ANÁLISIS DE LAS NORMATIVAS Y ESTRATEGIAS DE SEGURIDAD DIGITAL VIGENTES EN LA POLÍTICA NACIONAL Y SU EFICACIA EN EL TRATAMIENTO DE CIBERDELITOS EN EL SECTOR DE E-COMMERCE DURANTE COVID -19

ALEJANDRO ARTURO GONZÁLEZ GRIMALDOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

ANÁLISIS DE LAS NORMATIVAS Y ESTRATEGIAS DE SEGURIDAD DIGITAL VIGENTES EN LA POLÍTICA NACIONAL Y SU EFICACIA EN EL TRATAMIENTO DE CIBERDELITOS EN EL SECTOR DE E-COMMERCE DURANTE COVID -19

ALEJANDRO ARTURO GONZÁLEZ GRIMALDOS

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

ALEJANDRO ARTURO GONZÁLEZ GRIMALDOS

Director
EDGAR ROBERTO DULCE VILLARREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 21 de Junio de 2023

DEDICATORIA

Dedico este gran trabajo a mi hijo Miguel Ángel que en el corto tiempo que compartió conmigo me dio la fortaleza para continuar y no desfallecer. A mi hija Paula Alejandra que me enseña a ser una mejor persona y hace que cada día sea espectacular y lleno de esperanza. A mi esposa Viviana que me apoyo en todo momento y que con su amor y trabajo logra mantener unida la familia.

También lo dedico a mis Padres y hermano que con sus consejos y colaboración me ayudaron a continuar ante las adversidades.

Gracias a todos ellos ya que fueron mi pilar para poder avanzar y terminar con éxito este proyecto académico.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

TABLA DE CONTENIDO

INTRODUCCIÓN *3*

1. DEFINICIÓN DEL PROBLEMA *5*

1.1 ANTECEDENTES DEL PROBLEMA **5**

1.2 FORMULACIÓN DEL PROBLEMA **6**

2 JUSTIFICACIÓN *8*

3 OBJETIVOS *10*

3.1 OBJETIVO GENERAL **10**

3.2 OBJETIVOS ESPECÍFICOS **10**

4 MARCO REFERENCIAL *11*

4.1 MARCO TEÓRICO **11**

4.1.1 Ciberseguridad 11

4.1.2 E-commerce 13

4.1.3 Tipos de E-commerce 15

El comercio electrónico se encuentra a nivel global y es desde ahí donde se realizan las transacciones, desde un oferente a un consumidor que puede estar en cualquier país que tengo acceso o cobertura. Existen varios tipos de comercio electrónico los cuales tienen relación entre proveedores, consumidores y organizaciones gubernamentales de los cuales se muestran a continuación 15

4.1.3.1 Business to Business (B2B) 15

4.1.3.2 Business to Consumer (B2C) 16

4.1.3.3 Business to Employee (B2E) 16

4.1.3.4 Business to Goverment (B2G) 16

4.1.3.5 Consumer to Business (C2B) 16

4.1.3.6 Consumer to Consumer (C2C) 17

4.1.3.7 Government to Consumer (G2C) 17

5 DESARROLLO DE LOS OBJETIVOS *18*

5.1 PANORAMA ACTUAL DE LA SEGURIDAD DE lA INFORMACIÓN EN LAS PYMES DURANTE EL COVID-19 en el 2020-2021 ..... **18**

5.2 EVALUACIÓN DE LAS TRANSACCIONES EN EL E-commerce **22**

5.3 RIESGOS Y AMENAZAS DURANTE LA PANDEMIA **30**

5.3.1 Penetración banda ancha 32

5.3.2 Competencia 33

5.3.3 Miedo de los consumidores 33

5.3.4 Falta de contacto físico con el producto 33

5.3.5 Problemas de distribución 33

5.3.6 Reclamación y devoluciones 33

5.3.7 Phishing 33

5.3.8 Spoofing....34
5.3.9 Pharming....34
5.3.10 Amenazas OWASP TOP 10....35
5.4 PROPUESTA DE UN PLAN PARA LA MITIGACION DE RIESGOS GENERADOS A PARTIR DE LA PANDEMIA EN COLOMBIA DESDE EL 2020-2021 HACIA LA REACTIVACIÓN DEL E-COMMERCE....36
5.4.1 Plan de Seguridad del Ministerio de las TIC....37
5.4.1.1 Estrategias De Seguridad Digital....40
5.4.1.2 Instalar Protocolos Https....40
5.4.1.3 Implementa Sistemas De Verificación Cvv Y Avs....41
5.4.1.4 Realizar Backups Periódicos....42
5.4.1.5 Uso De Seguridad Multicapa O Multi-Layered....43
5.4.1.6 Realizar Un Monitoreo De Las Transacciones....43
5.4.1.7 Evita Almacenar Información De Tarjetas De Crédito/Débito....44
5.4.2 Plan de Gestión de Incidentes....44
5.4.3 Estrategia De Concientización De La Seguridad Informática....45
6 CONCLUSIONES....47
7 RECOMENDACIONES....49
8 BIBLIOGRAFÍA....50

LISTA DE FIGURAS

Pág.

Figura 1. *Ventas a través del E-commerce* 23
Figura 2. *Transacciones a través del E-commerce* 24
Figura 3. *Futuro del Retail y el Comercio Electrónico* 27
Figura 4. *Panorama del E-commerce* 31

GLOSARIO

ACTUALIZACIÓN DE SEGURIDAD: Modificaciones que se aplican, de forma automática o manual, en el software de los sistemas operativos o aplicaciones instalado en los dispositivos electrónicos, con el objetivo de corregir fallos de seguridad, errores de funcionamiento o bien para dotar a los dispositivos de nuevas funcionabilidades, así como incorporar mejoras de rendimiento.

AMENAZA: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

ANÁLISIS DE RIESGOS: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

ANÁLISIS DE VULNERABILIDADES: Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

AUTENTICACIÓN: Acción mediante la cual demuestran a otra persona o sistema que somos quien realmente dice y son, mediante un documento, una contraseña, rasgo biológico etc.

B2B: Abreviatura de «Business to Business». Este término se refiere a las transacciones comerciales entre empresas, utilizando medios telemáticos como EDI (Electronic Data Interchange) o el Comercio Electrónico.

B2C: Abreviatura de «Business to Consumer». Este término se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final. Suele también indicar las transacciones realizadas directamente entre un cliente y una empresa sin que medie un intermediario.

BACKUP: Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

CERTIFICADO DIGITAL: Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido para autenticar la existencia y validez de un usuario o sitio web por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet.

CIBERATAQUE: Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y

vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

CIBERDELINCUENTE: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

CONFIDENCIALIDAD: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

CONTRASEÑA: Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.

CONTROL DE ACCESO: Sistema de verificación que permite el acceso a un determinado recurso si la persona o entidad tiene los derechos necesarios para solicitarlo. Este acceso puede ser a recursos de tipo físico (por ejemplo, a un edificio o un departamento) o lógicos (por ejemplo, a un sistema o una aplicación software específica).

CRIPTOGRAFÍA: La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado. Existen dos tipos principales de criptografía: por un lado, la conocida

como criptografía simétrica, más tradicional, y la criptografía asimétrica o de clave pública.

CUARENTENA: Acción que desarrollan los antivirus para aislar un archivo infectado del resto del sistema. De este modo, se evita que el archivo aislado provoque daños en el sistema hasta que sea posible desinfectarlo con todas las garantías por parte del antivirus. En ocasiones esto no es posible, por lo que se procedería continuando la cuarentena o eliminándolo directamente del sistema.

DISPONIBILIDAD: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

INCIDENTE DE SEGURIDAD: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

INTEGRIDAD: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que, de un lado se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

KEYLOGGER: Es un tipo de spyware que se encarga de monitorizar toda la actividad realizada con el teclado (teclas que se pulsan) para luego enviarla al ciberdelincuente.

MALWARE: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

MITIGACIÓN: Reducción o atenuación de los daños potenciales sobre los sistemas, aplicaciones y dispositivos causados por un evento, como una vulnerabilidad o ataque.

PASARELA DE PAGO: Servicio de pago e intermediación que permite a las tiendas online realizar operaciones de pago con los clientes mediante el intercambio de datos, de forma segura y rápida, entre la entidad bancaria del vendedor y la del comprador.

PHARMING: Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

PHISHING: Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese

correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

POLÍTICA DE SEGURIDAD: Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

PRIVACIDAD: Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de actores.

PROTOCOLO: Es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

RANSOMWARE: Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.

RIESGO: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

SGSI: Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

SUPLANTACIÓN DE IDENTIDAD: Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling). Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

VULNERABILIDAD: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

RESUMEN

La importancia de la regulación de la normatividad en los países de Latinoamérica ya está implementada específicamente para Colombia se tiene la Ley 1273 de Enero de 2009, en la cual se describen los delitos informáticos a los que pueden ser aplicados para determinar un ilícito en Ciberseguridad.

La pandemia ha generado un cambio en las múltiples formas de cumplir con las obligaciones una de ellas es usando el comercio electrónico donde el número de transacciones ha aumentado significativamente y por ende los Ciberdelitos.

Las empresas se vieron en la necesidad de desarrollar estrategias de transformación digital para afrontar la nueva realidad.

Con esta nueva actualidad, con estos nuevos desarrollos y opciones en el E-commerce se requiere tener una mirada más profunda, un análisis eficaz en la normatividad de los delitos cibernéticos y las nuevas estrategias para protegerse de los nuevos desafíos en cuanto a la actualidad los apremian.

ABSTRACT

El propósito de esta monografía es encontrar las normas y estrategias para el tratamiento de la información que se ha venido incrementando durante la pandemia que generó el COVID-19.

Se evidencia que las transacciones comerciales han venido en aumento según los estudios y mediciones en América Latina a partir del confinamiento generado por el aislamiento de las personas. Esto ha hecho que las empresas medianas y pequeñas tengan la necesidad de fortalecer sus servicios digitales en el E-commerce.

Por esto se sugiere aplicar la metodología Modelo de Seguridad y Privacidad de la Información (MSPI), ya que ha sido avalada por el estado Colombiano para sus entidades, de la mano con el estándar Internacional ISO31000 el cual se adapta a cualquier tipo de organización y aplicaría a las pequeñas y medianas empresas privadas.

Adicionalmente se establecen las mejores estrategias de seguridad digital para que sean un complemento en la implementación de las empresas para la administración de la información siempre velando en su integridad, confidencialidad y disponibilidad.

Por último, se sugiere una estrategia pedagógica de concientización de la Seguridad Informática donde se dé un alcance a la educación digital y se formen todos los actores que intervienen en el proceso, para esto se utiliza la guía NIST SP 800-50

INTRODUCCIÓN

En el siguiente trabajo se encuentran las prioridades que actualmente requieren las transacciones electrónicas, su comercio y las características principales de seguridad que ameritan para que un flujo de comercio electrónico acorde al aumento de las transacciones que acarreo la pandemia del Codiv-19 desde el año 2020.

