EL IMPACTO DEL DELITO CIBERNÉTICO EN LAS OPERACIONES DE COMERCIO ELECTRÓNICO EN COLOMBIA

PRESENTADO POR:

MARY LUZ PERALTA CUADRADO

EDUARDO ENRIQUE ROA IBARRA

PROGRAMA DE ADMINISTRACIÓN EN FINANZAS Y NEGOCIOS INTERNACIONALESFACULTAD DE CIENCIAS ECONÓMICAS, JURÍDICAS Y ADMINISTRATIVAS
UNIVERSIDAD DE CÓRDOBA
MONTERÍA-CÓRDOBA
2020 – II

EL IMPACTO DEL DELITO CIBERNÉTICO EN LAS OPERACIONES DE COMERCIO ELECTRÓNICO EN COLOMBIA

DIRECTOR:

DANIEL RODRÍGUEZ BERMUDEZ

CODIRECTOR:

MARIO URZOLA ÁLVAREZ

PRESENTADO POR:

MARY LUZ PERALTA CUADRADO

EDUARDO ENRIQUE ROA IBARRA

PROGRAMA DE ADMINISTRACIÓN EN FINANZAS Y NEGOCIOS INTERNACIONALESFACULTAD DE CIENCIAS ECONÓMICAS, JURÍDICAS Y ADMINISTRATIVAS
UNIVERSIDAD DE CÓRDOBA
MONTERÍA-CÓRDOBA
2020 – II

Agradecimientos

Queremos agradecer a Dios primeramente por ser nuestro guía en cada paso que dimos durante toda nuestra carrera universitaria, a nuestros padres por brindarnos su apoyo incondicional desde el momento que elegimos esta carrera sin importar las condiciones, a nuestros amigos incondicionales que fueron el equipo de trabajo durante todos los semestres, a nuestros profesores y en especial a nuestros asesores DANIEL RODRIGUEZ BERMUDEZ Y MARIO URZOLA ÁLVAREZ que siempre nos brindaron sus conocimientos y colaboración, que fueron esos guías importantes durante el último paso que dimos en la carrera y por ser parte de nuestra formación profesional y finalmente, pero no menos importante a la UNIVERSIDAD DE CÓRDOBA por ser la casa de estudios que durante cinco años nos brindó sus instalaciones y herramientas para culminar nuestra formación profesional.

Dedicatoria

Este logro lo dedicamos primero a Dios que ha sido y es nuestro guía en cada uno de los pasos que damos en la vida y que hemos dado durante el trayecto de toda nuestra carrera universitaria. Así mismo nos llenó de mucha de fe y esperanza para no flaquear y poder vencer cada obstáculo que se nos atravesaba en el camino.

También queremos dedicar este logro a nuestros padres en especial a JAIME ANTONIO PERALTA ATENCIO Y EDEN ROA OYOLA, quienes han sido esas personas que siempre nos han apoyado en todo y que con un consejo nos alentaban a seguir adelante para culminar con éxito nuestra carrera profesional.

Tabla De Contenido

Índice De Gráficas

Índice De Figuras

1. Resumen

En el presente estudio monográfico se abordará el impacto del delito cibernético en las operaciones de comercio electrónico en Colombia, así mismo los riesgos que incurren al momento de hacer operaciones de compra o venta, transacciones en línea, etc, además de ello se conocerá el crecimiento que ha tenido Colombia durante los últimos años en cuanto a operaciones de comercio electrónico, los diferentes sectores en los que ha crecido considerablemente y el comportamiento que ha tenido con la actual situación de pandemia Covid-19.

Se han desarrollado tres capítulos, de los cuales el primero está conformado por un breve resumen de las operaciones de comercio electrónico en Colombia desde el año 2015 hasta el presente año, los diferentes tipos y el crecimiento que ha tenido Colombia en esta modalidad de hacer negocios. En el segundo capítulo se mencionan los riesgos a los que están expuestas las personas al momento de realizar cualquier operación de comercio electrónico. Y por último, en el tercer capítulo se explica a manera de ejemplo como han ido invirtiendo las organizaciones en seguridad digital hoy en día para crear entornos seguros en operaciones de compra y venta on line y brindar seguridad y confidencialidad en sus datos.

Palabras claves: comercio electrónico, delitos cibernéticos, seguridad, confianza, inseguridad.

2. Abstrac

This case study will address the impact of cyber-crime on e-commerce operations in Colombia, as well as the risks involved in buying or selling, online transactions, etc. In addition, it will show the growth that Colombia has had in recent years in terms of e-commerce operations, the different sectors in which it has grown considerably and the behavior it has had with the current situation of the Covid-19 pandemic.

Three chapters have been developed, of which the first one is conformed by a brief summary of the e-commerce operations in Colombia from the year 2015 to the present year, the different types and the growth that Colombia has had in this modality of doing business. The second chapter mentions the risks to which people are exposed at the time of performing any e-commerce operation. And finally, the third chapter explains, as an example, how organizations have been investing in digital security today to create safe environments for online buying and selling operations and to provide security and confidentiality to their data.

Keywords: e-commerce, cybercrime, security, trust, insecurity

3. Introducción

El comercio electrónico también conocido como e-commerce, comercio por internet o comercio en línea consiste en la distribución, compra, venta, marketing y suministro de información de productos o servicios a través de internet (Zamora, 2017), este ha venido creciendo en los últimos años a una velocidad vertiginosa, según cifras de la cámara colombiana de comercio electrónico hasta agosto del presente año las ventas acumuladas ascienden a $17,1 billones por medios digitales, es decir casi 3 billones por encima del mismo periodo del año 2019, en este mismo sentido, la tasa de delitos informáticos ha crecido de manera proporcional, algunos de éstos delitos como el hurto de identidad, el secuestro por internet, la proliferación de páginas web falsas creadas con el fin de hurtar datos financieros, la clonación de tarjetas débito y crédito, entre otras modalidades de delitos cibernéticos que afectan directamente a cualquier internauta que navega en la red. De acuerdo a la Cámara Colombiana de Informática y Telecomunicaciones, tan solo en 2019 en Colombia se reportaron 28.827 casos de fraudes, delitos e incidentes cibernéticos, un aumento del 54% con relación al año inmediatamente anterior (CCIT, 2019).

Ssegún un nuevo informe de la CCIT y el Tanque de Análisis y Seguridad de las TIC – TicTac, en el primer semestre del año se reportó, basado en cifras del C4 de la Policía Nacional de Colombia, un incremento de 59% derivado del incremento en las operaciones electrónicas de comercio producto de la pandemia covid-19, (CCIT, 2020).

El negocio del cibercrimen implica construir barreras seguras para la fluidez del comercio electrónico e implica considerar, no a individuos y delincuentes trabajando por separado, sino a grupos del crimen organizado internacional que tienen todas las herramientas para desarrollar un negocio que es casi tres veces más lucrativo que el negocio del narcotráfico, por lo que según

cifras publicadas por Digiware de Colombia S.A, afirman que el negocio del cibercrimen es mucho más rentable que otros negocios ilícitos como el narcotráfico, ya que en cifras mundiales el lucro derivado de estas operaciones delictivas asciende a USD 3 trillones mundialmente, mientras que el narcotráfico representa USD 1 trillón. (Digiware, 2019)

Es por lo anterior, que analizar el impacto que tienen los delitos cibernéticos en las operaciones de comercio tiene una gran relevancia en materia económica y social, ya que estos entes cuentan con habilidades informáticas que pueden llegar a destruir cualquier barrera para el comercio afectando fuertemente el crecimiento de algunos sectores como la banca y seguros, a manera de ejemplo; en cifras netas tan solo en 2015 la banca colombiana tuvo pérdidas equivalentes a 122.000 millones correspondientes al riesgo por estafas con pagos en internet, (SuperFinanciera de Colombia, 2016).

Aún Colombia se encuentra lejos de ser una nación segura para todo tipo de operaciones económicas digitales, después de Brasil y México, Colombia es el tercer país más afectado por el cibercrimen en América Latina representando un 21,73% de todo el negocio en la región, (Digiware, 2020).

El análisis económico de los factores que caracterizan el comercio electrónico, en especial la seguridad informática, hacen posible el entendimiento de una coyuntura social que afecta a la mayoría de la población, debido a que cualquier ciudadano puede verse impactado o vulnerado de manera digital en cualquier momento. No se requiere realizar una transacción económica por la web para que la identidad sea hurtada, y no se requiere tener una red social activa para que nuestra información personal y privada pueda ser secuestrada por organizaciones criminales (Romero, y otros, 2018).

Este entendimiento y análisis se hace necesario en un panorama de pandemia, en el que las operaciones económicas en la web crecieron sustancialmente, y en el que las empresas y organizaciones virtualizaron parte o la totalidad de sus operaciones comerciales y administrativas convirtiéndose en actores mucho más vulnerables ante un escenario de inseguridad cibernética que existe hace varios año (MinTic, 2019).

