestión de Seguridad que se administra, a través de políticas, estándares de seguridad, procesos e indicadores que ayudan a gestionar dichos riesgos.

En el caso colombiano, los estudios de seguridad informática de la Policía Nacional revelan que, en los procesos de compra y venta por internet, es donde se presentan los mayores delitos informáticos, lo que se convierte en una necesidad la implementación de sistemas de seguridad en estas empresas, dado que gran parte de estas denuncias se producen por incumplimientos y falsedad en la información que se generan en estos medios.

En términos generales se puede concluir que los Sistemas de Gestión de Seguridad de la Información SGSI encaminadas a fortalecer los procesos de ciberseguridad del comercio electrónico son modelos de gestión estructurados que permiten integrar todas las áreas y funcionarios de la organización para enfrentar con una cultura corporativa enfocada en la seguridad y el mejoramiento continuo con el propósito de reducir los riesgos de delitos informáticos en este tipo de actividades comerciales. De tal manera que estos modelos de gestión son importantes para las empresas que hacen parte de este sector, dado que define unos estándares mínimos que deben cumplir estas compañías para generar confianza al mercado, permitiendo a su vez consolidar un proceso que termine con una certificación internacional garantizando el acceso a nuevos mercados y como consecuencia unos mayores beneficios económicos para su negocio.

3. REFERENCIAS

Anteportamlatinam Valero, J. M. (Julio de 2014). Relevancia del E-comerce para la empresa actual. Soria, España: Programa de administración y dirección de empresas. Universidad de Valladolid.

Asociación Española de la Economía Digital. (2013). El libro blanco del comercio electrónico. Guía práctica de comercio electrónico para pymes. Madrid, España.

Asociación española de usuarios de telecomunicaciones y de la sociedad de la información. (2015). Sistema de Gestión de la Seguridad de la información ISO 27001. *Ambito*, 1-14.

Benitez, D. (Junio de 2016). Ciberseguridad en comercio electrónico. Una guía de aproximación para el empresario. Madrid, España.

BlackSip. (2017). Reporte de industria. El E-commerce en Colombia 2017. Bogotá, Colombia.

Cano, J. (2016). Fraude informatico: generoso caldo de cultivo. *Sistemas No. 139*, 4-6.

Chase, R., Aquilino, N., & Jacobs, F. (2006). *Administración de producción y operaciones.* Bogotá: Mcgraw Hill.

Chiriguayo Lozano, S. (2015). Comercio Electrónico: Importancia de la Seguridad en las Transacciones Electrónicas, Amenazas y Soluciones a Implementar. *Revista Empresarial, ICE-FEE-UCSG*, 8-14.

Consejo sobre Normas de seguridad de la PCI. (Abril de 2016). Norma de seguridad de datos de la industria de tarjetas de pago (PCI), versión 3.2.

Crosby, P. (1979). *Quality is free.* New York: Mcgraw Hill.

Deming, E. (1986). *Out of the crisis.* Michingan: Mit Press.

Ferrari Zamora, V. (2017). El comercio electrónico en Colombia: barreras y retos de la actualidad. Bogotá, Colombia: Especialización en derecho privado. Universidad Ponificia Javeriana.

Font, A. (2000). Seguridad y certificación en el comercio electrónico. Aspectos generales y consideraciones estratégicas. *Fundación Retevisión*, 35-49.

García Santiago, H. J. (Mayo de 2004). Seguridad en el comercio electrónico. Bogotá, Colombia: Facultad de Derecho. Universidad Pontificia Javerina.

Inteco. (Noviembre de 2017). Implantación de un Sistam de Gestión de Seguridad de la información en la empresa. Madrid, España.

Juran, J., & Grinna, F. (1980). *Quality planning and analisys.* New York: Mcgraw Hill.

Ministerio de comercio, industria y turismo. (27 de Junio de 2013). Decreto número 1377. Bogotá, Colombia.

Ministerio de Industria, Comercio y Turismo. (23 de Febrero de 2016). Reporte de Mypimes No 3. Bogotá, Colombia.

Montes Salazar, C. (2014). *Control y evaluación de la gestión organizacional.* Bogotá: Alfaomega.

Policia Nacional de Colombia. (2018). *Amenazas del cibercrimen en Colombia 2017 - 2016.* Bogotá: Dirección de investigación criminal de INTERPOL.

Portafolio. (2019). El secuestro de información desangra a las empresas del país. *Portafolio*, https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729.

Prieto Tellez, D. A. (2017). Seguridad de datos de tarjeta habiente, aplicando normas, regulación y buenas prácticas. *SIA 6*, 1-8.

Reyes, J. C. (2016). Fraude personal y corporativo. *Sistemas*, 12-16.