También se encuentran algunos estudios donde se demuestra la importancia del comercio electrónico y la aplicación inmediata de planes de seguridad de las empresas, para prestar un servicio acorde a las necesidades del mundo actual.
Según las métricas mostradas en el trabajo se evidencia el aumento en las transacciones del E-commerce y así mismo sus vulnerabilidades de las cuales se requiere un manejo adecuado para garantizar la seguridad de todas las partes.

Durante el trayecto del trabajo se abordan temas de ciberseguridad y su incidencia en la economía de los países de Latinoamérica y su estado actual en la implementación de políticas para el crecimiento económico ya que se evidencia el aumento en las transacciones electrónicas y un comportamiento del usuario en auge hacia el E-commerce.

El problema se crea en el momento del auge de las transacciones y donde se requiere una revisión a la normativa vigente y las estrategias que se son aplicables para Colombia a las empresas medianas y pequeñas.

Las empresas en Colombia han requerido servicios en Ciberseguridad y más ahora con el aumento en las transacciones electrónicas y el confinamiento creado por la pandemia, por esto se requiere mayor conocimiento en la normatividad en Colombia

y acceso a mejores prácticas a implementar para las empresas que prestan algún servicio y usan el E-commerce.

Los antecedentes demuestran que se requieren implementar estrategias que permitan que todos los actores en las transacciones electrónicas tengan seguridad al prestar, ofrecer, comprar, vender sus servicios en el E-commerce.

El propósito de este trabajo es proporcionar una claridad del estado de las transacciones en Colombia, su crecimiento y la importancia en proteger a todos los participantes que intervienen en el proceso adoptando medidas claras para el manejo de la Ciberseguridad.

En el desarrollo del trabajo se revisan estudios realizados tanto en América Latina como en Colombia para determinar el estado de las transacciones y así tener una mirada global de cómo se encuentra el país en la detección oportuna de vulnerabilidades y la Ciberdelincuencia.

Por último, se aconseja en lograr la implementación de un sistema de protección que permita llevar a un nivel de seguridad las medianas y pequeñas empresas para la protección contra la Ciberdelincuencia.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Según la reciente encuesta “Workplace of the Future” de Boston Consulting Group (BCG)[1] en cooperación del Foro Económico Mundial se realizaron dos informes donde se evidenciaba que las compañías medianas y pequeñas esperarían un aumento del teletrabajo en aproximadamente un 40%, y el 37% de esas empresas cree que el 25% sus empleados trabajaran en un modelo compuesto donde se combine la presencialidad y el teletrabajo.

Esta necesidad de trabajo hibrida hace que aumente el riesgo en ataques de Ciberseguridad y la seguridad de los datos ya que el 30% de la Ciberseguridad es tecnológica y el otro 70% corresponde a la capacitación del usuario final, su cultura, comportamiento y conciencia según BCG.

También como lo menciona el diario de La Republica[2] donde se manifiesta que ha habido un aumento en la solicitud de servicios de Ciberseguridad de más del 40% en Colombia según Gamma Ingenieros, hace que las PYMES se centren en prestar atención en llevar inversión tecnológica y humana que mitigue esos riesgos de acuerdo a las necesidades propias de cada una.

En una redacción del periódico El Espectador[3] en Diciembre del 2020 con el Centro de Capacidad para la Ciberseguridad de Colombia, administrada por la Policía

[1] BCG Global. [Sitio Web]. Atlanta EEUU. [Consulta14 de Marzo de 2021]. Disponible en: https://www.bcg.com/world-economic-forum/future-of-work
[2] Editorial La República S.A.S. [Sitio Web]. Bogotá. [Consulta 15 de Marzo de 2021]. Disponible en: https://www.larepublica.co/internet-economy/la-demanda-de-los-servicios-de-ciberseguridad-se-incremento-40-a-nivel-nacional-3039341
[3] ELESPECTADOR.COM. [Sitio Web]. Bogotá. [Consulta 15 de Marzo de 2021]. Disponible en: https://www.elespectador.com/noticias/judicial/los-ciberdelitos-aumentaron-un-84-durante-2020-policia/

Nacional el cabeza del Mayor Andrés Camilo Rodríguez hubo un incremento de los Ciberdelitos en la pandemia de un 84% y manifiesta la preocupación en la poca preparación para defenderse de la Ciberdelincuencia en Colombia.

Uno de los problemas durante la pandemia es que los ciberdelincuentes no están en confinamiento, se han detectado campañas de malware aprovechándose del temor en las personas sobre el covid-19. Una de las alertas de estas campañas en Colombia fue la que el Ministerio de Salud informó el 5/Marzo/2020 que se estaba filtrando una información por E-mail y WhatsApp donde advertía la llegada del coronavirus a su sector junto con un archivo (.PDF) que distribuía un código malicioso en el dispositivo móvil con el objetivo de robar información personal.

En Colombia el E-commerce ha venido creciendo de manera exponencial creando conductas de compra on-line, forzando a las empresas a usar estrategias para las ventas en línea. Un ejemplo es la jornada del IVA que impulsadas por el gobierno las cuales generaron problemas de páginas caídas, filas virtuales, demoras en los pagos, entre otras, haciendo que el Ciberfraude coja fuerza con las modalidades de Phishing, Hoax, Ransomware, Smishing, Keyloggers y Pharming.

Esto hace que se requiera realizar un análisis de riesgos de todos los factores que intervienen, de las estrategias actuales y de la normatividad vigente para que no se vea alcanzada por los riesgos en Ciberseguridad con el aumento del Comercio Electrónico.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué normativas y estrategias que se deben tener en cuenta para su efectiva aplicación en el tratamiento de los Ciberdelitos en el E-commerce durante el Covid-19?

2 JUSTIFICACIÓN

En la medida que crecieron en la pandemia con el Covid-19 las transacciones electrónicas crecieron los ataques cibernéticos y se tiene la necesidad de lograr la protección de la información en un mundo digital cada vez más accesible para todos, en Colombia las leyes se encuentran definidas en un marco legal creado en el año 2009 con la ley 1273 el cual según las estadísticas del Banco Interamericano de Desarrollo[4] en un reporte de Ciberseguridad de Julio de 2020 llamado "Riesgos, avances y el camino a seguir en América Latina y el Caribe" describe que Colombia ha adoptado una política Nacional en Seguridad Informática en el año 2016 donde se pretende responder de manera más rápida a las amenazas que se puedan presentar en Seguridad Cibernética y defensa en el país, adicionalmente adoptó dentro de sus políticas de gestión y desempeño la llamada política de Seguridad Digital como parte integral de las operaciones estratégicas de las entidades públicas y privadas.

También en Colombia se tiene implementado, por medio del Ministerio de Tecnología y las comunicaciones (MinTic) un sistema de seguridad y privacidad para apoyar las buenas prácticas y estándares en seguridad para proveer una mayor protección en los tres pilares de la Seguridad en la Información como son la Integridad, Disponibilidad y Confidencialidad.

Sin embargo, se encuentra en las pequeñas empresas la falta de integración a esas políticas y a la academia de lograr seguir capacitando y capacitándose frente a las actuales amenazas que se presentan.

[4] Organization of American States & Inter American Development Bank. [Sitio Web]. New York. [Consulta 14 de Marzo de 2021]. Disponible en: https://www.iadb.org/es

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las diferentes normativas y estrategias de seguridad digital vigentes en la política nacional y su eficiencia en el tratamiento de Ciberdelitos en el sector del E-commerce durante el Covid-19 en las Pymes empresas durante el 2020-2021, proponiendo un plan de gestión de riesgos mitigando las vulnerabilidades y amenazas incrementadas en las transacciones electrónicas.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer el panorama actual de la seguridad digital en las pequeñas y medianas empresas durante el Covid-19 en el 2020.
- Evaluar la trazabilidad de las transacciones en el E-commerce y su aumento en los riesgos y amenazas durante la pandemia en Colombia en el 2020-2021.
- Proponer un plan de gestión de riesgos para E-commerce que pueda ser implementado en las pequeñas y medianas empresas a partir de la reactivación en Colombia.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Ciberseguridad

Se define Ciberseguridad como el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

En la Real Academia Española la palabra Ciberseguridad no existe, pero al descomponerla Cyber indica relación con las redes informáticas y Seguridad es cualidad de seguro y que su función es evitar o prevenir acciones.

El 30 de noviembre es el día internacional de la Ciberseguridad o Seguridad de la Información, celebrada en mundo con el objetivo de concientizar sobre los riesgos a los que se están expuestas las organizaciones y las personas en general sobre los Ciberataques.

La Association For Computing Machinery[5] es la sociedad informática científica y educativa más grande del mundo que como organización ofrece recursos que hacen avanzar la informática como ciencia y profesión. Esta organización tiene como valor fundamental la promoción de la información como ciencia y profesión y le atribuye la creación del día Internacional que se celebró por primera vez en el año 1988.

Una de las primeras leyes que involucran la Ciberseguridad es la ley 527 de 1999 expedida por el congreso de la Republica en el mes de Agosto donde describe: “Por

[5] ACM Organization. [Sitio Web]. New York. [Consulta 27 de Marzo de 2021]. Disponible en: https://www.acm.org/about-acm/about-the-acm-organization

medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.”

En el artículo 2 define:

a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) Entidad de Certificación. Es aquella persona que, autorizada conforme a la

presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

e) Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

f) Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Es importante resaltar que en el análisis hacen referencia a que se debe tener en cuenta su origen internacional para tener una uniformidad en su aplicación.

Esto es muy importante en Latinoamérica ya que Colombia se sitúa en el puesto 80 de 174 países donde según el Banco Interamericano de Ciberseguridad[6] en su Reporte de Seguridad del 2020 se realiza una comparación dependiendo la cantidad de personas, la cantidad de abonados a teléfonos celulares, personas con acceso a internet y el porcentaje del territorio con acceso a internet.

4.1.2 E-commerce

El comercio electrónico también denominado E-commerce es la actividad de distribuir, comprar, vender cualquier producto o servicio en internet como su principal plataforma para ello.

[6] Organization of American States & Inter American Development Bank. [Sitio Web]. New York. [Consulta 14 de Marzo de 2021]. Disponible en: https://www.iadb.org/es

Esto hace que las transacciones y el comercio puedan acceder a múltiples proveedores, lograr precios competitivos y reducción de costos en las transacciones y envíos.

El comercio electrónico puede realizarse por medio de múltiples plataformas de aplicaciones como: correos electrónicos, catálogos y carritos de compras, intercambio electrónico (EDI), por medio de FTP y servicios Web.

Con el crecimiento de las transacciones en línea y la evolución de los negocios existen varios modelos del E-commerce como:

Tienda online: con las mismas características de las tiendas físicas, pero adaptadas para internet. Por ejemplo, las tiendas online de Falabella o Alkosto.

E-Commerce de afiliación: en este caso el cierre y la venta del producto no se hacen directamente con el productor, sino que se refiere a otra tienda a la que se le paga una comisión para conformar la venta. Funciona con una publicación en tu portal que cuando alguien está interesado en adquirirlo se redirige a una página de otro proveedor. Un modelo de gran popularidad porque no requiere inversión, ni inventarios, ni se tienen que ofrecer garantías, por ejemplo, la empresa ACH COLOMBIA ofrece el botón de pagos PSE[7].

