ANÁLISIS DE LA SEGURIDAD PARA PROTECCIÓN DE PÉRDIDA DE DATOS EN LAS PLATAFORMAS E-COMMERCE UTILIZADAS POR LAS MIPYMES EN TIEMPO DE PANDEMIA

EDUIN YAMITH MARTINEZ PEÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2022

ANÁLISIS DE LA SEGURIDAD PARA PROTECCIÓN DE PÉRDIDA DE DATOS EN LAS PLATAFORMAS E-COMMERCE UTILIZADAS POR LAS MIPYMES EN TIEMPO DE PANDEMIA

EDUIN YAMITH MARTINEZ PEÑA

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

Nombre
Director de Trabajo de grado
Edgar Mauricio López Rojas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor y perseverancia dedico este trabajo a mi familia, que con su esfuerzo y colaboración me acompañaron en cada proceso realizado, motivándome de manera constante, minimizando los factores de deserción, lo dedico especialmente a mis padres y a la dama, que últimamente ha estado a mi lado Llary Camacho que con su apoyo constante y paciencia permiten que logre alcanzar un triunfo más en mi vida.

AGRADECIMIENTOS

Agradezco primeramente a Dios, a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, en especial a la Consejería académica del CEAD de Tunja, quienes con su trabajo continuo nos brindan su acompañamiento permanente, motivación, logrando avanzar en mi proyecto de vida profesional. Por otro lado, a cada uno de los tutores que me han acompañado en este proceso, en especial la tutora Yenny Stella Núñez y a mi director Edgar Mauricio López Rojas, al igual, a los demás asesores que me acompañaron en el proceso, reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: es el hardware, software, datos o información, que hacen parte de la infraestructura tecnológica del sistema de información.

AMENAZAS: Es un acontecimiento o circunstancia que puede llegar a causar daño al sistema informático, representa los posibles ataques o factores que inciden de manera negativa sobre los factores del sistema.

COMERCIO ELECTRONICO: es una herramienta digital que le permite a las MiPymes interactuar con sus usuarios para promocionar y comercializar bienes de servicios o de productos.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Un Control es también es utilizado como sinónimo de salvaguarda o contramedida.

MIPYMES: Micro, pequeña y mediana empresa.

PLATAFORMA E-COMMERCE: es un medio tecnológico en forma de sitio web que permite a las personas, vender servicios o productos, ver promociones o adquirir dichos bienes, esto por medio de pagos en línea o por medio de un código de factura o un pin de compra, entre otros medios de pago.

POLÍTICAS: Son las que permiten establecer las bases para gestionar procesos de información, la optimización de recursos para la eficiencia de sistemas informáticos y tecnologías de información, en otras palabras, es un conjunto de requisitos que debe tener un sistema, donde le indica en términos generales que esta y que no está permitido en el área de seguridad durante la operación general de dicho sistema

RIESGO: La posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

SEGURIDAD DE LA INFORMACIÓN: es la protección que se le debe dar a la información o datos y a los diferentes sistemas de información, donde se asegura el acceso, divulgación, la destrucción no autoriza o interrupción.

SEGURIDAD INFORMÁTICA: es la que permite asegurar los recursos del sistema de información, ya sea material informática o programas, el cual esté libre de daños, riesgos o peligros, permitiendo un funcionamiento seguro y efectivo del mismo.

SKIMMING: Es una técnica que usan los ciberdelincuentes para robar información

de las tarjetas de crédito donde también pueden ser clonadas para uso fraudulento.

SMISHING: Es una técnica de ingeniería social donde los delincuentes informáticos envían mensajes de texto vía telefonía móvil con software malicioso.

VISHING: Es una técnica de ingeniería social donde ciberdelincuentes realizan suplantación de identidad por medio de llamadas telefónicas persiguiendo datos sensibles de los usuarios.

. **RESUMEN**

Por medio de este estudio monográfico se desarrolló un análisis conceptual de las MiPymes enfatizándose en la seguridad para protección de datos en las plataformas de comercio electrónico en tiempos de covid 19. En primera medida, se realizó un estudio a diferentes masas documentales sobre la seguridad que se implementó en las plataformas de E-commerce. A su vez, se desarrolló una metodología de compilación, mediante la cual se analizó información sobre la protección de datos en los sistemas de comercio digital, donde se pudo encontrar elementos de vulnerabilidad, incidentes informáticos, denegación de servicio, suplantación de identidad, alteración o interceptación de datos y entre otros factores, con el fin de analizar los mecanismos enfocados en la seguridad de las plataformas de E-commerce, que fueron utilizadas por las pequeñas MiPymes.

Este análisis permitió tener una mejor idea de cómo operaban las MiPymes en la protección de datos en sus sistemas de compra y ventas por internet, buscando nuevas estrategias de seguridad y la forma en cómo se enfrentaron a la seguridad de E-commerce.

En este contexto, la presente monografía busca ser un referente para analizar la situación de las MiPymes en momentos de pandemia, en aspectos de seguridad, mostrando los resultados obtenidos de seguridad en protección de perdida de datos en plataformas de E-commerce durante la crisis mundial de coronavirus.

ABSTRACT

By means of this monographic study, a conceptual analysis of MSMEs was developed with emphasis on security for data protection in e-commerce platforms in times of covid 19. First of all, a study was made of different documentary masses on the security implemented in E-commerce platforms. At the same time, a compilation methodology was developed, through which information on data protection in digital commerce systems was analyzed, where elements of vulnerability, computer incidents, denial of service, identity theft, alteration or interception of data and other factors could be found, in order to analyze the mechanisms focused on the security of E-commerce platforms, which were used by small MSMEs.

This analysis allowed to have a better idea of how the MSMEs operated in the protection of data in their systems of purchase and sales by Internet, looking for new security strategies and the way in which they faced the security of E-commerce.

In this context, this monograph seeks to be a reference to analyze the situation of MSMEs in times of pandemic, in security aspects, showing the results obtained in data loss protection security in E-commerce platforms during the global crisis of coronavirus.

INTRODUCCIÓN

En la actualidad, el avance que ha venido teniendo el comercio electrónico, es un activo muy importante para considerar en las micro, pequeñas y medianas empresas, con respecto a esto, la seguridad de las plataformas de e-commerce es un factor fundamental en los tiempos de pandemia, puesto que fue el medio más usado por empresas para ofertar y comercializar sus servicios o productos, al igual que para los clientes fue el medio más eficiente para adquirirlos.

Por lo anterior, es que las MiPymes deben documentasen, analizando sobre la seguridad implementada para proteger los datos en sus plataformas e-commerce. Por consiguiente, se pretende mediante la presente monografía buscar ser aquel referente de análisis de la situación de las MiPymes en tiempos de pandemia, en aspectos de seguridad, mostrando una investigación detallada de los resultados obtenidos en cuanto a seguridad en protección de perdida de datos en plataformas de E-commerce durante la crisis mundial de covid 19.

El presente documento recopila una serie de información, que muestra el contexto actual del comercio electrónico en las empresas y la seguridad de protección de datos en las plataformas de comercio digital, al final se realiza un tipo de comparación a las estrategias de seguridad más implementadas por las empresas, enfocada al uso de los sistemas de Prevención de Pérdida de Datos que detecte, supervise y proteja los datos confidenciales de las MiPymes cuando usan plataformas E-Commerce.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Cada vez son más los procedimientos o tramites que se tienen que hacer por medios digitales, las MiPymes son un ejemplo de ello, las cuales se valen de muchos medios tecnológicos para informar sobre productos o servicios que quieren ofrecer a sus clientes. Es por lo anterior, que, para alcanzar buenos resultados en la protección de perdida de datos en sus plataformas de comercio electrónico, se analicen políticas de seguridad informática, que salvaguarden toda su información, en autenticidad, disponibilidad, confiabilidad e integridad. Con respecto a lo anterior, Rodríguez, Ortiz, Quiroz y Parrales[1] sostienen que, la situación que se afronta actualmente de covid 19 forzó a que muchas empresas cambiaran sus modelos de negocio, obligando a realizar las habituales compras por medio de las transacciones electrónicas, esto muestra, que para las MiPymes no fueron suficientes los modelos de negocios que tradicionalmente solían sostener, permitiendo que la digitalización se convirtiera en una condición indispensable a nivel empresarial. Estos autores también sostienen, que las empresas tradicionales se ven enfrentadas a nuevos retos para comercializar sus productos, aquellas organizaciones que generen cambios y avancen hacia la digitalización se ven adaptadas al escenario comercial del e-commerce.

Según el diario LA NACION[2], con las constantes restricciones generadas por la pandemia, permitió que hubiera un mayor uso de tecnologías de comunicación remotas, lo que, también hizo que se disparara las denuncias por ciberdelitos, siendo en 2020, el año con un 140% de denuncias más que el acumulado de los años anteriores. Entre las amenazas digitales que estuvieron a la cabeza del listado se encontraron extorciones, suplantación de identidad, estafas, ingresos apócrifos a cuentas bancarias, víctimas de phishing (supuesto email de banco solicitando cambiar contraseña), malware. Con relación a lo que se viene mencionando, Cervera[3] sostiene que el uso de plataformas electrónicas en tiempos de pandemia aumentó en un 71%, que la plataforma de mercado libre aumento en un 367% en los meses de marzo y abril, los delitos informáticos también crecieron según lo mencionado por el centro cibernético de la policía nacional aumentando en un 150%

[1] RODRÍGUEZ, Kelly; ORTIZ, Olga; QUIROZ, Alicia; y PARRALES, Maria. El e-commerce y las Mipymes en tiempos de Covid-19. [en línea]. 2020, noviembre,05 [Consultado 05 de mayo 2021] Disponible en: http://w.revistaespacios.com/a20v41n42/a20v41n42p09.pdf

[2] LA NACION. [Sitio web]. Ciberdelitos: durante la pandemia hubo más del doble de denuncias que en los tres años previos. [Consulta: 08 de febrero 2021] Disponible en https://www.lanacion.com.ar/seguridad/ciberdelito-nid2593717/

[3] CERVERA, Carlos; Comercio electrónico: compras y pagos disparados en Colombia en medio de la pandemia. [Sitio web] Actualicese.com. [Consulta:15 de mayo 2020] Disponible en: https://actualicese.com/comercio-electronico-compras-y-pagos-disparados-en-colombia-en-medio-de-la-pandemia/

en tiempo de aislamiento, siendo el hurto a cuentas bancarias el más común, entre otros se encuentran los correos electrónicos (spam), web falsas, mensajes de texto y llamadas telefónicas extorsivas.

