Comercio electrónico:

Importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra online y en redes sociales en Colombia

Hugo Armando Restrepo

Trabajo de grado presentado como requisito para optar al título de Ingeniero de sistemas

Asesor

Ph. D Jhon Fernando Sanchez Álvarez

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Ingeniería de Sistemas

Marzo 2023

Nota de aceptación

Aprobado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y A Distancia UNAD para optar por el título de Ingeniero de Sistemas.

_____

Director de la opción de grado

_____

Jurado

Medellín, 10 de marzo de 2023

Declaración de derechos de propiedad intelectual

Los autores de la presente propuesta manifestamos que conocemos el contenido del Acuerdo 06 de 2008, Estatuto de Propiedad Intelectual de la UNAD, Artículo 39 referente a la cesión voluntaria y libre de los derechos de propiedad intelectual de los productos generados a partir de la presente propuesta. Asimismo, conocemos el contenido del Artículo 40 del mismo Acuerdo, relacionado con la autorización de uso del trabajo para fines de consulta y mención en los catálogos bibliográficos de la UNAD.

Dedicatoria

Este trabajo ha llegado a este nivel de maduración, gracias a la ayuda, inspiración, formación y orientación en la ejecución por parte del asesor de tesis, sin cuya guía, esto no habría sido posible.

Así mismo, con toda gratitud a todas las personas que contribuyeron al éxito de esta investigación.

A mi familia por su motivación y apoyo en todo el proceso formativo, por soportar todas mis ausencias y darme su amor y comprensión.

Resumen

El comercio electrónico está expuesto a diversas amenazas debido a los riesgos y vulnerabilidades de ciberseguridad que subyacen en sus procesos. Como derivación de la pandemia, entre los años 2019 y 2020, se incrementaron los delitos informáticos asociados a las transacciones de comercio electrónico que pasaron del 48% al 360% en el primer trimestre del 2021. Este estudio tiene como pretensión, analizar la importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra Online y en las redes sociales en Colombia. Para tal fin, se describen los lineamientos de las buenas prácticas del comercio electrónico en sitios web, redes sociales, plataformas y/o aplicaciones; se indaga sobre los peligros y riesgos subyacentes en estas transacciones y se plantean estrategias para mitigar los peligros y riesgos asociados. El estudio concluyó que el asunto de la ciberseguridad requiere de un enfoque comprensivo y holístico que posibilite la articulación de los esfuerzos de los actores implicados con la implementación de estrategias y herramientas basadas en la Inteligencia Artificial (IA) y el Aprendizaje automático (ML) y el Big Data (BD).

Palabras clave: ciberseguridad, ciberdelincuencia, comercio electrónico, riesgos, buenas prácticas.

Abstract

E-commerce is exposed to various threats due to the cybersecurity risks and vulnerabilities that underlie its processes. As a derivation of the pandemic, between 2019 and 2020, cybercrime associated with e-commerce transactions increased from 48% to 360% in the first quarter of 2021. This study aims to analyze the importance of cybersecurity in electronic transactions made on online shopping platforms and social networks in Colombia. To this end, it describes the guidelines for good e-commerce practices on websites, social networks, platforms and/or applications; it inquires about the underlying dangers and risks in these transactions and proposes strategies to mitigate the associated dangers and risks. The study concluded that the issue of cybersecurity requires a comprehensive and holistic approach that enables the articulation of the efforts of the actors involved with the implementation of strategies and tools based on Artificial Intelligence (AI) and Machine Learning (ML) and Big Data (BD).

Keywords: Cybersecurity, Cybercrime, E-commerce, Risks, Best practices.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

La globalización, la digitalización y las tecnologías inteligentes han incidido en la prevalencia y la gravedad del delito cibernético. Razón por la que se ha convertido en las últimas décadas en un campo emergente de investigación, considerando la relevancia que han cobrado los trabajos encaminados a la consolidación de sistemas de defensa de ciberseguridad robustos, especialmente en los ámbitos corporativo, nacional y supranacional.

Muestra de esta afirmación se halla en los reportes estadísticos sobre ciberdelincuencia que estiman que esta ha implicado un costo de poco menos de USD 1 billón en 2020 en la economía mundial, lo que indica un aumento de más del 50 % desde el año 2018. Con el aumento promedio de reclamos de seguros cibernéticos de USD 145,000 en 2019 a USD 359,000 en 2020, hay una creciente necesidad de mejoramiento de las fuentes de información cibernética, de las bases de datos estandarizadas, de los informes obligatorios y de la conciencia pública (Policía Nacional de Colombia, 2020).

En Colombia, las transacciones del comercio electrónico han venido incrementándose notablemente durante los últimos años; sin embargo, este crecimiento fue exponencial durante el año 2020, como consecuencia de los efectos de la pandemia del COVID-19 y del confinamiento adoptado como medida de protección, que como es bien sabido, trajo múltiples afectaciones y transformó los hábitos de las personas, entre ellos, la manera en que gestionan sus compras y los medios utilizados para pagarlas.

En el mismo sentido, la dinámica actual del cibercrimen en Colombia refleja un crecimiento gradual debido al incremento de los incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad. Según los reportes de la Policía Nacional de Colombia fueron registrados 28.827 casos durante el año 2019, de estos, 15.948 fueron

denunciados como infracciones a la ley 1273 de 2009, o lo que es lo mismo, un 57% del total de casos incluidos en el informe (Policía Nacional de Colombia, 2020).

Pese que respecto al 2018 las denuncias disminuyeron en un 5.8 %, con una variación negativa de 983 casos; se evidenció un incremento real en el reporte de casos del 54% respecto a los datos del año 2018. Según este mismo informe, los incidentes más reportados en Colombia son los casos de Phishing con un 42%, seguido de la Suplantación de Identidad con un 28%, el envío de malware con el 14% y los fraudes en medios de pago en línea con el 16% de los casos (Policía Nacional de Colombia, 2020).

Esto representa una problemática de notable complejidad considerando que el atacante puede utilizar maliciosamente la información compartida para fines ilegítimos, sin contar con que los riesgos son aún mayores si se trata de ataques a menores de edad. Las violaciones de datos a menudo involucran el detrimento de la confidencialidad por acceso no autorizado.

En correspondencia con lo anteriormente formulado, este estudio tiene como propósito fundamental analizar la importancia de la ciberseguridad en las transacciones electrónicas realizadas mediante las plataformas de compra Online y las redes sociales en Colombia. Para ello, acude a una estrategia de investigación cualitativa, tipo descriptiva, fundada en un análisis documental y centrado en la descripción de los lineamientos del compendio de buenas prácticas del comercio electrónico en sitios web y plataformas y/o aplicaciones; el planteo de estrategias para mitigar los peligros a los que se ven expuestas las personas al realizar las compras por medios electrónicos; junto con la indagación de los riesgos subyacentes y peligros asociados a los medios electrónicos al momento de hacer compras y transacciones.

Entretanto, para el desarrollo de este propósito y hechas estas consideraciones introductorias, en un primer capítulo se aborda la delimitación, descripción y formulación del

problema de investigación en el que centra la atención esta pesquisa; luego, en un segundo capítulo, se delimitan los marcos de referencia teórico, conceptual y legal; esto como antesala, para en un tercer capítulo, abordar las delimitaciones tecnológica, cognitiva, temporal y financiera del proyecto de investigación. Luego, los capítulos cuatro y cinco se destinan al análisis y discusión de los resultados obtenidos mediante el despliegue de la revisión y a la formulación de algunas conclusiones y recomendaciones respectivamente.

Justificación

Conviene centrar por un momento la atención en las razones que justifican la realización de un trabajo de investigación con el alcance y propósito formulado; esto desde el punto de vista teórico y conceptual, metodológico y práctico. En primer lugar, desde el punto de vista teórico y conceptual, esta investigación articula un compendio de nociones y conceptos que se han validado en la revisión bibliográfica y documental, y que se relacionan con las causas, derivaciones y alcances de la problemática de la ciberdelincuencia en el comercio electrónico. En este trabajo, esta problemática se aborda mediante la selección de un enfoque teórico que permite abarcar sus aspectos y relaciones principales, así como las estrategias para el abordaje de los riesgos conexos.

En segundo lugar, desde el punto de vista metodológico, implica un conjunto de instrumentos y herramientas encaminados al logro de los objetivos del trabajo, reflejados en la revisión, verificación, delimitación y valoración de los hallazgos de los trabajos e investigaciones relacionadas con las buenas prácticas del comercio electrónico, los riesgos subyacentes en este tipo de transacciones y las estrategias para su abordaje en función de la seguridad transaccional.

Finalmente, en tercer lugar, desde el punto de vista práctico, constituye un insumo de trabajo para nuevas investigaciones enfocadas en el estudio de los mismos focos o de otros que resulten emergentes. Este producto corresponde a la aplicación de los contenidos abordados en el programa de Ingeniería de sistemas de la Universidad Nacional Abierta y a Distancia enfocado para concebir, diseñar, implementar y operar sistemas y proyectos de TI sustentados en software, encaminados a la solución de problemáticas específicas de los sectores públicos o privados, que demanden la implementación de alternativas de mejoramiento o producción de conocimiento

frente a los procesos que desarrollan (UNAD, 2022) tal y como es el caso de la ciberseguridad en transacciones de comercio electrónico.

Objetivos

Objetivo General

Analizar la importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra Online y en las redes sociales en Colombia.

Objetivos Específicos

Describir los lineamientos de las buenas prácticas del comercio electrónico en sitios web, redes sociales, plataformas y/o aplicaciones.

Indagar sobre los peligros y riesgos subyacentes en las transacciones y compras realizadas en comercios electrónicos y redes sociales.

Plantear estrategias para mitigar los peligros y riesgos asociados a las compras realizadas por medios electrónicos y en redes sociales.

Consideraciones Generales Sobre el Problema de Investigación

Este capítulo presenta a consideración del lector algunas precisiones encaminadas a la delimitación, descripción y formulación del problema de investigación y de los objetivos general y específicos de la revisión, así como de la concreción de las preguntas orientadoras y la explicación de las razones que justifican la realización de un proyecto con el alcance y propósito indicado.

Descripción del Problema

Desde finales de la década de los noventa, que coincide con la culminación del siglo XX, la sociedad en general ha sufrido una transformación sin precedentes, debido a la aparición de la internet que ha revolucionado las relaciones existentes entre los individuos a partir del uso de dispositivos móviles, incluso determinando las formas y modos de relacionamiento e interacción entre las personas. Son muchas las derivaciones que este desarrollo ha tenido para la humanidad, incluyendo beneficios, pero también riesgos y nuevos peligros a los que se exponen las personas que navegan por el ciberespacio (Pérez, 2016).

Cuando Internet se hizo popular a mediados de la década de 1990, hizo posible compartir información de formas que nunca habían sido pensadas (Kraft, 2015). Luego, a principios de la década del 2000, los sitios de redes sociales introdujeron un toque personal al intercambio de información en línea que fue adoptado rápidamente por las masas (Hartman et al., 2001).

Después de la pandemia del COVID – 19, con todos los efectos de la propagación y el confinamiento, se produjo la masificación del uso de transacciones, con el subsecuente aumento de los riesgos digitales. De modo que al vertiginoso desarrollo que han tenido el internet y las Tecnologías de la Comunicación y la Información (TIC) en el último tiempo, se sumaron las transformaciones derivadas de la pandemia, transfigurando los usos que hasta el momento habían

tenido esas herramientas, que pasaron de ser simples instrumentos de entretención, distracción o relacionamiento social, para convertirse en parte fundamental de la cotidianidad y pilar de muchas actividades que se desarrollan cotidianamente, incluso, procesos transaccionales relacionados con la compra de bienes y servicios en comercios electrónicos y mediante redes sociales.

Estas transformaciones incluyen, cambio de hábitos, incremento de la presencia digital y particularmente, un aumento de las transacciones digitales; lo que también deriva en un acrecentamiento de exposición a los riesgos del mundo digital. No importa si la causa es la falla de un componente, bien sea de hardware o bien sea de software, o un corte de energía o la acción criminal de algún hacker desconocido en busca de ganancias. Esta problemática ha llevado a las organizaciones empresariales y a los gobiernos como el colombiano a emprender estrategias para el robustecimiento de la seguridad informática transaccional y medidas para la mitigación de los riesgos subyacentes.

Las compras en línea, las transacciones subsecuentes, la venta de acciones y negociación de instrumentos financieros, la compra y venta de bienes y servicios, de artículos blandos, mercancías, contenidos, gráficos, videos y software son ejemplos de tipologías del negocio de comercio electrónico. Las plataformas comerciales y electrónicas facilitan la admisión de compradores para realizar una compra de autoservicio.

Para este propósito, ofrecen transacciones en tiempo real en una amplia región geográfica durante todo el día. En los días en que las personas solían comprar en una tienda minorista, antes de que las compras en línea se hicieran populares, las amenazas cibernéticas eran solo prácticas primitivas dirigidas a causar infracciones en los sistemas POS (puntos de venta) en un intento por robar información personal de los propietarios de tarjetas de crédito.

Con la digitalización formando parte de la mayoría de las actividades y negocios diarios, las amenazas cibernéticas han crecido a un ritmo sin precedentes, brindando a los delincuentes nuevas formas de obtener activos más valiosos. Bajo esta perspectiva, debe reconocerse que en la actualidad se dispone de un nutrido compendio de herramientas que posibilitan transacciones y servicios financieros disponibles en línea. Asimismo, deben asumirse los riesgos que se encuentran implícitos en este tipo de transacciones y las brechas que representan nuevas entradas potenciales para los atacantes maliciosos.

Las redes sociales tienen distintos usos y aplicaciones, desde el entretenimiento, la creación de oportunidades comerciales, la creación de una carrera, hasta el mejoramiento de las habilidades sociales y establecimiento de relaciones con otras personas (Martínez & Ávila, 2021). Facebook se encuentra entre los sitios de redes sociales preferidos. Considerando que una gran parte de la población en línea utiliza las plataformas de redes sociales, estas se han convertido en un medio importante para la promoción de campañas comerciales, sociales y de concientización.

Las redes sociales son la práctica de expandir el contacto de una con otras personas principalmente a través de sitios web como Facebook, Twitter, Instagram, LinkedIn, entre otros (Martínez & Ávila, 2021). Se pueden utilizar tanto por razones personales como empresariales. Reúne a las personas para hablar, compartir ideas e intereses y hacer nuevos amigos; básicamente, ayuda a personas de diferentes regiones geográficas a colaborar y compartir sobre intereses y temáticas comunes. Las plataformas de redes sociales son de fácil usabilidad, por lo que su expansión, número de usuarios y crecimiento ha sido exponencial tanto como su popularidad.

La razón fundamental detrás de este fenómeno es la capacidad de las redes sociales para proporcionar una plataforma para que los usuarios se conecten con su familia, amigos y colegas. La información compartida en las redes sociales se propaga con facilidad y rapidez, casi instantáneamente, lo que hace que sea atractivo para los atacantes que desean obtener información por medios ilegales. Existen numerosos problemas de seguridad y privacidad relacionados con la información compartida por el usuario, especialmente cuando se comparte contenido en formato de fotos, videos y audios.

Los ataques cibernéticos, especialmente aquellos relacionados con las actividades maliciosas de suplantación de identidad, phishing, malware y ransomware, se han vuelto cada vez más populares en el sector financiero. Los piratas informáticos buscan continuamente vulnerar a los empleados y usuarios involucrados con los bancos digitales, ya que se han convertido en objetivos para la obtención de ganancias financieras (Fisch & White, 2000). Mediante el uso de correos electrónicos, dominios y comunicaciones relacionadas con dispositivos móviles, los atacantes intentan engañar a sus víctimas para que entreguen credenciales de inicio de sesión e información financiera al disfrazarse o hacerse pasar por el banco digital o la institución financiera oficial.