Teniendo en cuenta lo expuesto anteriormente, se plantea el siguiente interrogante: ¿Cuál es el impacto que tienen los delitos cibernéticos en las operaciones de comercio electrónico en Colombia y que estrategias se debe implementar para hacer de este una modalidad de comercio seguro? , para dar respuesta a lo anterior, se propone desarrollar la presente monografía relacionada con la seguridad en las operaciones comerciales y que se hace necesario en la medida en que cada vez más la certidumbre se convierte en un punto crítico en la economía digital, ya que dadas las cifras relacionadas con los delitos informáticos la confianza en las operaciones comerciales desaparece (Aguirre, 2006).

En un periodo de pandemia en el que las organizaciones se volvieron más virtuales, y las operaciones cotidianas se digitalizaron, la seguridad en la red online y en las transacciones electrónicas se vuelve el corazón de la economía digital, y los indicadores demuestran que la proliferación de nuevas y mejoradas formas de delinquir de manera cibernética como por ejemplo, phishing o suplantación de identidad en internet, pharming (posesión de servidores DNS), keylogging (rastreadores de teclado), entre otros, afecta de forma drástica el comercio de bienes y servicios electrónico en Colombia (MinTic, 2020).

Parte de la economía se virtualizó producto de un confinamiento social bastante drástico, y todo aquello que constituya una barrera para el crecimiento económico como lo es la inseguridad en la web y las operaciones electrónicas debe ser identificado y analizado en toda su estructura

con el fin de poder hallar soluciones oportunas y reales que contribuyan al mejoramiento de los procesos sociales y económicos (MinTic, 2020).

La gran mayoría de los cibernautas no conoce los riesgos, no tienen identificados a plenitud las formas de delinquir y por ende son más propensos a los riesgos que conlleva la inseguridad informática; es por esto que conocer e identificar dichos riesgos, y la forma como grupos ilegales internacionales operan de convierte en una necesidad inmediata para todo actor social que tenga una conexión a internet. (Baca, 2016).

Para concluir lo anteriormente dicho, esta monografía se desarrollará teniendo en cuenta tres objetivos, en el objetivo I se describirá el mercado del comercio electrónico en Colombia desde el año 2015 al año 2020; en el objetivo II se identificarán los riesgos de las operaciones de comercio electrónico en Colombia desde 2015 a 2020 y finalmente, en el objetivo III se ilustrará la seguridad de las operaciones de comercio electrónico en las entidades financieras de Colombia.

4. Objetivos

4.1 Objetivo General

Analizar el impacto de los delitos cibernéticos en las operaciones de comercio electrónico en Colombia

4.2 Objetivos Específicos

- Describir el mercado del comercio electrónico en Colombia desde el año 2015 al 2020.
- Identificar los riesgos de las operaciones de comercio electrónico en Colombia desde 2015 a 2020.
- Ilustrar la seguridad de las operaciones de comercio electrónico en las entidades financieras de Colombia

Capítulo I

5. Operaciones De Comercio Electrónico En El Mercado Colombiano

Actualmente, las empresas tienen el reto de buscar que sus procesos sean eficientes en cuanto a sus relaciones con proveedores, procesos productivos, calidad, servicios, entre otros. Y de esta manera respondan a las exigencias de sus clientes de una manera más eficiente, es aquí donde la interacción del hombre con las tecnologías ha adquirido mayor importancia y con la llegada del internet se ha abierto una puerta gigante al conocimiento de las compañías para interactuar, diseñar, ejecutar y tener acceso y control de estrategias innovadoras que le permitan llegar a un mercado más globalizado (CCCE, 2019).

De esta forma, con la llegada del internet y la globalización, las empresas requieren de una herramienta que facilite pero que sea eficiente y eficaz en cuanto a la realización de los procesos de compra y venta de productos y servicios, es aquí donde se habla del comercio electrónico como una herramienta que está adquiriendo fuerza en los procesos empresariales no solo de compras sino en todos los procesos de la cadena de abastecimiento desde los proveedores hasta el cliente final, creando valor en toda la cadena con procesos eficientes y marcando una ventaja competitiva en el mercado (CCCE, 2020)

Entonces, el comercio electrónico, también conocido como e-commerce (electronic commerce en inglés) consiste en la compra y venta de productos o servicios, a través de medios electrónicos, principalmente la Internet y otras redes de datos. Adicionalmente, con el avance de las Tecnologías de la Información y la Comunicación , el comercio electrónico facilita el comercio, puesto que reduce los costos de transacción, provee información a los usuarios, incrementa el acceso a una mayor cantidad de bienes y servicios, lo que genera ganancias en

eficiencia y aumentos en la economía. Es así, como desde mediados de los años 90 se ha considerado al comercio electrónico como un "motor potencial de crecimiento económico (CRC, 2020).

Por otro lado, existen diversas relaciones electrónicas entre las empresas, los consumidores, los gobiernos y los consumidores. Por lo anterior, según la Comisión de Regulación de Comunicaciones, se han desarrollado diferentes tipos de comercio electrónico, dentro de las cuales se pueden destacar: (*ver figura 1*)

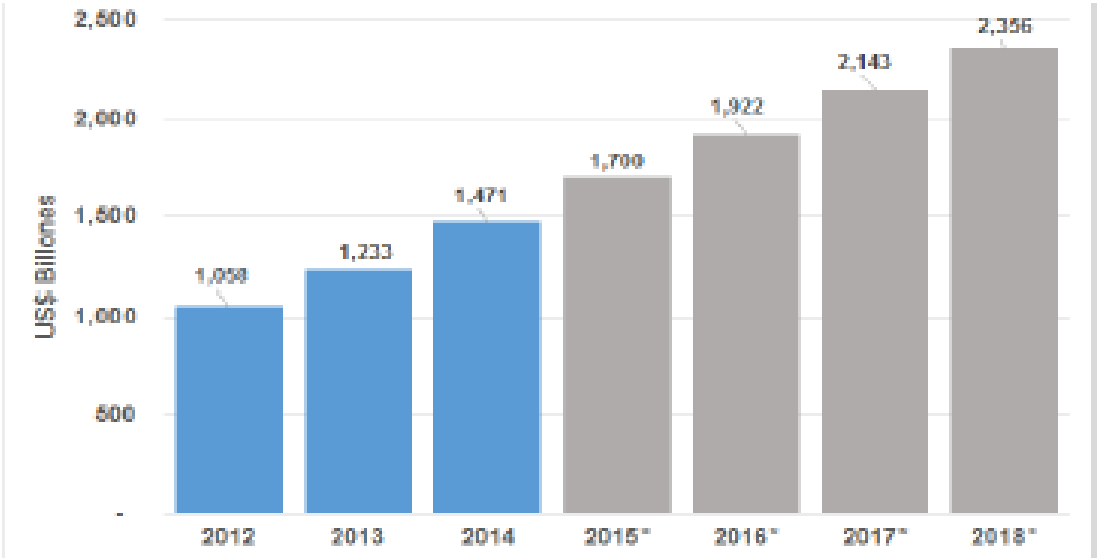
- **B2B (Business-to-Business):** Consiste en el comercio electrónico que se realiza entre empresas, esto con el fin de atraer a clientes nuevos, atendiendo eficazmente a los clientes nuevos y actuales, logrando eficiencias en la compra y mejores precios. Este tipo de negocio representa la mayor parte del comercio electrónico. Para una pequeña empresa, participar del comercio electrónico B2B puede ser un requisito y una oportunidad para participar en cadenas de valor de ámbito nacional o mundial (Naciones Unidas, 2015).
- **B2C (Business-to-Consumer)**: Este tipo de comercio electrónico se presenta entre los consumidores y las empresas. Donde el proceso de compra y pago del producto o servicio se realiza electrónicamente y de forma interactiva.
- **C2C (Consumer-to-Consumer):** Este tipo de comercio electrónico se realiza entre consumidores por medio de una plataforma especializada o mercado en línea (Marketplace) donde un consumidor pone a la venta un producto a otros consumidores. Este es el medio más moderno de comercio electrónico, que ofrece a las empresas informales la posibilidad de incursionar en este tipo de negocio.

- **B2G (Business-to-Government):** En este caso los compradores son instituciones del gobierno, es decir, comprende la comercialización de productos y/o servicios a diferentes entidades del Estado (CRC, 2017).

Figura 1: *Tipos de Comercio electrónico entre negocios, consumidores y gobierno, CRC (2017).*

De acuerdo con la Organización para la Cooperación y el Desarrollo Económico, la composición del comercio electrónico ha sido constante a lo largo del siglo XXI con el segmento B2B, principalmente a través de las transferencias de datos electrónicos, representando el 90% del valor de las ventas. El 10% que resta se encuentra representado en una combinación de B2C, B2G y C2C. Donde el segmento B2G representa alrededor del 5%, en tanto que el B2B representa un 4%, siendo este el mayor crecimiento en los últimos años (OCDE, 2019).