Las micro, pequeñas y medianas empresas en tiempos de pandemia se vieron obligadas a enfrentarse a un mundo digital desconocido, exponiendo sus plataformas de E-commerce a inseguridades informáticas, al analizar la situación en pandemia se percibe que la MiPymes no tenían presente un mecanismos adecuados en seguridad informática, un respaldo seguro de su información, seguridad en su sitio web de comercio electrónico, un servidor seguro para alojar datos, una red de telecomunicaciones con protocolos de seguridad, equipos de cómputo con sistemas de ingreso seguro, planes estratégicos o de respuesta inmediata ante incidentes informáticos y un personal laboral capacitado en temas de seguridad informática. Además, se analizó factores como la vulnerabilidad, los incidentes informáticos, el hurto a cuentas bancarias, la suplantación de identidad, la alteración o interceptación de datos que se hicieron presentes.
Por consiguiente, Villar[4] afirma que los delitos informáticos en el comercio electrónico son la principal causa de desconfianza en los consumidores, que en el estado de emergencia sanitaria los delitos informáticos que más se configuraron en la plataformas de comercio digital fueron la suplantación de identidad y los fraudes informáticos, dentro de estos delitos se pueden identificar el phishing, clonación o skimming, smishing, vishing y software malicioso, los primeros tienen impacto directo en los usuarios y el ultimo en el proveedor.

Todo lo anterior, es motivo para realizar un análisis de la seguridad para protección de perdida de datos en las plataformas E-commerce que las MiPymes utilizaron en tiempos de pandemia. En este orden se plantea esta investigación monográfica en base a masas documentales buscando analizar la seguridad informática, los mecanismos, las medidas, los controles y el tratamiento a incidentes informáticos que usaron las empresas para protección de su información en plataformas de comercio digital.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué estrategia de seguridad para protección de perdida de datos implementaron las MiPymes en sus plataformas de comercio electrónico en tiempos de pandemia?

[4] VILLAR ESTRADA, S. S. El obligado y acelerado desarrollo del e-commerce en el Perú durante la pandemia COVID-19: Cuando el miedo y la necesidad superaron la falta de confianza. [Articulo] [Consulta: 20 de agosto 2020] Disponible en: http://www.itaiusesto.com/wp-content/uploads/2020/11/El-obligado-y-acelerado-desarrollo-del-e-commerce-en-el-Per%C3%BA-durante-la-pandemia-COVID-19-Silvia-Villar.pdf

2 JUSTIFICACIÓN

El comercio electrónico en las MiPymes en los tiempos de pandemia ha tenido un gran crecimiento e importancia para el desarrollo de sus actividades económicas, por tratarse de un tema digital es importante abordar un análisis de seguridad en la protección de datos en las plataformas de comercio electrónico. Por consiguiente, es necesario examinar en detalle la situación en que se encontraban las pequeñas y medianas empresas en temas de seguridad informática a la llegada de la pandemia y en el transcurso de la misma.

En este sentido, se puede afirmar la necesidad de realizar un análisis de investigación apoyado en distintas fuentes bibliografías que corroboren a tener una mirada más detallada de la seguridad informática y de las estrategias en protección de datos usadas por las MiPymes para proteger a sus usuarios en sus plataformas de comercio electrónico. Con este tipo de proyecto se permite aportar información y un análisis significativo para la toma de futuras acciones en un plan de seguridad en protección de información en pequeñas y medianas empresas que cuentan con plataformas de comercio digital.

De igual manera, este estudio monográfico da pautas de conocimiento y estrategias a los futuros especialistas en seguridad informática o de carreras afines, para que tengan en cuenta en futuras circunstancias las vulnerabilidades, técnicas y herramientas usadas por las pequeñas empresas en sus plataformas de E-commerce en tiempos de covid 19. Esta investigación es de suma importancia ya que abre diferentes opiniones en un contexto empresarial y de seguridad informática.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los mecanismos de seguridad para protección de pérdida de datos ofrecidos por las plataformas E-commerce que brindan servicios a las MiPymes en tiempo de pandemia.

3.2 OBJETIVOS ESPECÍFICOS

Evaluar los principales riesgos de seguridad que afrontaron las MiPymes en sus plataformas de E-commerce en tiempos de pandemia.

Debatir los aspectos de seguridad informática más recomendados por las micro, pequeñas y medianas empresas para la protección de datos en sus plataformas de comercio digital.

Explicar las estrategias de seguridad más implementadas por las MiPymes en un entorno E-commerce para prevenir las fugas de información.

Comparar que estrategia de seguridad para prevención y protección de pérdida de datos fue la más apropiada en las MiPymes cuando usan plataformas E-Commerce.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

4.1.1 **Comercio electrónico:** La sociedad actual no estaba preparada para afrontar una pandemia mundial de coronavirus proporcionando que el sector empresarial hiciera una mayor implementación de herramientas digitales en sus negocios, donde las MiPymes se vieron obligadas hacer uso de E-commerce para no desaparecer en un mercado competitivo, en este orden de ideas, las plataformas de comercio electrónico prestaron un servicio muy importante a las empresas a la hora de promocionar, ofertar y vender sus productos o servicios, de esta manera pudieron sostener a sus clientes, interactuar con ellos y conseguir nuevos compradores. De acuerdo con lo anterior según Serrano una plataforma de comercio electrónico es un sitio web que permite a las organizaciones promocionar y vender servicios o productos en tiempo real, con el propósito de llegar a más consumidores[5].

De igual forma, también se conoce al comercio electrónico como un componente primordial de la economía digital, siendo la nueva forma de hacer intercambios comerciales, a través de internet, estos pueden ser bienes físicos adquiridos por medio de una web lo que se conoce como comercio electrónico indirecto o pueden ser intangibles conocido como comercio electrónico directo. El crecimiento que este ha venido alcanzando ha generado ventajas para el empresario y consumidor final, como menores costes de desplazamiento, de almacenamiento, de tiempo, incrementado el número de demandantes y oferentes[6].

En concordancia con los conceptos mencionados anteriormente, se comprende entonces, que el E-commerce es una herramienta digital que le permite a las MiPymes interactuar con sus usuarios para promocionar y comercializar bienes de servicios o de productos. Las plataformas de comercio electrónico son medios tecnológicos en forma de sitio web que permite a las personas, vender servicios o productos, ver promociones o adquirir dichos bienes, esto por medio de pagos en línea o por medio de un código de factura o un pin de compra, entre otros medios de pago. Por último, estas plataformas a las empresas les permiten promocionar, interactuar, vender y obtener nuevos clientes.

---

[5] SERRANO, Javier. Revista de Economía Plataformas De Comercio Electrónico E Internacionalización Empresarial. Información Comercial Española [en línea] España [Consulta:30 de abril 2020]. Disponible en: https://doi-org.bibliotecavirtual.unad.edu.co/10.32796/ice.2020.913.6987

[6] ÁLAMO CERRILLO, R. La economía digital y el comercio electrónico: su incidencia en el sistema tributario. Dykinson. (pp. 21) [Libro] [Consulta: 2016]

4.1.1.2. **Historia del comercio electrónico:** En 1920 en estados unidos las empresas optaban por vender sus productos por medio de catálogos estos incluían fotos de sus ofertas e información adecuada para que los usuarios pudieren escoger el producto de manera acertada junto con sus familias. Con la salida de los ordenadores las empresas optaban por hacer trasmisión de datos por medio de ellos y que algunos de sus clientes también tuvieran la oportunidad de tener computador en sus hogares para hacer los pedidos correspondientes. Años más tarde aparece el termino intercambio electrónico de datos (EDI) este consiste en que generalmente distintas compañías realicen transmisiones de datos entre computadoras, convirtiéndose en una herramienta importante para facturas, proformas, cotizaciones, entre otros. Más adelante nace un proyecto que procuraba técnicas para el intercambio de datos entre computadoras, que se incursiona en internet y, por último, se considera que actualmente el E-commerce hace uso de las telecomunicaciones y las tecnologías para llevar a cabo el intercambio de bienes y servicios[7].

4.1.1.3. **Tipos de comercio electrónico:**

Según Narváez & Ortega[8], se menciona que existen diferentes tipos de comercio electrónico de acuerdo con la relación que se tiene entre gobierno, empresa y consumidores.

Las empresas, los consumidores y el gobierno son tres agentes fundamentales que intervienen en las transacciones electrónicas, pero estos a su vez se dividen en cuatro categorías de comercio electrónico por medio de la red, estas son: “B2B” entre empresas, “B2C” Entre empresa y consumidor, “C2C” entre consumidor a consumidor, “B2G” entre empresa y gobierno.

En la Figura 1, se puede evidenciar diferentes plataformas de E-comerce agrupadas de acuerdo con el tipo de comercio electrónico, al que cada una pertenece[9].

[7] PASCUAL, S. I. Comercio electrónico. Mc Graw Hill Education. (pp.16) [sitio web] [s.f] Disponible en: http://www.ebooks724.com.bibliotecavirtual.unad.edu.co/?il=5357&pg=1

[8] NARVAEZ-CHINGAL, Madelin Yamileth; ORTEGA-MEZA, Laura Silvana. Importancia del comercio electrónico en la actualidad. *Travesía Emprendedora*, vol. 4, no 1, (p. 36-38) [Artículo] [Consulta: 2020] Disponible en: http://editorial.umariana.edu.co/revistas/index.php/travesiaemprendedora/article/view/2480/2745

[9] ESPITIA ZULUAGA, L.M. Comercio electrónico en Colombia: Un mercado pionero amenazado por los gigantes del e-commerce. (pp.19) [Trabajo de grado] [Consulta: 29 de noviembre de 2019] Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/47241/Trabajo%20de%20Grado%20FINAL%20CORREGIDA.pdf?sequence=1&isAllowed=y

Figura 1: Tipos de comercio electrónico.

Fuente: Espitia (2019)

4.1.1.4. **El comercio electrónico y los medios de pago más utilizados:** Según Pascual[10] en su libro 'comercio electrónico' afirma que existe varios medios de pago, entre estos están:

Plataformas de pago: son sitios donde vendedores y compradores se registran para ser miembros, donde para el comprador es un servicio gratuito y para el vendedor es un servicio en el cual tiene que dejar su comisión. Como ejemplo se tiene: PayPal, Safetypay, Pagantis, Moneybookers, ClickeBuy, Paysafecard, Allopass, entre otros.