Colombia ocupó el tercer puesto en términos de la comisión de ciberataques respecto al resto de países de Latinoamérica, después de México con 85.000 casos y Brasil con 31.500. Según el Centro Cibernético de la Policía Nacional, con corte al mes de octubre de 2022, se habían registrado 54.121 denuncias por delitos informáticos, superando en 11.223 casos el reporte del año inmediatamente anterior (Policía Nacional de Colombia, 2020). Según el reporte de National Cyber Security Index (NCSI), Colombia ocupa el puesto 65 en el listado global que mide la seguridad cibernética (NCSI, 2021).

Los últimos casos con relevancia nacional que se han presentado incluyen entidades de distintos sectores, especialmente el financiero. Es así como empresas como Bancolombia, Davivienda, EPS Sanitas, adscrita a Keralty y EPM han reportado inconvenientes en sus páginas web con afectaciones en los procesos de pago, consultas y asignaciones de flujos de trabajo. Asimismo, organismos gubernamentales como: Invima, DANE y la fiscalía general de la Nación (Arenales, 2022).

Según el reporte de inteligencia de amenazas Fortinet (2021) se han presentado un total de 137.000 intentos de ciberataques en Latinoamérica y el Caribe durante el primer semestre del año 2022, es decir, 50% más que lo registrado en el mismo periodo del año anterior con 91.000 casos (FORTINET, 2021).

Formulación del Problema de Investigación

La llegada de la nube, la inteligencia artificial (IA) y el aprendizaje automático (ML) han impulsado la consolidación de la integridad de las redes bancarias, en términos de seguridad de datos, operaciones fluidas y de respuesta rápida a las ciber amenazas. Si bien la introducción de la biometría y el análisis a nivel de red han promovido la protección contra las actividades fraudulentas en el mundo digital, los proveedores de productos y servicios Fintech deben adoptar un enfoque de seguridad estratégico para contextualizar, relacionar y perfilar con precisión todas las entidades digitales implicadas en las redes de su negocio.

El trabajo remoto se ha convertido en un modelo de trabajo muy popular desde el comienzo de la pandemia de COVID-19. Esta práctica fue adoptada por empleados de diferentes sectores económicos, incluido el financiero. Tanto los bancos digitales, como los tradicionales, deben asegurarse de satisfacer las necesidades laborales de seguridad requeridas de sus empleados. Esto incluye especialmente la protección de sus dispositivos de trabajo y de sus

sistemas. Es necesario recurrir a la implementación de medidas y controles de seguridad cibernética rigurosos para reemplazar los mecanismos y prácticas de defensa y seguridad cibernética que estaban disponibles en sus oficinas físicas. Las anteriores descripciones y enunciaciones se pueden concretar mediante la formulación de las preguntas que orientan los esfuerzos de la investigación, así:

Una pregunta orientadora enfocada a determinar: ¿Cuál es la importancia de la ciberseguridad en las transacciones electrónicas realizadas por medio de plataformas de compra Online y en las redes sociales en Colombia? Asimismo, unas preguntas auxiliares encaminadas: ¿Cuáles son los lineamientos de las buenas prácticas del comercio electrónico en sitios web, plataformas y/o aplicaciones?; ¿Qué peligros subyacen en las compras y transacciones por medios electrónicos?; ¿Qué importancia tiene la validación de la empresa y su razón social en la seguridad transaccional en el comercio electrónico? Y finalmente, ¿Qué estrategias sirven para la mitigación de los riesgos asociados a las compras y transacciones por medios electrónicos? Estos interrogantes se concretan a su vez en los objetivos a los que se encamina el trabajo de investigación.

Marcos de Referencia de la Investigación

Siguiendo con el hilo de exposición propuesto, en este apartado, se describen los marcos de referencia en los que se encuadran los esfuerzos de esta investigación; en tal sentido, en primer lugar, se valora el estado del arte de la cuestión; para luego, revisar las nociones, enfoques y teorías relacionadas con las categorías de estudio y finalmente, verificar el marco de referencia legal atinente al problema de investigación en el contexto legal colombiano.

Estado del Arte

La revisión permitió evidenciar que los estudios de las ciencias de la información se han centrado en el análisis del riesgo cibernético y lo han catalogado como un problema grave para la seguridad transaccional en el comercio electrónico. Algunos estudios indican que existe una laguna en las bases de datos abiertas que socava los esfuerzos colectivos para gestionar mejor este conjunto de riesgos.

Pese a la creciente relevancia para la economía internacional, la disponibilidad de datos sobre riesgos cibernéticos sigue siendo limitada. Las razones para esto son muchas. Por lo tanto, es un riesgo emergente y en evolución y adicionalmente, con fuentes de datos históricas limitadas. También podría deberse a que, por lo general, las instituciones que han sido hackeadas no publican los incidentes. La falta de datos plantea desafíos para muchas áreas, como la investigación, la gestión de riesgos y la ciberseguridad.

En el mismo sentido, la literatura indica que los ciberataques, las filtraciones de datos generan altos costos. En tal sentido, es una obligación de las empresas, brindar estrategias para la protección de los datos personales y salvaguardar los derechos de protección de datos, tal y como lo indica el Reglamento general de protección de datos (GDPR), (Organización de los Estados Americanos, 2017).

Un primer referente en el contexto internacional se encuentra en el trabajo desarrollado en Brasil sobre el estado actual de la ciberseguridad en este país, a partir del análisis de su estrategia nacional. Según Hurel (2021), los desafíos que deben abordarse incluyen: la carencia de un lenguaje para aludir cuestiones cibernéticas y digitales; la asociación de ciberseguridad con cuestiones, responsabilidades y competencias de las instituciones militares, lo que ha impedido una mayor masificación de sus nociones y prácticas; el desconocimiento de riesgos específicos y compartidos intersectoriales; la falta de mecanismos para intercambio de información sobre riesgos y peligros, así como conocimientos de seguridad entre sectores; la falta de normativa, estrategia y funcionamiento y alineación operativa para responder a incidentes; y la existencia de diferentes niveles de niveles de madurez de la sociedad en materia de ciberseguridad.

En el mismo sentido, el trabajo publicado por Aseri (2021) sobre Cuestiones de seguridad para los compradores en línea analiza este fenómeno como una nueva técnica que ha revolucionado la experiencia de compra y transformando los métodos de compra convencionales. Las plataformas de compra eliminan la necesidad de acudir a una tienda física permitiendo el acceso a información de modelos o productos relacionados con búsquedas frecuentes en las tiendas. Pese a sus notables ventajas, se encuentra sujeta a ataques maliciosos de malware que comprometen la seguridad y la integridad de los datos. Estos ataques incluyen, entre otros, técnicas de phishing y adware.

El trabajo indica que las numerosas violaciones de datos a empresas de renombre como Amazon y Google han incidido en los imaginarios de los particulares generando dudas en términos de la seguridad transaccional de las compras en línea debido a los fraudes. Estos temores se relacionan con incidentes en transacciones financieras y carencia de información

sobre los procedimientos relacionados con las compras electrónicas. En tal sentido, debe fortalecerse la percepción positiva del comercio electrónico.

Pasando a un contexto de investigación regional (América Latina y el Caribe) se encuentra el trabajo desarrollado por Souminen (2019) para la CEPAL. En este trabajo se realizó una encuesta en más de 1.400 empresas de América Latina y el Caribe, encontrando que aquellos que informan ventas en línea están inmersos en procesos de internacionalización en comparación con aquellos que no compran ni venden bienes servicios en línea. El estudio también permitió evidenciar que los vendedores en línea están más diversificados en sus mercados de exportación que los vendedores fuera de línea, y exportan más a los mercados extrarregionales, especialmente a los Estados Unidos.

Según el estudio, las empresas encuestadas en América Latina y el Caribe, aun cuando se encuentran digitalizadas, en un 36% según el informe, estas no reportan ventas en línea. Por su parte, las que sí lo hacen, informan obtener solo una parte limitada de los ingresos de las exportaciones. El autor concluye que uno de los desafíos de las empresas es la adopción del comercio electrónico, lo que incluye el conocimiento y comprensión rigurosa de los mercados nacionales de comercio electrónico, que, según el estudio, son pequeños, con logística y procesos de exportación en línea complicados (Souminen, 2019).

Finalmente, en el contexto nacional y local sobresale el trabajo de Cano (2022) quien propone un ejercicio prospectivo sobre la ciberseguridad nacional de Colombia a 2030, a partir de la revisión de fuentes académicas, reportes internacionales y entrevistas. Los resultados fueron agrupados en seis factores siguiendo el marco Pestel: político, económico, social, tecnológico, ecológico y legal, en función de la delimitación de un panorama integrado para la

comprensión del reto de la protección del Estado frente a las dinámicas internacionales de la transformación digital.

Conviene anotar que, en la actualidad, las naciones y empresas deben asumir el reto de construcción de dinámica de buenas prácticas y estándares cuidando que estos protocolos no queden obsoletos por el vertiginoso desarrollo de las tecnologías. Según Price Waterhouse Coopers (PwC), las iniciativas internacionales de organismos multilaterales, las tendencias alrededor de la responsabilidad digital empresarial y la exigencia de la protección de datos se han transformado en el eslabón fundamental en los procesos de revisión y actualización relacionados con la ciberseguridad, como un asunto, que como bien lo expresa la empresa auditora: "corresponde a un ejercicio de responsabilidad digital convergente, donde los derechos, deberes y libertades de los individuos siempre estarán en juego" (como se cita en Cano, 2022, p.16).

Marco de Referencia Teórico y Conceptual

En este punto se centra la atención en los marcos de referencia teórico y conceptual de la ciberseguridad y el comercio electrónico. De modo que en lo que sigue, se articulan una serie de nociones en función de la comprensión de la problemática de estudio. Antes de abordar estos conceptos, conviene delimitar el enfoque teórico que se utiliza para el abordaje de la ciberseguridad en el comercio electrónico. En tal sentido, se ha adoptado el enfoque propuesto en la Norma ISO 27032 de 2012 y 27001 de 2013 que concibe la Ciberseguridad como un proceso donde intervienen distintos actores que deben comprometerse con el cuidado de la información y en términos de los propósitos estratégicos del negocio y con enfoque en la seguridad transaccional y del cliente. Esta normativa resalta sobre la importancia de implementación de controles en todos los niveles encaminados a la mitigación de los riesgos asociados.

En términos generales y a guía de contextualización, debe indicarse que ISO es una organización global para la definición de estándares y el mandato de creación de reglas técnicas para que las organizaciones puedan garantizar que sus productos y procesos se encuentren en línea con el propósito previsto. En este caso, las normas referenciadas comprenden los procesos de seguridad de los datos y disponen de la implementación de sistemas de gestión de alta calidad; asimismo, aplicación de enfoques para la evasión de riesgos; la protección de datos y de las operaciones comerciales certificadas.

En estas normas técnicas, se asume el ciberespacio como un lugar común de las personas y las organizaciones, que en consecuencia deben comprometerse con la protección debido al beneficio que obtienen en la interacción que en este se realiza. El enfoque de este trabajo se funda principalmente en la norma NTC/ISO 27032:2012 y la NTC/ISO 27001:2013 Este marco se establece para contar con una guía para la implementación, operación, seguimiento, revisión y mejora de un sistema de gestión enfocado en la ciberseguridad con compromiso de los actores implicados comercialmente.

Estas normativas asumen el problema de la ciberdelincuencia desde la complejidad de sus dinámicas y componentes. Se apoya en otras disposiciones como las normativas relacionadas con Framework, Ciberseguridad del NIST y del CIS; Ciber protección o Cybersafety. En todo sentido, su propósito estriba en propiciar condiciones de protección en todos los estamentos y procesos, tanto desde el punto de vista físico, como social, político, financiero, emocional, laboral, psicológico, educacional, entre otros y resguardados de todo tipo de fallas, daños, errores o accidentes derivados de cualquier evento posible. Esto implica la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, que se asume como un entorno complejo donde se gesta la interacción de las personas, el software y los

servicios ofertados mediante internet, por medio de dispositivos tecnológicos conectadas mediante redes (ISO, 2019).

Los propósitos de este trabajo de investigación articulan las categorías conceptuales de Ciberseguridad y las transacciones electrónicas, relación que se enmarca en el proceso de compras y pagos realizados en comercios electrónicos y mediante redes sociales. Estas categorías se relacionan a su vez con otras nociones y conceptos que se detallan en lo que sigue.

Conviene definir en un primer momento, lo que significa una violación de datos, es decir, un incidente de seguridad en el que una persona no autorizada copia, transmite, ve, roba o utiliza datos sensibles, protegidos o confidenciales (IBD, 2017). Dependiendo de la cantidad de datos, el alcance del daño causado por una violación de datos puede ser significativo. Estas violaciones de datos suelen ser ejecutadas por los ciberdelincuentes. Según la literatura se han definido dos tipologías; los primeros son expertos y cometen delitos, esto como derivación del conocimiento de una vulnerabilidad en determinada plataforma, organización o entidad, aprovechándose para su beneficio, estos son llamados *insiders* (De la cuesta & Pérez, 2010). Luego, un segundo grupo integrado por empleados de la misma empresa que borran, dañan, sustraen información sensible en medios de almacenamiento masivo y documentos (INTERPOL, 2020).

Estas dinámicas se encuadran en el cibercrimen, compuesto en notable medida por desarrolladores de aplicaciones e investigadores que integran estas bandas criminales, quienes se encargan de crear nuevos métodos para ingresar sin permiso a dominios de sistemas de datos o explotar las vulnerabilidades de seguridad en entornos operativos, además aprovechan la ingeniería social para infectar computadoras. a través de una serie de trucos, ocultar información y resistir las acciones de los protectores del sistema o cortafuegos.

También se encuentran otros actores en el escenario de la ciberseguridad; se trata de los estudiantes habilidosos e inquietos, que poseedores de amplios conocimientos en sistemas operativos e infraestructura, se retan poniendo a prueba sus habilidades mediante la generación de malware dirigido a empresas donde identifican vulnerabilidades. Esto considerando que en la actualidad se accede con facilidad a manuales y cursos en diferentes sitios web que explican cómo crear y desarrollar virus informáticos y cómo eludir el software antivirus. El comercio electrónico (E-Commerce) es una tipología de transacción comercial que se ejecuta electrónicamente mediante el uso de una computadora, teléfono inteligente o tableta a través de una red conectada a internet (Kraft, 2015). Las transacciones incluyen intercambio de información entre las partes, bien sea, mediante correo electrónico, transmisión de fax, o transferencia de dinero virtual (PayPal, Skrill, Neteller, entre otros).

En el comercio electrónico, varios acrónimos son comunes, como PCI DSS, qué es el Estándar de seguridad de datos de la industria de tarjetas de pago, Seguridad de la capa de transporte (TLS), Organización internacional para la estandarización (ISO), Datos personales, Capa de conexión segura (SSL) y HTTPS. autenticación, autenticación multifactor (MFA), autenticación de 2 factores (2FA) o verificación de 2 pasos (2SV), denegación de servicio distribuida (DDoS) y malware y ransomware, entre otros (PCI, 2010).

PCI DSS o simplemente PCI se refiere a un estándar de la industria destinado a garantizar que la información relacionada con las tarjetas de crédito se transmita de forma segura y se mantenga en línea. Los datos personales se refieren a cualquier tipo de información asociada con una persona en particular. Puede incluir nombres, números de teléfono móvil, número de identificación, direcciones de correo electrónico, entre otros (NQA, 2017).