Ahora bien, durante el año 2015 los bienes y servicios comprados a través de Internet representaron 7.3% del mercado minorista mundial, es decir, que las ventas en el segmento B2C se incrementaron en un 16% (OCDE, 2019).



Gráfica 1: *Comportamiento del segmento B2C. Billones de US$, OCDE (2019).*

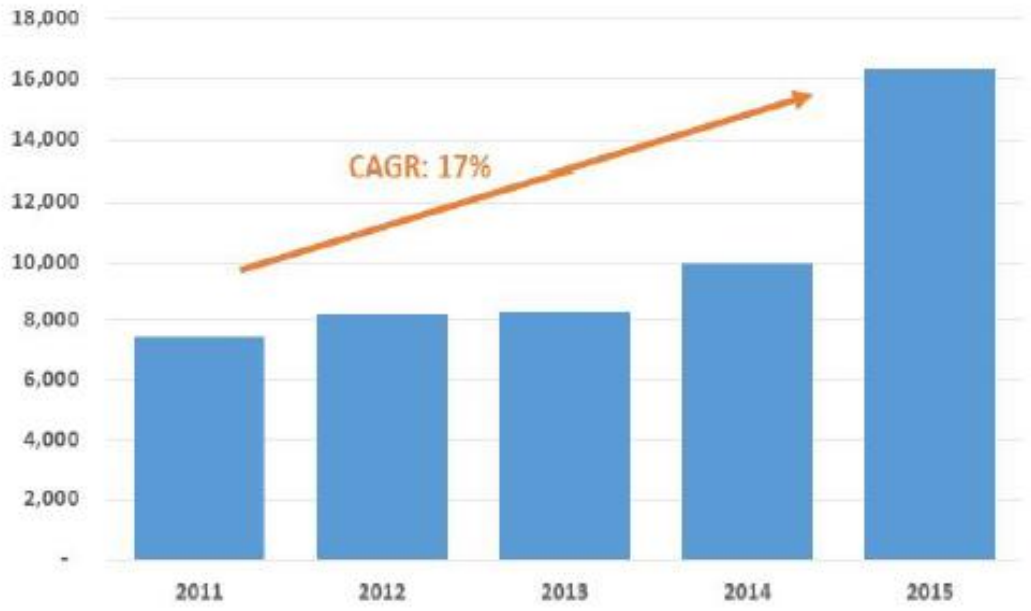
Recientemente, debido al gran volumen de teléfonos inteligentes, el segmento B2C ha crecido de forma acelerada a diferencia de los demás segmentos. Esto debido a que los teléfonos inteligentes permiten y tienen acceso a las compras en línea, pagos en línea, ventas en línea, entre otros. Por su parte, el Observatorio Nacional de las Telecomunicaciones y de la SI – sustentan que este crecimiento acelerado se debe que sistemas como Google Wallet y Apple Pay, entre otros, están surgiendo como una modalidad de pago electrónico y han impulsado la facilidad de hacer transacciones y compras en línea (ONTSI, 2015).

5.1 Comportamiento del Comercio electrónico en Colombia en el periodo comprendido desde 2015 a 2020

En Colombia las empresas no son ajenas a esta herramienta que ha tenido un auge significativo en los últimos años. De acuerdo con Asobancaria (2016) para el año 2015 las transacciones por internet representaron el 2,6% del PIB nacional con un crecimiento de más del

30% en ese año; y sigue en aumento, puesto que la tecnología por medio de la internet y con la implementación de la telefonía móvil los usuarios tienen mayor y fácil acceso a los mercados nacionales e internacionales, y se hace aún más fácil con las entidades financieras desarrollando aplicaciones para realizar y agilizar los pagos.

En Colombia las entidades encargadas de dimensionar el crecimiento del mercado del comercio electrónico son principalmente por la Cámara Colombiana de Comercio Electrónico y por la Superintendencia de Industria y Comercio (CCCE, 2019).

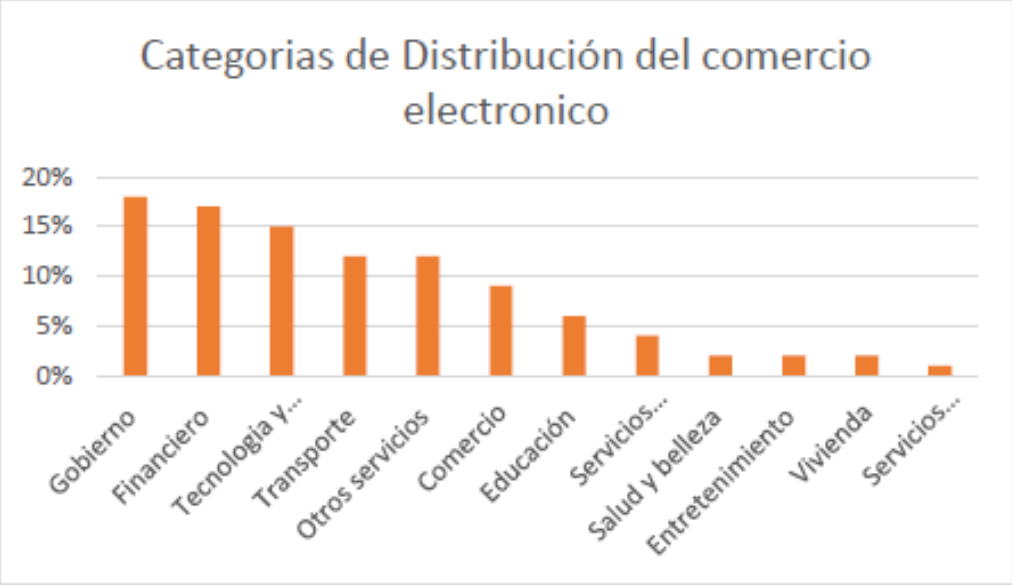


Gráfica 2: *Comportamiento del Comercio Electrónico en Colombia – 2011 – 2015, CCCE (2019)*

De acuerdo a los estudios realizados por CCCE (2019), las ventas de comercio electrónico en Colombia ascendieron a US$8.283 millones en 2013, US$9.961 millones en 2014, y US$16.329 millones en 2015, con un incremento de 64% frente al 2014. Lo anterior representa el 2.19% del

Producto Interno Bruto - PIB para 2013, 2.62% del PIB para 2014 y 4.08% para 2015. Para el año 2015, 56% de las transacciones se originaron en tarjetas de crédito y 44% en tarjetas débito.

Así mismo, muestra las categorías de distribución que implementan este sistema.

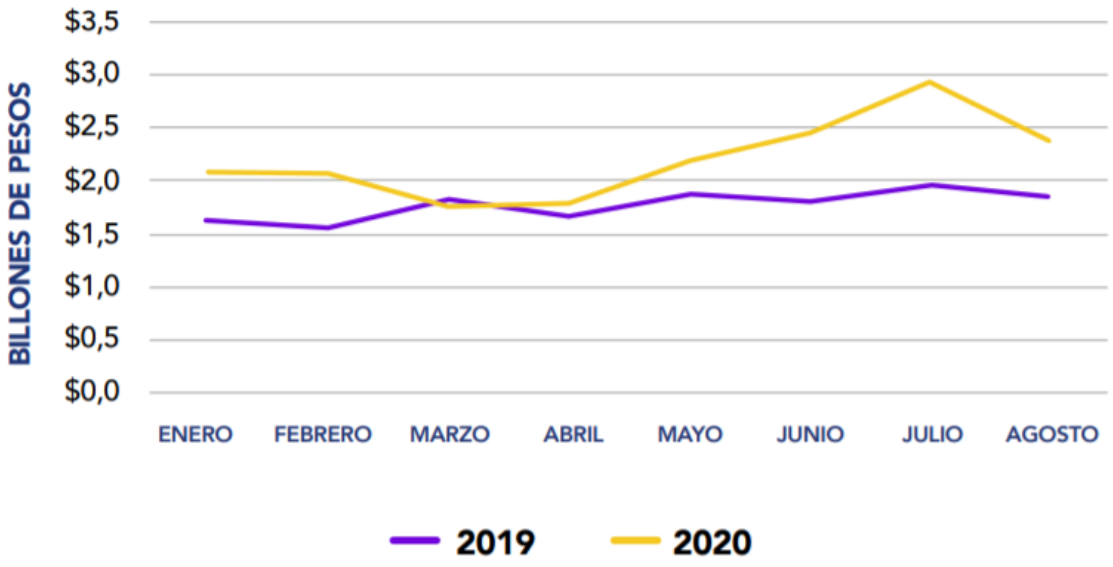


Gráfica 3: *Categorías de distribución del comercio electrónico en Colombia, CCCE (2019).*

De tal manera, la cámara colombiana de comercio electrónico se encuentra en constante trabajo para incentivar que tanto usuarios como organizaciones implementen esta herramienta, y consolidar este sector. Por ello, desarrollan programas o eventos como los cyberlunes, hot sales, black Fridays etc., donde las empresas disponen de espacios para promocionar y vender sus productos y servicios en la web (CCCE, 2020).