Transferencia Bancaria: cuenta bancaria que el comercio le facilita al comprador para que realice la compra por medio de una transferencia de pago.

Pago por teléfono: Por medio de cargo directo a la cuenta o factura de plan del teléfono o por medio de la tecnología NFC que consiste en el intercambio de datos entre el dispositivo móvil y el punto de venta.

Contra reembolso: es un pago que se hace de manera en efectivo donde el comprador recibe la compra sin antes haberla pagado y luego de recibirla realiza el pago a la empresa que le transporto el producto.

Tarjetas de crédito/debito: Es un medio de pago más utilizado donde las empresas bancarias cobran una cuota de manejo al vendedor por cada transacción recibida.

[10] PASCUAL, S. I. Op Cit, p.16

Domiciliación bancaria: Es la más habitual en esta se hace una suscripción periódica, donde el comercio gira un recibo al número de cuenta bancaria del comprador.

4.1.1.5. **Ventajas y desventajas del comercio electrónico:** El uso de E-commerce en las MiPymes tiene sus ventajas y desventajas, Peña[11], las identifica de la siguiente manera:

Ventajas

- ✓ Se evitan brechas geográficas.
- ✓ Mas clientes online y offline debido a la facilidad de dar a conocer los productos o servicios a través de internet.
- ✓ Menos costos de mantenimiento y promoción que en los negocios tradicionales.
- ✓ Disponibilidad de tiempo 24/7.
- ✓ Mayor facilidad para los consumidores demandar el producto o servicio a necesitar.
- ✓ Mayor facilidad para los vendedores ofertar el producto o servicio.
- ✓ Servicios o productos fuera de la localidad.
- ✓ Ahorro de tiempo para pedir asesoría por el producto o servicio.
- ✓ Optimización de tiempo para recibir el producto o servicio.
- ✓ Facilidad para poner en marcha una estrategia de marketing y dar mayor información al comprador.
- ✓ Comodidad para realizar la compra.
- ✓ Incrementación de ganancias
- ✓ Aumentar ventas y reducir costos.
- ✓ Aumentar oportunidades de venta y posibilidades de compra.
- ✓ Encontrar nuevos clientes y ser una empresa más competitiva.

Desventajas:

- ✓ Mas competencia, donde cualquier usuario puede implementar el comercio electrónico en su negocio.
- ✓ Falta de confiabilidad en las transacciones online por parte de los consumidores.
- ✓ Mas dificultad para lograr una exitosa fidelización de clientes.

[11] JIMÉNEZ, Y. J. Comercio electrónico ventajas y desventajas. 2019. (pp. 10-11) [Proyecto de Grado] [consulta: noviembre 2019] Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/16999/3/2019_Comercio_electronico_ventajas.pdf

- ✓ Gastos de envió excesivos cuando los negocios son pequeños o no se tiene un valor agregado del producto.
- ✓ Inseguridad en la plataforma de comercio electrónico.
- ✓ Amenazas constantes de hackers a las plataformas de comercio electrónico.
- ✓ Sabotaje en los servidores y bases de datos de la tienda virtual.
- ✓ Estafas al cliente por medio del 'phishing' es la técnica de hacerse pasar por empresas falsas.

En concordancia a lo mencionado anteriormente, se tienen otras desventajas importantes a considerar:

- ✓ Desconocimiento y falta de personal capacitado en temas de seguridad en protección de datos.
- ✓ Consumidores inseguros en las características del producto.
- ✓ Virus informáticos en los equipos de cómputo de los compradores, que sustraen datos de navegación o información confidencial del consumidor.
- ✓ La red de conexión del consumidor vulnerable a ataques informáticos.
- ✓ Suplantación de identidad e interceptación de datos.

4.1.2. **Seguridad en el comercio electrónico:** La seguridad en el ámbito de la informática se considera como un mecanismo para salvaguardar la información de las empresas, además se dice que es un conjunto de procedimientos o medidas con el propósito de que los datos estén siempre disponibles, asegurando los recursos del sistema, salvaguardando la información, donde tenga acceso solo el personal autorizado y que los procesos cumplan con estándares de seguridad.
Por consiguiente, se considera que la seguridad en el comercio electrónico es la utilización de técnicas de protección de datos o la forma de salvaguardar la información que se administre en dichas plataformas de comercio digital con el fin de asegurar las ventas y compras por internet. De acuerdo a lo anterior, según Vega sostiene, que las nuevas tecnologías para que tengan un desarrollo positivo deben ofrecer a cada uno de los usuarios una protección apropiada de su intimidad y así de esta manera el comercio electrónico se desarrolle de manera adecuada donde consumidores y empresarios tengan confianza en que las transacciones no serán modificadas o interceptadas, para que así en este clima de confianza se acuda a esta modalidad de transacción.[12]

Por otro lado, se considera que internet no es que sea un medio inseguro, lo que se considera es que en los usuarios hay un problema de percepción, considerar que el dar o no dar el número de tarjeta de crédito en una tienda virtual es de fiar o no, es ahí donde falta en los usuarios aquella confianza online en cuanto a temas de seguridad digital. Las tiendas virtuales deben luchar por adquirir ese sello de

[12] VEGA CLEMENTE, V. Comercio electrónico y protección de datos. Revista de Estudios Económicos y Empresariales, (pp. 213-214) [Libro] [consulta: 2021]

confianza en línea donde se pretende ese manual de buenas prácticas para conseguir nuevos e-consumidores. Algunos de los objetivos de confianza Online son: Aumentar en el comercio electrónico la confianza de los consumidores, dotar al comercio electrónico un instrumento de resolución extrajudicial de controversia económica, eficaz y rápida siendo herramienta útil para empresas y consumidores. Por último, tener un compromiso ético con los participantes que influyen en actividades de comercio electrónico. Otro aspecto a tener en cuenta en el tema que se viene mencionando es mediante una sección de auditoría y garantía de calidad en el comercio electrónico teniendo en cuenta el código de conducta de los asociados

También cabe resaltar que la seguridad en el comercio electrónico incluye que las empresas u organizaciones día a día se esfuercen, se capaciten e inviertan más en temas de seguridad para la protección de los datos por medio de las plataformas digitales, que estas capaciten a sus empleados en ciberseguridad para que en conjunto se brinde la confianza suficiente entre vendedores y compradores.

Argumentando el párrafo anterior, según Esparza[13] manifiesta que las empresas que hacen uso de plataformas web de ventas son garantes a brindar a sus consumidores condiciones óptimas de seguridad para salvaguardar sus datos personales, si bien, la falta de confianza en los usuarios es lo que afecta las compras en portales de venta y esto hace que no se tenga un crecimiento adecuado del comercio electrónico.

Siguiendo con el tema de seguridad y E-commerce se establece que se debe tener en cuenta el estudio a aspectos tales como: infraestructuras de claves públicas, algoritmos asimétricos y simétricos, certificados de seguridad, criptografía, seguridad en la web, protección a datos alojados en la web y la protección de software, además la parte de normatividad y legalidad.

Complementando lo anterior Ribagorda sostiene en su revista ‘Seguridad y comercio en el web’ que son varios los libros que hablan de este tema, pero que en especial se tiene el libro ‘seguridad y comercio en la web’ que lleva un orden de secciones que menciona de manera estructurada la seguridad en el comercio electrónico. La primera sección habla del panorama de la seguridad en la web, la segunda, la seguridad en el usuario, la tercera, los certificados digitales, la cuarta sección, criptografía, la quinta sección, seguridad de los servidores web y por último la sección sexta, comercio y sociedad[14].

[13] ESPARZA CRUZ, Nelly. El comercio electrónico en el Ecuador. Ecuador [en Linea] [consulta: 2021] Disponible en: https://revistas.utb.edu.ec/index.php/sr/article/view/119/pdf

[14] RIBAGORDA, Arturo. Seguridad y comercio en el web. Universidad Carlos III de Madrid. España [en linea][consulta:2020] Disponible en: https://revistasic.com/revista41/pdf_41/SIC_41_bibliografia.PDF

4.1.2.1. **Problemas de seguridad en la protección de datos en el comercio electrónico:** Desde que se hace uso del comercio electrónico siempre surgen una serie de problemas en la protección de datos de las plataformas digitales, a medida que avanza el tiempo, la tecnología también va avanzando, nuevas herramientas de seguridad o actualizaciones salen, pero al igual los delincuentes informáticos salen con nuevas técnicas o estrategias que atentan contra estos sistemas. Por otro lado, se tiene la desactualización o el desconocimiento en temas de ciberseguridad por parte del personal que labora en estas empresas y de sus usuarios.

Hablando del tema, Labodia sostiene, que existen problemas tales como: Pedidos que llegan en mal estado, pedidos que no llegan, transacciones irrealizables, productos que no cumplen lo anunciado, pedidos que incumplen el tiempo de espera, devoluciones que no se reembolsan, lentitud de red y el síndrome "de la muerte en un millón de clics". Ante estas problemáticas reales, surgen una serie de preguntas: ¿Es segura la red para el desarrollo del comercio electrónico?, ¿Es posible que un tercero se apodere de la tarjeta de crédito y se robe el dinero? ¿Son seguras las transacciones? ¿Qué sucede cuando se envía el número de la tarjeta de crédito por internet? El autor expone que las transacciones electrónicas están predispuestas ataques como Hackers, empleados desleales, ingeniería social y carding. Por otra parte, se tiene adicionalmente una serie de problemas como lo son: Riesgos de seguridad del cliente (JAVA, navegadores, Applets maliciosas, etc.) Riesgos de seguridad del server (Malas políticas de seguridad y de configuración, bugs, CGI's, permisos a usuarios locales, etc.) Problema de virus, virus troyanos, virus macro, Phising, etc. Problemas de seguridad de la comunicación, falta de integridad, confidencialidad, autenticidad y disponibilidad y por último, problemas de acceso a archivos del computador, borrado de información, denegación de servicio, entre otros[15].

4.1.2.2. Vulnerabilidades más comunes en la seguridad del comercio electrónico: Una vulnerabilidad es considerada una debilidad que los delincuentes cibernéticos aprovechan para explotarla por medio de un ataque cibernético para obtener un acceso no autorizado a los datos o información de las plataformas del comercio digital.