Marketplace: es un tipo de “Tienda de tiendas” en la que una gran plataforma alberga espacio online para que diversos vendedores ofrezcan sus productos, y el gran ejemplo es Amazon.

[7] Zapata, J. F., Escorcia, J. A., & Quintero, E. S. (2021). PRODUCTOS Y SERVICIOS. ACH COLOMBIA. [Consulta 14 de Marzo de 2021]. Disponible en: https://www.achcolombia.com.co/productos-y-servicios

E-commerce de Subscripción: un modelo de negocio con automatización donde un cliente paga por suscribirse a contenidos digitales o a productos y servicios con frecuencia de compra recurrente. Este permite recibir ingresos por adelantado; así como programar las ventas de forma periódica[8].

4.1.3 Tipos de E-commerce

El comercio electrónico se encuentra a nivel global y es desde ahí donde se realizan las transacciones, desde un oferente a un consumidor que puede estar en cualquier país que tengo acceso o cobertura. Existen varios tipos de comercio electrónico los cuales tienen relación entre proveedores, consumidores y organizaciones gubernamentales de los cuales se muestran a continuación[9]:

4.1.3.1 Business to Business (B2B)

Este tipo de transacción se produce entre dos empresas donde no intervienen consumidores finales. Es muy común cuando entre distribuidores mayoristas y minoristas. Se puede dar en tres modalidades:

- Un vendedor busca compradores
- Un comprador busca proveedores
- Intermediario busca que se produzca una transacción entre comprador y vendedor.
- Este tipo de comercio ayuda a fortalecer la venta y mejora las relaciones entre las pequeñas y medianas empresas.

---

[8] Ramos, M. (2020, 2 junio). Qué es el eCommerce: definición modelos y ventajas. Marketing 4 ECommerce - Tu revista de marketing online para E-commerce. México. [Consulta 20 de Mayo de 2021]. Disponible en: https://marketing4ecommerce.mx/que-es-el-ecommerce/

[9] Zamora, V. F. (2017). Obtenido de EL COMERCIO ELECTRÓNICO EN COLOMBIA: BARRERAS Y RETOS. Colombia. [Consulta 20 de Mayo de 2021]. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/36499/FerrariZamoraVanessa2018..pdf?sequence=1&isAllowed=y

4.1.3.2 Business to Consumer (B2C)

Es el que se da entre una empresa y un consumidor o persona particular. Es el más común en el E-commerce y tiene la gran ventaja de convertirse en un canal de venta fuerte para las empresas, donde lo más importante es tener estrategias de marketing y fidelización de clientes.

4.1.3.3 Business to Employee (B2E)

Se trata de todo lo que una empresa puede ofrecer a sus empleados a través de internet. Por lo general los productos o servicios tendrán precios especiales con el objetivo de incentivar a los colaboradores y fortalecer la relación con la empresa.

Además, este tipo de comercio electrónico se realiza en una sesión con control de acceso exclusivo para cada compañía.

4.1.3.4 Business to Goverment (B2G)

Consiste en el intercambio de que se da entre las empresas y el gobierno por medio de una herramienta de gestión de la información y provisión de servicios internos como externos.

4.1.3.5 Consumer to Business (C2B)

Aunque no es tan común, este tipo de transacción se da entre una persona que ofrece sus servicios o productos a empresas u organizaciones. Una forma común como se puede dar a través de los freelances que venden sus servicios.

4.1.3.6 Consumer to Consumer (C2C)

Este comercio se da entre consumidores y usuarios finales, sin que intervenga ninguna empresa. Por lo general son productos de segunda mano, lo que permite la reutilización de productos a menores precios.

4.1.3.7 Government to Consumer (G2C)

Es cuando un gobierno permite que los ciudadanos realicen sus trámites y los paguen a través de un portal. Su gran ventaja es el ahorro del tiempo y la seguridad que puede brindar el respaldo electrónico, y es muy común para el pago de impuestos.

5 DESARROLLO DE LOS OBJETIVOS

5.1 PANORAMA ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS PYMES DURANTE EL COVID-19 EN EL 2020-2021

La pandemia en Colombia comenzó en el primer trimestre del año 2020 esto hizo que el gobierno tomara varias medidas como son cuarentenas, confinamientos, pico y placa, restricciones sectorizadas y toques de queda entre otras, estas medidas para tratar de frenar la expansión del COVID-19 ocasionaron que las operaciones financieras mediante transferencias, telefonía móvil e internet se incrementaran.

De acuerdo con un informe de la Superintendencia Financiera, el año pasado se realizaron 9,9 billones de transacciones, con un incremento superior al 21% frente a las que se realizaron en el 2019. De estos 9,9 billones de transacciones que se realizaron en el 2020 el 45% del monto total se realizaron sobre el E-commerce.[10]

La empresa de consultoría de estrategia global EY Parthenon realizo un estudio "Covid-19 Financial Sector Perspective"[11] donde explica el uso de las plataformas tecnológicas y la realidad de las Pymes en medio de la crisis por la pandemia.

"La crisis sanitaria aceleró la migración a plataformas virtuales en Colombia; durante la pandemia el uso de aplicaciones de banca digital aumentó a un 59%. Sin embargo, la cultura sigue siendo la principal barrera para aumentar la digitalización en el país, en promedio, el 40% de los usuarios utilizan las sucursales físicas para

[10] Portafolio.co. (2021, Marzo 23). *Portafolio*. Colombia. [Consulta 20 de Mayo de 2021] From https://www.portafolio.co/economia/finanzas/pandemia-disparo-las-operaciones-financieras-550329

[11] Lacayo, J. (2020, 14 diciembre). ¿Usamos más la banca digital? COVID-19 Financial Sector Perspective: el panorama de los servicios financieros en Latinoamérica. Latinoamérica Norte. [Consulta 23 de Marzo de 2021] EY Parthenon. Disponible en: https://www.ey.com/es_co/strategy/panorama-de-los-servicios-financieros-en-latinoamerica
.

la mayoría de sus servicios financieros, en los que abrir una cuenta, hacer depósitos, pagar servicios, tramitar dudas, solicitar préstamos y negociar deudas, todavía no se concibe hacerlo de forma digital y las personas se siguen desplazando para hacerlo presencialmente. En Colombia el 53% de los encuestados continúan visitando las sucursales, frente al 67% de Perú y el 77% de México" aseguró, Juan Felipe Arango, líder de la práctica de EY Parthenon en Colombia.[12]

Esto hace evidencia de las principales razones por la que las cuales los colombianos no usan las transacciones digitales y es por la preocupación de la seguridad ya que en ese estudio se identificó que el 8% de los encuestados fueron víctimas de fraude electrónico, además de la dificultad del uso de herramientas y requerimientos en internet."

Para establecer un panorama actualizado del estado de la Ciberseguridad en las empresas PYMES la compañía ESET que es una compañía líder en protección de la información y ciberseguridad realizo un reporte de "Tendencias 2021 en la Ciberseguridad" donde se abordaron temas como el aumento de la tecnología para el teletrabajo, cambios de hábitos en la forma de realizar transacciones comerciales y su incidencia en el accionar de los Cibercriminales durante el 2019-2020.

A continuación, se presentan los 10 datos principales sobre Ciberseguridad que en la actualidad se requieren para realizar una estrategia para evitar los Ciberdelitos:

[12] Portafolio. (2021, marzo 1). Uso de plataformas de banca digital aumentó en un 59% en la pandemia. Portafolio.co. Colombia. [Consulta 20 de Mayo de 2021]. Disponible en: https://www.portafolio.co/economia/en-colombia-el-uso-de-plataformas-de-banca-digital-aumento-en-un-59-durante-la-pandemia-549606

1. El 60% de los usuarios cree que sus conocimientos sobre seguridad son insuficientes[13].

2. Apenas el 17% de las empresas en América Latina implementa el doble factor de autenticación[14].

3. Solo el 33% de las organizaciones en América Latina cuenta con un plan de continuidad del negocio y el 39% de las empresas no cuenta con políticas de seguridad[15].

4. Durante el primer semestre del 2020 la cantidad de brechas de datos disminuyó en comparación con años anteriores. Sin embargo, el número de registros expuestos (27 mil millones) es cuatro veces mayor que los reportados en cualquier otro reporte previo para el mismo período de tiempo[16].

---

[13] ESET. (2020, 12 02). Welivesecurity.com. Eslovaquia. [Consulta 20 de Mayo de 2021]. From https://www.welivesecurity.com/la-es/infographics/educacion-ciberseguridad-usuarios-mas-conscientes-de-importancia/

[14] ESET. (2020, 08 02). Welivesecurity.com. Apenas el 17% de las empresas implementa el doble factor de autenticación. Eslovaquia. [Consulta 20 de Mayo de 2021] Disponible en: https://www.welivesecurity.com/la-es/2020/08/14/pocas-empresas-implementa-doble-factor-autenticacion/

[15] Harán, J. M. (2020, Agosto 14). Welivesecurity.com by ESET. Eslovaquia. [Consulta 20 de Mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/08/14/pocas-empresas-implementa-doble-factor-autenticacion/

[16] Goddijn, I. (2020). Risk Based Security. U.S. [Consulta 15 de Marzo de 2021]. Disponible en: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Mid%20Year%20Data%20Breach%20QuickView%20Report.pdf

5. 280 días es el tiempo promedio que tarda una organización a nivel global para identificar y contener una brecha de datos. En América Latina, el tiempo promedio es de 328 días[17].

6. Los errores de configuración en servidores en la nube (19%) y el uso de credenciales robadas y/o comprometidas (19%) fueron los principales causantes de brechas de datos, seguidos por la explotación de vulnerabilidades en software de terceras partes (16%) y el phishing (14%). (IBM Corporation, 2020).

7. El 52% de las brechas de datos fueron provocadas por ataques maliciosos, mientras que el 23% fue debido a errores humanos. (IBM Corporation, 2020).

8. El 30% de las brechas de datos involucraron a actores al interior de la empresa u organización, mientras que el 70% fueron provocadas por externos[18].

9. El incremento de denuncias por ataques cibernéticos creció un 400% durante la pandemia, aseguran reportes de abril de 2020[19].

10. Entre julio de 2018 y junio de 2020 se registraron más de 100 000 millones de ataques de Credential Stuffing, de los cuales de los cuales más de 63000

[17] IBM Corporation. (2020, Julio). ibm.com. U.S. [Consulta 15 de Marzo de 2021]. Disponible en: https://www.ibm.com/downloads/cas/RZAX14GX

[18] DBIR 2020. (2020). VERIZON. Informe de investigaciones sobre filtraciones de datos de 2020 - Resumen ejecutivo. U.S. [Consulta 15 de Marzo de 2021]. Disponible en: https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

[19] Miller, M. (2020, 16 Abril). FBI sees spike in cyber-crime reports during coronavirus pandemic. TheHill. U.S. [Consulta 16 de Marzo de 2021]. Disponible en: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

millones se dirigieron a los sectores de retail, turismo y hotelería, 17000 millones al sector multimedia y 10000 millones al sector de los videojuegos[20].