Según la CCCE (2020) en el año 2019, las ventas a través del comercio electrónico en Colombia crecieron en un 2.74% de la tasa mensual; mientras que, entre enero y agosto de 2020, la tasa mensual fue del 1.9%.

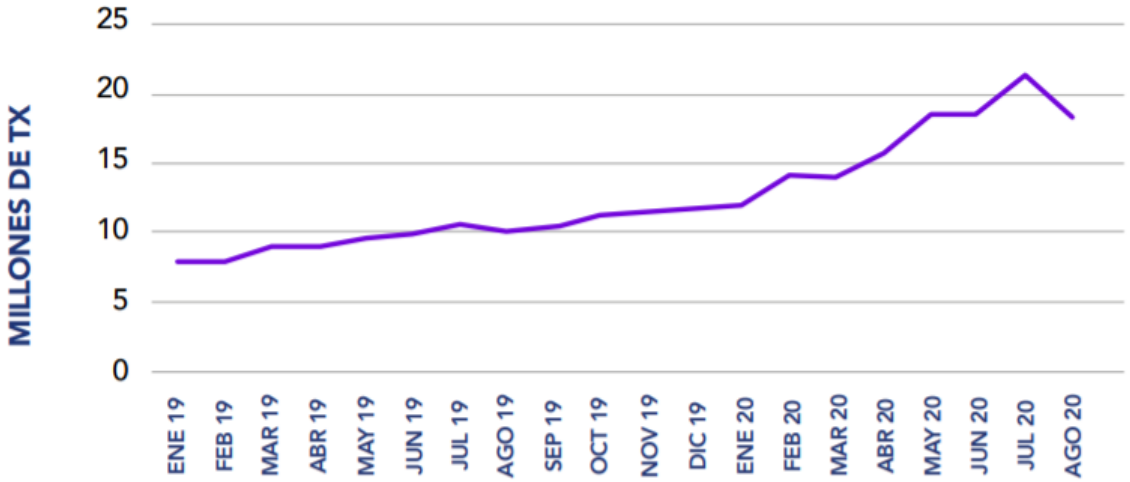
Si bien resulta sorprendente que en el 2020 se esté presentando una tasa mensual de crecimiento inferior a la de 2019, pero es importante tener en cuenta que entre febrero y marzo ocurrió un alza del 14.4% en las ventas realizadas a través de comercio electrónico y, mientras que entre marzo y abril hubo un crecimiento de tan solo el 1%. Así mismo, entre abril y julio el comercio electrónico creció 65,7%, es decir, tuvo una tasa mensual del 11%; mientras que entre julio y agosto se presentó una caída del 19% en las ventas. De esta forma, si se compara el periodo comprendido entre enero y agosto del año 2019 con el del presente año, se hace más notoria la aceleración en el crecimiento del sector que ocurrió entre abril y julio del 2020. Así, por ejemplo, en abril de 2020 se logró un crecimiento del 7.6%, mientras que, en julio este crecimiento fue del 51% (CCCE, 2020)



Gráfica 4: *Ventas a través del comercio electrónico entre enero y agosto de 2019 y 2020, (CCCE, 2020).*

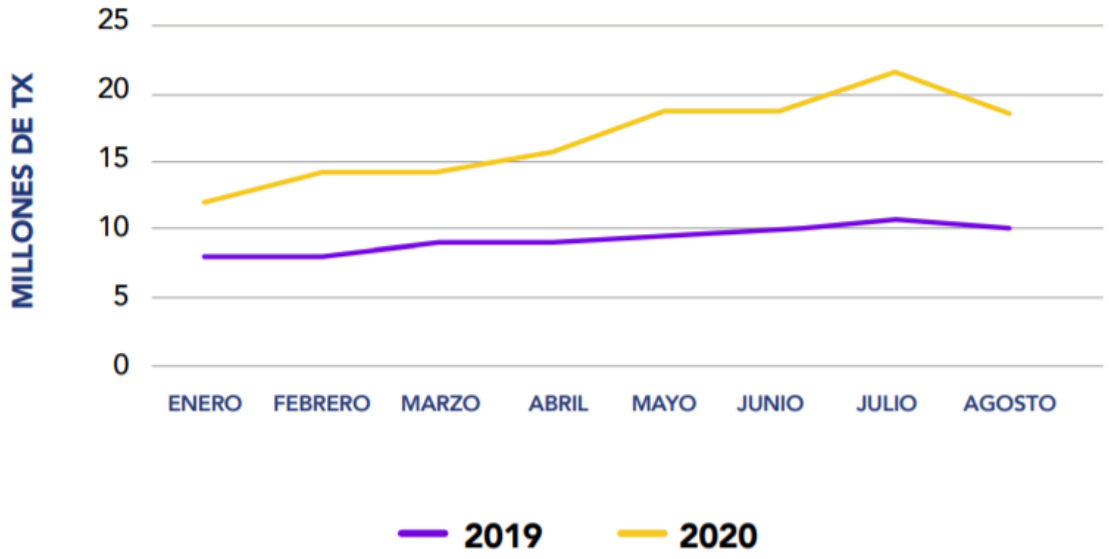
Por otro lado, a diferencia del comportamiento observado en las ventas 2019 - 2020, el número de transacciones presentó un crecimiento sostenido entre enero y julio del presente año. En este periodo las transacciones a través de las compras virtuales crecieron en un 78.5%. Sin embargo, entre julio y agosto ocurrió una caída del 14% en el número de transacciones realizadas

a través de este medio, comportamiento similar al observado en el valor de las ventas (CCCE, 2020)



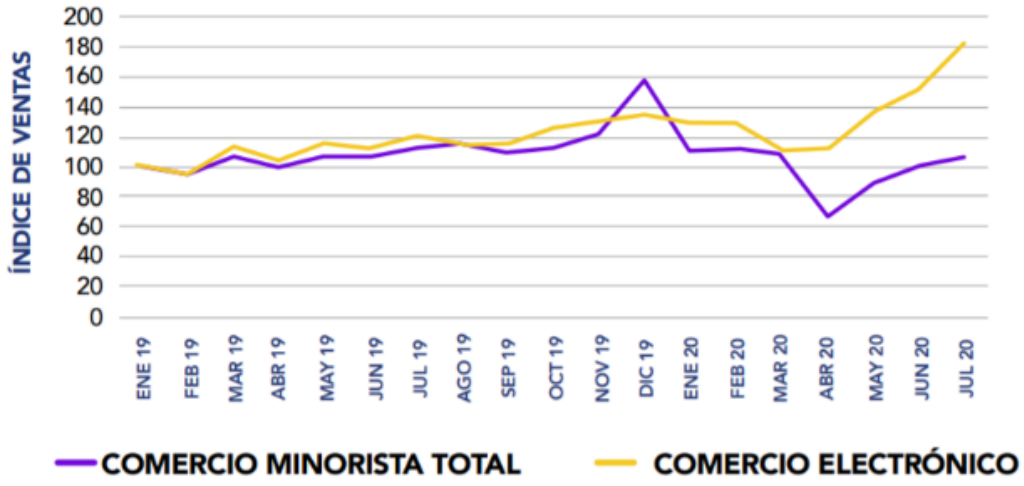
Gráfica 5: *Número de transacciones mensuales de comercio electrónico, (CCCE, 2020).*

De esta forma, si se compara el mismo periodo entre enero y agosto del año 2019 y del presente año se evidencia un crecimiento acelerado en las transacciones realizadas a través del comercio electrónico en Colombia. Para enero del presente año el número de transacciones de compra realizadas a través de este canal creció en un 52.2% respecto a enero de 2019. Mientras que para julio del presente año, el número de transacciones, respecto a julio del año 2019, creció en un 100.4%. Sin embargo, para agosto de este año, el crecimiento en el número de transacciones en comparación con agosto del año 2019 se redujo a un 78.8% (CCCE, 2020).



Gráfica 6: *Número de transacciones de comercio electrónico entre enero y agosto de 2019 y 2020, (CCCE, 2020).*

Por otra parte, el comercio en Colombia recibió un impacto negativo como consecuencia de las medidas de distanciamiento social tomadas para contener el virus del COVID-19. De acuerdo con el DANE (2020) en abril del presente año, el sector comercio -sin vehículos y combustible- se redujo en un 37.1%. Sin embargo, desde este mes se ha presentado una recuperación paulatina con un crecimiento mensual promedio entre abril y julio de 11.8% (CCCE, 2020).



Gráfica 7: *Comportamiento del comercio electrónico respecto al comercio en general, (CCCE, 2020).*

Según la CCCE (2020) hasta agosto del 2020, el crecimiento acumulado de las ventas de comercio electrónico, respecto al mismo periodo de 2019, fue de 25.3%. Sin embargo, para los meses restantes del año 2020 se advierte una incertidumbre muy propia que dificulta la construcción de perspectivas de cierre de año para el sector comercial.