Según Fusario[16] las vulnerabilidades se pueden definir como aquellos aspectos operativos, técnicos o procedimientos que ocasionan la captura de manera intencional de la información confidencial con el propósito de ejecutar acciones que afectan económicamente al vendedor o comprador. Los sistemas de comercio por internet pueden ser vulnerables a:

- Código malicioso o programa maligno.

[15] LABODIA, BONASTRE, José. Seguridad en el comercio electrónico. (pp.108-109). [en linea] [s.f] Disponible en: https://www.acta.es/medios/articulos/ergonomia_y_seguridad/014105.pdf

[16] FUSARIO, R. J. Vulnerabilidades en la seguridad de las transacciones interactivas de comercio electrónico a través de la web. (pp. 81-86). [Libro] [consulta:2021]

- Archivos infectados.
- PDF incrustado con código malicioso.
- Mensajes de correo electrónico que llevan archivos adjuntos que infectan los ordenadores.
- Vínculos para llevar a los usuarios a sitios falsos.
- Personas que se valen de conocimientos para realizar acciones ilegales como hackers.
- Los Botnets que son como una red de robots que realizan tareas maliciosas como envió de spam.
- Programas potencialmente indeseables los PUPs que instalan códigos maliciosos autoejecutables donde no se tiene consentimiento por parte del usuario.
- Ramsoware código malicioso que se instala en el equipo del usuario para encriptarla los archivos por medio de un encriptado simétrico.
- Suplantación de identidad.
- Programas maliciosos parásitos software spyware.

Publicidad emergente que infecta al equipo cuando se visitan ciertos sitios web, lo que se conoce como programa aware.

4.1.3. Protección de datos en plataformas de E-commerce: Según la CELE[17], 'Colombia ley de protección de datos personales', en la 'ley estatutaria 1581 de 2012' donde se dictan las disposiciones generales para proteger los datos personales, promoviendo el derecho constitucional que todas las personas tienen por sus datos y las obligaciones que se tienen a la hora de dar tratamiento a los datos recolectados en base de datos o archivos.

Se considera que la protección de datos es la forma en cómo se puede asegurar o proteger los datos personales de las personas en medios digitales, según la superintendencia de industria y comercio manifiesta que "**La Ley de Protección de Datos Personales** reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.[18]"

Comprendiendo el concepto se conoce como dato personal a toda información intima de una persona, como su identificación, edad, trayectoria académica, laboral o profesional, estado civil, lugar de residencia, numero de contacto, correo, cuentas bancarias, entre otros datos. Si bien es cierto que existen muchas formas de

[17] OBSERVATORIO LEGISLATIVO CELE. (2019). [Sitio web] [consulta:2021] Disponible en: https://observatoriolegislativocele.com/colombia-ley-de-proteccion-de-datos-personales-2012/pdf?sequence=6&isAllowed=y

[18] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de datos personales. [Sitio web] [consulta:2021] Disponible en: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

recolectar datos personales que son de carácter privado de cada persona, pero si no fuese así sería imposible para las empresas u organizaciones la interacción con los usuarios, el flujo económico y el mejoramiento de sus bienes o servicios.

En términos generales, la protección de los datos es un deber que las empresas tienen con cada de una de las personas que la integran, garantizando el cuidado y la seguridad en el tratamiento de sus datos, al igual es un derecho y responsabilidad de cada uno de los usuarios. Por su parte, el sistema de información sobre comercio exterior[19], menciona la ley nacional colombiana sobre comercio electrónico, 'ley N°527' donde se menciona el 'reglamento de acceso y uso de los mensajes de datos del comercio electrónico' y las disposiciones de ley que se tienen frente a este tema.

Según el reportaje de González[20], se debe tener presente la concordancia con la normas que hablan sobre la protección de datos del consumidor, al igual el sostener mecanismos que permitan prevenir la suplantación de identidad en los consumidores, identificando completamente al comprador que obtiene productos utilizando medios electrónicos dispuestos, velando por el acatamiento de los principios de modificación, acceso, seguridad y veracidad en lo que se fundamenta la norma de datos personales.

4.1.4. Seguridad del comercio electrónico en Colombia en tiempos de pandemia: Según la CCCE[21] (cámara colombiana de comercio electrónico) en su portal de noticias sostiene que el crecimiento de los delititos informáticos en 2020 alerta de blindar los sistemas de información, correos electrónicos, sitios web, documentos digitales que generan entidades públicas y empresas. Colombia en los primeros seis meses del 2020 paso por un panorama desalentador en cuanto a delitos informáticos donde según cifras de la policía nacional fueron registrados más de 17 mil casos y del 1 de enero al 1 octubre se registraron más de 1200 denuncias por suplantación de identidad.

Complementando lo dicho anteriormente, la CCCE cita lo dicho por Laura Echeverría, Gerente Legal y Corporativa de Certicámara S.A donde afirma que: "Lamentablemente, aún se observa un amplio desconocimiento acerca de la

[19] SICE. Comercio Electrónico/Legislación Nacional - Colombia. [Sitio web] [consulta:2021] Disponible en: http://www.sice.oas.org/e-comm/legislation/col2.asp

[20]GONZALES, Carolina. Los datos personales en días de comercio electrónico. Editorial La República S.A.S. [Libro] [consulta:2021] Disponible en: https://www.asuntoslegales.com.co/consultorio/los-datos-personales-en-dias-de-comercio-electronico-3007397

[21] CCCE. Noticias: Con la "nueva normalidad", los delitos informáticos se multiplicaron en el país, pero pueden contrarrestarse con inversiones en seguridad digital. [Sitio web] [consulta:2021] https://www.ccce.org.co/noticias/con-la-nueva-normalidad-los-delitos-informaticos-se-multiplicaron-en-el-pais-pero-pueden-contrarrestarse-con-inversiones-en-seguridad-digital/

existencia de mecanismos tecnológicos seguros para proteger la información electrónica. Por ejemplo, en esta nueva realidad se evidenció el uso desmedido de las firmas escaneadas en documentos críticos para los negocios y esta situación abre las puertas al robo de identidad."

Para concluir, se contempla que la seguridad del comercio electrónico en momentos de covid 19 se vio en una serie desbordada de delitos informáticos, generando desconfianza en los usuarios considerando que falto más capacitación, inversión y conocimientos en temas de seguridad y delitos informáticos por parte de las empresas que hacen uso de las plataformas de E-commerce.

4.2 MARCO CONCEPTUAL

Para la continuidad de la presente monografía es importante tener claro los siguientes conceptos:

4.2.1 Vulnerabilidad: El término vulnerabilidad se considera como una debilidad que tienen los sistemas de información y que son propensos hacer atacados por una y otra técnica de ciberdelincuencia. También se considera como una puerta abierta para ejecutar un ataque en un sistema.

También se puede considerar que las vulnerabilidades informáticas son riesgos que los sistemas pueden sufrir frente a peligros que puedan suceder. En el contexto de la informática una vulnerabilidad "se refiere a los puntos débiles de un sistema computacional donde su seguridad informática no tiene defensas necesarias en caso de un ataque"[22]

4.2.2 Amenaza: Se considera como un acontecimiento o circunstancia que puede llegar a causar daño al sistema informático, representa los posibles ataques o factores que inciden de manera negativa sobre los factores del sistema. Se complementa con el siguiente concepto "una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de un sistema. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de

[22] SIGNIFICADOS. Significado de Vulnerabilidad. [Sitio web] [consulta:2021] Disponible en: https://www.significados.com/vulnerabilidad/

vista de una organización pueden ser tanto internas como externas"[23]
Se puede considerar una amenaza como aquella fuente que causa daño a un sistema informático, como, por ejemplo: denegación de servicio, divulgación, robo, suplantación, modificación o destrucción de datos.

4.2.3 Riesgo: Este término se considera como **l**a posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos de un sistema de información. El riesgo se mide en términos de impacto y probabilidad. Según Pinzón, se le considera riesgo informático a toda amenaza que explote una vulnerabilidad de uno o varios activos informáticos, afectando el buen funcionamiento de un sistema, teniendo presente que probablemente se materialice un evento o impacto en alguna de las características principales de la seguridad informática como la integridad, confidencialidad o disponibilidad[24].

Los riesgos informáticos generan grandes daños o perdidas administrativas o financieras en las empresas u organizaciones, las empresas deben incurrir a buscar o identificar los activos informáticos que se ven vulnerables a amenazas, con el propósito de determinar controles que ayuden a disminuir, mitigar, evitar o transferir la materialización del riesgo.

4.2.4 SGSI: Según Gómez & Fernández[25], un sistema de gestión de riesgos informáticos es un conjunto de técnicas que establecen, implementan, mejoran y mantienen la prolongación de la seguridad informática en una organización, basándose de sus riesgos. Este SGSI establece unos procesos formales y responsabilidades de acuerdo con una serie de políticas y procesos que constan de información documentada. En el sistema de gestión de riesgos informáticos establece dos procesos, el proceso de seguridad y el proceso de gestión; el primero se centra, en la seguridad de la información y el segundo se centra, en el funcionamiento del sistema y de su mejora constante.
Para diseñar un SGIS se debe tener en cuenta el modelo PDCA, el cual está conformado de la siguiente manera:
Planificar: Establecer el SGSI
En este proceso se crea un sistema de gestión de seguridad de la información, definiendo la política de seguridad y su alcance, se comenzará por analizar los riesgos de la organización para obtener unos resultados y así poder definir el plan de tratamiento de estos, para finalmente implementar unos controles de seguridad.

---

[23] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? España: CIBER. [Sitio web] [consulta:2021] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vsvulnerabilidad-sabes-se-diferencian

[24] PINZÓN PARADA, I. Gestión del riesgo en seguridad informática. Universidad Piloto de Colombia. [Sitio web] [consulta: 2021]

[25] GÓMEZ, F. L., y FERNÁNDEZ, R. P. P. Cómo implantar un sgsi según une-en iso/iec 27001 y su aplicación en el esquema nacional de seguridad. (p.90 - 125) [Sitio web] [consulta:2021] Disponible en https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/reader.action?docID=5486388

Hacer: Implementar y operar el SGSI
En este proceso se pondrá en ejecución el plan de tratamiento de riesgos, los procesos, procedimientos y controles del SGSI.
Verificar**:** Hacer un seguimiento y verificar el SGSI.
En este proceso se realizará los distintos tipos de revisiones para comprobar una correcta implementación del SGSI, según ISO27001, también se realizarán auditorías internas con el fin de proponer nuevas metas para cumplirse en un nuevo ciclo SGSI.
Actuar: Mantener y mejorar el SGSI
En este último proceso se plasmarán las acciones preventivas, correctivas y de mejora para el SGSI, con el propósito de tener un sistema de seguridad eficiente y eficaz.