La autenticación multi factor (MFA), la autenticación de dos (2) factores (2FA) o la verificación de dos (2) pasos (2SV) se usan indistintamente, son lo mismo, pero existen diferencias entre ellos; mientras que un ataque de denegación de servicio distribuido (DDoS) es una interferencia de un servidor, servicio, sistema y/o tráfico de red cuando una inundación de tráfico lo abruma (PCI, 2010). El malware es un programa malicioso instalado en un sistema informático por piratas informáticos. El ransomware es un tipo de malware que impide que una víctima acceda a sus datos en un sistema informático hasta que se pague una determinada tarifa (rescate) (PCI, 2010).

En Colombia, suele utilizarse el término hacker cuando hay compromiso o pérdida de información o se presenta un ataque a una empresa, red social o una cuenta bancaria, pero el término se encuentra acompañado de un halo de desinformación, considerando que, recurriendo a la definición del vocablo en el Diccionario de la Real Academia de la Lengua Española (2017), Hacker y su correspondiente forma idiomática jáquer es una "persona experta en el manejo de ordenadores, que se ocupa de la seguridad de los sistemas y desarrolla técnicas de mejora". Este tipo de delito se denomina ciberdelito y se entiende como una actividad realizada por una o varias personas con conocimientos en redes de comunicación y en programación informática y dirigido a la materialización de medios delictivos para perjudicar o sacar un beneficio particular de la información en infraestructura tecnológica de las entidades. instituciones financieras, corporaciones, universidades, entidades gubernamentales y a la población en general (Stanikzai & Shah, 2021).

Teniendo en cuenta que la ciberseguridad corresponde a la práctica de protección de los sistemas y dispositivos digitales de atacantes maliciosos, esta se ha vuelto cada vez más relevante para las instituciones financieras especializadas en ofrecer sus servicios en línea, con el

fin de proteger los activos de sus clientes y las actividades transaccionales en línea. Incluso la brecha más pequeña identificada por los atacantes podría convertirse en una vulnerabilidad explotada en los sistemas de la empresa, causando daños masivos en la información valiosa tanto de los usuarios como de los bancos digitales. Las buenas prácticas en ciberseguridad permiten a los bancos digitales garantizar la seguridad de los datos confidenciales almacenados en sus sistemas, evitando pérdidas financieras drásticas a sus usuarios y asegurando una reputación confiable entre las partes interesadas.

Marco de Referencia Legal

En Colombia rige la Ley 1273 de 2009, que modificó el Código Penal (Ley 599 de 2000) y crea un bien jurídico denominado Protección de información y datos. Las disposiciones de este texto de ley se enfocan, por un lado, en los ataques a la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y, por otro lado, en los ataques y en otro tipo de infracciones (Congreso de la República de Colombia, 2009a). Esta ley fue creada para condenar a los ciberdelincuentes en caso de infracciones a los tipos penales allí definidos.

Colombia es un referente en América Latina y el Caribe por sus esfuerzos para combatir el ciberdelito. Esta política se plasma en dos documentos del Consejo Nacional de Política Económica y Social (CONPES). Según el CONPES, la ciberseguridad es un compromiso de integración de instituciones, entidades estatales, empresas privadas, comunidad y operadores de infraestructura, y se enfoca en la gestión de amenazas cibernéticas en la lucha contra el cibercrimen, incluyendo el tema de gestión de riesgos. Lineamientos de política en ciberseguridad y ciberdefensa. El CONPES se halla orientado al desarrollo de una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país (Departamento Nacional de Planeación, 1936). En la siguiente tabla se

resumen las principales disposiciones y directivas relacionadas con la regulación de la ciberdelincuencia en el contexto legal colombiano.

Tabla 1

Marco de referencia legal Ciberseguridad y Ciberdelincuencia en Colombia

Norma	**Año**	**Contenido**
Ley 527.	1999	Validez jurídica y probatoria de la información electrónica.
Ley 594.	2000	Ley General de Archivos – Criterios de Seguridad.
Ley 679.	2001	Pornografía Infantil – Responsabilidad ISPs.
Ley 962.	2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150	2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266.	2008	Habeas data financiera, y seguridad en datos personales.
Ley 1273.	2008	Delitos Informáticos y protección del bien jurídico tutelado que es la información.
Ley 1341.	2009	Tecnologías de la Información y aplicación de seguridad.
Ley 1437.	2011	Procedimiento Administrativo y aplicación de criterios de seguridad.
Ley 1480.	2011	Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas.
Ley 019.	2012	Racionalización de trámites a través de medios electrónicos. Criterio de seguridad.
Ley 1581.	2012	Ley estatutaria de Protección de datos personales.
Ley 1712.	1991	Transparencia en el acceso a la información pública.
		Marco reglamentario
Decreto 2364.	2012	Firma electrónica.
Decreto 2609.	2012	Expediente electrónico.
Decreto 2693.	2012	Gobierno electrónico.
Decreto 1377.	2013	Protección de datos personales.
Decreto 1510.	2013	Contratación Pública electrónica.
Decreto 333.	2014	Entidades de certificación digital.

Fuente: elaboración propia basado en Rincón, 2014.

Delimitaciones de la Investigación

En este capítulo se realiza una delimitación tecnológica, cognitiva, temporal, financiera y legal de la investigación:

Delimitación Tecnológica

El marco tecnológico de este proyecto se sitúa en la ciberseguridad con enfoque en las transacciones electrónicas de las plataformas de compra Online y redes sociales en Colombia. La protección de la integridad de los activos corporativos depende de factores organizativos, de gestión, de esta forma; por lo que resulta necesario la dinamización de procesos activos con las áreas directamente involucradas. La ciberseguridad es una práctica enfocada a asegurar la integridad, la confidencialidad y la disponibilidad de la información (Kapersky Lab, 2022). Representa la habilidad de defenderse contra posibles accidentes como fallos en el disco duro o interrupciones en los sistemas, además de protegerse ante ataques de adversarios o hackers (Kapersky Lab, 2022).

Delimitación Cognitiva

Se revisan los desarrollos informáticos y su relación con la ciberseguridad en las transacciones del comercio electrónico. Los ejemplos de estudios recientes ilustran una tendencia de desarrollo especializado en la ciberseguridad centrada en las transacciones electrónicas. Se estima la adquisición de pautas para el uso de software con relación a la ciberseguridad centrada desde las transacciones electrónicas de las plataformas de compra Online como redes sociales.

Delimitación Temporal

Para el desarrollo del proyecto se establece el cronograma de actividades que se muestra en el Anexo 2, habiendo cumplido el cronograma hasta el cuarto mes, de acuerdo con lo

planificado, el desarrollo de anteproyecto, recolección de información y presentación de informe final.

Delimitación Financiera

Para el desarrollo del proyecto se define un presupuesto de acuerdo con lo planificado tal y como se muestra en el Anexo 3.

Delimitación Legal

La intensificación del comercio electrónico y el uso de Internet ha llevado a los legisladores a enmarcar estas prácticas, así como tipificar conductas como delitos cuando operan en detrimento de la confidencialidad y patrimonio económico, esto con el fin de proteger a los usuarios de estos sitios y consumidores. Este trabajo de investigación se enmarca en las disposiciones que se han desarrollado en el apartado destinado a los marcos de referencia de la investigación, entre ellos, el marco legal. Para mayor detalle de la delimitación legal de esta pesquisa se debe revisar el contenido de la Tabla No 1. Conviene anotar que un primer referente de este marco se halla en la Ley de Comercio Electrónico (Ley 527 del 18 de agosto de 1999) que establece las bases para el E-Commerce, el uso y acceso de los mensajes de datos, las firmas digitales y las bases para la construcción de un marco regulatorio más amplio para el sector de los *e-commerce* (Congreso de la República de Colombia, 1999).

Metodología

En este capítulo se define el marco metodológico que se desarrolló en función del logro de los propósitos de este trabajo de investigación.

Diseño Metodológico

El enfoque utilizado para el desarrollo de este trabajo se propone en correspondencia con una investigación de carácter cualitativo, de tipo descriptivo, mediante la revisión bibliográfica y documental. De esta forma, se plantea identificar los conceptos y sus relaciones, mediante la aplicación de un método analítico y descriptivo para consolidar un marco actualizado de referencias en el contexto nacional e internacional.

La revisión sistemática de la literatura, que ha llamado la atención de diversos estudiosos de diferentes campos de estudio, es una forma de recopilar y sintetizar investigaciones previas (Hernández et al., 2001). Este enfoque de revisión caracteriza los estudios para abordar problemas particulares e identificar tendencias en los esfuerzos de investigación.

Una revisión de la literatura resulta especialmente útil en términos de la identificación de patrones y direcciones de los esfuerzos de investigación sobre temas emergentes al tiempo que identifica los desafíos y la necesidad de futuras investigaciones. Muchos estudiosos han aplicado con éxito el enfoque para resumir los resultados de la investigación sobre temas similares en función de criterios predefinidos. Una revisión en profundidad, como una revisión de la literatura proporciona evidencia del efecto que puede informar la práctica al sintetizar la colección de estudios que aborden la ciberseguridad en los procesos transaccionales del comercio electrónico. En este estudio se tuvieron en cuenta los estudios publicados entre los años 2018 y 2022.

Fuentes de Datos

Para lograr el objetivo de este estudio, se realizó una búsqueda electrónica, a través de *Google Scholar, Scopus, Dialnet, Redalyc, ScienceDirect, Ebsco Business Source Complete*, entre otras, de artículos relevantes sobre la temática y periodo delimitado. Las bases de datos fueron seleccionadas porque se consideran integrales y cubren muchos campos de estudio y disciplinas. Para la ejecución de la búsqueda se aplicó la siguiente llave de búsqueda:

Español:

TS= ("Ciberseguridad" AND "Comercio electrónico") OR TI= (" Ciberseguridad" AND " Comercio electrónico") OR TI= ("Ciberseguridad " AND " Comercio electrónico"; "redes sociales") OR TS= (" Ciberseguridad " AND " Comercio electrónico"; "plataformas compra online") OR TI= (" Ciberseguridad" AND "Comercio electrónico"; "buenas prácticas").

Inglés:

TS= ("cybersecurity" AND "e-commerce") OR TI= ("cybersecurity" AND " e-commerce ") OR TI= ("cybersecurity" AND " e-commerce"; "social networks") OR TS= ("cybersecurity" AND " e-commerce"; "online shopping platforms") OR TI= ("cybersecurity " AND "e-commerce"; "good practices").

Portugués:

TS= ("ciber-segurança" AND "comércio electrónico") OR TI= ("ciber-segurança" AND "comércio electrónico") OR TI= ("ciber-segurança" AND "comércio electrónico"; "redes sociais") OR TS= ("ciber-segurança" AND "comércio electrónico"; "plataformas de compras em linha") OR TI= ("ciber-segurança" AND "comércio electrónico"; "boas práticas").

En este punto, se utilizó un proceso de dos etapas para seleccionar e identificar estudios relevantes y apropiados. Primero, los autores verificaron los artículos de revistas generados a través de los términos y/o frases de búsqueda en busca de registros duplicados y relevancia. Se identificaron y eliminaron los registros duplicados de los artículos recuperados, extrayendo la información de los artículos resultantes categorizados como relevantes. Después de eso, se verificó la relevancia de los artículos restantes al leer el resumen y el contenido para establecer

que todos los artículos abordan las categorías previamente definidas. En esta etapa, se realizó un análisis para verificar que la discusión de todos los artículos de revistas seleccionados tuviera relación con lo indicado.

Tabla 2

Criterios de inclusión revisión bibliográfica

Criterios de Inclusión	Periodo de estudio: 2018-2022 Idiomas: español, inglés y portugués Tipo de Publicación: especializada Población estudio: artículos y publicaciones especializadas en la temática abordada. Área geográfica: global. Tipo de documentos: artículos derivados de investigación, revisiones sistemáticas y metaanálisis y libros.
Fuentes de Información	IDB Publications; Brekiedata; The Cochrane Library; DIALNET; Scielo; Google Scholar; Google académico; Repositorios de IES con artículos especializados.
Estrategia de Búsqueda	*Español* TS=("Ciberseguridad" AND "Comercio electrónico") OR TI=(" Ciberseguridad" AND " Comercio electrónico") OR TI= ("Ciberseguridad " AND " Comercio electrónico"; "redes sociales") OR TS=(" Ciberseguridad " AND " Comercio electrónico "; "plataformas compra online") OR TI=(" Ciberseguridad" AND " Comercio electrónico"; "buenas prácticas"). *Inglés* TS=("cybersecurity" AND "e-commerce") OR TI=("cybersecurity" AND " e-commerce ") OR TI= ("cybersecurity" AND " e-commerce"; "social networks") OR TS=("cybersecurity" AND " e-commerce"; "online shopping platforms") OR TI=("cybersecurity " AND "e-commerce"; "good practices"). *Portugués* TS=("ciber-segurança" AND "comércio electrónico") OR TI=("ciber-segurança" AND "comércio electrónico") OR TI= ("ciber-segurança" AND "comércio electrónico"; "redes sociais") OR TS=("ciber-segurança" AND "comércio electrónico"; "plataformas de compras em linha") OR TI=("ciber-segurança" AND "comércio electrónico"; "boas práticas").
Selección y Clasificación de Estudios	1. Empírico o teórico 2. Tipo de metodología aplicada: cuantitativa, cualitativa o ambas 3. Tipo de diseño de los estudios: de cohorte, de casos y controles, transversales o cualitativos
Extracción de Datos	Lectura crítica y obtención de información.
Resultados	
Suma de la tasa de publicaciones que se incluyeron en la revisión	Se incluyeron: 25 Se excluyeron: 17