Se tiene entonces como panorama actual de la seguridad de la información en las PYMES durante el COVID-19 entre el 2020 y 2021 que hubo un gran aumento de migración de las PYMES a plataformas virtuales llevando a las empresas a prestar más atención e inversión en proteger sus aplicaciones del ECommerce.

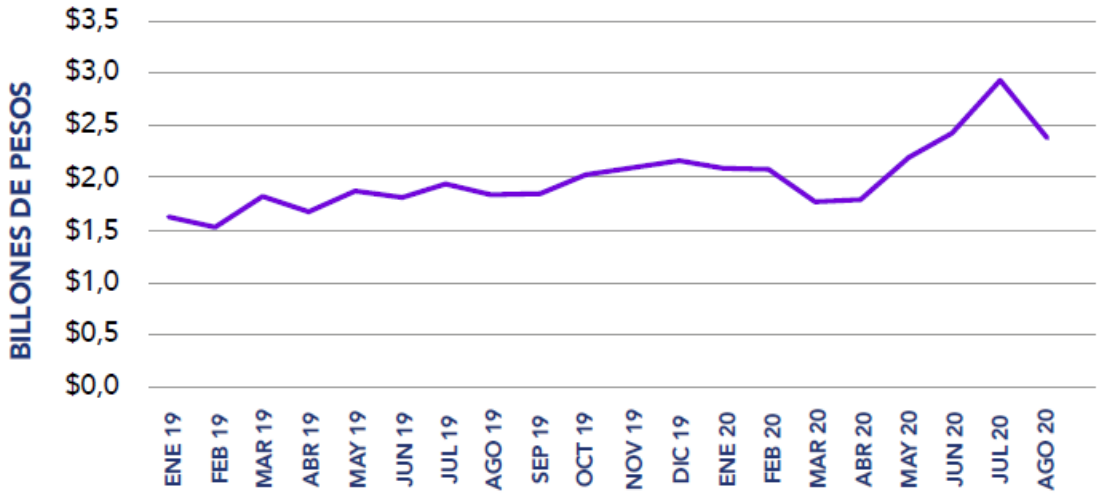
5.2 EVALUACIÓN DE LAS TRANSACCIONES EN EL E-COMMERCE

Para evaluar la trazabilidad de las transacciones se evidencia en el informe de la Cámara Colombiana de Comercio Electrónico[21] en la cual se muestra el aumento paulatino de las transacciones realizadas en el E-commerce durante los años 2019 y hasta agosto del 2020 tanto en ventas como en número de transacciones.

[20] Colaboradores de la investigación, SOTI. (2021, Marzo 21). Akamai. Análisis de la nueva era de la seguridad de la información. U.S. [Consulta 15 de Marzo de 2021]. Disponible en: https://www.akamai.com/es/es/multimedia/documents/state-of-the-internet/soti-security-research-adapting-to-the-unpredictable-report-2021.pdf

[21] Cámara Colombiana de Comercio Electrónico. (2021, Abril 08). Comportamiento del E-commerce en Colombia Durante el 2020. Colombia. [Consulta 20 de Mayo de 2021] Disponible en: https://www.ccce.org.co/gestion_gremial/informe-el-comercio-electronico-en-2020-y-perspectivas-2021/

Figura 1. ***Ventas a través del E-commerce***



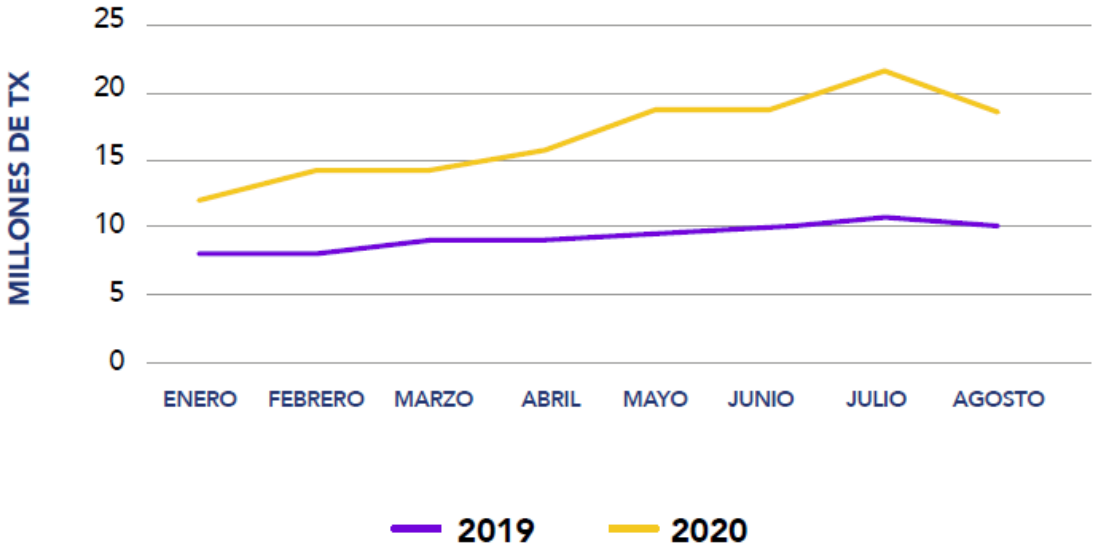
Nota. Fuente: Cámara Colombiana de Comercio Electrónico. (2021, abril 08). Comportamiento del E-commerce en Colombia Durante el 2020. Disponible en: **https://www.ccce.org.co/gestion_gremial/informe-el-comercio-electronico-en-2020-y-perspectivas-2021/**

Se puede evidenciar que durante el año 2019 las ventas crecieron un promedio mensual de 2,74% y para el año 2020 de enero a agosto el promedio mensual fue de 1,9%, esto hace referencia a que, si en el periodo del 2020 fue menor, se compensa entre abril y julio con un aumento significativo del 65,7%.

Aunque se obtuvieron meses con caída en las ventas como en febrero y agosto de 2020 el crecimiento fue siempre acelerado aumentando las mismas.

Realizando un análisis del mismo periodo, pero analizando el número de las transacciones se obtiene:

Figura 2. ***Transacciones a través del E-commerce***



Nota. Fuente: Cámara Colombiana de Comercio Electrónico. (2021, abril 08). Comportamiento del E-commerce en Colombia Durante el 2020. Disponible en: https://www.ccce.org.co/gestion_gremial/informe-el-comercio-electronico-en-2020-y-perspectivas-2021/

Se evidencia un comportamiento exponencial creciendo para enero de 2020 un 52,2%, para julio un 100,4% y en agosto un 78,8% con respecto al 2019.

Es de conocimiento que la pandemia del Covid-19 en Colombia y el resto del mundo se aplicaron medidas de prevención y distanciamiento que tuvo un impacto negativo en el comercio, pero las campañas del día sin IVA y las cuarentenas han contribuido al aumento del E-commerce en Colombia que se traduce en el aumento del PIB incentivando a las empresas al emprendimiento y a aplicar la tecnología de la información.

Según la Cámara de Colombiana de Comercio Electrónico se espera que para el año 2021 se termine con un crecimiento del 16% respecto al 2020.

También según un artículo de la revista semana[22] donde explican la consolidación de las transacciones virtuales en el país dice “El consumidor colombiano ya incorpora el comercio electrónico dentro de sus decisiones de consumo. Esto se evidencia no solamente en el crecimiento, ya que las ventas alcanzaron cerca de $10 billones, sino también en la reducción del tiquete promedio, que en enero de 2021 era de $123.000. Eso quiere decir que los bienes que se compran en línea son cada vez más cotidianos”, afirmó María Fernanda Quiñones, presidenta de la CCCE.

En el primer semestre del 2021 la Ministra de Educación que en su momento era Karen Abudinen estuvieron en un dialogo sobre comercio digital en Colombia realizado por la Agencia de los Estados Unidos para el Desarrollo (USAID) donde exponían los retos y avances que presenta al país en materia de digitalización[23].

En esa conferencia estuvieron María Fernanda Quiñones, presidenta ejecutiva de la Ccce, Marcos Pueyrredon, presidente de eCommerce Institute, además de Larry Sacks, director de la Misión USAID Colombia.

Se resaltó que las transacciones pasaron de 201 millones a 405 millones de transacciones y que mejoró notablemente la conectividad en los hogares colombianos realizando aproximadamente 3000 nuevas conexiones diarias.

[22] S. (2021e, agosto 20). Transacciones virtuales aumentaron 72 % en el segundo trimestre de 2021. Semana.com Últimas Noticias de Colombia y el Mundo. Disponible en: https://www.semana.com/economia/tecnologia/articulo/transacciones-virtuales-aumentaron-72-en-el-segundo-trimestre-de-2021/202121/

[23] Colombia aumentó 44 % sus ventas en línea durante el primer trimestre de 2021: Karen Abudinen, ministra TIC. (2021, 28 julio). MINTIC Colombia. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/178698:Colombia-aumento-44-sus-ventas-en-linea-durante-el-primer-trimestre-de-2021-Karen-Abudinen-ministra-TIC

Adicionalmente en un estudio realizado por Euromonitor International y que fue desarrollado para Google sobre el futuro del retail en Colombia[24].

En la siguiente imagen se puede analizar lo siguiente:

[24] E-commerce in Colombia. (2020). Euromonitor. Disponible en: https://www.euromonitor.com/E-commerce-in-colombia/report

Figura 3. ***Futuro del Retail y el Comercio Electrónico***

Nota. Fuente: Editorial La República S.A.S. (2021a, abril 16). Comercio electrónico creció 11% por semana en los días más críticos de la cuarentena. Diario La República. Disponible en: https://www.larepublica.co/internet-economy/E-commerce-en-colombia-crecio-11-por-semana-durante-el-primer-ano-de-pandemia-3154941

Se puede identificar que el futuro de las ventas va ligado con la posibilidad de adquirir diferentes bienes y servicios a través del mundo on-line. En el 2020 el E-commerce creció y 53% en Colombia y según el estudio se espera que en el año 2025 se encuentre en un 74%.

“No es un secreto que la tecnología se aceleró en el último año y medio a nivel global; esta forma permanente en la que los negocios se relacionan con los usuarios y consumidores, sumado al cambio del comportamiento de los mismos, inclusive en la forma en la que se trabaja, ha despertado toda oportunidad de aceleración de la transformación digital; Latinoamérica y Colombia no son ajenos a esta realidad”, aseguró Juan Restrepo, líder del segmento Retail en Google Colombia.

“El comercio electrónico en el país seguirá siendo una palanca muy importante de cara al futuro y, en el corto plazo, es un dinamizador súper relevante para la reactivación económica en el país. Colombia tiene una gran oportunidad de fortalecer los eventos de activación de ventas que son puros del comercio electrónico como pueden ser los Cyberlunes, Hotsale y BlackFriday”, complementó el ejecutivo de Google.

Para Daniel Enríquez Delgado, fundador y director de Estrategias Impacta, estas proyecciones se acomodan a la nueva realidad que trajo el covid-19.