4.2.5 Plataforma de comercio electrónico: Son sitios en internet en donde las empresas u organizaciones promocionan, ofrecen, venden, comercializan bienes de productos y servicios. También son sitios donde los usuarios que navegan por internet pueden ver las promociones o realizar compras de los servicios o productos ofertados.
Según VISA[26], las plataformas de E-commerce son interfaces en línea en la cual los empresarios podrán ofrecer sus servicios o productos y donde usuarios podrán adquirirlos. Estas interfaces cuentan con dos vistas una la administración del (back-end) administrada por la empresa y la otra visualización de la tienda (front-end) que es la que ven los usuarios. En la primera vista administración del back-end, es donde el administrador puede, dar de alta los productos, administrar niveles de usuario, definir promociones y precios, llevar el control y la revisión de inventarios, ver tendencias y características, entre otros. En la segunda visualización del front-end, es la vista del usuario, donde se puede desplegar los productos o servicios, precios y promociones, permitir a los usuarios registrarse para la realización de compras y donde los clientes pueden interactuar para realizar pedidos al comercio por medio de la tienda virtual.

4.2.6 Seguridad E-commerce: El proceso de seguridad en el comercio electrónico es un aspecto importante para las empresa u organizaciones que en la actualidad hacen uso de las tiendas virtuales, dado que en los tiempos de pandemia se ha incrementado el uso del comercio digital para poder subsistir, la seguridad en el comercio electrónico se considera como las técnicas que se pueden usar para la protección de datos en plataformas de comercio virtual garantizando la disponibilidad, confiabilidad e integridad.
Según Falcones[27], la seguridad se convierte en un aspecto muy delicado e

[26] VISA. Capítulo 2 Dominio, Plataforma y Hosting. Plataformas e-commerce. Seminario visa e-commerce. [Sitio web] [consulta: 2021] Disponible en: https://visaempresarial.com/Content/pdf/seminarios/Capitulo2/Tema/PlataformasEcommerce.pdf
[27] FALCONES ESTRADA, J. Estándares de seguridad y confidencialidad de la información aplicables al e-commerce [Sitio web] [consulta:2021]. Disponible en:

importante, al involucrar información confidencial o referente a temas económicos, sostiene que existen diferentes fraudes y amenazas que atentan contra la seguridad del comercio digital, enumerando algunos de ellos se tiene, datos falsos, manipulación de software maligno, virus troyanos, robo de información, Phising, ingeniería social, ataque DDoS, entre otros.

4.2.7 MYPIME: Este término significa micro, pequeña y mediana empresa, según lo definido por Ley 590 de 2000**,** "se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana"[28] Para la clasificación de estas empresas la ley las 590 las estableció de acuerdo con los activos totales y el número de personal de planta.

Se entiende por microempresa a aquellas empresas que manejan activos totales por un valor inferior de 501 salario mínimo legal vigente y con una planta de personal no mayor a 10 trabajadores.

Se entiende por pequeña empresa a aquellas empresas que manejan activos totales por un valor mayor a 501 e inferior a 5.001 salarios mínimo legal vigente y con una planta de personal entre 11 a 50 trabajadores.

Se entiende por mediana empresa a aquellas empresas que manejan activos totales por un valor mayor a 5001 e inferior a 15.000 salarios mínimo legal vigente y con una planta de personal entre 51 a 200 trabajadores.

4.2.8 Pandemia de COVID-19: La OMS[29] declaro COVID-19 como una pandemia de Coronavirus generada por el virus SARS-CoV-2 cuyo primer caso se generó en Wuhan China en diciembre de 2019 y esta organización la declaro pandemia el 11 de marzo de 2020. Los síntomas de este virus son tos, fiebre, cansancio. Otros síntomas menos frecuentes son la pérdida del gusto, conjuntivitis, congestión nasal, dolor de cabeza, dolor de garganta, escalofríos, vértigo, náuseas o vómito, dolores musculares, diferentes tipos de erupciones cutáneas. Por último, se tienen los síntomas de cuadro grave, pérdida de apetito, confusión, dificultad respiratoria, temperatura alta, dolor u opresión persistente en el pecho.

Las personas que desarrollan los síntomas de COVID-19 en un 80% se recuperan sin recibir tratamiento hospitalario, un 15 % desarrollan enfermedad grave que requieren oxígeno y un 5% precisan cuidados intensivos y estado crítico.

---

https://repositorio.pucese.edu.ec/bitstream/123456789/1502/1/FALCONES%20ESTRADA%20JAHIRO.pdf

[28] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 590. Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Bogotá: El Congreso. 2000.

[29] OMS. Información básica sobre la COVID-19. [Sitio web] [consulta:2021] Disponible en: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19

Para la protección de este virus se utilizan medidas, como distanciamiento físico, uso de tapabocas, uso de mascarillas, gel antibacterial o alcohol, bañado constante de manos, lugares ventilados, evitar aglomeraciones, toser cubriéndose la boca con codo flexionado o pañuelos.

Para la prevención de propagación de este virus se recomienda a las personas que tuvieron expuestas al covid-19 alejarse de otras personas durante 14 días, ya que los primeros síntomas se presentan entre los 5 o 6 días o entre el 1 a los 14 días.

A la fecha aún la pandemia se encuentra vigente, generando muchas controversias a nivel mundial cuyos efectos se ven reflejados en todos los grupos poblacionales, aunque ya hay luz de esperanza con el inicio de la vacunación aún siguen las secuelas y las consecuencias se ven reflejas a corto y mediano plazo.

4.3 MARCO LEGAL

4.3.1 Normatividad sobre la protección de datos personales.

Según la Unión Europea en su Reglamento General de Protección de Datos (RGPD)[30] considera que es un derecho de las personas la protección de datos personales, como lo menciona la carta de los derechos fundamentales de la Unión Europea en sus artículos 8 y 16 en su parágrafo 1.

Es importante seguir recordando que las MiPymes en tiempos de crisis hicieron uso de las plataformas de comercio digital, para recolectar una serie de información como nombre de los clientes, cedula, número de celular, dirección de residencia, entre otros aspectos que son de carácter personal. Las empresas se ven obligadas a cumplir la normativa de protección de datos personales y a velar por la información de cada uno de los usuarios.

De acuerdo, a la Ley Estatutaria 1581 de 2012[31], donde se ordenan generalidades de la protección de los datos, resaltando que todas las personas tienen derecho a la privacidad, intimidad de datos sensibles, al igual se menciona las categorías especiales de datos, el tratamiento que deben tener, derechos de autorización o de suministro de información. De acuerdo con esta ley se tienen unos principios con respecto al tratamiento que deben recibir los datos refiriendo el principio de la

[30] DIARIO OFICIAL DE LA UNIÓN EUROPEA. Reglamento (ue) 2016/679 del parlamento europeo y del consejo. [Sitio web] [consulta:2021] Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY ESTATUTARIA 1581 DE 2012. Reglamentada parcialmente por el decreto nacional 1377 de 2013. [Sitio web] [consulta: 2021] Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

legalidad, finalidad, libertad, veracidad o calidad, transparencia, seguridad, confidencialidad, acceso y circulación restringida. De acuerdo con lo anterior cada principio expone el respectivo tratamiento que se debe tener en cuenta a la hora de tratar datos personales.

Las empresas que hacen uso del comercio electrónico deben incluir en su actividad comercial la normatividad vigente que permitan facilitar e impulsar la legalidad que deben tener los medios electrónicos además asociarse con el código civil, el código del comercio y el código penal.

Continuando, el ministerio de tecnologías de la información y las comunicaciones en 2020 hace pública la resolución n° 002256 del 06 de noviembre de 2020, considerando las políticas generales de privacidad y seguridad de la información, la continuidad de la operación de servicios del fondo TIC y la seguridad digital. Donde se tiene presente el capítulo II que habla sobre las políticas específicas de manejo de información y el capítulo III responsabilidades de los colaboradores frente al uso de servicios tecnológicos[32].

4.3.2 Tratamiento de los datos personales con fines de E-commerce.

Según la OCDE[33] recomienda que es obligación de las empresas proteger los datos del consumidor, que en toda operación mercantil se debe otorgar seguridad en la recopilación, uso de datos legales, justos, transparentes, que se permita la adecuada elección y participación del consumidor. Por otra parte, las empresas deben implementar medidas de seguridad y gestionar riesgos en seguridad digital con el fin de mitigar todos los diversos efectos donde se encuentre involucrado el consumidor en el comercio electrónico.

El comercio electrónico en el siglo XXI es una herramienta fundamental para realizar todo tipo de operación mercantil, es un motor y un canal de comunicación efectivo para realizar negocios, hacer ese intercambio entre proveedores y consumidores con el propósito de comercializar toda clase de productos o servicios. Es por lo anterior que las MiPymes deben analizar la situación que en tiempos de pandemia de covid 19 se tuvieron en temas de legalidad, revisar si las estrategias implementadas cumplieron con la normatividad sobre tratamiento de datos personales (TDP).

---

[32] MINISTERIO DE TECNOLOGIA DE LA INFORMACIÓN Y LAS COMUNICACIONES. RESOLUCIÓN NÚMERO 002256 DE 06 de NOVIEMBRE DE 2020. [Sitio web] [consulta:2021] Disponible en: https://www.mintic.gov.co/portal/715/articles-2627_politica_seguridad_privacidad_informacion_resolucion_2256_2020.pdf

[33] OECD. Recommendation of the Council on Consumer Protection in E-Commerce, OECD Publishing, Paris. [Sitio web] [Consulta: 2021] https://doi.org/10.1787/9789264255258-en.

5 DISEÑO METODOLÓGICO

La actual monografía será de tipo compilación, bajo un modo descriptivo, por medio de la cual se analizó diferentes fuentes bibliográficas, sobre la seguridad para protección de pérdida de datos en las plataformas e-commerce utilizada por las MiPymes en tiempo de pandemia, en donde se encontraron los principales riesgos de seguridad, también se compararon las estrategias de seguridad más apropiadas para prevención y protección de pérdida de datos que implementaron las MiPymes cuando usan plataformas E-Commerce.