Sin embargo, la expectativa de crecimiento en ventas para el cierre de 2020 respecto al 2019 es del 20%, mientras que la expectativa de crecimiento en ventas para el cierre de 2021 respecto al 2020 es del 16% (CCCE, 2020).

Finalmente, de acuerdo a la recopilación de datos e información presentada anteriormente, el número de usuarios de comercio electrónico aumentó de forma importante durante la pandemia. No obstante, se espera una reducción en la frecuencia de compras a medida que avance la reactivación económica. De igual forma, se espera que esta modalidad de comercio electrónico le permita a las empresas llegar a un mercado mucho más amplio que el previo a la pandemia, aunque posiblemente habrá una frecuencia menor de compra que la experimentada entre abril y julio de 2020.

Capítulo II

6. Riesgos En Las Operaciones De Comercio Electrónico En Colombia Desde 2015 A 2020.

De acuerdo a los autores Álvarez y Pérez (2004) las organizaciones actuales adquieren, requieren y encuentran disponible una gran variedad, amplitud y complejidad en los sistemas de información que adquieren. De esta forma, la dinámica del permanente cambio observado en las tecnologías de la información y las comunicaciones, han impulsado y condicionado las grandes transformaciones de las organizaciones, los mercados y el mundo de la modernidad y la posmodernidad. Son cambios que, además de sus innegables ventajas, han traído simultáneamente para las personas y las organizaciones incertidumbre, riesgos, y amenazas, en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas informáticos.

Así mismo, con mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de la información como los servidores, estaciones de trabajo o simplemente PC son vulnerados en sus elementos más sensibles, dejando expuestos significativos datos de valor financiero, crediticio, estratégico, y productivo; así como también el patrimonio y los bienes muebles e inmuebles de las personas y las organizaciones (Ojeda, Rincón y otros, 2010).

De esta forma, según Montañez (2017) con los avances de la tecnología de la información y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos denominados de manera genérica "*delitos informáticos"*, que han abierto un amplio campo de riesgos y también de estudio e investigación, en distintas disciplinas jurídicas y técnicas (Gómez, 2006).

6.1 Contexto de los delitos informáticos En Colombia.

Los autores Ojeda et al. (2010) comparan al ser humano actual con sus antepasados históricos, aludiendo que les sucedió lo mismo como cuando fabricaron el primer cuchillo. Pues este tuvo un gran alivio en sus labores diarias, así mismo contaba con una herramienta que le ayudaba en sus tareas cotidianas de supervivencia. Pero no faltó quien usara dicha herramienta con otras fines o intenciones en contra de sus semejantes y terminara cometiendo delitos que, seguramente, en su momento no se llamaron así, pero se entendían como actos en contra de la supervivencia de los demás.

En la actualidad, a los sistemas informáticos le ha ocurrido algo similar a lo observado en la historia. La sociedad se ha interesado y condicionado a los avances tecnológicos e informáticos, debido a su eficaz desarrollo y a la enorme influencia que ha alcanzado en muchas de las actividades diarias de las personas y las organizaciones. De esta forma, son pocas las personas que pueden abstraerse de tener contacto directo o indirecto con sistemas informáticos, lo cual muestra de distintas maneras el poder y alcance de la tecnología informática en las sociedades del mundo. De modo que, así como la tecnología y su desarrollo han incidido prácticamente en todas las actividades del ser humano a lo largo de su historia, en la actualidad, la dependencia tecnológica se ha concentrado en el fenómeno de la tecnología informática, la información y la comunicación. Pero muy tarde se descubrió que dicho desarrollo venía acompañado de distintos y novedosos riesgos, por ello, a medida que aumenta el uso del internet, aumenta el riesgo de su uso inadecuado (Ojeda et al., 2010).

Para los autores Álvarez y Pérez (2004) los denominados "*delincuentes cibernéticos"* viajan por el mundo virtual realizando incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude

financiero, sabotaje informático, entre otros. Así mismo, sustentan que para enfrentarlos, varios países han desarrollado y dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. A ese grupo de países se unió Colombia en el año 2009.

Por otra parte, las herramientas que implementan los ciberdelincuentes han evolucionado más o paralelamente al desarrollo tecnológico, ejemplo de ello son los virus informáticos. Según el autor Montañez (2017) los ciberdelincuentes en sus inicios infectaban los equipos de sus víctimas, al transportar los virus desarrollados en los medios de almacenamiento de información disponibles en ese momento: los disquetes

Más tarde, implementaron las redes de datos al aprovechar el internet, pero se encontraron con barreras como las restricciones de acceso para evitar precisamente los contagios por virus informáticos. Entonces optaron por emplear las memorias móviles con puerto USB e incrementaron los ataques de *malware*[1] en el internet. Así mismo, han implementado el correo electrónico o las salas de conversación virtual de internet para buscar posibles víctimas vulnerables (Montañez, 2017).

Por consiguiente, las entidades se vieron en la necesidad de desarrollar instrumentos de control y sanción para quienes en forma inescrupulosa utilizaran la informática para delinquir. Sin embargo, se encontraron que los entes encargados de sancionar a quienes hacían uso ilegal y delictivo de las herramientas informáticas, no tenían cómo judicializar a los nuevos delincuentes. Por lo tanto, la ley inglesa sirvió como ejemplo para que otros países, en especial para aquellos donde la internet y las tecnologías de la información están más desarrolladas, se sumaron al

[1] Software o código malicioso: Se trata de cualquier software, mensaje o documento con capacidad de producir daños en los sistemas informáticos y en las redes. En este grupo de programas peligrosos, se encuentran las bombas lógicas, los gusanos, los virus y los troyanos, entre otros (Gómez, 2006).

esfuerzo de discutir y promulgar leyes orientadas a proteger y sancionar el robo y la violación de la información y los sistemas informáticos (Gómez, 2006).

De esta forma, la seguridad informática y cualquier delito informático se debe entender y analizar de manera global, puesto que no ya hay fronteras que se interpongan entre ellos y la información resguardada en los dispositivos tecnológicos; además de que no existe una legislación que logre limitar sus fronteras. Se debe entender que los delitos informáticos no tienen barreras ya que es un mundo cibernético, conectado a cientos de ordenadores y solo está a un clic de acceder a un mundo totalmente virtual (Montañez, 2017).

6.2 Tendencia de los delitos cibernéticos en Colombia

Según la Cámara Colombiana de Informática y Telecomunicaciones, en Colombia los delitos cibernéticos han experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques, sitúan a dicha problemática como una de las principales economías ilegales en el País (CCIT, 2020).

Por ello, el impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones sobre productividad e incluso conlleva a implicaciones de carácter legal por fuga de información privilegiada y data sensible (Acuña y Villa, 2018).

De esta forma, la dinámica actual de los delitos cibernéticos en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad. De tal forma, que a través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019. Del total de los casos registrados, 15.948 fueron denunciados como infracciones a la ley 1273 de

2009 por parte de las víctimas, esta cifra corresponde al 57% del total de casos informados. Respecto al 2018 las denuncias disminuyeron en un 5.8 % tras una variación negativa de 983 casos (CCIT, 2020).

***Figura 2**: Cifras denuncias 2015- 2019, CCIT (2020).*

Por otro lado, el 45% del total de las denuncias realizadas por delitos cibernéticos en el país se realizan a través de la aplicación ADenunciar. Según la cámara colombiana de informática y telecomunicaciones desde julio del año 2017 se han recibido un total 24.711 denuncias por ciberdelitos en esta plataforma virtual (CCIT, 2020).

Así mismo, 12.879 incidentes cibernéticos es decir un 43% de los casos reportados en 2019, fueron gestionados sin que se llegara a instaurar una denuncia física ante la Fiscalía General de la Nacional. Dicha cifra representa un incremento del 54% respecto del 2018, cuando fueron gestionados 8.363 casos (CCIT, 2020).

A su vez, Acuña y Villa (2018) consideran que el principal interés de los Cibercriminales en Colombia se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada Ciberataque.

Así mismo, CCIT (2020) sustenta que los cibercriminales implementan cinco modalidades de hurto:

- En primer lugar, se encuentra el hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.
- En según lugar, se encuentra la violación de datos personales con 8.037 casos. Este dato revela que la segunda amenaza en Colombia para empresas y ciudadanos es el robo de identidad.
- El tercer delito más denunciado es el acceso abusivo a sistemas de información con 7.994 casos, y esto se explica en razón a que, en las primeras fases los ciberataques, los cibercriminales buscan comprometer los sistemas informáticos y lograr tener acceso a los mismos.
- En cuarto lugar, con 3.425 casos se encuentra las transferencias no consentida de activos, conducta criminal que facilita al atacante sustraer el dinero o transferir valiosos activos financieros de las víctimas.
- Finalmente, en quinto lugar se sitúa el delito de uso de Software Malicioso con 2.387 casos.

La comprensión de dichas modalidades de hurto y como ellos trabajan en el mundo físico, pueden ayudar a explicar cómo estos daños y dimensiones se encuentran en el mundo de la red y dónde se sitúan las dificultades, desde el punto de vista de la protección de la información.