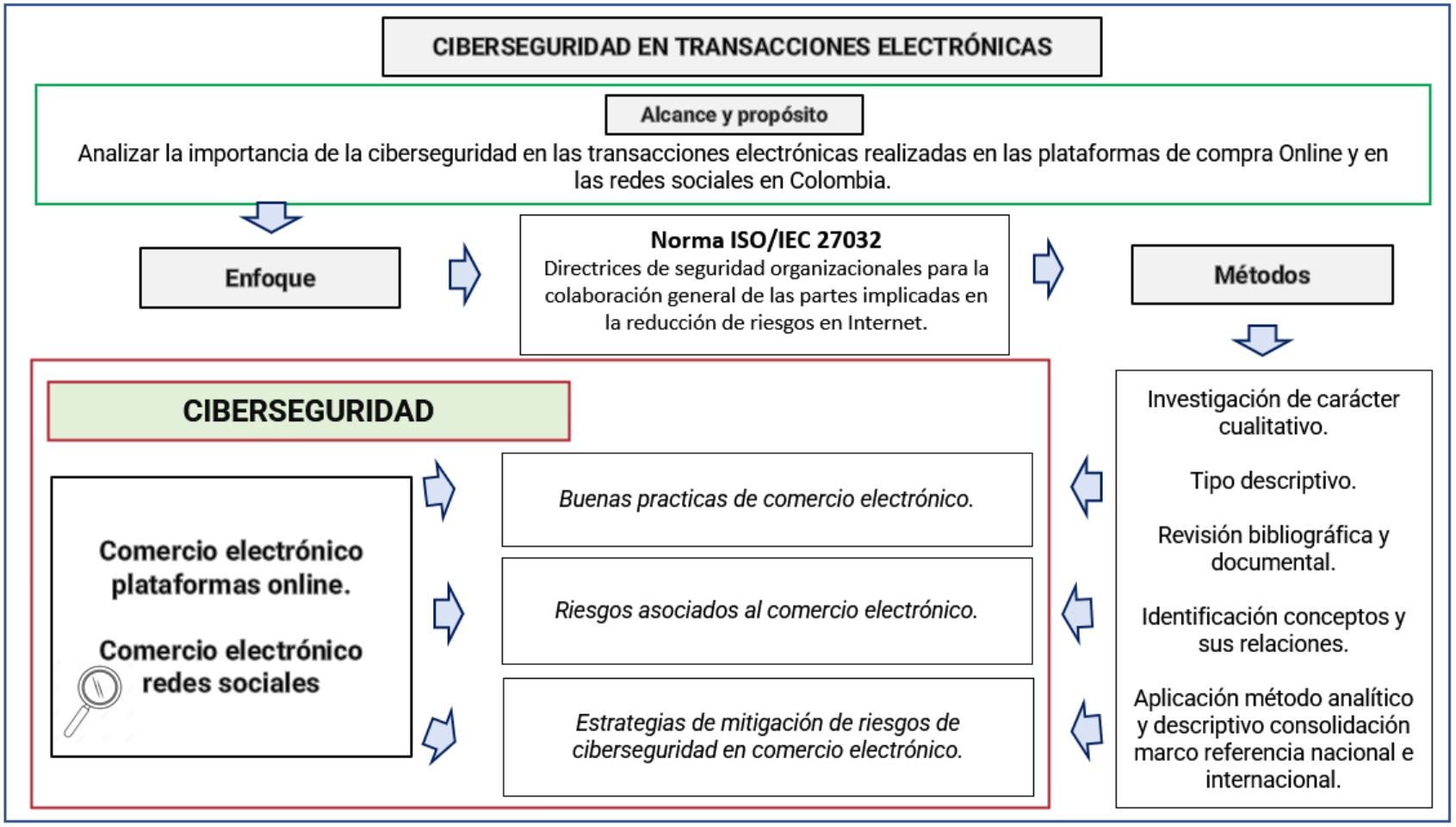
Fuente. Elaboración propia

Análisis y Codificación de Datos

Entretanto, se estudió la producción por año, afiliación y país con el fin de conocer el estado de la generación del conocimiento relacionado con las categorías de estudio y análisis. Por último, las fases y procedimientos (Apéndice B), al igual que otros métodos de análisis en la investigación cualitativa, el análisis de documentos requiere una revisión, examen e interpretación repetidos de los datos para obtener significado y conocimiento empírico del constructo que se está estudiando. En tal sentido, se realizó la búsqueda en los principales repositorios y revistas especializadas en la materia y con publicaciones vigentes en los últimos cinco años. La siguiente ilustración muestra el resumen y la articulación de las categorías conceptuales con las herramientas e instrumentos metodológicos utilizados en la revisión bibliográfica y documental.

Figura 1

Alcance de la Investigación



Fuente. Elaboración propia.

Buenas Prácticas del Comercio Electrónico

El despliegue del marco metodológico enunciado en un apartado anterior permite que en lo que sigue, se presentan los hallazgos obtenidos mediante la valoración de los trabajos y estudios que, para claridad en la exposición, se han agrupado en función de los propósitos específicos de la investigación. En tal sentido, en un primer momento, se extraen las principales referencias obtenidas relacionadas con los lineamientos para las buenas prácticas del comercio electrónico; luego, en un segundo momento, se analizan los hallazgos relacionados con la definición de los peligros y riesgos subyacentes en este tipo de transaccionalidad; para finalmente, en un tercer momento, formular algunas estrategias encaminadas a la mitigación de estos riesgos.

En total, 25 artículos de revistas revisadas por pares se consideraron relevantes para esta revisión bibliométrica (Apéndice A, formato de ficha bibliográfica). Cabe señalar que el enfoque de esta revisión de la literatura es la presentación de datos sobre la ciberseguridad en transacciones de comercio electrónico, lo que pudo influir en la cantidad de artículos recuperados de cada revista. El paso posterior, que se centró en la codificación de los artículos relevantes en este estudio, implicó la extracción y síntesis de datos para analizar los estudios revisados por pares seleccionados. Posteriormente se registró información como el año de publicación, el nombre de los autores, el enfoque del estudio, el contexto del estudio, la industria del análisis, los métodos de recopilación de datos, el tipo de estudio, la herramienta analítica y el continente.

Estos datos juntos formaron la base del análisis del estudio. Los hallazgos de la revisión de la literatura se presentaron utilizando el marco de codificación que agrupa los hallazgos en buenas prácticas del comercio electrónico, peligros y riesgos asociados y estrategias de mitigación.

Un primer grupo de hallazgos de la revisión bibliográfica y documental se agruparon en términos de la delimitación de un compendio de buenas prácticas para el comercio electrónico. Las buenas prácticas comprometen a todos los actores implicados en la cadena de valor del comercio electrónico; pues compete no solo al desarrollador o ingeniero de software que diseña e implementa una tienda virtual; sino también a las instituciones financieras que soportan las pasarelas de pago; a los entes gubernamentales implicados en la regulación y a los usuarios que realizan las compras por estos medios virtuales, entre otros implicados.

Lo anterior es un aspecto que considerar, teniendo en cuenta que la ciberseguridad es un asunto que ha sido asumido por algunos sectores como una responsabilidad exclusiva del usuario. Sin embargo, en este sentido, también debe aclararse que uno de los principales desafíos de ciberseguridad se halla precisamente en el comportamiento del consumidor, quien podría incurrir en malas prácticas de ciberseguridad que podrían poner en riesgo su información confidencial (Roa & Cuellar, 2019).

En los países desarrollados, casi todas las empresas utilizan el comercio electrónico para interactuar con sus clientes. En países como la India, el comercio electrónico ha mostrado un crecimiento vertiginoso tanto en popularidad como en la cantidad de dinero generado por ventas en estas plataformas (Del Águila, 2000). Sin embargo, este vasto mercado virtual en crecimiento también enfrenta algunos desafíos como las graves amenazas cibernéticas, el robo de identidad de los compradores, lo que genera pérdidas y notables daños económicos.

Y es que las instituciones financieras son uno de los blancos de los ataques cibernéticos teniendo en cuenta su papel como recipiendario del pago en los procesos relacionados con el comercio electrónico. El incremento de las amenazas cibernéticas da relevancia a la gestión y administración del riesgo de ciberseguridad, que de este modo se constituye en uno de los

principales desafíos para las entidades financieras quienes han debido adaptarse rápidamente para satisfacer las necesidades de seguridad de sus clientes y así dar cumplimiento a los requerimientos normativos en esta materia.

Las buenas prácticas del comercio electrónico en sitios web, plataformas, redes sociales y/o aplicaciones Internet se han fortalecido como vehículos del comercio electrónico incidiendo en notables cambios en los modelos de intercambio de mercado y los niveles de competitividad en casi todos los sectores, especialmente en la industria. En particular, Internet y la Web como sistemas para la reducción de costos, el incremento de eficiencia de la cadena de valor, la construcción de relaciones con los clientes, el intercambio de información e ideas, el fortalecimiento de marcas y la generación de ingresos (Hartman et al., 2001).

El Rol del Usuario en la Ciberseguridad y la Evasión de la Ciberdelincuencia

Los usuarios son el eslabón más débil de la cadena, pero interactúa con otros que también son determinantes en ciberseguridad del comercio electrónico. En esta cadena, el usuario debe asumir los riesgos implícitos en el uso y reutilización de contraseñas débiles o la apertura de enlaces maliciosos en Internet (Fisch & White, 2000).

La falta de integración de e-business con otros canales y herramientas deriva no solo en dificultades para el mantenimiento de clientes y la construcción de relaciones y vínculos, sino que también constituye una brecha de seguridad. En tal sentido, el fortalecimiento de la ciberseguridad posibilita la reafirmación de las ventajas incuestionables del comercio electrónico; la flexibilidad, capacidad de adaptación, optimización de la cadena de producción y distribución, productividad a bajos costos operacionales y significativo ahorro de tiempo y fluidez en las diferentes transacciones y proceso relacionados (Rogel et al., 2019).

El Rol de las Empresas y las Entidades Financieras

En términos de la interacción con el usuario, tanto las empresas como los bancos digitales deben propender por la creación de un entorno digital altamente seguro que incorpore las tecnologías asociadas a los dispositivos usados por los consumidores. En el mismo sentido, la contención de ciberataques requiere de la implementación de campañas de comunicación y concientización para empleados, consumidores y público en general para contener las actividades maliciosas y las trampas de los atacantes. En la actualidad se utiliza el análisis de comportamiento y la IA (Inteligencia Artificial) como herramientas de ciberseguridad, enfocadas a la identificación de amenazas avanzadas de malware y ransomware (Fisch & White, 2000).

El principal objetivo del e-business es la realización de transacciones entre clientes proveedores y socios en línea, siendo la información que las webs presentan el recurso principal para la compra y venta de los productos y servicios. Al inicio de los negocios es difícil calcular el costo de inversiones para la puesta en marcha del negocio electrónico, y predecir en esta etapa que tipo de tecnología de seguridad es requerida según las particularidades del negocio. Otro error muy común es la programación de transacciones inadecuadas que utilizan protocolos poco seguros y hacen vulnerable la estafa en línea. También existen errores tecnológicos por el uso de tecnología inadecuada u obsoleta que ralentizan y ponen en riesgo el flujo de información de la tienda online.

La Auditoría Como Línea De Defensa de la Ciberseguridad

Las áreas de la auditoría son catalogadas como la tercera línea de defensa y han permitido la transformación de los procesos y adecuar las capacidades para garantizar un control interno efectivo en materia de ciberseguridad. Si bien se han llevado a cabo esfuerzos significativos por construir políticas internas frente al riesgo cibernético jalonadas por las disposiciones de la CE

N°007 de la SFC (Superintendencia Financiera de Colombia), resulta necesario alinear los programas de aseguramiento con los marcos internacionales para garantizar la resiliencia de las organizaciones ante un ciberataque. En este sentido, es necesario resaltar la importancia de los estándares internacionales de ciberseguridad del NIST, COBIT 5 e ISO, y las pruebas propuestas en esta guía para garantizar una adecuada administración del riesgo cibernético.

Lo anterior, posibilita la instauración de controles de identificación de incidentes de ciberseguridad, y la subsecuente, reacción efectiva y resiliente como respuesta a los ciberataques. Por ello, la auditoría interna se convierte en un factor importante en términos de la revisión y evaluación independiente sobre la eficacia de las líneas de defensa y el seguimiento y comprensión holística del perfil de riesgo organizacional, teniendo en cuenta las nuevas tecnologías y los riesgos emergentes que derivan en la sofisticación de los ataques cibernéticos. Este propósito, según ASOBANCARIA (2020) requiere de la coordinación efectiva de todas las áreas de la entidad, desde la alta gerencia hasta los clientes, estos últimos asumidos como el eslabón más débil de la cadena de la ciberseguridad.

Para la Consolidación de un Compendio de Buenas Prácticas Para el Comercio Electrónico

La revisión de la literatura permitió delimitar las siguientes dimensiones en términos de la definición de un compendio de buenas prácticas de comercio electrónico, a saber: evaluación y mantenimiento con enfoque en el cliente; maximización de la seguridad; mejoramiento de la experiencia del cliente; equilibro de la interacción humana y en línea; comunicación efectiva; mantenimiento del sitio web; configuración del correo electrónico y de las aplicaciones conexas; actualización de precios; pasarela de pago segura; ajuste a tendencias de pago y ROI; inversión en servicio al cliente; y uso de herramientas de integración.

El asunto del comercio electrónico requiere de la evaluación constante y el mantenimiento de la cadena de valor enfocado en el cliente, es decir, centrado en el mejoramiento de la experiencia del cliente; lo que implica que las empresas dedicadas a la compra y venta de bienes y servicios en línea deban establecer relaciones de valor y confianza con una infraestructura robusta, que no solo permita comprender y satisfacer las necesidades en términos de la concreción de la venta, sino también resguardar la información y blindar los procesos relacionados con el pago. Las relaciones seguras desde la virtualidad requieren que las empresas de comercio electrónico muestren a sus clientes que efectivamente representan sus intereses y que la posición de este es defendida y resguardada con la infraestructura que se oferta para la realización de los negocios.

Las empresas de comercio electrónico requieren de la co innovación, lo que implica la utilización de software seguro que trascienda la mera transaccionalidad en las ventas y servicios y que permita la utilización de la información recopilada de manera inteligente. Las estrategias de personalización resultan fundamentales en el mejoramiento de los procesos transaccionales del comercio electrónico.

Otro asunto que resulta fundamental es el principio de equilibrio en la interacción humana y en línea. Nada se puede presuponer en la experiencia de pago del cliente; en tal sentido, conviene encaminar esfuerzos en la construcción de una sinergia entre los canales de venta en línea y los demás recursos disponibles, presentando una cara unificada a los clientes.

Otro aspecto de las buenas prácticas de comercio electrónico es la propensión por la comunicación efectiva, considerando que el comercio electrónico es inmediato y directo y resulta menester que cada contacto se convierta en una oportunidad de enriquecimiento de los datos y los procesos de la empresa. Las cookies han sido utilizadas habitualmente como sistemas de

seguimiento en la construcción de los perfiles de cliente, sin embargo, deben tratarse como una variable relacionada con la seguridad transaccional en el comercio electrónico.

La seguridad también debe incorporarse como pilar en procesos que impliquen la oferta de incentivos, concursos, premios y registros de visitantes, que, si bien pueden ser efectivos en términos de persuasión y llegada a nuevos públicos, también puede constituir una brecha de seguridad si no se asume integralmente.

Todos los datos recibidos deben integrarse en un sistema centralizado para ayudar a identificar las necesidades y los comportamientos de los clientes. Pero en términos de la seguridad y las exigencias normativas, es necesario que el cliente conozca cómo se utilizará sus datos y los mecanismos provistos por la empresa para su resguardo.

El mantenimiento del sitio web es una práctica rutinaria y determinante en la seguridad transaccional. Debe considerarse en este punto que el uso inteligente del sitio web incide directamente en el rendimiento; por ello, con el mantenimiento se asume el comercio electrónico como una integración compleja de procesos que implican dinero para los clientes y para la empresa. Los estudios indican que los clientes prefieren transacciones fáciles donde no se presenten fallas de orden tecnológico que puedan generar impresiones de riesgos en la seguridad transaccional.

De nuevo en este punto, la comunicación efectiva cobra relevancia, esta vez desde la dimensión de la información que proporcionan los mecanismos de comunicación y retroalimentación con el cliente que pueden servir para monitorear en tiempo real, la información de fallas que los clientes reportan cuando estas se presentan en su interacción comercial electrónica.

Como parte de la estrategia de comunicación se debe incluir la claridad y actualización constante de los precios, las tendencias de pago y el ROI (Retorno de Inversión). Dentro de las herramientas que sirven para este propósito se encuentra CRM que se ha incorporado como una utilidad para la alineación de procesos en distintos frentes o dimensiones; oficiando como estrategia comercial centralizada en el cliente mediante la oferta de servicios personalizados y seguros combinando las potencialidades del correo electrónico, el mercadeo y la gestión de bases de datos.

En la siguiente tabla se muestra un compendio de las buenas prácticas de comercio electrónico definidas por la literatura especializada sobre el tema, según lo evidenciado en la muestra documental admitida en este estudio. Se han agrupado las buenas prácticas en tres dimensiones: ciberseguridad y evasión de la ciberdelincuencia, correo electrónico y cumplimiento de la normatividad conexa. Estas dimensiones están relacionadas con los factores que aseguran la ejecución de la buena práctica.