En este aspecto, se tomó como fuente de consulta, diferentes artículos investigativos y teóricos que hablan del tema, los cuales centran su estudio en la seguridad y protección de datos en tiempos de covid 19 y las diferentes estrategias de seguridad para la protección de datos en plataformas de comercio digital.

Para la recolección de la información se hizo un rastreo a diferentes fuentes bibliográficas usando como referente las siguientes variables:

- Riesgos de seguridad en las plataformas de comercio electrónico.
- Aspectos de seguridad más usados por las MiPymes para proteger los datos de sus clientes por medio de las plataformas E-commerce.
- Estrategia de seguridad para prevención y protección de pérdida de datos.

Las fuentes de recolección de información que se utilizó en primera medida son fuentes primarias como libros, artículos, prensa escrita y grabaciones audiovisuales, la mayoría de información se consultó en la biblioteca de la UNAD y en sitios oficiales de instituciones reconocidas.

Como segunda medida, las fuentes de recolección secundaria como revistas indexadas, trabajos de investigación de grado, publicaciones científicas, material cargado en los repositorios de universidades o plataformas académicas.

6 DESARROLLO DE LOS OBJETIVOS

6.1 EVALUAR LOS PRINCIPALES RIESGOS DE SEGURIDAD QUE AFRONTARON LAS MIPYMES EN SUS PLATAFORMAS DE E-COMMERCE EN TIEMPOS DE PANDEMIA.

La presente investigación se enfoca en analizar la seguridad para la protección de datos personales en plataformas de comercio digital en momentos de covid 19, en esta primera parte, se centra en encontrar los riesgos que más se presentaron en dichas plataformas.

6.1.1 Ataques que sufren las plataformas de comercio electrónico en tiempos de pandemia.

En tiempos de pandemia las plataformas de comercio electrónico prestaron muchos beneficios a las MiPymes como la promoción, venta y comercialización de sus productos, pero a su vez estuvieron expuestas a una gran serie de ataques por parte de los cibercriminales, esto debido a la falta de un análisis riguroso sobre estrategias eficientes que permitan la protección de los datos confidenciales de las MiPymes cuando hacen uso de este tipo de plataformas digitales. Entre algunos de los ataques más frecuentes se encuentran, el ataque por malware, por adware, por cryptojaking, por phishing, por exploid, entre otros.

Según Candanoza[34] la mayoría de los ataques se efectúan por medio de código malicioso, a continuación, se mencionan algunos de ellos:

- Ataques por medio de virus informáticos como gusanos, troyanos, PUPs, botnets, etc.
- Ataque por software malicioso afectando las transacciones que se realizan por medio de tarjetas de crédito.
- Phising: El cibercriminal ataca a su víctima por medio de la técnica de suplantación por el robo de contraseñas.
- Ransomware: Ataque por medio de mensajes de carácter extorsivos.
- Smishing: Ataque donde se hace uso de enlaces fraudulentos por medio de correo electrónico.
- Pharming: Ataque donde se hace redireccionamiento de un sitio seguro y real a otro fraudulento.
- Keyloggers: Ataque por medio de programas que espían todo lo que se

[34] CANDANOZA, E. El comercio electrónico en tiempos de pandemia. Editorial La República S.A.S. (p.20) [Tesis] [consulta:2021] Disponible en: http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1279_FusarioRJ.pdf

hace en el equipo.
- Hoax: Ataque por medio de notificaciones falsas por medio de envíos o cadenas falsas.

También el autor sostiene que en estos tiempos de covid 19, se aprovecha el uso de las herramientas tecnológicas, a su vez se debe ofrecer respaldo y seguridad a los usuarios y al comercio; Por otro lado, realizar pedagogía aquellas personas que no son expertas con los canales virtuales. Según el autor los fraudes digitales han aumentado en los últimos tiempos, de ahí la importancia de conocerlos y de saber cómo mitigarlos.

Además, según la revista atalayar[35], estima que desde el comienzo de la pandemia las instituciones han sido blanco de ataques por parte de los piratas informáticos, esta revista cita a la INTERPOL, donde afirma como fue testigo en agosto del 2020 de un número considerable de amenazas cibernéticas con respecto del covid 19, como estafas en línea, correos electrónicos de suplantación de identidad, software malicioso. El autor sostiene que faltan conocimientos y recursos necesarios por parte de las empresas u organizaciones para tener salvaguardas adecuadas.

Si bien, la extensión del confinamiento por covid 19 ha generado que más usuarios se vean obligados a utilizar las plataformas de comercio electrónico para adquirir servicios o productos, realizar transacciones virtuales, llenar formularios para solicitar información de algún bien, entre otras tareas. Es tema importante para que las empresas no descuiden la ciberseguridad en estos momentos de pandemia, en este sentido, señala la cámara colombiana de comercio electrónico, que la pandemia no debe ser excusa para que se descuide la ciberseguridad en las organizaciones y así evitar delitos como "phishing o suplantación de sitios web, la infección y propagación de códigos maliciosos, los fraudes en medios de pago en línea, más conocido como malware y el acceso no autorizado a la información" también concluye que el ramsonware o secuestro de datos es la principal amenaza recibiendo de este tipo un 30% de los ataques en el año anterior[36].

6.1.2 Los Riesgos más presentados en plataformas de comercio electrónico en tiempos de pandemia.

El comercio digital además de presentar ventajas para las empresas y para los consumidores, también presenta una serie de riesgos tanto para empresas como

[35]ATALAYAR. Aumenta la ciberdelincuencia durante la pandemia de la COVID-19. [Sitio web] [consulta: 11 de abril 2021] Disponible en: https://atalayar.com/content/aumenta-la-ciberdelincuencia-durante-la-pandemia-de-la-covid-19

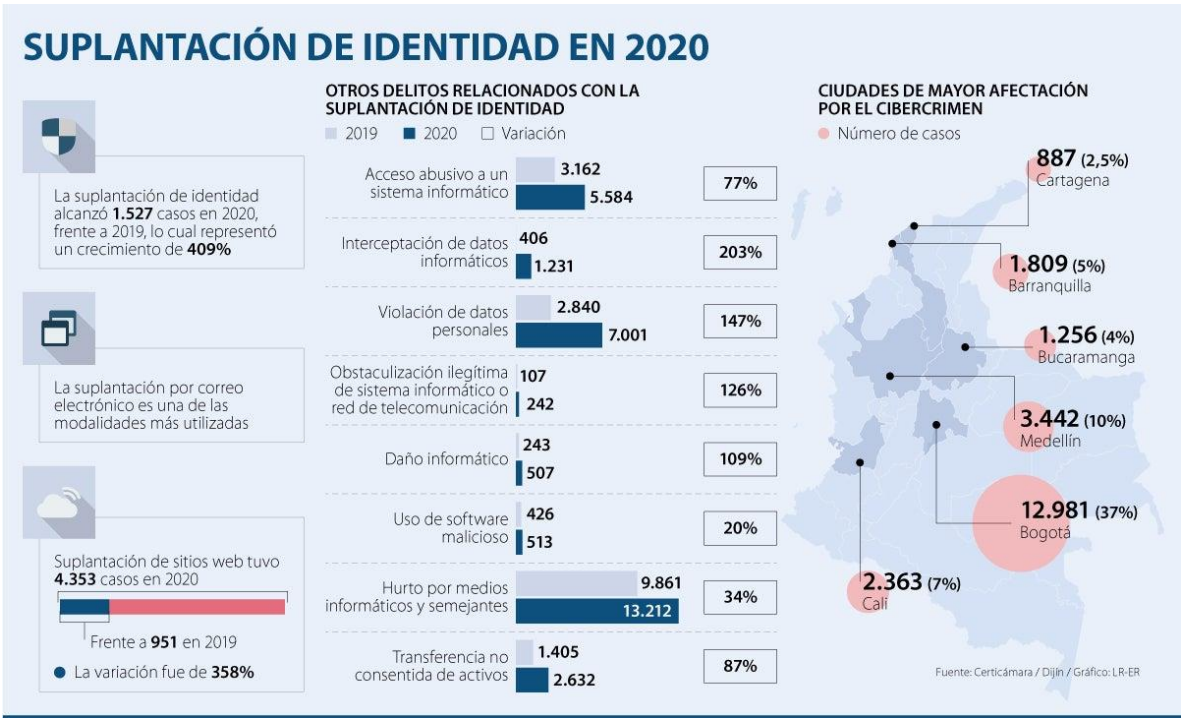
[36] CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO. Que la pandemia no sea excusa para descuidar la ciberseguridad de su organización. [Sitio web] [consulta:2021] Disponible en: https://www.ccce.org.co/noticias/que-la-pandemia-no-sea-excusa-para-descuidar-la-ciberseguridad-de-su-organizacion/

para compradores. Según el equipo Health&Benefits[37], consideran los siguientes riesgos:

Robo de identidad: Es una intervención fraudulenta que se hace para sustraer datos personales, número de tarjetas bancarias, nombres de usuario o contraseñas.

En la figura 2 se puede evidenciar como este riesgo está relacionado con accesos abusivos a sistemas de información, violación de datos personales, daño informático, interceptación de datos, uso de software malicioso, transferencias sin consentimientos y daño informático[38].

Figura 2: Robo de identidad.



Fuente: Acosta (2021)

Phising: Es donde un estafador engaña al usuario por medio de un correo spam enviándole información supuestamente de una página de confianza para realizar una operación bancaria.

[37] EQUIPO HEALTH&BENEFITS. Ecommerce: riesgos a los que se enfrentan los vendedores en internet. Willis Towers Watson Update. [Sitio web] [consulta: 2021] Disponible en: https://willistowerswatsonupdate.es/ciberseguridad/e-commerce-riesgos-enfrentan-e-vendedores/

[38] ACOSTA ARGOTE, C. Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. [Artículo] [consulta: 2021] Disponible en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

En la figura 3 se puede observar como un alto porcentaje de usuarios de diferentes países se vieron atacados por Phishing en tiempos de Covid 19, donde Venezuela presenta el mayor índice y China el menor[39].

Figura 3: Intentos de phishing en tiempos de pandemia.

Fuente: statista (2021)

[39] STATISTA. Los intentos de phishing en tiempos de COVID-19. [Artículo] [consulta: 2020] Disponible en: https://es.statista.com/grafico/18427/intentos-de-phishing-durante-la-pandemia/

Otro de los riesgos es el desconocimiento por parte de los empresarios en el tema de comercio electrónico generando desconfianza en los consumidores. Al igual que el desconocimiento que los empresarios tienen en el funcionamiento de las plataformas transaccionales[40].