Por otro lado, los autores Mora y Agudelo (2017) sustentan que en la actualidad el tratamiento de la información, en su gran mayoría se realiza por medios digitales que permiten

un mejor rendimiento y manipulación de la información para la obtención de resultados mucho más precisos. Dichos resultados impactan directamente en la estabilidad financiera y administrativa de las organizaciones ya sea pública o privada (Mora, Agudelo y otros, 2017).

De tal forma, que las compañías invierten grandes sumas de dinero en la adquisición de soluciones de infraestructura tecnológica para seguridad de la información, como apoyo a sus equipos para la detección, reacción y prevención ante las amenazas a las que pueda estar expuesta la información. A pesar de esto, todas las inversiones tecnológicas en materia de seguridad son insuficientes si los usuarios no toman conciencia de la importancia de la información y los cuidados asociados a ella (Acuña y Villa, 2018).

Según Chiriguayo (2015) el reto más significativo que tienen las entidades es considerar a la información como el activo más valioso de la organización para el desarrollo de sus funciones, y sin la cual sería inviable permanecer en el mercado de una forma competitiva. De tal forma, que las estrategias de negocio, los datos financieros, la información de los clientes y empleados, constituyen de alguna manera, datos informativos que no deben estar manos de desconocidos por la competencia o peor aún en manos de mafias dedicadas a aprovechar el descuido con la información.

Por otro lado, la seguridad informática considera tres pilares fundamentales: confidencialidad, integridad y disponibilidad (Montañez, 2017).

- El primer pilar es la confidencialidad, que hace referencia al valor que obtiene dentro de una red de datos, al mantener la información reservada únicamente a los usuarios autorizados para utilizarla.

- El segundo pilar es la integridad, que busca mantener todos los datos sin modificación alguna.
- Y el tercer pilar es la disponibilidad, la cual hace posible que la información esté lista para ser consultada en cualquier momento que se requiera.

Elementos esenciales para el manejo y control de la información dentro de la entidad.

Según un informe realizado por Cisco (2016) los directores de las empresas han descuidado los procesos y herramientas para combatir los ataques informáticos, al punto de que varios de estos sistemas ya están "obsoletos".

Y es que el número de organizaciones con una infraestructura de seguridad actualizada se redujo en un 10% entre 2015 y 2014 a nivel global, y agrega que mientras eso sucede los atacantes lanzan campañas más sofisticadas, audaces y resistentes (Cisco, 2016).

De esta forma, el envejecimiento de la tecnología y las fallas en los procesos a nivel institucional, son solo algunos de los factores que explican por qué solo el 45% de las empresas confían ciegamente en sus protocolos de seguridad. Así mismo, sostiene que uno de los aspectos más preocupantes es que el 31% de los dispositivos tecnológicos en las empresas, ya no reciben soporte o mantenimiento por parte del vendedor, lo cual supone un enorme atraso en materia de actualización. Este fenómeno ha afectado en gran medida a las pequeñas y medianas empresas (pymes), las cuales se han convertido en víctimas potenciales de los cibercriminales debido a la fragilidad de su infraestructura y a la falta de personal especializado en el control de esas amenazas (Cisco, 2017).

De igual forma Cisco (2016) menciona que resulta preocupante la fuga de datos a través de los navegadores, situación que afecta a más del 85% de las organizaciones a nivel mundial

debido a la falta de actualización de sus plataformas. A esta problemática se suman las distintas formas de secuestrar la información en internet, dentro de los más destacados se encuentra un programa especializado que se denomina “RANSOMWARE” este tipo de delito mueve alrededor de US$34 millones cada año.

Por otra parte, en la actualidad, el coronavirus también ha sido un agente de impacto negativo en términos de ciberseguridad en el país. Según las cifras más recientes del Centro Cibernético de la Policía Nacional (2020), los delitos informáticos aumentaron en un 59% en el primer semestre del presente año, respecto al mismo periodo del año pasado.

Así mismo, menciona que entre enero y junio del presente año se registraron alrededor de 17.211 denuncias, 6.340 más que en el primer semestre del 2019. También se presentaron 2.103 casos de suplantación de sitios web, un delito que creció en 364%. No obstante, cabe resaltar que las transacciones financieras por Internet son muy seguras, pero es importante que los usuarios sean muy cuidadosos al momento de realizarlas (Centro Cibernético de la Policía Nacional, 2020).

De esta forma, ante la rápida evolución de los sistemas informáticos y las nuevas tecnologías, es de esperarse que surjan fallas en la seguridad de los dispositivos. Sin embargo, no es algo por lo cual preocuparse; por el contrario, es importante tomar conciencia e informarse al respecto. Esto implica que las entidades se preparen de manera proactiva para mitigar, detener y prevenir ataques cibernéticos, que pueden representar pérdidas millonarias para la entidad. Por lo tanto, invertir en seguridad de la información siempre será un factor clave en la protección de los datos, más que todo en estos tiempos donde se ha presentado un incremento considerable en de dispositivos tecnológicos y sistemas de la información, por ello, es indispensable que las entidades estén alerta más que nunca (Romero, Figueroa y otros, 2018).

Capitulo III

7. Seguridad Digital En Entidades Financieras De Colombia

La dinámica del mercado ha llevado a las organizaciones a un enfoque hacia la satisfacción del cliente donde las tecnologías de la información y la comunicación se constituyen en herramientas fundamentales para vender bienes y servicios a través de la red, conocido como comercio electrónico (Albarracín, 2014)

Este es un fenómeno ha venido tomando fuerza no solo en el país, sino en todo el mundo, ya que cada vez más va aumentando el número de consumidores que prefieren realizar sus movimientos financieros a través de la web, por la comodidad que representa para ellos. Este modelo permite generar mayor productividad y competitividad a las empresas debido a la reducción de costos de transacción y a la visibilidad que generan a través de factores como el fundamento del negocio, las oportunidades de tecnología y la percepción de los empresarios (Medina, 2012).

Según el autor Raymond (2011), al transferir información implementamos los medios informáticos y esto implica la exposición a numerosos riesgos. Es por esto, que la seguridad representa una gran importancia en la viabilidad del comercio electrónico. El gran avance de las redes de información ha puesto en evidencia la importancia de poder detectar, prevenir y detener los ataques a la seguridad de los usuarios; deben ser conscientes de los riesgos que implica el uso de la red, para tomar las medidas de seguridad necesarias y, prevenir así, el acceso de fraudulentos a información confidencial.

El acceso masivo a las nuevas tecnologías ha permitido a los bancos ofrecer a través de internet acceso de forma virtual a sus sucursales. En los últimos años se han encontrado graves

vulnerabilidades en los protocolos de seguridad sobre los cuales se transmite la información entre los clientes y los bancos. Estas vulnerabilidades son descubiertas de forma periódica, por lo cual es importante que las instituciones que prestan servicios en línea hagan una validación regular de las mismas. Se realizó una validación sobre los cinco bancos más grandes del mercado colombiano (Asobancaria, 2019).

- Banco de Bogotá
- Bancolombia
- Banco de Occidente
- Banco Popular
- Davivienda

  La validación se realizó a través de la herramienta SSL Labs de la firma Qualys. La herramienta pondera una calificación con letras (A-F), siendo A la nota más alta y F la más baja con un corte de aprobación mínimo de C.

Resumen de hallazgos

A continuación se presentan los resultados obtenidos luego de probar cada una de las páginas web transaccionales de los bancos.

- Banco de Bogotá: **F**
- Bancolombia: **C**
- Banco de occidente: **F**
- Banco Popular: **F**
- Davivienda: **F**

Promedio: **F**

Se evidencia falencias endémicas sobre la configuración de los protocolos de seguridad en los servicios virtuales ofrecidos por los grandes bancos colombianos. Lo cual pone en riesgo a sus clientes quienes realicen transacciones sobre redes compartidas o públicas. Por lo cual es necesario que se implemente un plan de acción inmediato en busca de solucionar estas falencias (Asobancaria 2019).

La cuarta revolución industrial sumada a las nuevas necesidades de los consumidores de vivir experiencias simples y personalizadas han llevado a las entidades financieras a redefinir lo que es ser banco en una era donde lo digital apalanca la cotidianidad; es por esto que ante las nuevas expectativas que han surgido, estas entidades han reaccionado con soluciones digitales, entendiendo que la articulación de los bancos y las fintech es una prioridad. En Bancolombia se ven a las fintech como un aliado estratégico para desarrollar productos que permiten llegar a algunos segmentos a los que probablemente no se lleguen solos. Un ejemplo de esto es Nequi, la plataforma 100% digital que busca que los clientes tengan una mejor relación con el dinero, para que logren lo que se desee con ella. Nequi además de ser un depósito de bajo monto, sin cuota de manejo o comisiones, es una plataforma que brinda una completa seguridad. (Grupo Bancolombia, 2019).

En Nequi solo se puede entrar con las siguientes llaves:

Tu celular: solo tú lo tienes. Si se cambia este te va a pedir reconocimiento facial o de voz.