“Antes de la pandemia no eran muchas las empresas que estaban dedicadas a esta actividad y ven ahora en el comercio electrónico una oportunidad; se vieron obligadas a mirar nuevas formas de distribución y entendieron que no es costoso acceder a plataformas electrónicas. La diversificación de plataformas ha llevado a que se aventuren más empresas a participar del E-commerce”, comentó.[25]

[25] Editorial La República S.A.S. (2021a, abril 16). Comercio electrónico creció 11% por semana en los días más críticos de la cuarentena. Diario La República. Disponible en: https://www.larepublica.co/internet-economy/E-commerce-en-colombia-crecio-11-por-semana-durante-el-primer-ano-de-pandemia-3154941

A medida que las transacciones van en aumento los delitos informáticos también, según los datos del Centro Cibernético de la Policía Nacional[26] en el año 2019 se registraron más de 17.000 casos denunciados como infracciones a la ley 1273 del 2009, esto corresponde al 57% del total de denuncias realizadas por los usuarios víctimas de la Ciberdelincuencia.

Los incidentes más reportados en Colombia siguen siendo los casos de Phishing con un 42%, la suplantación de identidad 28%, el envío de Malware 14% y los fraudes en E-commerce 16%.
Según el informe de Tendencias del Cibercrimen en Colombia 2019-2020 emitido por la Policía Nacional muestra que los delitos informáticos se concentra en las ciudades principales como Bogotá, Medellín, Cali, Barranquilla y Bucaramanga.

Al centrarse en las ciudades con mayor densidad de población y desarrollo económico influye en los objetivos de los Ciberdelincuentes que se enfocan en atacar las PYMES y según el informe “el 60% de las pequeñas y medianas empresas no pueden sostener sus negocios por más de 6 meses luego de sufrir un ciberataque importante. Esto demuestra que los factores entorno a los Ciberataques a las PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías”[27].

El comercio electrónico ha tomado un papel protagónico en los últimos dos años, pues ha sido la respuesta de muchas empresas y emprendimientos a las limitaciones que ha traído la pandemia.

---

[26] Policía Nacional de Colombia. (2019, Octubre 20). Centro Cibernético Policial. Colombia. [Consulta 15 de Marzo de 2021]. Disponible en: https://caivirtual.policia.gov.co/#ciberseguridad

[27] Policía Nacional de Colombia. (2019, Octubre 20). Colombia. [Consulta 15 de Marzo de 2021]. Centro Cibernético Policial. Disponible en: https://caivirtual.policia.gov.co/#ciberseguridad

En la Evaluación del comercio Electrónico se puede destacar lo siguiente:

- La conectividad es la base del E-commerce.
- El crecimiento en transacciones es exponencial y continuara en aumento por lo menos en 5 años más.
- Para la reactivación económica se encamina en prestar nuevas, seguras y mejores posibilidades de realizar pagos electrónicos.
- El crecimiento de los delitos Cibernéticos es una señal de alerta para blindar los sistemas de información y las transacciones realizadas en el E-commerce.
- La educación en el manejo de la seguridad y protección de los datos es fundamental.

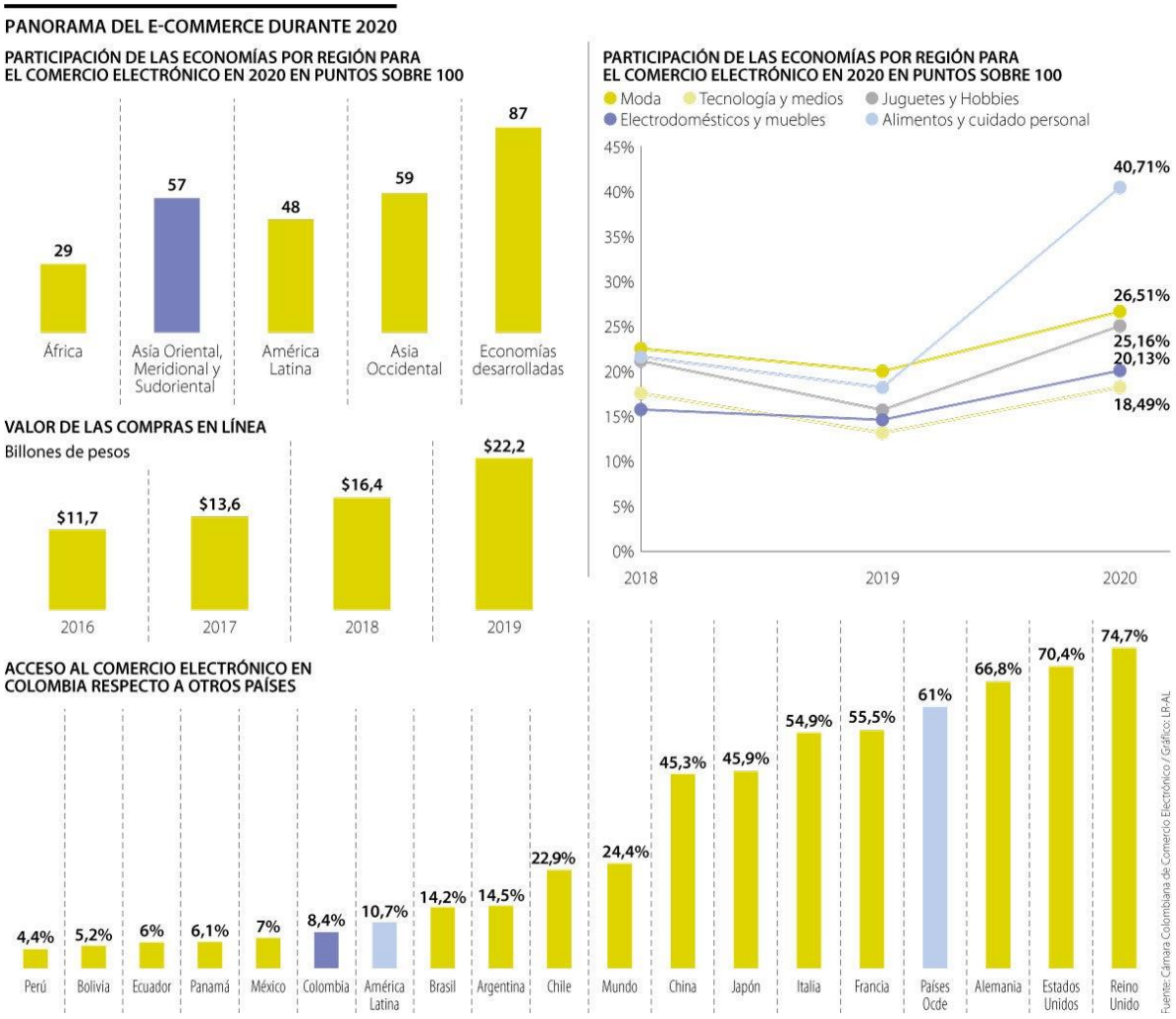
Se puede concluir que el aumento de las transacciones hizo que se consolidara el ECommerce en Colombia haciendo que se puedan incluir bienes y servicios de todo tipo satisfaciendo la demanda y ayudando en la economía del país.

5.3 RIESGOS Y AMENAZAS DURANTE LA PANDEMIA

Para el año 2020 la Cámara Colombiana de Comercio Electrónico mostro un informe publicado por el Diario la Republica[28] en el que se incrementó el E-commerce aproximadamente un 11% semanal en los momentos más difíciles de la cuarentena.

[28] Editorial La República S.A.S. (2021, 16 abril). Comercio electrónico creció 11% por semana en los días más críticos de la cuarentena. Diario La República. Colombia. [Consulta 15 de Marzo de 2021]. Disponible en: https://www.larepublica.co/internet-economy/E-commerce-en-colombia-crecio-11-por-semana-durante-el-primer-ano-de-pandemia-3154941

Figura 4. ***Panorama del E-commerce***



Nota. Fuente: Cámara Colombiana de Comercio Electrónico. (2021, abril 08). Comportamiento del E-commerce en Colombia Durante el 2020. Disponible en: https://www.ccce.org.co/gestion_gremial/informe-el-comercio-electronico-en-2020-y-perspectivas-2021/

En el informe se puede identificar que el sector del comercio electrónico se consolido para satisfacer las necesidades y ayudar en la economía, se muestra un incremento en ventas del 31% donde logra pasar los 22,3 Billones, y un crecimiento en las transacciones del 86% con 119 millones de transacciones en línea en lo corrido del año 2020.

De los riesgos identificados se encuentran los indicados por María Fernanda Quiñones, presidenta de la Cámara Colombiana de Comercio Electrónico[29], advirtió que para que el crecimiento del E-commerce o comercio online sea sostenido este año “se debe mejorar la confianza del consumidor a la hora de hacer transacciones digitales” partiendo de la protección de los datos personales y las buenas prácticas en el uso digital.

Dentro del auge del comercio electrónico, son demasiadas las consecuencias que se consideran a que el E-commerce genere cierta inseguridad e incertidumbre a los usuarios, por eso es necesario se apliquen las medidas pertinentes para mitigar los riesgos, para los comercios electrónicos con categoría B2C (Negocios hacia Consumidores) se encuentran con mayores riesgos de afectación, estos riesgos son[30]:

5.3.1 Penetración banda ancha

Actualmente la banda ancha es una infraestructura esencial de cualquier economía moderna, tan importante como las redes de transporte, la electricidad entre otros. En el comercio electrónico no contar con banda ancha sería un riesgo para las empresas, pues los usuarios al no tenerla se convertirían en un obstáculo para visitar los portales.

[29] A. (2021a). Prueba Slider. Cámara Colombiana de Comercio Electrónico. Colombia. [Consulta 20 de Mayo de 2021]. Disponible en: https://www.ccce.org.co/

[30] ARANGO, L. F. (2013). COMERCIO ELECTRÓNICO, LOS RIESGOS QUE ENFRENTA AMERICA LATINA PARA SU MASIFICACIÓN. Biblioteca Digital Universidad de San Buenaventura. Colombia. [Consulta 20 de Mayo de 2021]. Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/2598/1/Comercio_Electronico_Riesgos_Arango_2013.pdf

5.3.2 Competencia

En el mundo físico y en el mundo on-line siempre existirán las competencias. En el mundo virtual cada vez hay más empresas lo que se convierte en una amenaza para las compañías existentes.

5.3.3 Miedo de los consumidores

Muchas personas prefieren comprar en almacenes físicos que en sitios web, lo que se convierte en un riesgo para las empresas del comercio electrónico ya que muchas personas dejan de visitar los portales por miedo a que vulneren su información mediante delitos informáticos.

5.3.4 Falta de contacto físico con el producto

Al ser una compra virtual el consumidor no tiene contacto con el producto generando cierto grado de incertidumbre en él, y más cuando el usuario es primerizo en compras online lo que influye en la decisión de compra.

5.3.5 Problemas de distribución

Problemas o alteraciones de las condiciones por parte de las empresas que distribuyen y transportan los productos vendidos.