Continuando, se considera que las MiPymes no estaban preparadas para asumir una serie de cambios en su modelo de negocio, que para poder sostener su economía debían de hacer uso de herramientas digitales que garanticen la promoción, venta y compra de productos o servicios, es ahí donde las empresas se ven obligadas hacer uso de plataformas de E-commerce, a su vez se encontraron con una serie de riesgos, como suplantación de identidad, robo de credenciales de acceso a sistemas bancarios, fraudes en transacciones financieras, fuga de datos sensibles, estafas, captura de información con software malicioso, entre otros riesgos importantes.

De acuerdo con lo mencionado en el párrafo anterior, Según la KPMG[41] estimula que la gestión del riesgo tecnológico es muy importante en las organizaciones para dar permanencia y continuidad en los negocios. Con el crecimiento que ha venido teniendo este sector en operaciones electrónicas, también se ha visto en los últimos tiempos incrementados los riesgos tecnológicos, entre los más comunes se tiene:
- Fraude en transacciones bancarias y financieras.
- Robo de datos personales o de identidad.
- Perdida de trazabilidad en transacciones de tipo electrónicas.
- Fuga de datos personales.
- Sabotaje.
- Fallas de continuidad de servicio en plataformas de comercio electrónico tanto en software como en hardware.
- Fuga de datos sensibles.

Según el portal web de Noticias Caracol[42], en tiempos de pandemia lo más denunciado del comercio electrónico por los usuarios fue el bombardeo de anuncios falsos en redes sociales, exceso de publicidad, invasión o robo de datos personales, engaños por correos o por mensajes a celulares. Es bien sabido, que al conocerse que todos estos riesgos iban a ser ejecutados en muchas de las plataformas de

[40] TIRADO RÍOS, N. R. Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. Revista Publicando [Sitio web] [consulta: 2021]
[41] KPGM. Riesgos del e-commerce a raíz de COVID-19. Cárdenas Dosal, S.C., Sociedad civil mexicana. [Sitio web] [consulta: 2021] Disponible en: https://home.kpmg/mx/es/home/tendencias/2021/01/riesgos-del-e-commerce-a-raiz-de-covid-19.html
[42] NOTICIAS CARACOL. Comercio electrónico en Colombia creció exponencialmente y también lo hicieron las quejas. Caracol. [Sitio web] [consulta: 2021] Disponible en https://noticias.caracoltv.com/actualidad/al-pie-de-la-letra/comercio-electronico-en-colombia-crecio-exponencialmente-y-tambien-lo-hicieron-las-quejas

comercio digital, las MiPymes se hubieran adelantado a proteger de una mejor manera cada una de las ventas realizadas por estos medios, para evitar mayores pérdidas económicas.

El año 2020 fue un año de mucha incertidumbre, por un lado, un virus que ocasiono confinamiento a un millar de personas, donde las empresas pequeñas y medianas se vieron obligadas a cerrar sus tiendas físicas, a su vez también se decide reinventar nuevas estrategias de mercado, los vendedores y compradores se hicieron a nuevos comercios, es ahí donde una serie de delincuentes informáticos también aprovechan la ocasión para hacer de las suyas por medio de los canales tecnológicos. Según el periódico EL TIEMPO[43] manifiesta que se presentó un caso de suplantación de sitios web de la plataforma de comercio electrónico MERCADO LIBRE, donde resalta que el sitio web suplantado tenía las mimas características de la plataforma, una URL muy similar, incluía un mismo menú, secciones de e-commerce, tenía el candado de seguridad y una interfaz con el mismo diseño de marca, con el fin de mostrar que era una conexión segura. En este mismo artículo también refiere que los ciberdelincuentes engañan a las personas por medio de la suplantación con el fin de realizar robos económicos o robos de acceso de contraseñas o credenciales de tarjetas de crédito. Además, también en esta noticia se cita a la cámara colombiana de informática y Telecomunicaciones donde afirma que durante el año 2020 se presentaron más de 5.440 casos de prácticas de suplantación de sitios web siendo este el delito más denunciado.

Continuando con el mismo tema, la Cámara Colombiana de Informática y Telecomunicaciones[44] valora que, en el periodo de marzo a diciembre del 2020 en plena pandemia, se incrementaron a más de 45000 casos de ciberdelitos, un 89% más que el año anterior. El delito con un crecimiento del 303% fue la suplantación de sitios web para capturar datos personales, este delito se vale de modalidades directas como el spoofing, phishing y pharming que fueron los ataques más sufridos por las empresas, con esto los cibercriminales dispersaron malware y capturaron datos en las redes corporativas. El segundo delito con un incremento del 174% fue la violación de datos personales con 9.487 casos registrados, lo que genero perdida de información sensible en consecuencia del robo y filtración de datos. Por último, un tercer delito con un crecimiento del 375% fue el hurto por medio de medios informáticos registrando más de 16.000 casos reportados donde la modalidad más usada fue la apropiación de credenciales de acceso de servicios bancarios en línea, consiguiendo suplantar al titular de la cuenta bancaria y terminar robándole todo su

[43] EL TIEMPO. Así están suplantando sitios web de comercio electrónico. Casa Editorial NIT. 860.001.022-7. [Sitio web] [consulta: 2021] Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/tacticas-de-suplantacion-de-sitios-web-de-comercio-electronico-578204

[44] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Ciberseguridad en entornos cotidianos; estudio del cibercrimen 2020. [Sitio web] [consulta:2021] Disponible en: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020/

dinero.

Por ende, según la CCIT en Colombia en los últimos años se han incremento los hurtos a través de medios informáticos con un total de 31.058 nuevos casos y en seguida se menciona el robo de identidad con 8.037 nuevos casos, donde Bogotá, Cali y Medellín se encuentran el mayor número de incidentes informáticos. Se analiza que en Colombia se recibió un gran ataque por ransomware donde los usuarios tenían que pagar un rescate para librarse de este software extorsivo[45].

Además, se conoce que algunas empresas si estaban preparadas para usar plataformas de comercio digital y garantizar la protección de datos personales para los usuarios, mientras que otras estaban en vía de hacerlo posible siendo para estas un tema totalmente nuevo, sobre todo para la micro y pequeña empresa. Con respecto a esto, es importante mencionar lo que dice la ACIS[46], una vez puestas la cuarentena en los distintos países del mundo, se observó que hubo un aumento de las compras online, que algunos emprendimientos y negocios ya estaban preparados para hacer uso del E-commerce, pero que otros estaban a mitad de camino sin tener conocimientos en ciberseguridad por ende tuvieron que iniciar su uso a la fuerza incrementado los riesgos de estafas. La Asociación Colombiana de Ingeniero de Sistemas en este mismo artículo cita los resultados obtenidos de las encuestas realizadas por la ESET durante la pandemia de COVID 19, donde se resalta que los delincuentes informáticos estuvieron atentos a este tipo de fenómenos para hacer de las suyas, se valieron de estrategias como el uso de anuncios falsos en plataformas sociales, perfiles falsos en plataformas de comercio electrónico, ataques de web skimming, campañas de phishing todo con el fin del robo de datos de las tarjetas de crédito, robo de contraseñas o información personal, realizar estafas económicas, entre otros tipos de cibercrímenes.

El diario el Portafolio[47] determina que un nuevo panorama que afronto el país en tiempos de Covid 19 fue el phishing una modalidad en que un cibercriminal crea una página web, enlace o archivo falso idéntico al original para redirigir a cualquier victima al engaño para proceder a un robo monetario o de datos personales. Este portal afirma que un 21% de los estudiados manifiestan haber sido engañados a través de enlaces de sitios web fraudulentos del comercio en línea y también que un 19% refiere haber sido engañados por medio de supuestos fondos de caridad. Este diario también cita al director de laboratorio de informática forense de Adalid

[45] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del Cibercrimen en Colombia 2019-2020. [Sitio web] [consulta:2021] Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[46] ACIS. Crece el E-Commerce aumenta las estafas y los incidentes informáticos. [Sitio web] [consulta:2021] Disponible en: https://acis.org.co/portal/content/noticiasdelsector/eset-crece-el-ecommerce-aumentan-las-estafas-y-los-incidentes-de-seguridad

[47] PORTAFOLIO. Delitos informáticos, la otra pandemia en tiempos de coronavirus. [Sitio web] [consulta:2021] Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

Corp, donde Axel Díaz dice que los delincuentes informáticos aprovecharon la oportunidad para crear sitios web llamativos para vender servicios o productos que los consumidores necesitan a precios inimaginables.

6.1.3 Afectaciones que causaron los riesgos anteriormente mencionados en las empresas que hacen uso de plataformas de comercio electrónico entre los años 2020 y 2021.

Al conocer estos riesgos, las MiPymes se vieron afectadas por un bajo número de ventas, una parte de ello se debe por la gran desconfianza que los clientes presentan al hacer uso de las plataformas de comercio digital, se presenta la desconfianza de proporcionar información confidencial, sospechan de los medios de pago, hay suspicacia a la hora de adquirir el producto por los multitudinarios riesgos que se pueden presentar, además correr el riesgo de que el producto solicitado no llegue o no sea el solicitado[48].

Según el Portal Infosecurity Mexico[49], cualquier empresa corre el riesgo de asumir algún riesgo por ciberataque, cita a (CONDUSEF) donde estima que el fraude a costado a minoristas unos $130 mil millones de dólares. Además, estima que el sector de comercio electrónico tuvo objetivos cibercriminales como suplantación de identidad, robo de información y paralización de redes informáticas donde se considera que el fraude a las empresas a costado 35,540 millones de dólares a nivel mundial siendo las micro, medianas y pequeñas empresas las más afectadas.

Con base al párrafo anterior, es evidente que las MiPymes son las más afectadas por varias razones, como, por ejemplo, debido a que hasta ahora estaban iniciando o creciendo en el mercado, algunas hasta ahora hacían uso de plataformas de comercio electrónico, otras desconocían los ciberataques que se pueden presentar en el mundo digital, varias tenían ya una plataforma de e-commerce, pero no contaban con tecnicas eficientes en seguridad informática, entre otros.

Ahora bien, en tiempos de pandemia el ataque mas relevante que sufrieron muchos usuarios es sin duda, el robo de identidad, según la organización Skiba[50], el robo de identidad en 2020 en tan solo en estados unidos se disparó en 1.4 millones. En su artículo cita a la Comisión Federal de Comercio (FTC) que afirma que en el año 2020 se triplico el numero de denuncias por este delito. La FTC Clasifica a los 4.7 millones de reclamaciones que hubo por parte los consumidores entre los que están: Robo de identidad, fraude y todo lo demás que afecta a consumidores.