Tabla 3

Compendio de Buenas prácticas del comercio electrónico

Dimensión	**Factores asegurados**	**Buena práctica**
Ciberseguridad y evasión de la ciberdelincuencia	Controles Código malicioso.	Implementación efectiva de controles para la detección, retiro y evasión de códigos maliciosos.
	Controles Criptográficos.	Creación e implementación de una política para la aplicación de controles criptográficos.
	Gestión de llaves.	Documentación de políticas y procedimientos de gestión de llaves criptográficas.
	Seguridad Operativa	Definición de prácticas aplicables a la seguridad física y lógica.
	Código reutilizable, limpio y modular	Nombres de clases, identificadores y variables consistentes.
	Protección código malicioso.	Definir una política que dé cumplimiento a las licencias de software y que prohíba la instalación de software malicioso no autorizado.
	Gestión de actualizaciones de seguridad.	Prácticas de seguridad aplicables al portal web de comercio electrónico.

	Código fuente cerrado	Permite controlar el entorno de desarrollo; mantener un registro de quién ha trabajado en qué y con un alcance más pequeño; evitar que los problemas se escapen por las grietas; evaluar la calidad de los desarrolladores y del producto.
	Experiencia de usuario - Versiones móviles.	La seguridad de la información de las empresas se relaciona con las pérdidas financieras derivadas de la vulneración de datos y la afectación reputacional y de confianza del cliente.
	Uso de HTTPS	HTTPS proporciona una capa de cifrado para estos datos. Con HTTPS, puedes evitar la mayoría de los ataques de intermediarios.
	autenticación multifactor para una mayor protección de datos	Protección de las compras de los clientes y evasión de la pérdida de datos.
	Lenguajes de programación y frameworks	Uso de frameworks (esqueletos) que te permitan hacer una aplicación escalable y que al igual que el lenguaje, sea compatible con la mayoría de los navegadores y dispositivos,
	Cifrado de dispositivos	Políticas y procedimientos para la realización de backup y pruebas de restauración.
	Copias Seguridad de la Información	Prevención y atención de contingencias con posibilidad de ejecución de backup de software y bases de datos.
	Gestión de Contingencias.	Mitigar el riesgo de no poder continuar con las operaciones por períodos que se prolongan más allá de lo soportado por los procesos de negocio.
Gestión del comercio electrónico	Seguridad de portal web	Solución de correo electrónico para la configuración adecuada de los parámetros de seguridad en el uso del correo electrónico. Se deben elegir soluciones de correo electrónico en la nube y no soluciones Onpremise, de este modo se evita el uso de un servidor local con aplicaciones locales.
	Configuración de seguridad de correo electrónico.	Optimización de contraseñas.
	Gestión de contraseñas	Método de autenticación de correo electrónico diseñado para detectar la falsificación de la dirección del remitente (encabezado de ruta de retorno) durante la entrega de un correo electrónico.
	Garantizar la creación de contraseñas seguras	Una contraseña segura incluye al menos ocho caracteres, que contienen una combinación de números en mayúsculas y minúsculas, letras y caracteres especiales.
	Sender Policy Framework (SPF)	Método de autenticación de correo electrónico diseñado para detectar direcciones de remitente falsificadas en correos electrónicos.
	DomainKeys Identified Mail (DKIM)	Protocolo de autenticación de correo electrónico creado para otorgar a los propietarios de correo electrónico la capacidad de proteger su dominio del uso no autorizado, por ejemplo, suplantación de correo electrónico.
	Plan de pruebas.	Controlar datos con una bóveda de recuperación segura y habilitar soluciones de seguridad de datos para combatir el ransomware y los ciberataques.
	Permisos, licencias y condiciones de uso.	Se debe verificar que sea explícita la solicitud de permisos al usuario para acceder a contactos, realizar pagos, ceder datos; asimismo, valorar los términos y condiciones de uso.

	Protección de datos.	Política de protección de los datos personales de sus clientes que sea acorde con las normas internacionales, las disposiciones constitucionales y los desarrollos jurisprudenciales sobre la materia.
	Revisiones de rutina de integraciones de terceros.	Eliminación de obsolescencias y garantizar la minimización de cantidad de partes externas con acceso a datos.
	Implementar un sistema de conmutación por error	Tomar medidas contra las interrupciones imprevistas, especialmente durante las temporadas de mayor volumen, es tan vital como evitar las violaciones de datos, y una forma confiable de hacerlo es a través de sistemas de conmutación por error.
	Autenticación, notificación y conformidad de mensajes basados en dominio (DMARC).	Método de autenticación de correo estándar. Con DMARC, los administradores de correo pueden evitar que los hackers y otros atacantes suplanten la identidad de su organización o falsifiquen su dominio.
	Controles adicionales de seguridad de correo electrónico	Cifrado de correo electrónico, Puerta de enlace de correo electrónico segura, Anti-spam.
Cumplimiento de la normatividad	Gestión documental.	Ley General de Archivos – Criterios de Seguridad.
	Seguridad en las comunicaciones.	Actividades centradas en mecanismos defensivos y ofensivos empleados tanto para proteger el ciberespacio contra el uso indebido como la infraestructura.
	Sistema de pagos.	Habilitar una solución de seguridad de datos para combatir el ransomware y los ciberataques.
	Plataforma segura de procesamiento de pagos.	Protegen tu información financiera para cada transacción, asegurando que no se roben tarjetas de crédito ni se intercepten transacciones.
	Verificación de condiciones de seguridad.	Proporcionar la autentificación necesaria; garantizar la confidencialidad de la información sensible; preservar la integridad de la información; definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.
	Seguridad de plataformas.	Articulación de normativas de ciberseguridad que permiten que las transacciones electrónicas sean seguras.
	Verificación de condiciones de almacenamiento.	Establecer unos requisitos de seguridad para una experiencia digital segura.
	Para la protección de datos personales.	Garantizar los derechos y libertades fundamentales de los clientes de comercio electrónico.
	Integración con otros sistemas.	Una visión de 360 grados para el análisis de conjuntos de datos y brechas de seguridad.
	Certificación de buenas prácticas.	Cumplimiento de normativas técnicas relacionadas.
	Capacitación y sensibilización de los usuarios.	Mitigar el error humano.

Fuente. Elaboración propia.

Peligros y Riesgos Subyacentes en el Comercio Electrónico

Las anteriores reflexiones permiten que, en lo que sigue, se centre la atención en la identificación de los peligros y riesgos que subyacen en las operaciones de comercio electrónico. Según lo verificado en la revisión bibliográfica y documental es posible diferenciar y relacionar la comisión de fraudes financieros con la realización de ciertas prácticas que afectan procesos del comercio electrónico.

Los riesgos cibernéticos se definen como "riesgos operativos para los activos de información y tecnología que tienen consecuencias que afectan la confidencialidad, disponibilidad y/o integridad de la información o los sistemas de información" (Smith, 2004, p. 44). Los ciberdelincuentes están cosechando grandes ganancias al robar información crítica de las plataformas de comercio electrónico. La complejidad y la prevalencia de los ciberataques han aumentado. La seguridad del comercio electrónico es esencial, considerando que protege a las empresas y los compradores contra estas amenazas (Delgado, 2016). Los eventos de riesgo cibernético incluyen fundamentalmente procedimientos encaminado a la violación de datos y a la ejecución de ataques cibernéticos. La exposición creciente y el impacto potencial del riesgo cibernético se han destacado en informes recientes de la industria (Allianz, 2022).

Los ataques cibernéticos a infraestructuras críticas ocupan el quinto lugar según el reporte del Informe de riesgo global del Foro Económico Mundial. Según el informe, el ransomware, el malware y la denegación de servicio distribuida (DDoS) constituyen modalidades actuales de ciberataque. Colonial Pipeline es un referente en este tipo de ataques, considerando las afectaciones que produjo por el cierre del sistema de tuberías de 5500 millas destinado al suministro de 2,5 millones de barriles de combustible por día. De este modo, mediante este ransonware se bloqueó la infraestructura crítica de combustible líquido desde las refinerías de

petróleo hasta los estados a lo largo de la costa este de EE. UU. (Organización de los Estados Americanos, 2017).

Debe recordarse que los principios de seguridad de la información incluyen la integridad, es decir, que esta no se altere en ningún proceso de principio a fin; la confidencialidad que alude al hecho de que la información solo sea conocida por los autorizados en el acceso; la disponibilidad; la autenticidad, verificando con el uso de usuario y contraseña para identificación y de esta manera no se puede negar la responsabilidad en el manejo de la información y; la trazabilidad para la evidencia o el registro del traspaso de información de un usuario a otro.

Los incidentes cibernéticos que han sucedido en la historia de los EE. UU. Ha posibilitado el fortalecimiento de la ciberseguridad. Se destaca la creación de un organismo público encaminado al análisis de las causas de los principales incidentes cibernéticos sucedió y partir de este, formular recomendaciones para que estos no se repitan, otro referente de ransomware se halla en Not Petya en el año 2017, con afectaciones que ascendieron a USD 10 mil millones, por explotación de una vulnerabilidad en el sistema de Windows, que propició su propagación independiente También en el año 2017, se desplegó el ransomware WannaCry que con un ataque en Windows, secuestro los datos de los usuarios que para recuperarlos debían pagar un precio en la criptomoneda Bitcoin (Organización de los Estados Americanos, 2017).

Durante la pandemia de COVID-19, los ataques de ransomware aumentaron significativamente, ya que los arreglos para trabajar desde casa aumentaron la vulnerabilidad. Entre las víctimas se encontró el Servicio Nacional de Salud de Gran Bretaña que fue atacado para redirigir a las ambulancias a otros hospitales debido a fallas en los sistemas de tecnología de la información (TI), lo que dejó esperando a las personas que necesitaban asistencia urgente. Se

estima que 19.000 citas de tratamiento canceladas fueron el resultado de pérdidas de GBP 92 millones (Organización de los Estados Americanos, 2017).

Las redes sociales como plataformas ofrecen una notable cantidad de ventajas, especialmente la posibilidad de conectarse con otras personas y de establecer negocios ofreciendo productos y servicios, sin embargo, también encarnan un compendio importante de riesgos. Es así como 'Facebook', 'Twitter', 'Google' se han convertido en herramientas fundamentales para el despliegue del comercio electrónico. Estos sitios resultan especialmente vulnerables a los ataques de phishing, incluso con la creación de portales falsos que parezca idéntico a una página de Facebook. Esto le permite al ciber atacante atraer a los usuarios para que ingresen información confidencial como sus credenciales.

Los métodos utilizados en esta modalidad incluyen: el envío de mensajes falsos que indican que su cuenta de Facebook está a punto de ser deshabilitada en unos días; engaño al usuario para que haga clic en un enlace del mensaje personal enviado por su amigo que indica que alguien ha subido fotos personales del usuario en el enlace dado; envío de un mensaje que afirma que la cuenta del usuario debe actualizarse para seguir usándola o envío de un enlace para descargar esa actualización que contiene una dirección que aloja un sitio malicioso.

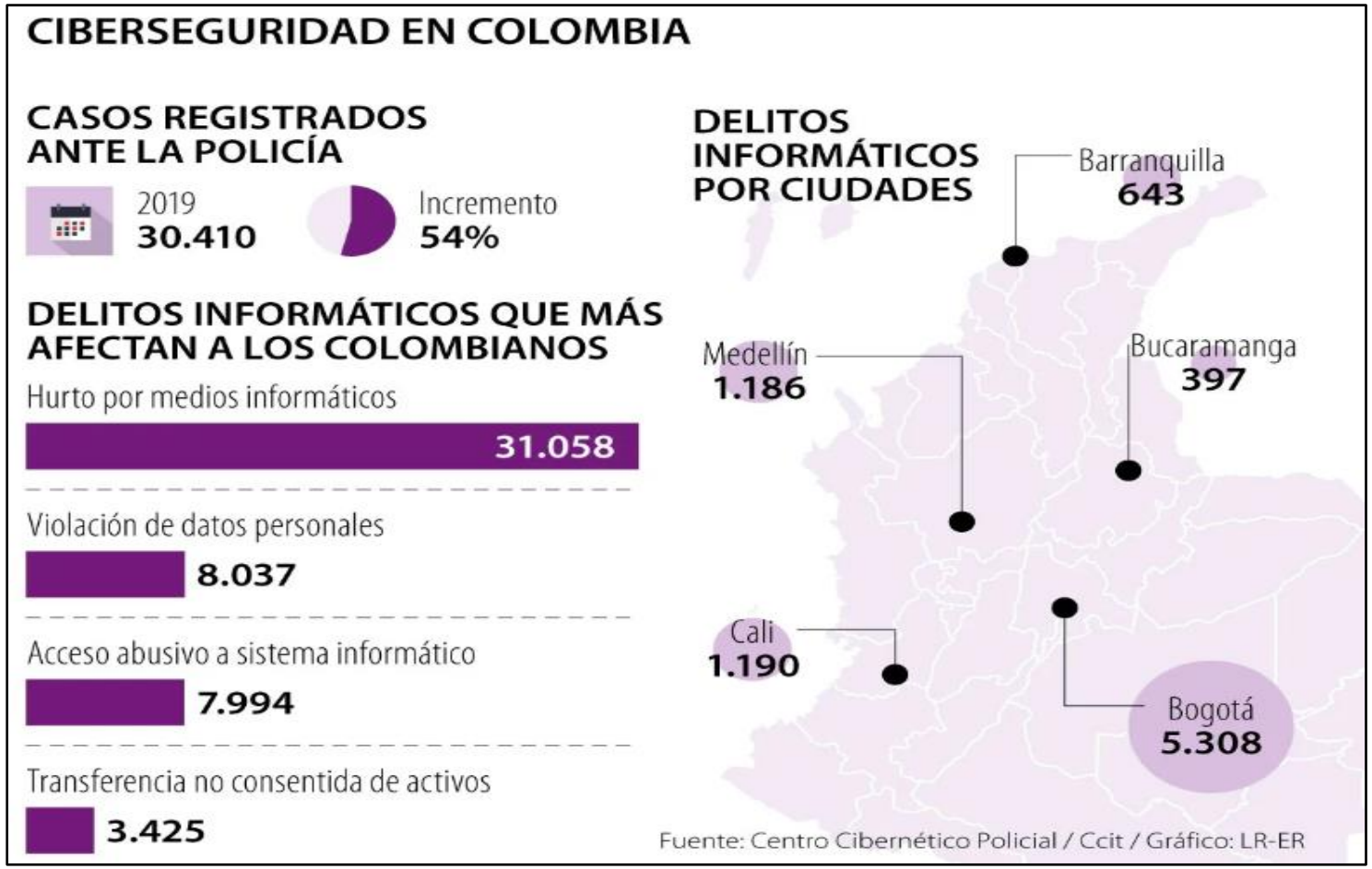
Las redes sociales dedicadas a la gestión de contenidos multimedia y que permiten compartir imágenes, vídeos, videos en vivo y otros medios en línea; tales como: 'YouTube', 'Flickr', 'Instagram', 'Snapchat', entre otras, han implementado la funcionalidad de bandeja de entrada en sus aplicaciones, lo que las convierte en un medio para los objetivos de los ciberatacantes que ven en esta funcionalidad una oportunidad de phishing. De este modo, puede enviar una URL abreviada en el mensaje y redirigir al usuario a sitios maliciosos (Martínez & Ávila, 2021). Los atacantes suelen aprovecharse del contenido malicioso de URL acortadas.

Los siguientes apartados se dedican a la revisión de estas prácticas y a la presentación de las conclusiones de los estudios que sobre la materia se han publicado recientemente. Se han delimitado el Phishing, el Spamming, Dos y DDos attacks, Malware, Bots, la explotación de vulnerabilidades conocidas y los ataques de fuerza bruta como las principales modalidades de la ciberdelincuencia para el aprovechamiento de los riesgos y brechas de ciberseguridad que operan en detrimento de los procesos de comercio electrónico en puntos de venta electrónicos y en redes sociales.