5.3.6 Reclamación y devoluciones

La principal problemática en las compras a través de la Red es que el producto o servicio adquirido no responda a lo que se ofrecía en Internet. La inseguridad de a quién dirigirse en caso de reclamación es otro de los problemas que conlleva el comercio electrónico. Además, cuando se hacen transacciones comerciales por medio de internet las partes involucradas pueden estar expuestas amenazas como

5.3.7 Phishing

Es una modalidad de estafa, con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjetas de crédito etc. Proviene de la

palabra inglesa (pesca) y hace alusión al intento que los usuarios "muerdan el anzuelo", es uno de los términos más utilizados por delincuentes para estafar y obtener información confidencial.

En el Owasp top 10 es la causa número A07 en la cual advierte sobre el proceso de autenticación, también aplica a fallos en los desarrollos con el número A04.

A07:2021: Fallos de identificación y autenticación. Aplicación errada de la seguridad en ingreso de las aplicaciones.

A04:2021: Diseño inseguro, refiere a los defectos en los diseños y arquitecturas manejadas en los desarrollos.

5.3.8 Spoofing

Se refiere a la falsificación de unos datos, modificándolos de algún modo para obtener por ello un beneficio. Los ataques de seguridad en las redes a través de técnicas de spoofing ponen en riesgo la privacidad de los usuarios que navegan por Internet, así como la integridad de sus datos.

En el Owasp top 10 es la causa número A01 en la cual advierte sobre los permisos de control de acceso.

A01:2021: Control de acceso roto, se convierte en la principal causa de amenaza.

5.3.9 Pharming

En este tipo de ataque, los delincuentes redireccionan a sus víctimas a páginas web falsas utilizando varios métodos, como por ejemplo correos electrónicos con asuntos llamativos para que las víctimas los abran y sean atacadas; poniendo en peligro información privada.

La técnica de pharming opera para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, de igual apariencia, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

En el Owasp top 10 es la causa número A04 en la cual advierte sobre el mal diseño de sitios. También aplica al numeral A06 ya que permite vulnerabilidades para copiar sitios.

A04:2021: Diseño inseguro, refiere a los defectos en los diseños y arquitecturas manejadas en los desarrollos.

A06:2021: Componentes vulnerables y desactualizados, aplica a los componentes, plugins, frameworks y otros módulos de software que se ejecutan dentro de la aplicación.

5.3.10 Amenazas OWASP TOP 10[31]

Continuando con el proyecto abierto OWASP en su actualización del 2021 orienta para minimizar los riesgos desde el desarrollo de aplicaciones, completando el Top 10 se encuentran:

A02:2021: Fallas criptográficas, aduce a las fallas relacionadas con la criptografía que constantemente llevan a la exposición de datos confidenciales o al compromiso del sistema.

A03:2021: Inyección, fallos en la Inyección tales como SQL, Sistema Operativo y LDAP. Cross-site Scripting ahora es parte de esta categoría en esta edición.

[31] OWASP Top 10:2021. (2021). Owasp Top 10 - 2021. Disponible en: https://owasp.org/Top10/

A05:2021: La configuración incorrecta de seguridad, revisión para detectar algún tipo de error de configuración.

A08:2021: Fallas en la integridad de datos y software, se enfoca en hacer suposiciones relacionadas con actualizaciones de software, datos críticos y canalizaciones de CI/CD sin verificar la integridad.

A09:2021: Fallas de registro y monitoreo de seguridad, pueden afectar directamente la visibilidad, las alertas de incidentes y el análisis forense.

A10: 2021: Falsificación de solicitudes del lado del servidor, es un ataque al sitio del servidor que conduce a la divulgación de la información confidencial.

Con el aumento de E-commerce aumentaron los riesgos y amenazas tanto para las empresas como para el consumidor en el momento de realizar las transacciones digitales, por eso es de inmediato proceder que se tomen las medidas necesarias para la mitigación de los riesgos y el bloqueo de nuevas amenazas.

5.4 PROPUESTA DE UN PLAN PARA LA MITIGACION DE RIESGOS GENERADOS A PARTIR DE LA PANDEMIA EN COLOMBIA DESDE EL 2020-2021 HACIA LA REACTIVACIÓN DEL E-COMMERCE

Para obtener los resultados que requieren que las pequeñas y medianas empresas en el cumplimiento de la seguridad en las transacciones electrónicas se propone un plan que abarque las medidas necesarias para que todos los actores se fortalezcan en el E-commerce y se logre una reactivación económica en Colombia que mantenga la confianza en el comercio.

El plan de mitigación contiene 3 pasos:

- La implementación de un plan de seguridad para las Pymes.
- Adoptar unas normas de seguridad estándar para los sistemas de las empresas.
- Crear una estrategia de concienciación para capacitar e informar a todos los actores que intervienen en una transacción electrónica.

5.4.1 Plan de Seguridad del Ministerio de las TIC

Se propone una metodología para la implementación que contribuya a la mitigación de los riesgos del E-commerce en las pymes.

Se propone el estándar Internacional ISO31000 el cual se adapta a cualquier tipo de organización y aplicaría a las pequeñas y medianas empresas.

Entre sus beneficios están:

- La organización aumenta sus probabilidades de alcanzar las metas propuestas.
- Permite el cumplimiento de requisitos legales en varias áreas.
- Mejora el conocimiento en administración.
- Protege los recursos de la organización.
- Aumenta la eficacia y la eficiencia operativa de la organización.

En específico para la implementación de un modelo de seguridad que permita a las empresas que puedan ofrecer sus servicios y que el usuario pueda sentirse seguro para realizar las transacciones y que concluya con un mejoramiento en la calidad de la seguridad, se sugiere el Modelo de Seguridad y Privacidad de la Información (MSPI) el cual tiene las siguientes características:

- Se mantiene actualizado periódicamente.

- Reúne las pautas y cambios técnicos de la norma ISO27001 del 2013.
- Legislación de la Ley de protección de datos personales.
- Transparencia y acceso a la información.
- Cuenta con guías anexas detalladas para la ayuda de las entidades a cumplir con lo solicitado.

Este modelo es publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC[32] se encuentra dirigido a las empresas del sector público, pero puede ser implementado en cualquier empresa.

El MSPI conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información permitiendo garantizar la privacidad de los datos aplicando procesos de gestión del riesgo logrando así la confianza entre las partes interesadas que para el caso es el comercio y los clientes.

Para la implementación del MSPI aplicado a las PYMES se deben adoptar adecuadamente el modelo de seguridad y privacidad de la información según las necesidades de cada empresa, pero se pude tener una guía de ruta la cual conduce hacia el mismo objetivo.

Se plantean las siguientes acciones como pasos a seguir para la implementación de un modelo de SGSI[33]:

1. Definición de un Líder Oficial de Seguridad de la Información y empoderamiento.
    1.1. Definición de Responsabilidades.

[32] Modelo de Seguridad - Fortalecimiento TI. (2018). Modelo de Seguridad. Disponible en: https://mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

[33] ALTA CONSEJERIA DISTRITAL TIC. (2017, 3 agosto). Implementación de la Estrategia del MSPI. Disponible en: https://tic.bogota.gov.co/

2. Garantizar el compromiso de la alta dirección.

3. Determinar la política y alcances de la seguridad de la información.

    3.1. Objetivos y metas lo más concretos posible en materia de seguridad

4. Definir el estado actual de la información.

    4.1. Definir el estado de madurez de los controles existentes.

    4.2. Determinación de los procesos y procedimientos

5. Definir el método para evaluar los riesgos.

    5.1. Recursos a utilizar y activos a evaluar

    5.2. Definir accione y objetivos para gestionar los riesgos

    5.3. Identificar, analizar y evaluar los riesgos

6. Análisis de vulnerabilidades.

7. Procedimientos de seguridad y privacidad de la información.

8. Integración del Modelo de Seguridad y Privacidad de la Información (MSPI) con el sistema de gestión documental de la entidad.

9. Plan de comunicaciones.

10. Medición de indicadores de gestión.

11. Plan de transición de ipv4 a ipv6.

12. Auditoría interna, revisión del proceso y mejoras continuas.

5.4.1.1 Estrategias De Seguridad Digital

Como ya conocieron la importancia de la seguridad en el E-commerce es necesaria la implementación de medidas eficaces puesto que cada vez son más los comercios y empresas online conscientes de su valor.

Con el auge del aumento en las transacciones, la inversión de esas empresas en ciberseguridad continuara su dinámica de crecimiento casi en la misma línea de las amenazas digitales.

Para esto se disponen de las estrategias para adoptar, adicionales al plan de mitigación de riesgos propuesto:

5.4.1.2 Instalar Protocolos Https

Estos protocolos han incrementado su popularidad en los últimos años, frente a los tradicionales HTTP, más vulnerables que los HTTPS.

El protocolo HTTPS se ha utilizado normalmente en partes del sitio web destinadas a los pagos, debido a la necesidad de blindar la información de clientes y empresas.

En la actualidad el uso de estos protocolos se ha generalizado. Ahora son necesarios en la totalidad del sitio web, lo que ha condenado a los antiguos protocolos HTTP al aislamiento, por así decirlo.

De forma paralela a estos protocolos, también resulta indispensable la instalación de certificados SSL (secure sockets layer), responsables de proteger los datos en tránsito durante el proceso de pago.

Además, la instalación de servidores HTTPS influye positivamente en la confianza de los usuarios durante la navegación.

Esto se debe a que los navegadores muestran un candado y un texto verde junto a la URL indicando que el sitio web utiliza HTTPS y certificados SSL[34].

De esta forma los clientes saben que sus datos son debidamente encriptados y protegidos.

También se conoce que Google y otros buscadores dan prioridad a los E-commerce con protocolos HTTPS frente a los HTTP.

5.4.1.3 Implementa Sistemas De Verificación Cvv Y Avs

El procesamiento de pagos es uno de los aspectos más delicados de la ciberseguridad de E-commerce. Las empresas deben extremar la precaución, sobre todo cuando intervienen tarjetas de crédito o de débito.

Requerir el código CVV (Card Verification Value)[35] es una práctica muy recomendable:

- Incrementan la seguridad en los pagos online. Exigir códigos CVV hace que sea mucho más difícil procesar una transacción fraudulenta. Los ciberdelincuentes pueden haber robado un número de tarjeta de crédito, pero no la tarjeta física.

[34] Adeva, R. (2021, 28 abril). ¿Tu web no tiene HTTPS? Cómo instalar el certificado SSL. ADSLZone. Disponible en: https://www.adslzone.net/como-se-hace/internet/web-certificado-https/

[35] Consideraciones de seguridad para tu comercio electrónico. (2021, 12 abril). INCIBE. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/consideraciones-seguridad-tu-comercio-electronico

- Tener un buen escudo para frenar transacciones fraudulentas es utilizar un AVS (Address Verification System). Este sistema permite diferenciar las transacciones fraudulentas de las legítimas[36].

Aunque no es infalible, su funcionamiento es simple y permite mejorar la ciberseguridad en los pagos.

5.4.1.4 Realizar Backups Periódicos

Esta es otra de las estrategias de seguridad en comercio electrónico más eficaces y que tengan políticas de copias de seguridad para las PYMES[37].

Basta con instalar UpdraftPlus, BackupBuddy, BoldGrid Backup, BackWPup y otros plugins de seguridad y realizar copias periódicas de las bases de datos del E-commerce.