La clave: solo el cliente la posee. La clave es única y no se debe decir a nadie. Además cada año Nequi pide que se cambie para que sea más que seguro.

Reconocimiento facial: la cara es solo tuya. Esta se usa para reforzar la seguridad cuando se cambia alguna de las otras llaves. Por ejemplo si olvidas tu clave, desinstalas la App, entre otras.

Reconocimiento de voz: tu voz es solo tuya y te podría sacar de apuros cuando el reconocimiento facial no funcione. Para activarla se debe ir a Ajustes de tu Nequi en la App.

Huella: si tu celular lo permite puedes usar tu huella en lugar de tu clave. Se activa yendo a Ajustes de tu Nequi en la App.

Otro ejemplo claro que esta entidad bancaria recomienda cuando se realicen transacciones a través de canales digitales son:

- Asegurarse que el equipo esté protegido con un antivirus.
- Nunca conectarse a redes WIFI públicas, ya que por medio de estas los hacker pueden robar la información bancaria y utilizarlas a su conveniencia.
- Para ingresar al sitio transaccional de Bancolombia, digita siempre la dirección www.grupobancolombia.com directamente en la barra del navegador. Nunca ingresar por buscadores o a través de vínculos guardados como “Mis favoritos”
- En la barra del navegador, haz doble clic en el ícono en forma de candado para verificar que el certificado de seguridad del sitio sea emitido para www.grupobancolombia.com, esto indica que el sitio es seguro y protege la información.

La cámara Colombiana de Comercio Electrónico (2019) ha logrado que los negocios electrónicos que anteriormente podrían parecer inseguros e inestables, hoy sean exitosos en términos económicos; esto es porque el consumidor no requiere movilizarse a ningún lugar para realizar todos los movimientos financieros que desee y esta es una de las principales ventajas del comercio electrónico, además de que son:

- Rápidas y fácil acceso a los productos y servicios en cualquier parte del mundo.

- Comodidad para el consumidor en la adquisición del producto, ya que lo puede hacer desde cualquier lugar en el que se encuentre, sin necesidad de desplazamiento.
- Comparación de precios del mismo producto en diferentes sitios que lo ofrecen de manera fácil y rápida.
- Rápido contacto con el vendedor.

Por otro lado, a pesar de las grandes ventajas que trae el comercio electrónico, el consumidor se encuentra expuesto a numerosas desventajas, algunas de ellas son:

- Error en el producto en cuanto a la calidad.
- Publicidad engañosa.
- Fallas en el producto, como por ejemplo que el producto no tenga las mismas características que el que se creía haber comprado.
- Falta de protección de la información personal: Vale la pena destacar que este es considerado como uno de los principales obstáculos en el comercio electrónico, ello se debe a que los comerciantes dudan de las garantías existentes en la protección de su información personal ya que con el desarrollo de las nuevas tecnologías, resulta mucho más fácil tener acceso a la información personal de otras personas, sin necesidad siquiera del consentimiento o conocimiento de su titular, es por esto que con la ley 1266 de 2008, se ha dado mayor seguridad en este tema ya que se regula todo lo concerniente al manejo de la información personal contenida en bases de datos.
- Inseguridad en cuanto a los mecanismos de pago.

En su informe, Asobancaria (2019), titulado E-Commerce, crecimiento y ecosistema digital en Colombia, indica que para la industria colombiana el posicionamiento del comercio electrónico como una cultura de compra y venta en internet tiene grandes retos: únicamente el 19 % de la población realiza efectivamente actividades de compra y pago en línea, es decir, solo 2 de cada 10 personas mayores de 15 años, usuarios de internet, realizan E-Commerce, en contraste con el 91% de personas que realizan alguna actividad asociada al comercio electrónico.

En los últimos años Colombia ha presentado un crecimiento exponencial del comercio electrónico. Los últimos cinco años muestran un crecimiento de 24 %, lo que permite prever que para 2021 el país alcanzará ventas superiores a los USD 26.073 millones (Asobancaria, 2019).

Este gran aumento del consumo de los colombianos de productos y servicios a través del comercio electrónico es lo que ha hecho que las empresas tengan en cuenta varios aspectos que deben considerarse en cuanto a seguridad electrónica se refiere. La CCIT (2019) sostiene que cuando una organización planea tener presencia en el "web", y realizar transacciones comerciales por internet, debe garantizar la seguridad del comprador a través de métodos que le permitan reconocer la identidad del usuario; por ejemplo:

1. Autenticación o verificación de la identidad del cliente
2. Seguridad de las transacciones comerciales electrónicas
3. Seguridad del sitio web
4. Privacidad
5. Utilidad de la Criptografía
6. Autenticidad del sitio web desde el punto de vista del cliente

Desde el punto de vista del comprador, sea este un individuo, o una empresa adquiriendo bienes de un proveedor por Internet, es necesario tener seguridad sobre quién está realmente tras las páginas web que ve, si es realmente quien dice ser y no se trata de una suplantación de identidad. Como Internet es una red pública, no privada, los compradores aún son temerosos y reacios a enviar a través de ella el número de su tarjeta de crédito (Motta y Alderete, 2016).

De acuerdo a Benítez (2016), pueden existir motivaciones de tipo organizacional las cuales están representadas en:

- Daños a la imagen de la empresa: donde tienden a modificar las páginas 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. (Benítez, 2016).

- Ataque a terceros con la tecnología de las empresas: En este escenario los ciberdelincuentes utilizan la web de las empresas que son inseguras para enviar malware, alojar un phishing, infectar los servidores web con el propósito de realizar estafas económicas en nombre de la compañía. (Benítez, 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 hadware, 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”. En efecto, cada ataque pone en riesgo la

seguridad de la información ocasionando pérdidas económicas 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.

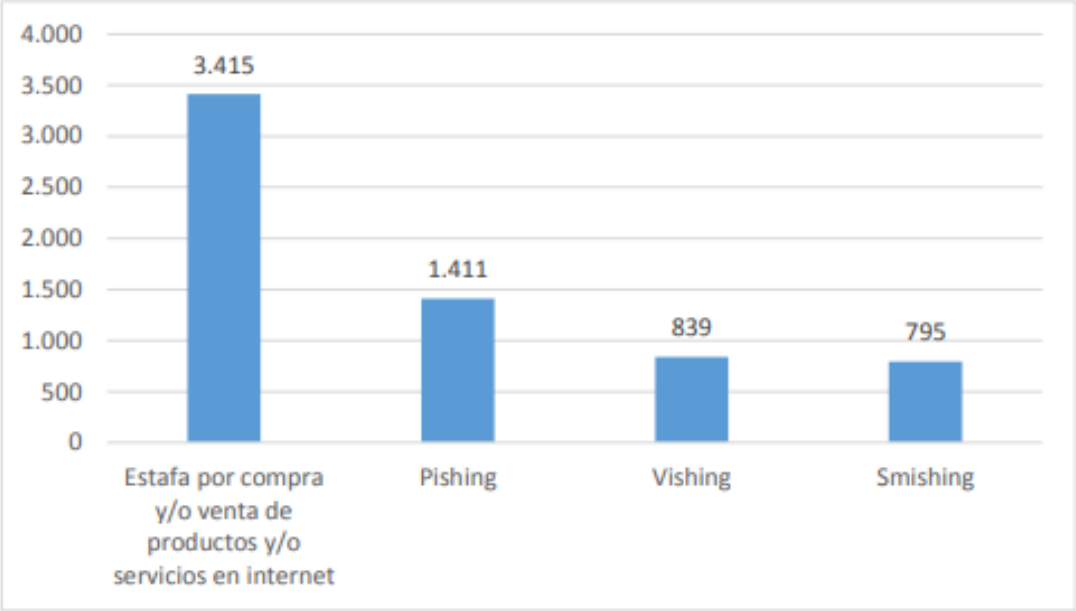
Hay autores como Font (2000) que agrupan por categorizan las amenazas informáticas para darle una mejora identificación a los empresarios que promueven estrategias de seguridad:

- "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 informáticos 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 áreas claves con el propósito de robar información de tipo económico 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 carácter externo que se describió anteriormente con Chiriguayo (2015), donde se destacan los virus y los gusanos.

Por otro lado, se debe destacar que en el entorno colombiano las cifras de delitos informáticos vienen aumentando de manera preocupante, las estadísticas oficiales de la Policía Nacional advierten que para el año 2017 las denuncias por estos crímenes se incrementaron en un 28,3%, respecto al año anterior, afectando a 446 empresas del país (Asobancaria, 2019). Dichas estadísticas apuntan que las acciones más delictivas se presentan en el comercio electrónico.