Según los reportes de la Policía Nacional de Colombia, dentro de los principales ciber delitos que se materializan en Colombia se encuentran: la suplantación de identidad, el fraude cibernético, la denegación de servicio, la fuga de información, el phishing, la divulgación indebida de contenidos, la pornografía infantil, el uso de spyware, la violación de los derechos de autor y la piratería en Internet (Policía Nacional de Colombia, 2020).

Figura 2

Ciberseguridad en Colombia



Fuente. Elaboración propia.

Phishing

Según el Reporte de PANDA sobre Ciberseguridad y Ciberdelincuencia (2015), la técnica del phishing data del año 1996, como un vocablo anglosajón que alude al verbo pescar o *"fishing*" teniendo en cuenta que el método consiste en la "pesca" de usuarios en la red. De este modo, el phishers o lo que es lo mismo, el cibercriminal que practica el phishing procede ilícitamente con acciones que van desde el robo de información financiera, la obtención de beneficios económicos por extorsión, hasta la ejecución de algún daño informático. Su método principal se sustenta en el engaño de del usuario víctima mediante el envío de correos electrónicos con links y páginas web falsas, con el fin de suplantar una página principal, entre ellas, las de los bancos y de este modo solicitar actualización de los datos para la ejecución de robos en línea y acceder a información confidencial (PANDA Security, 2015).

Sobre el Phishing Alabdan (2020), en estudio sobre tipos, vectores y enfoques técnicos considera que este constituye uno de los principales vectores de infección del malware; asimismo, corresponde al principal método de infiltración utilizado en las brechas y el número uno en los ataques de ingeniería social. Conforme al avance tecnológico, y el subsecuente número de vectores implicados, se ha evidenciado un incremento notable de los sitios de Phishing desde el año 2016 y especialmente en el año 2019 con ataques de phishing más sofisticados y vanguardistas. Por ejemplo, el desarrollo del QRishing o la aplicación del squatting de sonido en asistentes de voz como Alexa de Amazon (Alabdan, 2020).

En los últimos años, el principal objetivo de los phishers ha sido el SaaS (Software as a Service) y el correo web, que representaron el 33% de los ataques contra diversos sectores industriales. IBM identificó que el 27% de los ataques de phishing en 2018 se centraron en servicios de correo web. También se observó que el 29 por ciento de los ataques contra empresas

que fueron analizados por X-Force identificaron la fuente de la brecha como un correo electrónico de phishing (Alabdan, 2020).

En cuanto a los aspectos financieros del phishing, Symantec descubrió que en la economía sumergida los servicios de páginas de phishing personalizadas se venden por entre 3 y 12 USD. También se ha descubierto que las tarjetas regalo es una de las formas más comunes que tienen los estafadores de cobrar sus ganancias. El FBI estimó la pérdida de víctimas en 2018 debido al phishing fue de 48.241.748 USD, con 26.379 personas afectadas por este tipo de estafa (Alabdan, 2020).

Spamming

Según el estudio realizado por Krishnamurthy & Santhadevi (2019), el 28% de los usuarios con una cuenta de correo electrónico personal afirma recibir más spam que hace un año, por otra parte, el 22% de los usuarios de correo electrónico afirman que el spam ha reducido su uso general del correo electrónico. Asimismo, el 21% de los usuarios con una cuenta de correo electrónico laboral afirma recibir más spam que hace un año, mientras que el 16% afirma recibir menos. El 67% de los usuarios de correo electrónico dicen que el spam ha hecho que estar en línea sea desagradable o molesto y el 53% de los usuarios de correo electrónico afirman que el spam les ha hecho confiar menos en el correo electrónico (Krishnamurthy & Santhadevi, 2019).

Los spammers utilizan generalmente la técnica de confusión en las líneas del asunto con el fin de evadir los filtros de spam. Para provocar tal confusión suelen incluirse caracteres especiales, espacios en blanco o errores ortográficos para eludir filtros de spam configurados por el dominio u ordenador del destinatario. La técnica de filtrado por palabras clave acuse a la utilización de palabras predefinidas de un mensaje para su identificación y etiquetado. Esta

técnica se conoce como ofuscación, por la confusión resultante de la imposibilidad de comprender (Krishnamurthy & Santhadevi, 2019).

Un estudio sobre spam y phishing sobre malos vecinos del internet concluyó que la mayoría de los ataques se concentraban en India, Brasil, África Occidental y Vietnam. El 62% de todas las direcciones de Spectranet, un PSI de Nigeria, enviaban spam alojando botnets, es decir, redes de ordenadores comprometidos. Estos han proliferado y posibilitado el envío rápido de grandes volúmenes de spam coordinado, amplificando el riesgo de ciberdelincuencia (Krishnamurthy & Santhadevi, 2019).

La empresa de seguridad en Internet CYREN informó que se podían distribuir entre 40 y 50 millones de correos electrónicos distribuidos en menos de cinco minutos. Con costes mínimos y utilizando un ordenador normal y con configuraciones básicas. De este modo, un spammer puede enviar decenas de miles de mensajes en segundos. Una vez establecidas las configuraciones, se pueden enviar mayores volúmenes de spam casi sin coste alguno, exceptuando para los ISP y los destinatarios (Krishnamurthy & Santhadevi, 2019).

La internet posee una estructura descentralizada, lo que posibilita la rapidez en los procesos de comunicación de alcance mundial; asimismo, proporciona anonimato que se relaciona estrechamente con la posibilidad de comisión de actividades ilícitas. En tal sentido, la ciberdelincuencia ha evolucionado paralelamente con la difusión de Internet y el comercio electrónico. El mecanismo tradicional de operación consiste en el envío de un correo electrónico con contenido malicioso encaminado a incitar que el destinatario active un enlace URL que vincula a un sitio web malicioso o deriva en la descarga de un archivo malicioso (Alazab & Broadhurst, 2017)**.**

El correo electrónico no solicitado, o spam es una forma básica utilizada por la ciberdelincuencia. Es un producto de una de las primeras asociaciones entre los autores de malware y los de correo electrónico no solicitado, o spam. El correo electrónico ha sido uno de los principales vectores de difusión de programas maliciosos. Esto sirve para diferenciar a la ciberdelincuencia dirigida a víctimas de bajo volumen y alto valor, como los bancos con alta capacidad de pirateo, y a la ciberdelincuencia que utiliza el spam para llegar a víctimas de notable volumen y escaso valor, con menos probabilidad de ser contenido por medio de antivirus o contramedidas (Alazab & Broadhurst, 2017)**.**

El correo electrónico engañoso y de ingeniería social es una técnica que ha sido ampliamente documentada por los estudios relacionados con el tema. Sin embargo, se requieren más estudios sobre nuevos métodos avanzados como el spear phishing, o aquellos que relacionan diferentes formas de ingeniería social con otros tipos de malware y de ciberdelincuencia. En esta modalidad se incluyen métodos de camuflaje de archivos ejecutables maliciosos que se hacen pasar como inofensivos, incluso de Microsoft Word, en formato PDF u otros documentos de texto; la manipulación del método de codificación la aplicación de dobles extensiones falsas en formato comprimido para la imitación de servicios de acortamiento de URL para difundir archivos maliciosos (Alazab & Broadhurst, 2017)

Dos & Ddos Attacks

Son ataques de denegación de servicio (DoS); un tipo de ciberataque dirigido a una aplicación o sitio web específico y encaminado al agotamiento de los recursos del sistema objetivo y volviendo inaccesible al equipo de la víctima por inoperatividad y negación de los servicios a los usuarios legítimos del acceso. Hay muchas formas de ataques DoS, los tipos más comunes incluyen: la sobrecarga de recursos de red para el consumo de la capacidad del

hardware; uso de software o ancho de banda de red disponible del objetivo; ataque directo para sobrecarga de recursos de red mediante tácticas de explotación de vulnerabilidades del servidor inundando los servidores con peticiones.

En un ataque de amplificación por reflexión, el atacante consume recursos de la red reflejando un alto volumen de peticiones o de tráfico de red hacia el objetivo. El actor utiliza un servidor de terceros, conocido como reflector que oficia como intermediario que aloja y responde a la dirección IP de origen falsificada dada. La sobrecarga de recursos del protocolo consume los recursos de sesión o conexión disponibles del objetivo.

Así las cosas, según lo identificado en la revisión bibliográfica, que un ataque DoS se categoriza por la denegación de servicio distribuido (DDoS) cuando el tráfico de sobrecarga se origina desde más de una máquina atacante operando en red (DDoS) de forma concertada. Los atacantes DDoS suelen utilizar una botnet, es decir, un conglomerado de dispositivos secuestrados y conectados a Internet para la comisión de ataques a gran escala que, desde la perspectiva de la entidad objetivo, parecen proceder de muchos atacantes diferentes (MS-ISAC, 2022).

Las tácticas de ciberataque conocidas utilizan vectores de ataque DDoS para saturar las herramientas de seguridad de las aplicaciones; es decir bloquea los cortafuegos, el sistema de Intrusion Prevention System y de este modo provocar que pare su funcionamiento. Así las cosas, las actividades fraudulentas pueden desarrollarse. Como consecuencia, se presentan un mayor número de ataques, largos periodos de inactividad y un servicio degradado, incluso derivando en la pérdida de ingresos económicos (Radware, 2010).

Conviene considerar que la superficie de ataque que puede ser explotada por los piratas informáticos ha aumentado paralelamente a la expansión de la huella digital de los bancos.

Existen herramientas como Banking Dataset que opera como una base de datos de los intentos de denegación de servicio distribuido (DDOS) contra instituciones financieras y otras organizaciones. Esta herramienta implica la incorporación de algoritmos de aprendizaje automático encaminados a la detección de asaltos a la industria financiera como SVM, KNN y RF, entre otros (Islam et al., 2022).

Estos modelos han obtenido índices de precisión del 99,5%, 97,5% y 98,74 respectivamente, para la detección de ataques DDOS. Los resultados comparativos indican que SVM es más robusto que KNN, RF y los enfoques de aprendizaje automático (ML/DL) existentes. Este modelo se limita a conjuntos de datos fuera de línea, pero también permite trabajar con conjuntos de datos en tiempo real con los modelos de aprendizaje supervisado (Islam et al., 2022).

Malware

El Malware o software malicioso se define como una pieza de software insertada en un sistema de información con miras a subvertir el uso del sistema o de otros sistemas. De este modo, el malware propende por la manipulación de datos; la interferencia del funcionamiento de los sistemas de información las redes de datos; la eliminación o supresión de información o bloqueo al acceso y el redireccionamiento de los recursos informáticos a fines delictivos. Según Aaron (2021), diariamente se registran usos de malware y de aplicaciones potencialmente no deseadas. Esta tipología de fraude ha aumentado exponencialmente desde el año 2013 (Chapin et al., 2021).

Durante el año 2021, según el reporte de la empresa Malware bytes, se detectó un 77% más de software malicioso que en el año 2020; especialmente relacionadas con el minado de criptomonedas. Adicionalmente, se registraron operaciones de adware, spyware y gusanos con

un aumento del 200% frente al año anterior. Las detecciones en ordenadores domésticos Windows aumentaron un 65%; mientras que las detecciones de amenazas en ordenadores empresariales con Windows en un 143%.

El trabajo remoto derivado de la pandemia genero un cambio en los objetivos potenciales de este tipo de fraude, por lo que los ciberdelincuentes se vieron obligados a la exploración de métodos alternativos de ataque a las cadenas de suministro; registros de deuda técnica; parches glaciales; ecosistemas de aplicaciones entre otros métodos para acechar a las víctimas. Según el Informe IBM (2020) sobre resiliencia organizacional indicó que, desde la perspectiva de los administradores, se ha alcanzado un punto de inflexión en el que el aumento de la complejidad de la pila de seguridad está oficiando en detrimento de la seguridad. En consecuencia, resulta necesario proporcionar la formación y los recursos necesarios para garantizar que las herramientas de seguridad se utilicen bien y se encuentren integradas (MalwareBytes cyber protection, 2022).

Exploitation of Known Vulnerabilities

Alude al uso de software y de técnicas especiales para el aprovechamiento de las vulnerabilidades encontradas y usarlas como puerta de entrada al sistema de la víctima. Este ataque se ejecuta por medio de herramientas conocidas como exploits, entre otros métodos. El 49% de las entidades bancarias aún no han implementado herramientas de seguridad en sus procesos a través de tecnologías digitales emergentes como el Big Data (BD), Machine Learning (ML) o Inteligencia Artificial (IA), que han resultado muy útiles en la prevención de ciberataques; la determinación de patrones sospechosos asociados a la comisión de fraudes; la detección de posibles vulnerabilidades relacionadas con el lavado de dinero y el financiamiento del terrorismo. En tal sentido, la literatura especializada coincide en recomendar los trabajos de

investigación para aumentar la comprensión y conocimiento sobre el tema y de este modo, garantizar que la innovación financiera se desarrolle en consideración de las vulnerabilidades relacionadas con los delitos de lavado de dinero y financiamiento del terrorismo.

Este tipo de ataques surge de las brechas de seguridad y vulnerabilidades que los ciberdelincuentes han detectado en las infraestructuras tecnológicas de las entidades financieras que tradicionalmente han actuado reactivamente ante la problemática desplegando esfuerzos preventivos pero escasos. Según la OEA (2018), El 85% de las entidades bancarias de la región han implementado tanto Sistemas de Detección / Prevención de intrusiones (IDS e IPS), como Procesos de Monitoreo de Amenazas y Vulnerabilidades; mientras que el 66% ha implementado sistemas de gestión de identidades y accesos (OEA, 2018).

Según la OEA, los procesos más comunes implementados por los bancos están enfocados en un 85% al monitoreo de amenazas y detección de vulnerabilidades y en un 70% en los procesos de gestión de cuentas privilegiadas. Según ACCENTURE (2017), en términos globales, tan solo el 40% de los Bancos tiene sistemas y procesos diseñados adecuadamente de acuerdo con los requisitos de la resiliencia cibernética (OEA, 2018).

Bots

Una red de bots implica la yuxtaposición de un número significativo de dispositivos infectados que en consecuencia son controlados. Cuanto mayor sea el número de bots conectados, mayor impacto tendrá su despliegue que generalmente se encuentra encaminado a la obtención de un beneficio económico, la propagación de malware o generar la interrupción de servicios de Internet.

Las redes de bots no buscan comprometer a un solo equipo, sino que son diseñadas para infectar a millones de dispositivos. Los ‘pastores de bots’ seleccionan equipos para su uso y los

infectan mediante virus tipo Troyano. De este modo, el usuario infecta su propio sistema tras abrir un archivo adjunto a un correo, hacer clic en un anuncio malicioso, o descargar software peligroso de un sitio web. Esta infección posibilita que la red de bots acceda, borre o modifique información personal, que a su vez permitirá atacar a otros equipos o cometer otros delitos.

Las redes de bots complejas tienen capacidad de auto propagación lo que permite la infección de otros dispositivos de manera automática. Estos bots autónomos están diseñados para la búsqueda, infección y exploración de la internet constantemente en busca de dispositivos vulnerables conectados a Internet, a los que les falte alguna actualización del sistema operativo o no dispongan de software antivirus.

Las redes de bots son complejas debido a la dificultad para su detección. Estos solo utilizan una mínima parte de la capacidad de procesamiento de los equipos infectados, de este modo, se evita la interrupción del funcionamiento normal del equipo para que el usuario no sea alertado. Las redes de bots más complejas son diseñadas con la posibilidad de adaptar su comportamiento y evadir las barreras de los programas de seguridad informática. El diseño de las redes de bots ha evolucionado notablemente en los últimos años con versiones evasivas más avanzadas.