Es extremadamente importante realizar copias de seguridad periódicas de los datos de su sitio. Entre las grandes amenazas al E-commerce no destacan únicamente los malwares o el phishing. También está el error humano.

Si bien hay formas de hacer una copia de seguridad manual de sus datos, es fácil olvidarse o dejar de hacerlo de manera tan sistemática.

---

[36] What is AVS (Address Verification Service). (2017, 29 agosto). Verifi. Disponible en: https://www.verifi.com/chargebacks-disputes-faq/what-is-address-verification-service-avs/

[37] Políticas de Seguridad para las PYME. (2021, 12 abril). Instituto Nacional de Ciberseguridad. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/copias-seguridad.pdf

En consecuencia, el uso de plugins y herramientas de backups es obligado para blindar las bases de datos y toda la información sensible del E-commerce adicional a las políticas de la empresa o comercio.

5.4.1.5 Uso De Seguridad Multicapa O Multi-Layered

Por seguridad multicapa se entiende el uso de diferentes medidas, como la instalación de un firewall, que ofrece una defensa inicial contra las Ciber-amenazas.

Pero, además usar un CDN (content delivery network) permite añadir una capa extra de seguridad, ya que este sistema diversifica las copias de datos en varios puntos geográficos.

Esta medida también es útil para prevenir los ataques DDoS (denial-of-service attack). Esta es una de las estrategias de seguridad en comercio electrónico más importantes[38].

5.4.1.6 Realizar Un Monitoreo De Las Transacciones

Se requiere configurar alertas para movimientos sospechosos en las transacciones que sean eficientes por la cantidad de movimientos realizados.

Uno de los más populares es bloquear una transacción cuando las direcciones de facturación y de envío no coincidan. Esta es una anomalía que podría esconder algún tipo de fraude o robo de tarjetas de crédito.

[38] AlfredoECN. (2019a, abril 26). Estrategias de seguridad en comercio electrónico. ECN | E-commerce Nation • 1a Comunidad Global sobre E-commerce. Disponible en: https://www.ecommerce-nation.es/cuales-son-las-mejores-estrategias-de-seguridad-en-comercio-electronico/

5.4.1.7 Evita Almacenar Información De Tarjetas De Crédito/Débito

La mejor forma que evitar filtraciones de información de tarjetas de crédito y de débito es no almacenándolas.

En la actualidad, el almacenamiento violaría las reglas establecidas en los estándares PCI.

Y es que la pérdida de esta información no sólo compromete la reputación de los usuarios de un E-commerce, también pone en jaque a las entidades y empresas financieras.

Una excelente alternativa es utilizar pasarelas de pago como Wompi, PayU o PSE, entre otras.

De esta forma la información sensible será responsabilidad de estas plataformas, quienes además disponen de mejores protocolos de seguridad que un E-commerce convencional[39].

5.4.2 Plan de Gestión de Incidentes

Un plan de gestión de incidentes es una estrategia para manejar ordenadamente un incidente de seguridad que se presente en una red.

Este plan da una guía para las personas encargadas del área de tecnología donde pueden detectar, reportar, evaluar, responder, recuperarse y aprender frente a un incidente de seguridad de la información.

---

[39] Información de tarjetas bancarias. (2021, 12 abril). INCIBE. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/si-manejas-informacion-tarjetas-bancarias-este-articulo-te-interesa

Cada entidad puede crear su plan de gestión de incidentes de seguridad de la información y se recomienda que tenga al menos la siguiente estructura:

• Planificación y preparación para la gestión del Incidente
• Detección y análisis.
• Contención, erradicación y recuperación.
• Actividades Post-Incidente.

5.4.3 Estrategia De Concientización De La Seguridad Informática

Un plan de concientización de la seguridad informática es un programa formal para capacitar al personal e informar a todos los que intervienen en el sistema de como mitigar y evitar situaciones que ponen en riesgo la información.

Estrategia para usuarios:

Se catalogan como usuarios a cualquier persona que utilice los sistemas para adquirir o prestar un servicio o un producto del E-commerce. En Ciberseguridad las personas son el punto débil del proceso, la única defensa conocida para los ataques de ingeniería social es un programa o estrategia efectiva que genere conciencia en la seguridad de la información.

Para lograr esa estrategia se deben apoyar en la guía que publicó la [40] *Creación de un programa de capacitación y concientización sobre la seguridad de la tecnología de la información* en donde cubre las principales áreas y sigue los siguientes pasos:

a. Identificar las necesidades de sensibilización y formación de la organización.
b. Planificación y diseño del programa de sensibilización y formación.

[40] SP 800–50 Rev. 1 (Draft), Building a Cyber and Privacy Awareness and Training Program | CSRC. (2021, 21 septiembre). NIST. CENTRO DE RECURSOS DE SEGURIDAD INFORMATICA. https://csrc.nist.gov/publications/detail/sp/800-50/rev-1/draft

c. Desarrollar los materiales de concientización y capacitación.
d. Implementación del contenido del programa.
e. Evaluación posterior a la implementación.

El seguimiento de la guía permite la concientización del personal y concluye con un mejoramiento continuo para los procesos de Seguridad de la Información.

En conclusión, se requiere implementar una metodología internacional, un modelo de seguridad y confidencialidad de la información, mitigar los riesgos con estrategias de tecnología que estén a la vanguardia del crecimiento del ECommerce y un plan para fomentar la educación de la seguridad informática en los usuarios.

6 CONCLUSIONES

En el presente trabajo se estable un panorama actual de la seguridad digital en las pequeñas y medianas empresas durante el Covid-19.

Con el análisis realizado de las diferentes normativas y estrategias de seguridad digital se puede concluir que se tienen buenas bases para la identificación y procesamiento de delitos cibernéticos en Colombia, ya que fueron pioneros en adoptar estrategias de Ciberseguridad en América Latina, además de las herramientas que ya se encuentran implementadas en empresas del estado mitigando las vulnerabilidades y amenazas que se evidencian y que continúan en crecimiento.

Con la información de los últimos años la Ciberseguridad se convierte en un pilar importante para el crecimiento de las organizaciones y su protección frente a las vulnerabilidades, ataques o fuga de la información para que siempre garantice la disponibilidad, integridad y confidencialidad de los datos.

Se identifica que con el aumento de las transacciones aumentaron los riesgos y más con el confinamiento generado por el COVID-19 en Colombia, pero también se identificaron nuevos conocimientos y mejores herramientas de mitigación para estas amenazas proporcionando a los usuarios mayor confianza y tranquilidad al momento de realizar transacciones en el comercio electrónico.

Se establece con la evaluación de las transacciones que se puede tener una comprensión del auge en el comercio electrónico para reconocer las próximas oportunidades. El E-commerce ofrece distintas ventajas para las Pymes y comercios reduciendo costos y generando ganancias. Para los usuarios evita las

aglomeraciones, compras más rápidas, comodidad a la hora de adquirir productos, esto conlleva a asumir responsabilidades de cuidado frente a la pandemia.

Se identifica que el apoyo y compromiso de la alta gerencia en las compañías es de vital importancia al desarrollo de los procesos de gestión en seguridad informática.

Se plantean los temores y falta de acceso de los usuarios frente al E-commerce donde se ha generado un cambio cultural para la utilización de las transacciones electrónicas y ya no es tan desconocido el ámbito de transacciones electrónicas.

Se concluye de manera precisa la metodología a implementar y estrategias a utilizar para mitigar las amenazas y crear confianza con el aumento de las transacciones en el E-commerce.

Se concluye como fundamental para el mejoramiento de una implementación del plan de riesgos para el E-commerce la capacitación de los usuarios, sensibilizándolos acerca de las amenazas y vulnerabilidades a los que se exponen y que pueden tener un gran impacto en la organización.

7 RECOMENDACIONES

Realizar actividades educativas que busquen en los usuarios un mayor acercamiento a las nuevas tecnologías, como conocimiento de las plataformas, enseñar características prevalentes de sus portales evitando que ingresen a páginas fraudulentas, certificar los portales como lugares seguros y con políticas de seguridad tanto para las Pymes como a los comercios en general.

Los usuarios también deben culturizarse en el ámbito de las transacciones, como no realizar transacciones en el E-commerce en dispositivos públicos, generar conciencia de su información personal, conocer sus derechos y deberes al realizar transacciones.

El complemento educativo debe ser de fácil acceso para todos, con inclusión y siempre de frente a las nuevas tecnologías de la información.

Reforzar y avanzar en proveer de acceso a toda la población, proveyéndola de herramientas tecnológicas y de educación para que la masa de usuarios siga aumentado y así mismo la reactivación económica.

Aplicar la propuesta de un plan de gestión de riesgos para E-commerce para que pueda ser implementado en las pequeñas y medianas empresas a partir de la reactivación en Colombia. Tener presente que la inversión de las empresas en su Ciberseguridad es de gran impacto y no debe tomarse a la ligera.

Siempre se debe contar con un plan de respuesta de incidentes de Ciberseguridad en las empresas, este plan debe tener unos principios de detección y registro del problema, análisis y evaluación, notificación y plan de mejora.

8 BIBLIOGRAFÍA

A. Prueba Slider. Cámara Colombiana de Comercio Electrónico. {En línea}. (2021). Disponible en: https://www.ccce.org.co/

Agencia de EE. UU. para el Desarrollo Internacional | USAGov. Agencia de EE. UU. para el Desarrollo Internacional. {En línea}. (2021) Disponible en: https://www.usa.gov/espanol/agencias-federales/agencia-de-ee-uu-para-el-desarrollointernacional#:%7E:text=La%20Agencia%20de%20EE.,y%20humanitaria%20en%20el%20mundo.

ALTA CONSEJERIA DISTRITAL TIC. Implementación de la Estrategia del MSPI. {En línea} (2017, 3 agosto). Disponible en: https://tic.bogota.gov.co/

ARANGO, L. F.. COMERCIO ELECTRÓNICO, LOS RIESGOS QUE ENFRENTA AMERICA LATINA PARA SU MASIFICACIÓN. Biblioteca Digital Universidad de San Buenaventura. {En línea}. (2013). Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/2598/1/Comercio_Electronico_Riesgos_Arango_2013.pdf

Biblioguias: Gestión de datos de investigación: Estrategias para la seguridad de los datos. {En línea}. (2020, 18 diciembre). Gestión de Datos de Investigación. Disponible en: https://biblioguias.cepal.org/c.php?g=495473&p=4398100

Bienvenidos a eCommerce Institute | De Latinoamérica al Mundo. {En línea}. (2021, 19 noviembre). eCommerce Institute | Empowering the Global Digital Ecosystem. Disponible en: https://ecommerce.institute/

Cámara Colombiana de Comercio Electrónico. {En línea}. (2021, abril 08). Comportamiento del E-commerce en Colombia Durante el 2020. Disponible en: https://www.ccce.org.co/gestion_gremial/informe-el-comercio-electronico-en-2020-y-perspectivas-2021/

Campos Ramírez, J. F. SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO COLOMBIANO. Seguridad de la Información. {En línea}. Septiembre de 2021. Disponible en, de http://polux.unipiloto.edu.co:8080/00002657.pdf

Ciberseguridad. {En línea}. (2021). Disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html#ciberseguridad

Colombia aumentó 44 % sus ventas en línea durante el primer trimestre de 2021: Karen Abudinen, ministra TIC. {En línea}. (2021, 28 julio). MINTIC Colombia. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/178698:Colombia-aumento-44-sus-ventas-en-linea-durante-el-primer-trimestre-de-2021-Karen-Abudinen-ministra-TIC

DBIR. VERIZON. {En línea}. (2020). Disponible en: https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

Diario, E. N. (2014, 27 agosto). Gobierno y gestión de las tecnologías de la información. El Nuevo Diario. {En línea}. (2014, 27 agosto) Disponible en: https://www.elnuevodiario.com.ni/economia/328368-gobierno-gestion-tecnologias-informacion/#:%7E:text=El%20gobierno%20se%20encarga%20de,necesidades%20de%20las%20partes%20interesadas.&text=La%20gesti%C3%B3n%20se%20encarga%20de,por%20el%20cuerpo%20de%20gobierno.