Gráfica 8: *Relación de crímenes informáticos más comunes en Colombia año 2017. Adaptado de Policía Nacional de Colombia (2018).*

De acuerdo al estudio de la Policía 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, o en el cambio de las condiciones y calidad de los mismos". Es por esto que se presentan modalidades como el pishing, donde el ciberdelincuente toma los datos confidenciales de un consumidor como correos, contraseñas, datos bancarios, ect, para realizar fraudes mientras que en los delitos vía vishing y smishing, hacen referencia al uso de marcas de empresas reconocidas para publicar mensajes y después hacer llamadas ofreciendo obsequios 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" (Policía Nacional de Colombia, 2018).

Con el comercio electrónico, que se hace efectivo mediante los ordenadores conectados a redes de comunicación, los servicios financieros pasan a integrarse con el estilo de vida del

consumidor, que puede hacer sus compras y transacciones bancarias, pagar sus recibos, entre otras operaciones comerciales, a cualquier hora del día; permitiendo así un sistema de "oferta global", que se caracteriza por la interacción de las entidades financieras y los clientes. La aceptación y expansión del e-commerce en la actualidad se debe principalmente a los cambios en os comportamientos de los consumidores, ya que se vuelven cada vez más exigentes, valoran el ahorro del tiempo y analizan más la información sobre la calidad y los precios de los múltiples productos y servicios. La generalización del comercio electrónico se ve impulsada por el avance de las tecnologías y su difusión entre los clientes; así como los avances en materia de seguridad en las transacciones y por el trabajo mancomunado entre los agentes involucrados en este tipo de comercio. (Melle Hernandez, 2008)

8. Conclusiones

Los cambios acelerados producto de la globalización son innumerables y cada vez más atractivos y que brindan infinidad posibilidades de económicas y culturales a la humanidad entera. Es así, como impulsados por los avances tecnológicos de las comunicaciones y la informática se han convertido en el medio que desarrolla las relaciones personales, organizacionales, locales e internacionales, del conocimiento y el desarrollo. El comercio electrónico está generando y estructurando una mejor manera de pensamiento que se adapte al mundo digital; las maneras de hacer negocio que se utilizan tradicionalmente están siendo poco a poco reemplazadas en la media que los negocios se realizan a través de medios electrónicos y se pueden soportar en bases de datos de los computadores al no requerir documentos físicos

Pero este importante y dinámico cambio que ha condicionado los nuevos comportamientos sociales, económicos, políticos y éticos de las personas y los pueblos, ha venido acompañado de un no menos dinámico y, a la vez, peligroso proceso de una nueva delincuencia que, al utilizar o impactar los sistemas de información y comunicación de las organizaciones y el mundo, ha llegado a posicionarse como uno de los mayores peligros para la seguridad, la honra, vida y bienes de las personas y las organizaciones de todos los países.

De tal forma, que nos encontramos con dos fenómenos significativos frente a esta situación:

- El primero, hace referencia a lo positivo que se relaciona con la globalización, la tecnología, la información y las comunicaciones.
- Y el segundo, es el negativo, es decir, la ciberdelincuencia, que promovido que las organizaciones y algunos gobiernos del mundo tomen conciencia de la perspectiva del futuro y la subyacente amenaza, para actuar mancomunadamente y construir barreras

> no sólo tecnológicas, sino también jurídicas y sociales que permitan enfrentar y mitigar ese gran mapa de riesgos generado por los delitos informáticos.

La seguridad es el factor primordial del comercio en redes digitales, y el eje sobre el cual el mundo digital debe apoyarse. La fragilidad en los sistemas operativos genera desconfianza e inseguridad de tipo legal la cual debe ser enfrentada por el derecho interno de cada país soportado en los tratados internacionales.

Dentro del ámbito empresarial, es relevante destacar que en el aspecto competitivo que identifica al comercio, los gastos invertidos en seguridad digital no han tenido mucha participación. La decisión de invertir en seguridad digital implica un alto costo; si la organización que invierte en seguridad no experimenta alguna violación de riesgo en su sistema informático, la inversión no producirá ningún retorno y las utilidades serán menor que la de la competencia, por ello debe buscar un equilibrio financiero entre los riesgos de seguridad digital y rentabilidad; por ejemplo en Colombia entidades financieras como Bancolombia están invirtiendo en seguridad digital para que los clientes se sientan seguros al momento de hacer cualquier operación bancaria.

9. Recomendaciones

Se puede decir que el apogeo que genera el crecimiento del comercio electrónico a nivel mundial, ha obligado a las organizaciones a tomar las medidas necesarias para minimizar los riesgos de seguridad en sus sistemas de información.

En base a esto, es recomendable que las organizaciones inviertan en Sistemas de Gestión de Seguridad de la Información SGS, ya que es una herramienta estratégica que le permite a las compañías mejorar su imagen en el mercado donde se desenvuelven y crean un ambiente de seguridad, ya que estos modelos de gestión facilitan sus procesos de seguridad electrónica, las cuales como ya lo hemos mencionado antes, son de vital importancia para establecer relaciones de confianza con los consumidores.

Así que no es exagerado destacar que el reto del cibercrimen, implica un reto para las propias condiciones de supervivencia y desarrollo de las personas, las organizaciones y las instituciones del país y del mundo. No se puede subestimar su poder, complejidad y alcance, pues puede llegar no sólo a los recursos, propiedades y derechos, sino a las posibilidades de vida. No basta con formar grupos de defensa o ataque al cibercrimen, si no se construye la conciencia organizacional y ciudadana de la seguridad digital, como parte integral de la cultura de mejoramiento de las condiciones de vida de las personas.

10. Referencias Bibliográficas

Acuña, L. y Villa, S. (2018). Estado actual del cibercrimen en Colombia con respecto a Latinoamérica. (Monografía de Especialización, Universidad Nacional Abierta y A Distancia, Colombia)

Grupo Bancolombia . (2020). Obtenido de https://ayuda.nequi.com.co/hc/es/articles/115003904112-La-seguridad-de-mi-Nequi

Aguilera, P. (2011). *Redes seguras (seguridad informática).* España: Editex.

Aguirre, J. R. (2006). *Libro electrónico de seguridad Informática y Criptografía.* España: Universidad Politécnica de Madrid.

Asobancaria. (2016). Obtenido de https://www.asobancaria.com/semanseconomicas/Sem-1051.pdf

Asobancaria. (2016).

Asobancaria. (2016). *Informe sobre un nuevo mecanismo para mejorar la confianza en el comercio electrónico* . Obtenido de https://www.asobancaria.com/semanseconomicas/Sem-1051.pdf

Asobancaria. (2016). *un nuevo mecanismo para la confianza en el comercio electrónico.*

Asobancaria. (2019). *Informe sobre E-commerce.*

Asobancaria. (s.f.). *Asobancaria.* Obtenido de https://www.asobancaria.com/

Avenío, C. A. (2017). *Fundamentos de seguridad informática* . Bogotá: Fundación Universitaria del Área Andina.

Baca, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria.

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

CCCE. (2019). *Medición de Indicadores de consumo del Observatorio eCommerce.* BOGOTA: MinTic.

CCCE. (2020). *Informe sobre crecimiento del comercio electrónico en cuarentena.* BOGOTA: MinTic.

CCIT. (2020). *Tendencias del Cibercrimen en Colombia.* BOGOTA: MinTic.

Digiware. (2019). *Las utilidades del cibercrimen en América Latina.* Bogota: Institucional.

Digiware. (2020). *Maximización del internet global y los datos para un crecimiento sostenible e inclusivo en América Latina.* Bogota: Insitucional.

Edgar Julián Galvez Albarracín, S. R. (2014). *Influencias De Las Tecnologías De La Información Y La Comunicación En El Rendimineto De Las Pymes.*

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

Jones, C. Motta, J. & Alderete, María. (2016). Gestión estratégica de tecnologías de información y comunicación y adopción del comercio electrónico en Mipymes de Córdoba, Argentina. Estudios Gerenciales, 32 (138), 4-13.

Medina, M., Verástegui, L. & Melo, P. N. A. (2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. Contaduría y Administración, 57(4), 11–34.

Melle Hernandez, M. (2008). *El comercio electrónico y la seguridad de las transacciones.*

MIntic. (s.f.). Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Mintic. (27 de 6 de 2013). Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Raymond, L. Croteau, A. & Bergeron, F. (2011). The strategic role of IT as an antecedent to the IT sophistication and IT performance of manufacturing SMEs. International Journal on Advances in Systems and Measurements, 4(3), 203–21.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., y otros. (2018). *Introducción a la seguridad informática y al análisis de vulnerabilidades.* España: Área de Innovación y Desarrollo,S.L.

Santiago, H. J. (3 de 2004). Obtenido de https://www.javeriana.edu.co/biblos/tesis/derecho/dere6/DEFINITIVA/TESIS24.pdf

Vidal, M., & Garcia, G. (2005). Seguridad, información y salud. *Revista Cubana de Informática Médica*, 22-31.

Zamora, V. F. (2017). Obtenido de EL COMERCIO ELECTRÓNICO EN COLOMBIA: BARRERAS Y RETOS: https://repository.javeriana.edu.co/bitstream/handle/10554/36499/FerrariZamoraVanessa2018..pdf?sequence=1&isAllowed=y