Las redes de bots tardan en crecer, incluso permaneciendo en estado latente dentro de los dispositivos, esperando una señal de lanzamiento de un ataque de DDoS o la propagación de un spam. Según el reporte de SIFT, el 49% de los usuarios incluidos en el estudio han sido víctimas de fraude en los pagos. De estas víctimas, el 77% corresponde a compras no autorizadas con uso ilícito de información de pago almacenada en un sitio web o una aplicación. La economía del fraude implica la ejecución de estrategias sofisticadas, automatizadas y distribuidas por parte de los ciberdelincuentes a los demás actores del comercio electrónico (SIFT, 2022).

Según Siften (2021), los intentos de fraude en los pagos de pago aumentaron en un 23% interanual, impulsado en gran medida por las redes de fraude organizadas que lanzan ataques respaldados por bots contra empresas de todos los tamaños y sectores. La mayor complejidad de los abusos en línea cambia la metodología de prevención del fraude (SIFT, 2022).

Brute Force

Los actuales sistemas de autenticación de banca por Internet se basan en contraseñas, metodología que implica cierta vulnerabilidad para los ataques basados en contraseña como el ataque de fuerza bruta, el ataque de diccionario, el ataque de tabla arco iris o el ataque main-in-the middle. Cuando un usuario malicioso intenta el acceso no autorizado a una cuenta bancaria tratando de adivinar su contraseña, en lugar de en lugar de rechazar su acceso a la cuenta con el mecanismo de autenticación contraseña, el algoritmo HE ampliado genera una cuenta de usuario falsa indistinguible que está estrechamente relacionada con la cuenta de usuario real, en la que el ataque podría no puede determinar si la contraseña adivinada funciona correctamente o no. Se requiere espacio de almacenamiento adicional para mantener las tablas de muestreo inverso y la información de la cuenta falsa (SooFun & Samsudin, 2018).

Los ataques de fuerza bruta y o de adivinación consisten en la ejecución de pruebas repetidas con pares de credenciales para intentar acceder a una cuenta; bien sea, contra una sola cuenta, o bien, contra varias cuentas. Esto se realiza probando las contraseñas posibles o con diferentes pares de ID de usuario-contraseña. Estos ataques suelen contenerse mediante una política de bloqueo de tipo tres strikes que tiene asociada una política de denegación de servicio. Conviene anotar que un atacante que intenta entrar a la fuerza, no necesariamente conoce nombre, dirección u otra información sobre la víctima (Herley & Florêncio, 2008).

Este procedimiento resulta detectable considerando que sólo se intentan un reducido número de inicios de sesión fallidos para cada ID de usuario individual. En el caso de contraseñas no numéricas, puede aumentar su rendimiento probando las contraseñas por orden de probabilidad. (Herley & Florêncio, 2008).

Una vez que un atacante fuerza la entrada, el servidor tiene pocos medios para distinguirlo del usuario legítimo. Los activos se convierten en un lugar seguro para poder acceder, que el atacante controle y que esté fuera del alcance del banco o de las autoridades judiciales. Es importante que las transferencias que realice no puedan anularse cuando se detecte el robo; asimismo, que ninguna de las cuentas intermedias pueda utilizarse para identificar al atacante.

La literatura especializada ha descrito un complejo ecosistema subyacente en la recolección de credenciales robadas; incluso con la utilización de cajeros y drop men para la recolección del dinero obtenido en las operaciones ilícitas con cuentas comprometidas (Herley & Florêncio, 2008). 'LinkedIn', 'Classroom 2.0', 'Pinterest' son algunos de los ejemplos de sitios de redes sociales profesionales. Dado que estos sitios de redes sociales contienen toda la información profesional del usuario, incluida la identificación del correo electrónico, un atacante puede usar estos detalles para enviar a la víctima un correo personalizado.

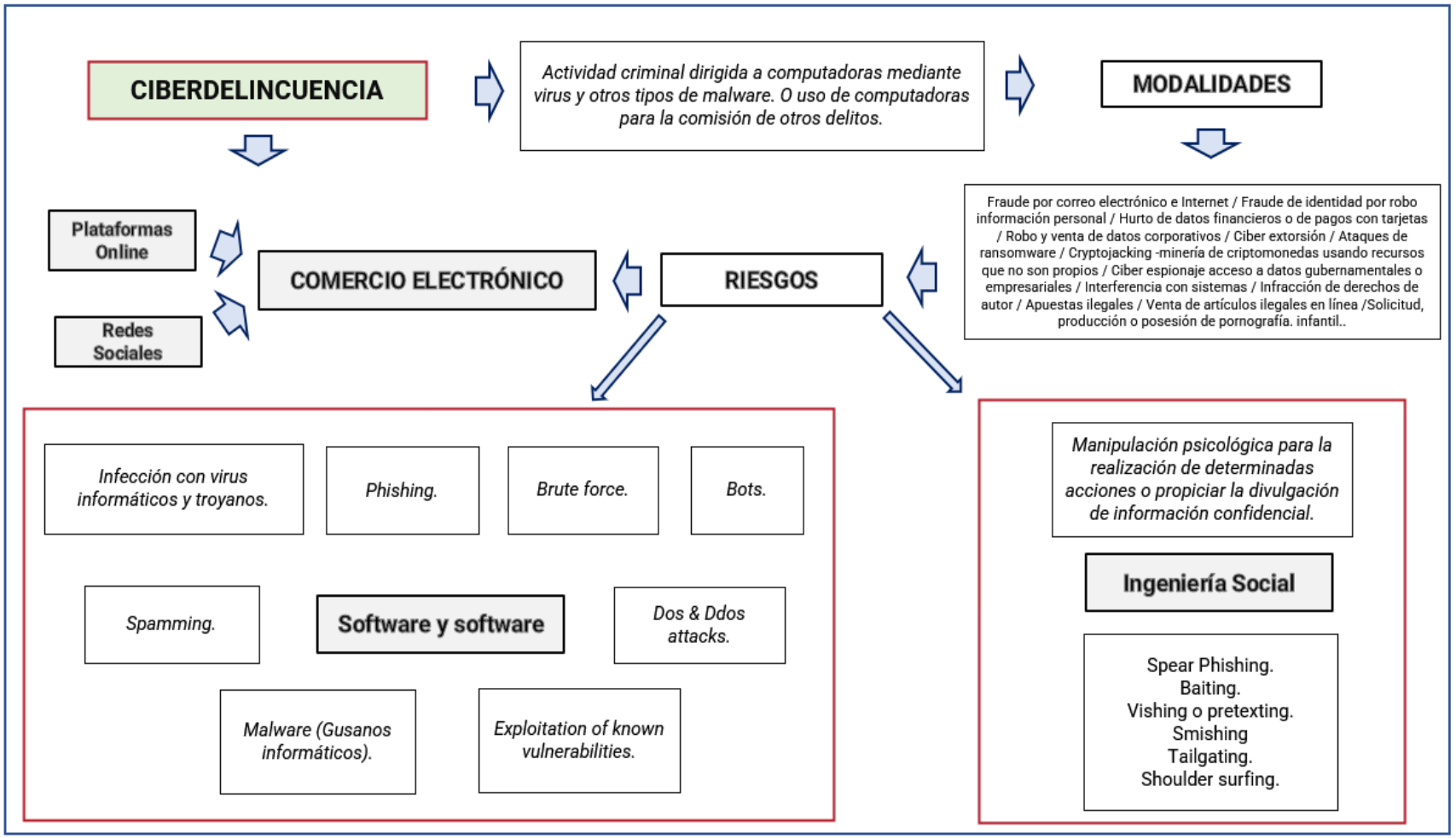
En estos correos electrónicos se envían invitaciones para reclamar premios mediante la activación de un enlace malicioso. Asimismo, esparcidos mediante los foros de discusión. Estas redes son un recurso para la investigación de mercado y una forma antigua de red social. 'Reddit', 'Quora' y 'Digg' son ejemplos de estos foros de discusión populares. En estos foros, las personas también comparten enlaces relacionados con su investigación para que los usuarios puedan obtener más información sobre su tema de investigación. Sin embargo, los ciber atacantes

comparten enlaces maliciosos para desviar a los usuarios a algunos sitios web de phishing (Herley & Florêncio, 2008).

.

Figura 3

Peligros y riesgos asociados al comercio electrónico



Fuente. Elaboración propia.

Estrategias De Mitigación De Riesgos En Compras Por Medios Electrónicos

En una revisión del impacto de Internet en la estructura de la industria, Porter encontró casos de empresas de comercio electrónico que se enfocan en el precio en lugar de continuar con sus estrategias existentes de características, calidad y servicio. Es decir, las empresas estaban optando por una estrategia de diferenciación de precios y descuidando las brechas de seguridad y el hecho de que Internet puede brindar oportunidades adicionales e incluso mejores para establecer una posición estratégica distintiva y obtener una ventaja competitiva.

El servicio al cliente se ha organizado tradicionalmente alrededor y después de la transacción completada. Es decir, ha consistido en recibir y atender personalmente la correspondencia de los clientes con dudas, inquietudes o reclamos. Luego vino la mesa de ayuda en la que el cliente podía hablar directamente con un representante de servicio. Ahora, los centros de soporte y servicio al cliente (CSS) o centros de interacción con el cliente (CIC) también cuentan con herramientas como Internet, comunicaciones inalámbricas, reconocimiento de voz y vídeo. Otras tecnologías de atención al cliente incluyen la distribución automática de llamadas, la respuesta de voz interactiva, la integración de teléfonos informáticos, la gestión de llamadas por Internet, los agentes cibernéticos de servicios, los bots, los avatares, el análisis del centro de llamadas y el rendimiento. Estas herramientas están dedicadas a cómo un producto es entregado, agrupado, explicado, facturado, instalado, reparado, renovado y rediseñado y en estas subyacen algunas vulnerabilidades que deben identificarse.

Los datos abiertos pueden ayudar a las aseguradoras cibernéticas en sus esfuerzos por desarrollar productos sostenibles. Hasta la fecha, los métodos tradicionales de evaluación de riesgos han sido insostenibles para las compañías de seguros debido a la ausencia de datos históricos de reclamaciones. Estos altos niveles de incertidumbre significan que las aseguradoras

cibernéticas están más inclinadas a sobrevalorar la cobertura de riesgos cibernéticos. Por lo tanto, la combinación de datos externos con los datos de la cartera de seguros parece ser esencial para mejorar la evaluación del riesgo y, por lo tanto, conducir a una fijación de precios ajustada al riesgo (Lis et al., 2014). Este argumento también está respaldado por el hecho de que algunas reaseguradoras informaron que están trabajando para mejorar sus modelos de precios cibernéticos (por ejemplo, creando o comprando bases de datos de proveedores externos).

Además de la ventaja de los precios ajustados al riesgo, la disponibilidad de conjuntos de datos abiertos ayuda a las empresas a comparar su postura cibernética interna y sus medidas de seguridad cibernética. La investigación también puede ayudar a mejorar la concienciación sobre los riesgos y el comportamiento empresarial. Muchas empresas aún subestiman su riesgo cibernético.

Para los formuladores de políticas, esta investigación ofrece puntos de partida para un registro completo de los riesgos cibernéticos. Si bien en muchos países, las empresas están obligadas a informar las violaciones de datos a la autoridad supervisora respectiva, esta información generalmente no es accesible para la comunidad investigadora. Además, el impacto económico de estas infracciones no suele estar claro.

Conclusiones

Los hallazgos obtenidos permitieron el análisis y la discusión que se desarrolló en el anterior capítulo; asimismo, permiten la formulación de algunas ideas y reflexiones que ofician como cierre y conclusión al desarrollo de la presente investigación.

Los hallazgos de la revisión bibliográfica permiten formular las siguientes conclusiones. La ciberseguridad y la evasión de la ciberdelincuencia en el comercio electrónico implica la consolidación de un enfoque holístico que abarque la complejidad y multiplicidad de dinámicas y componentes del mundo híbrido evidenciables en la misma infraestructura que subyace en el comercio electrónico, la industria, las cadenas de suministro entre otras, convergentes con la vida individual y social de las personas que interactúan cotidianamente entre el mundo físico y el virtual.

La forma en que se produce y consume el contenido digital debe ser capaz de distinguir las falsificaciones en (Deep Fakes); la tecnología operativa (TO) debe ser protegida para asegurar la operación industrial y productiva; las transacciones de personas, empresas y estados deben ser seguras y confiables.

Colombia ha sido un país blanco de muchos delitos y malintencionados que vienen de otras partes del mundo con el interés de perjudicar tanto a empresarios, industriales y entidades financieras, por ello es importante que cada sector conozca sus debilidades y tome conciencia de la importancia de cuidar, salvaguardar y no difundir información importante sobre las empresas, manteniendo actualizadas las políticas de seguridad y siendo informado de nuevos modelos de ataque por ciberdelincuentes, especialmente, en las redes sociales.

Recomendaciones

En correspondencia con el hilo de exposición propuesto para este capítulo, se formulan algunas recomendaciones a partir de los hallazgos de la revisión bibliográfica de este estudio. La ciberseguridad para el comercio electrónico requiere de la convergencia de esfuerzos gubernamentales y organizacionales, que deberán establecer políticas y mecanismos para la identificación de vulnerabilidades cibernéticas explotables. Esto implica trascender de la planeación y concretar en la ejecución, con el despliegue de herramientas tecnológicas y la asignación correspondiente de presupuestos para la gestión de las vulnerabilidades de red y el fortalecimiento de la seguridad de la infraestructura de manera inteligente, eficaz y eficiente; y en correspondencia con el vertiginoso avance de la tecnología.

En consonancia con lo indicado por ASOBANCARIA (2020), resulta conveniente que las instituciones financieras como eslabón de la cadena del comercio electrónico, garantice el despliegue de un importante grupo de redes de seguridad y de niveles de supervisión en caso de violación, bajo la premisa de que independientemente de cuán preparados estén, siempre se presentaran brechas explotables y riesgos subyacentes.

Teniendo en cuenta que durante los últimos años se desplegó tecnología más avanzada pero no necesariamente segura; resulta necesario el diseño de planes de capacitación con públicos objetivos específicos, esto incluye: empleados internos, insourcing, proveedores, clientes, entre otros; orientados al fortalecimiento de la cultura de seguridad digital, el desarrollo de capacidades y la sensibilización, garantizando su ejecución periódica y estableciendo evaluaciones a efecto de determinar su impacto. Esta capacitación debe incluir el desarrollo de capacidades tempranas en aspectos cibernéticos de forma que se cierre la brecha en cuanto a personal capacitado y se fomente una cultura de seguridad digital.

Las organizaciones deben buscar las mejores herramientas reconociendo que la seguridad es un asunto complejo en el que intervienen múltiples actores y que se construye cotidianamente. La ciberseguridad implica el aseguramiento de recursos para impedir los ataques, asimismo, constituye un esfuerzo por comprender las brechas y vulnerabilidades en función de la caza de amenazas, su contención, la protección de sistemas críticos, la reducción de daños y la recuperación rápida.