E-commerce in Colombia. Euromonitor. {En línea}. (2020). Disponible en: https://www.euromonitor.com/E-commerce-in-colombia/report

Editorial La República S.A.S. Comercio electrónico creció 11% por semana en los días más críticos de la cuarentena. Diario La República. {En línea}. (2021, 16 abril). Disponible en: https://www.larepublica.co/internet-economy/E-commerce-en-colombia-crecio-11-por-semana-durante-el-primer-ano-de-pandemia-3154941

Editorial La República S.A.S.. La demanda de los servicios de ciberseguridad se incrementó 40% a nivel nacional. {En línea}. (2020, 31 julio) Disponible en: https://www.larepublica.co/internet-economy/la-demanda-de-los-servicios-de-ciberseguridad-se-incremento-40-a-nivel-nacional-3039341

El reto del E-commerce en Colombia en plena pandemia | Universidad El Bosque. {En línea}. (2020, 25 marzo). Disponible en: https://www.unbosque.edu.co/centro-informacion/noticias/el-reto-del-E-commerce-en-colombia-en-plena-pandemia

ESET. Welivesecurity.com. {En línea}. (2020, 12 02). Disponible en: https://www.welivesecurity.com/la-es/infographics/educacion-ciberseguridad-usuarios-mas-conscientes-de-importancia/

ESET.. Welivesecurity.com. From Apenas el 17% de las empresas implementa el doble factor de autenticación. {En línea}. (2020, 08 02) Disponible en: https://www.welivesecurity.com/la-es/2020/08/14/pocas-empresas-implementa-doble-factor-autenticacion/

Everything you need to know about cyber-security - Panda Security. Everything You Need to Know about Cyber-Security. {En línea}. (2022). Disponible en: https://www.pandasecurity.com/en/security-info/

General, A. Boletines de ciberseguridad Gamma CSOC-CERT. Gamma Ingenieros S.A.S. {En línea}. (2021, 26 enero). Disponible en: https://gammaingenieros.com/boletines-gamma-csoc-cert/

Gerentes, D. Y.¿Qué estrategias de seguridad son más eficaces frente a las ciberamenazas? Dir&Ge | Directivos y Gerentes. {En línea}. (2017, 9 octubre). Disponible en: https://directivosygerentes.es/innovacion/transformacion-digital/td-estrategia/estrategias-seguridad-eficaces

Goddijn, I. Risk Based Security. {En línea}. (2020). Disponible en: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Mid%20Year%20Data%20Breach%20QuickView%20Report.pdf

Gubern, A. Phishing y Email Spoofing: qué es, diferencias y cómo detectarlo | Servicios de Email Marketing. Agencia de Email Marketing. Servicios de Email Marketing. Agencia de Email Marketing | Email Marketing y Marketing Automation. {En línea}. (2021, 18 febrero). Disponible en: https://www.digitalresponse.es/blog/phishing-y-email-spoofing-que-es-diferencias-como-detectarlo/

Haran, Juan Manuel. Cibercriminales están utilizando el coronavirus como excusa para infectar a los usuarios. WeliveSecurity by ESET. {En línea}. (2020, 6 marzo). Disponible en: https://www.welivesecurity.com/la-es/2020/03/06/cibercriminales-utilizan-coronavirus-excusa-infectar-usuarios/

Haran, Juan Manuel. WeliveSecurity by ESET. Crecen las campañas de malware que intentan aprovechar el temor provocado por el COVID-19. {En línea}. (2020, 18 marzo). Disponible en: https://www.welivesecurity.com/la-es/2020/03/18/crecen-campanas-malware-aprovechar-temor-covid-19/

Harán, J. M. Welivesecurity.com by ESET. {En línea}. (2020, Agosto 14). Disponible en: https://www.welivesecurity.com/la-es/2020/08/14/pocas-empresas-implementa-doble-factor-autenticacion/

IBM Corporation. ibm.com. {En línea}. (2020, Julio). Disponible en: https://www.ibm.com/downloads/cas/RZAX14GX

Investigación, S. C. Akamai. Análisis de la nueva era de la seguridad de la información. {En línea}. (2021, marzo 21). Disponible en: https://www.akamai.com/es/es/multimedia/documents/state-of-the-internet/soti-security-research-adapting-to-the-unpredictable-report-2021.pdf

Jorge, L. EY Parthenon. {En línea}. (2020, diciembre 14). Disponible en: https://www.ey.com/es_co/strategy/panorama-de-los-servicios-financieros-en-latinoamerica

Judicial, R. En 2020 se profesionalizaron los delitos en la web y crecieron en un 84%. ELESPECTADOR.COM. {En línea}. (2020, 23 diciembre). Disponible en: https://www.elespectador.com/noticias/judicial/los-ciberdelitos-aumentaron-un-84-durante-2020-policia/

Kaspersky. Beware being breached: why data protection is vital for small businesses. AO Kaspersky Lab. {En línea}. (2021). Disponible en: https://www.kaspersky.com/blog/data-protection-for-smb/

Lacayo, J.¿Usamos más la banca digital? COVID-19 Financial Sector Perspective: el panorama de los servicios financieros en Latinoamérica. EY Parthenon. {En línea}. {En línea}. (2020, 14 diciembre). Disponible en: https://www.ey.com/es_co/strategy/panorama-de-los-servicios-financieros-en-latinoamerica

LatinPyme. PANORAMA DEL ESTADO ACTUAL DE LA CIBERSEGURIDAD: ESET. {En línea}. (2020, diciembre 23). Disponible en: https://www.latinpymes.com/panorama-del-estado-actual-de-la-ciberseguridad-eset/

Martínez Cortez, Fredy. Seguridad de la Información en pequeñas y medianas empresas (pymes). Universidad Piloto de Colombia. {En línea}. 2015. Disponible en: http://polux.unipiloto.edu.co:8080/00002332.pdf

Mendoza, Miguel Ángel. WeliveSecurity by ESET. 8 lecciones en materia de seguridad que el COVID-19 dejó a las organizaciones. {En línea}. (2020, 5 mayo). Disponible en: https://www.welivesecurity.com/la-es/2020/05/05/lecciones-seguridad-informatica-covid-19-dejo-organizaciones/

Miller, M. FBI sees spike in cyber-crime reports during coronavirus pandemic. TheHill. {En línea}. (2020, 16 Abril). Disponible en: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

MinTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital. MINTIC Colombia. {En línea}. (2021). Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/162626:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

Organization of American States & Inter American Development Bank. 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://www.iadb.org/es. {En línea}. (2020, 28 Julio). Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-

camino-a-seguir-en-america-latina-y-el-caribe

OWASP Top 10:2021. Owasp Top 10 - 2021. {En línea}. (2021). Disponible en: https://owasp.org/Top10/

Pérez, A. Seis estrategias para mejorar la ciberseguridad IoT de las compañías. KPMG Tendencias. {En línea}. (2018, 23 abril). Disponible en: https://www.tendencias.kpmg.es/2017/05/6-estrategias-para-mejorar-la-ciberseguridad-iot-de-las-companias/

Policía Nacional de Colombia. Centro Cibernético Policial. {En línea}. (2019, octubre 20). Disponible en: https://caivirtual.policia.gov.co/#ciberseguridad

Portafolio. Pandemia disparó las operaciones financieras. Portafolio.co. {En línea}. (2021, marzo 23). Disponible en: https://www.portafolio.co/economia/finanzas/pandemia-disparo-las-operaciones-financieras-550329

Portafolio. Uso de plataformas de banca digital aumentó en un 59% en la pandemia. Portafolio.co. {En línea}. (2021, marzo 1). Disponible en: https://www.portafolio.co/economia/en-colombia-el-uso-de-plataformas-de-banca-digital-aumento-en-un-59-durante-la-pandemia-549606

Ramos, M. Qué es el eCommerce: definición modelos y ventajas. Marketing 4 ECommerce - Tu revista de marketing online para E-commerce. {En línea}. (2020, 2 junio). Disponible en: https://marketing4ecommerce.mx/que-es-el-ecommerce/

Rodríguez, P. Análisis de riesgos informáticos y ciberseguridad. Ambit. {En línea}. (2020, 7 mayo).Disponible en: https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

S. Transacciones virtuales aumentaron 72 % en el segundo trimestre de 2021. Semana.com Últimas Noticias de Colombia y el Mundo. {En línea}. (2021, agosto 20). Disponible en: https://www.semana.com/economia/tecnologia/articulo/transacciones-virtuales-aumentaron-72-en-el-segundo-trimestre-de-2021/202121/

Software Advisory Service. Las 3 mejores estrategias de ciberseguridad para 2019. {En línea}. (2020). Disponible en: https://www.softwareadvisoryservice.com/es/blog/las-3-mejores-estrategias-de-ciberseguridad-para-2019/

The Future of Work. BCG Global. {En línea}. (2021). Disponible en: https://www.bcg.com/world-economic-forum/future-of-work

US-CERT (United States Computer Emergency Readiness Team) - Glossary | CSRC. US-CERT. {En línea}. (2022). Disponible en: https://csrc.nist.gov/glossary/term/US_CERT

Vega Villamil, Gustavo. Los nuevos desafíos del sector financiero. El Tiempo. {En línea}. (2021, 2 marzo). Disponible en: https://blogs.eltiempo.com/losnuevosjugadores/2021/03/02/pagos-electronicos-y-uso-del-efectivo-en-la-nueva-normalidad/

What is AVS (Address Verification Service). Verifi. {En línea}. (2017, 29 agosto). Disponible en: https://www.verifi.com/chargebacks-disputes-faq/what-is-address-verification-service-avs/

W.E.F. Towards a Reskilling Revolution A Future of Jobs for All. World Economic Forum. {En línea}. (2018, enero). Disponible en: https://www.weforum.org/

Zapata, J. F., Escorcia, J. A., & Quintero, E. S. PRODUCTOS Y SERVICIOS. ACH COLOMBIA. {En línea}. (2021). Disponible en: https://www.achcolombia.com.co/productos-y-servicios

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