Referencias Bibliográficas

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10), 1–39. https://doi.org/10.3390/fi12100168

Alazab, M. & Broadhurst, R. G. (2017). Cyber-Physical Security. *Cyber-Physical Security, January 2017*. https://doi.org/10.1007/978-3-319-32824-9

Allianz. (2022). Construyendo co nfianza en el futuro Mensaje de nuestro CEO Sobre este informe. *Reporte de Sostenibilidad*. https://www.allianz.co/content/dam/onemarketing/iberolatam/allianz-co/quienes-somos/responsabilidad-social/Allianz-Reporte-de-Sostenibilidad-2021.pdf

Arenales, J. (2022, December). Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles. *La República*, 1. https://www.larepublica.co/empresas/ataques-ciberneticos-en-colombia-han-crecido-30-epm-y-sanitas-son-dos-de-miles-3508452

Aseri, D. A. M. (2021). Security Issues For Online Shoppers. *International Journal of Scientific & Technology Research*, *10*(3), 112–116. https://www.researchgate.net/publication/350220654

ASOBANCARIA. (2020). Guía de buenas prácticas para auditar la ciberseguridad. *Guía Buenas Prácticas*, 28–29. https://www.asobancaria.com/wp-content/uploads/2020/09/Guía-de-Buenas-Prácticas-para-Auditar-la-CiberseguridadV4_compressed.pdf

Cano, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, *6586*. https://revistacientificaesmic.com/index.php/esmic/article/view/866/836

Chapin, L., Piscitello, D. & Strutt, C. (2021). *Malware Landscape 2021 A Study of the Scope and Distribution of Malware*. *November*. https://interisle.net/MalwareLandscape2022.pdf

Congreso de la República. (2001). *Ley 679 de 2001*. *2*(5), 255. https://www.unidadvictimas.gov.co

Congreso de la República. (2007). Ley 1150 de 2007. *Gaceta Del Congreso de Colombia*, *46.691*, 1–24. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=25678#32

Congreso de la República de Colombia. (2012). *Decreto 2364*. 1–4. http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRETO 2364 DEL 22 DE NOVIEMBRE DE 2012.pdf

Congreso de la República de Colombia. (s.f.). *Decreto 1377 de 2013*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Congreso de la República de Colombia. (1999). *Ley 527 de 1999* (Vol. 1999, Issue agosto 18). http://www.oas.org/juridico/spanish/cyb_col_Ley_527_de_1999.pdf

Congreso de la República de Colombia. (2000). Ley 594 de 2000. In *Archivo General de la Nación de Colombia* (Vol. 1, Issue Julio 14, pp. 1–17). https://normativa.archivogeneral.gov.co/ley-594-de-2000/

Congreso de la República de Colombia. (2009a). Ley 1273 de 2009. In *Gaceta del Congreso* (Vol. 2009, Issue 36). http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Congreso de la República de Colombia. (2009b). Ley 1341 de 2009. *Gaceta Del Congreso*, 1–34. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913

Congreso de la República de Colombia. (2010). Decreto 2693 de 2012. *Gaceta Del Congreso*, *2003*(marzo 13), 1–18. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9863

Congreso de la República de Colombia. (2011a). *Ley 1437 de 2011* (p. 115). https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/INEC/IGUB/ley-1437-de-2011.pdf

Congreso de la República de Colombia. (2011b). Ley 1480 de 2011. *Gaceta Del Congreso*, 33. https://www.sic.gov.co/sites/default/files/normatividad/042017/Ley_1480_Estatuto_Consumidor_2.pdf

Congreso de la República de Colombia. (2012a). *Decreto 2609 del 14 de diciembre de 2012*. Diario Oficial 48647. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50958#

Congreso de la República de Colombia. (2012b). Ley 1581 de 2012. *Gaceta Del Congreso*, *48*(9), 1–11. https://www.unicauca.edu.co/versionP/sites/default/files/files/LEY_1581_DE_2012.pdf

Congreso de la República de Colombia. (2014). Ley 1712 de 2014. *Gaceta Del Congreso Congreso*, *2014*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882#:~:text=Regula el derecho de acceso,la publicidad de la información.

Congreso de la República de Colombia. (2015). Ley 962 de 2005. *Gaceta Del Congreso*, *13*(3), 1576–1580. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=17004

De la cuesta, J. L. & Pérez, A. (2010). Ciberdelicuentes y ciber víctimas. In *Derecho penal informático* (Issue 3, pp. 99–120). http://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimas.pdf

Decreto 019. (2012). Decreto 019 de 2012. *Departamento Administrativo de la Función Pública*. https://www.funcionpublica.gov.co/documents/418537/604808/1888.pdf/21acb602-d97b-4715-9722-1144ab0a8f03

Del Aguila, A. (2000). *Comercio Electrónico y Estrategia Empresarial* (2nd ed.). https://www.casadellibro.com.co/libro-comercio-electronico-y-estrategia-empresarial-2-

ed/9788478974412/743552

Delgado, A. (2016). *Cómo digitalizar tu empresa*. www.ecoeediciones.com

Departamento Nacional de Planeación. (1936). CONPES 3701. *The American Mathematical Monthly*, *43*(3), 196. https://doi.org/10.2307/2300376

Española, R. A. de la L. (2022). *Diccionario Real Academia de la Lengua Española*. https://dle.rae.es/hacker

Fisch, E. & White, G. (2000). *Secure Computers and Networks Analysis, Design, and Implementation* (1st ed.).

FORTINET. (2021). Sustainability report 2021 About Fortinet. *Fortinet Report*. https://www.fortinet.com/content/dam/fortinet/assets/reports/fortinet-sustainability-report-2021.pdf

Hartman, A., Sifonis, J. & Kador, J. (2001). *E-business: Estrategias para el éxito en la economía de Internet, métodos probados para organizar empresas de comercio electrónico*. https://eki.pl/index.php?br1=100000&page=2&detailed=LIB103

Herley, C. & Florêncio, D. (2008). Protecting financial institutions from brute-force attacks. In *IFIP International Federation for Information Processing* (Vol. 278, pp. 681–685). https://doi.org/10.1007/978-0-387-09699-5_45

Hernández Sampieri, R., Fernández Collado, C. & Baptista Lucio, M. del P. (2001). *Metodología de la investigación* (Vol. 6).

Hurel, L. M. (2021). Uma análise da estratégia nacional de cibersegurança - Instituto Igarapé. *Instituto Igarapé*. https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/

IBD. (2017). Impact of Digital Security incidents in Colombia 2017. In *Organización de Estados*

Americanos (Vol. 4, Issue 1). https://publications.iadb.org/en/impact-digital-security-incidents-colombia-2017

INTERPOL. (2020). *Estratégia Mundial contra la Ciberdelincuencia* (Vol. 4, Issue 1). https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_SP LR.pdf?inLanguage=esl-ES

Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., Khan, J. A., Rehman, A. U. & Shafiq, M. (2022). Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. *Sustainability (Switzerland)*, *14*(14). https://doi.org/10.3390/su14148374

ISO. (2019). *ISO 27032:2012*. https://sisteseg.com/blog/wp-content/uploads/2018/12/Implementación-ciberseguridad-ISO-27032.pdf

Kapersky Lab. (2022). *¿Qué es la ciberseguridad?* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kraft, T. A. (2015). *E-Commerce Security E-Commerce Security*. *September*. https://www.researchgate.net/publication/281976555

Krishnamurthy, V. & Santhadevi, P. (2019). Internet spam threats and email exploitation – A scuffle with inbox attack. *International Journal of Applied Sciences and Engineering Research*, *3*(4), 907–912. https://doi.org/10.6088/ijaser.030400015

MalwareBytes cyberprotection. (2022). *2022 Threat Review*. 1–41. https://www.malwarebytes.com/resources/malwarebytes-threat-review-2022/mwb_threatreview_2022_ss_v1.pdf

Martinez, W. & Ávila, D. (2021). Ciberseguridad en las redes sociales : una revisión teórica. *Uniandes EPISTEME. Revista Digital de Ciencia, Tecnología e Innovación*, *8*(2), 211–234.

https://www.researchgate.net/publication/351510512_Ciberseguridad_en_las_redes_sociales_una_revision_teorica

MS-ISAC. (2022). Understanding and Responding to Distributed Denial of Service Attacks. *Cybersecurity Infraestructure Security Agency*. https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

NCSI. (2021). *Reporte Ciberseguridad Colombia* (Vol. 5). https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

NQA. (2017). ISO 27001:2013 Guía De Implantación Para La Seguridad De La Información. *NQA*, *1*, 1–30. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

OEA. (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe* (Vol. 1). http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

PANDA Security. (2015). Entendiendo los Ciber-Ataques. *Adaptative Defense*, 15. pandasecurity.com/intelligence-platform/

PCI. (2010). Requisitos y procedimientos de evaluación de Seguridad de Datos. *Norma de Tarjetas de Pago*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2es-LA.pdf

Pérez, Y. (2016). Importancia de la Ciberseguridad en Colombia. *Universidad Piloto de Colombia*, *42*(31), 1–9. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/00003620.pdf?sequence=1

Policia Nacional de Colombia. (2020). Tendencias de cibercrimen en Colombia. In *Tendencias de*

cibercrimen en Colombia. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Radware. (2010). Mitigating DDos attacks in the financial community. *Solution Brief*, 1–4. http://cstor.com/wp-content/uploads/2016/10/Radware_Mitigating-DDoS-Attacks-in-the-Financial-Community_Solution-Brief.pdf

Rincon, E. (2014). Instrumentos Normativos de Ciberseguridad. *Certicamara S.A.*, 6. https://web.certicamara.com/media/58493/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

Roa, E. & Cuellar, D. (2019). Evolución del comercio electrónico en Colombia en la última década. *Ciencia Unisalle*, 33. https://ciencia.lasalle.edu.co/administracion_de_empresas/3080/

Rogel, E., Sánchez, L. & Pacheco, A. (2019). Herramientas y buenas prácticas del negocio electrónico como una nueva tendencia en la economía utilizando la comunicación TI. *Espacios*, *40*(4), 14. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065603742&partnerID=40&md5=82ccf27378c47c93940129a959de6029

SIFT. (2022). Outsmarting payment fraud in the age of automation. *DIGITAL TRUST & SAFETY INDEX*. https://pages.sift.com/rs/526-PCC-974/images/2022_Q1_Digital_Trust_Safety_Index.pdf

Smith, G. (2004). *Control and security of E-commerce*. https://indaga.ual.es/discovery/fulldisplay?docid=alma991001794991604991&context=L&vid=34CBUA_UAL:VU1&search_scope=MyInstitution&tab=LibraryCatalog&lang=es

SooFun, T. & Samsudin, A. (2018). Enhanced security of internet banking authentication with extended honey encryption (Xhe) scheme. *Studies in Computational Intelligence*, *741*(January), 201–216. https://doi.org/10.1007/978-3-319-66984-7_12

Souminen, K. (2019). El comercio digital en América Latina. *Comercio Internacional*, *145*, 31–35. https://dialnet.unirioja.es/servlet/articulo?codigo=7167041

Stanikzai, A. Q. & Shah, M. A. (2021). Evaluation of Cyber Security Threats in Banking Systems. *2021 IEEE Symposium Series on Computational Intelligence, SSCI 2021 - Proceedings, December*, 3–7. https://doi.org/10.1109/SSCI50451.2021.9659862

Superintendencia de Industria y Comercio. (2008). *Ley 1266 de 2008, HÁBEAS DATA* (pp. 1–14). http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Ley_1266_de_2008_Habeas_Data.pdf

UNAD. (2022). *Ingeniería de Sistemas UNAD.* Perfil Ingeniero de Sistemas. https://estudios.unad.edu.co/ingenieria-de-sistemas

Apéndices

Apéndice A

Formato ficha referenciación bibliográfica

FICHA BIBLIOGRÁFICA	
I. RESEÑA BIBLIOGRÁFICA	
Área	
Autor	
Título y subtitulo del libro	
Nombre de la editorial	
Ciudad	
Título y subtitulo del articulo	
Dirección electrónica	
Fecha de consulta	
Número de páginas	

II. ASPECTOS GENERALES		**PALABAS CLAVE**
Objetivos		
Contenido		
Metodología		
Resultados		
Vacíos		
ASPECTOS CONCRETOS		
Tema		**ELABORA:**
Idea Principal		
Comentario		

Apéndice B

Matriz de descripción y programación de actividades

Cronograma de actividades

Tiempo	***semana***				***semana***				***semana***				***semana***				***semana***				***semana***				***semana***			
Actividad	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Anteproyecto	■	■	■	■	■	■	■	■	■	■	■	■																				
Análisis documental										■	■	■	■	■	■																	
Análisis comparativo																■	■															
Construcción de resultados																	■	■	■													
Consolidación informe final																				■												
Análisis y presentación de resultados																					■	■	■	■	■	■	■	■	■	■	■	■

Apéndice C

Plan de gestión de recursos

Tipo de recurso	Descripción	Presupuesto
Equipo humano	(01) Un Investigador.	**$** 6.000.000.00 (Total).
Equipos y software	(01) Un ordenador gama media.	$ 1.200.000.00 (Total).
Acceso a repositorios especializados	Ingreso a bases de datos especializadas.	$ 600.000.00
Total, gastos en pesos colombianos:		$ 7.800.000.00

Apéndice D

Lista de siglas y acrósticos

2FA:	Autenticación de 2 factores.
2FA:	Autenticación de dos (2) factore
2SV:	Verificación de 2 pasos.
CONPES:	Consejo Nacional de Política Económica y Social.
DDOS:	Ataque de denegación de servicio distribuido.
DDoS:	Denegación de servicio distribuida.
E-COMMERCE:	Comercio electrónico.
GDPR:	Reglamento general de protección de datos.
IA:	Inteligencia artificial.
ISO:	Organización internacional para la estandarización.
MFA:	Autenticación multifactor.
ML:	Aprendizaje Automático.
NCSI:	National Cyber Security Index.
PCI DSS:	Estándar de seguridad de datos de la industria de tarjetas de pago
POS:	Sistemas de puntos de venta.
PWC:	Pricewaterhouse Coopers.
TLS:	Seguridad de la capa de transporte (TLS).

Apéndice E

Glosario

Información: conjunto de datos de distinta naturaleza que opera como recurso de notable valor en el desarrollo de las actividades humanas, entre ellas, las empresariales y de negocios. Esta información es gestionada por diferentes tipos de software que facilita su tratamiento y soporte físico y lógico.

Amenaza: Acción con capacidad para vulnerar la seguridad de la información. Estas surgen de las vulnerabilidades, que es aprovechada por los ciber atacantes y que puede o no comprometer la seguridad de un sistema de información.

Confidencialidad: Principio básico de la implementación de la seguridad de la información. Es la protección y resguardo de la información frente a terceros.

Delito informático: Acción tipificada antijurídicamente que implica el uso de la tecnología computacional con fines de afectación de la información contenida en un sistema de tratamiento autorizado.

Disponibilidad: Principios básicos, junto con la integridad y la confidencialidad, para la implementación de la seguridad de la información. Implica la protección de la información en forma de contraseñas y los detalles de tarjetas de crédito mediante el despliegue de procesos de comunicación confiable y legítima.

Smishing: Hurto de información de los usuarios a través de mensajes de texto en dispositivos móviles.

Tabnabbing: Método de Phishing en Internet que aprovecha la acostumbrada navegación por pestañas. El método se centra en las pestañas abiertas en el navegador y las páginas visitadas por el usuario anteriormente.

Telecomunicación: Sistema de transmisión y recepción de señales a distancia. Estas pueden ser de distinta naturaleza, transmitida por medios electromagnéticos.

Trazabilidad: Posibilidad de verificar la procedencia y flujo de actividades relacionadas con un evento. De este modo, se puede determinar quién hizo qué y en qué momento.

Vishing: Estafa que pretende suplantar la identidad del afectado a través de VoIP (Voice over IP), recreando una voz automatizada semejante a la de las entidades bancarias.

Whaling: Técnicas de phishing dirigidas contra objetivos de alta importancia dentro de una organización, esto es, directivos de empresa, políticos, entre otros; o de trascendencia social, cantantes, artistas, famosos, etc.