---

[48] RODRÍGUEZ, K, G. ORTIZ, O, J. QUIROZ, A, I. y PARRALES, M, L. Op. cit., p. 11.

[49] INFOSECURITY. Los ciberataques más costosos en la industria del eCommerce. [Sitio web] [consulta: 21 de abril de 2021] Disponible en: https://www.infosecuritymexico.com/es/blog/los-ciberataques-mas-costosos-en-la-industria-del-eCommerce.html

[50] SKIBA, K. La pandemia resulta terreno fértil para los ladrones de identidad. [Articulo] [consulta: 6 de febrero de 2021] Disponible en: https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2021/ladrones-de-identidad-aumentan-en-la-pandemia.html

En la Figura 4 se puede observar las perdidas por fraude en 2020 según la edad del consumidor, según la FTC[51], los consumidores que fueron más afectados por estos ciberdelitos son las personas mayores de 80 años, con un total de $1300 dólares, en seguida le siguen los de 70 a 79 años, con un total de $635 dólares y de ultimas, está la población de 0 a 19 años con un total de $180 dólares.

Figura 4: Perdidas económicas por fraude en 2020 según la edad del consumidor.

Fuente: FTC (2020)

Por último, se evidencia que las perdidas son significativas en las MiPymes, donde muchos de sus consumidores se vieron afectados por este tipo de riesgos cibernéticos, según los tres autores anteriores, muestran que el principal riesgo que han vivido las empresas y consumidores en tiempos de pandemia es el robo de identidad, siendo el factor económico el más afectado.

[51] FTC. Libro de datos de Consumer Sentinel Network 2020. [Sitio web] [consulta: febrero 2021] Disponible en: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020

6.1.3 ¿Cómo subsanaron estos riesgos las MiPymes que usan plataformas E-commerce en tiempos de pandemia?

Al presentarse la pandemia de COVID-19, muchas de las MiPymes estaban en la incertidumbre de qué hacer con sus ventas, unas optaron por cerrar su espacio físico e implementar plataformas de Comercio electrónico, pero cuando empezaron a presenciar riesgos en las plataformas de E-commerce y grandes pérdidas económicas, decidieron de manera inmediata crear o publicar en sus sitios web o plataformas de comercio digital, información para los consumidores, sobre el cuidado y la seguridad de los datos que se debe tener en los medios digitales, con el fin de lograr transacciones o compras seguras por internet.

En relación con lo anterior, la plataforma de comercio electrónico mercado libre[52], lanza una serie de consejos en pandemia para cuidar la seguridad en ventas, compras, pagos y cobros, con el propósito de evitar cualquier tipo de engaño u operación fraudulenta. Algunos consejos son: realizar todo tipo de transacción desde la plataforma oficial, usar únicamente los canales oficiales de la plataforma, Siempre solucionar todo en el chat de mercado libre, siempre revisar la reputación del vendedor, no compartir datos personales como número de teléfono, identificación fiscal, cuentas bancarias, claves de seguridad, hacer los reclamos inmediatamente a través de la plataforma, no compartir números de cuentas bancarias, tarjetas de crédito o débito por medios externos como WhatsApp, correo, redes sociales, importante que siempre se verifique la autenticidad de los correos validando el dominio que se la (url) de la página oficial. Corroborar muy bien el sitio a pagar que tenga el candado junto a la dirección web “Https”. No se recomienda descargar archivos o dar clic en enlaces sospechosos para evitar software malicioso y, por último, aconseja siempre denunciar cuando se detecte irregularidades, al igual crear contraseñas seguras.

En relación con este tema, la empresa claro[53] menciona que se debe romper el tabú de comprar en línea siempre y cuando se tengan en cuenta las siguientes recomendaciones: En caso de comprar en Colombia comprobar que toda tienda virtual o aplicación este vigilada y avalada por la superintendencia de industria y comercio. Acudir a revisar los comentarios que compradores les hacen a vendedores, verificar la política de privacidad y tratamiento de datos, tomar pantallazos que soporten los inconvenientes, guardar las facturas solicitando que siempre sean enviadas directamente al correo personal.

---

[52] MERCADO LIBRE. Consejos para cuidar la seguridad de tus transacciones online. [Sitio web] [consulta: julio 2021] Disponible en: https://www.mercadolibre.com.pe/institucional/comunicamos/noticias/consejos-para-cuidar-la-seguridad-de-tus-transacciones-online

[53] CLARO. Lo que debes saber de las compras por internet. [Sitio web] [consulta: 29 de mayo 2020] Disponible en: https://www.claro.com.co/institucional/compras-por-internet/

Por otro lado, según el especialista científico en transformación de datos Ferapontov[54], propone una serie de reglas para evitar riesgos de seguridad a los usuarios de la plataforma eBay, menciona que se debe crear contraseñas robustas para evitar ataques de fuerza bruta, activar en la aplicación de eBay la autenticación en dos factores, que sea por medio de código o push, elegir tres preguntas de seguridad cuya respuesta sea difícil de descubrir, aprender sobre tácticas en seguridad para evitar ataques de phishing, recomienda que todo pago que se haga en eBay sea mediante PayPal, y no realizar transferencias por medios externos, al igual, no comunicarse con personas que no hacen parte de la plataforma para evitar que se dé información confidencial a ciberdelincuentes, contactar a soporte si existen notas sospechosas, actualizar el sistema operativo, el navegador, el antivirus y actualizar la aplicación móvil en caso de ser usada en el celular, cerrar sesión todas las veces que se ingrese desde un equipo de trabajo o público, por último, también refiere las normas de seguridad que deben cumplir los vendedores y compradores.

En esta perspectiva, la empresa mata[55] aconseja que para superar los ataques por Ransomware se deben tener buenas prácticas de seguridad, concientizando y educando a los usuarios en temas de ingeniería social, medidas para evitar ataques contra el phishing, al igual contar con un respaldo de información de la empresa como personal, la empresa debe disponer de un departamento de ciberseguridad donde se disponga de un responsable que implemente políticas de seguridad, revisión, actualización y mantenimiento de sistemas. Por otro lado, propone que para subsanar estos riesgos se debe activar herramientas de ciberseguridad, que permitan proteger, detectar y bloquear amenazas en tiempo real más conocida como protección de End Point. Al igual, protección de red, donde se prevenga potenciales ataques y que la red tenga un monitoreo continuo para evitar robo o perdida de información.

En conclusión, se evidencia que la mayoría de las empresas subsanaron los riesgos implementando en sus sitios oficiales consejos relacionados con seguridad, que van dirigidos directamente a consumidores y trabajadores, al igual, otras MiPymes fortalecieron la seguridad en sus plataformas de comercio electrónico activando herramientas de ciberseguridad. Complementando lo anterior Gómez[56] señala que toda empresa está dispuesta a sufría algún ataque, por lo que es indispensable implementar soluciones que permitan prevenir instrucciones en tiempo real, activando firewalls de ultima generación que permitan analizar acciones sospechosas que se puedan adherir a la red, resalta que con una estructura de

[54] FERAPONTOV. A. Consejos sobre transacciones y seguridad en eBay. [Sitio web] [consulta: 30 de septiembre 2020] Disponible en: https://latam.kaspersky.com/blog/secure-ebay-trade/20194/

[55] MATA. Ransomware en tiempos de pandemia. [Sitio web] [consulta: s.f] Disponible en: https://madata.com/ransomware-en-tiempos-de-pandemia/

[56] GOMEZ RESTREPO, C. Seguridad, pilar para el auge del e-commerce. [Sitio web] [consulta: 4 de septiembre de 2021] Disponible en: https://www.larepublica.co/internet-economy/seguridad-pilar-para-el-auge-del-e-commerce-3227286

seguridad robusta y confiable las empresas lograran cumplir todas las necesidades demandas por sus consumidores.

6.2 DEBATIR LOS ASPECTOS DE SEGURIDAD INFORMÁTICA MÁS RECOMENDADOS POR LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS PARA LA PROTECCIÓN DE DATOS EN SUS PLATAFORMAS DE COMERCIO DIGITAL.

La seguridad informática se debe considerar el bien económico más importante para una organización, a raíz de la pandemia las empresas y clientes, tuvieron que hacer uso del E-commerce, para poder promocionar, vender y comprar productos o servicios, es acá donde las MiPymes aprovechan poner en marcha las plataformas de comercio electrónico, algunas ya las usaban como estrategia de negocio y otras aún no, pero de todas maneras se vieron obligadas hacer uso de ellas; es de esta misma manera que algunas empresas ya tenían muy claro el tema de seguridad en protección de datos personales pero otras no, esta situación permitió que las MiPymes se aceleraran a buscar una serie de aspectos de seguridad para salvaguardar la información de sus clientes.

En primer lugar, la revista semana[57] expresa que un 62% de los consumidores manifiestan con seguridad que el robo de identidad y el fraude son su mayor preocupación, por ende, las empresas deben dar prioridad a la protección de datos personales de sus usuarios. Partiendo de esta situación, se destaca los diferentes aspectos de seguridad que en pandemia distintas empresas recomendaron para proteger los datos de sus usuarios cuando se hace uso del comercio electrónico.

Entrando en tema, según ESET[58] considera que, para proteger los datos personales en las plataformas de comercio electrónico en tiempos de pandemia, las empresas deben:

- Revisar que la plataforma de comercio electrónico corre en su última versión.
- Verificar los plugins.
- El vendedor comprobar la reputación del consumidor y los consumidores, la de los vendedores.
- Sostener un robusto sistema de contraseñas.
- Evitar enviar información personal o privilegiada por fuera de la plataforma.
- Omitir el bombardeo de información por redes sociales.
- Verificar la legitimidad del sitio.

[57] SEMANA. Usuarios no están satisfechos con beneficios a cambio de sus datos. Revista Semana. [en linea] [consulta:2021] Disponible en https://www.semana.com/empresas/articulo/uso-de-datos-personales-por-parte-de-las-empresas-no-agrada-a-usuarios/296775/

[58] ESET. Crece el Ecommerce y aumentan las estafas y los incidentes de seguridad. [Sitio web] [consulta:2021] Disponible en https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

- Comprobar que sean usuarios reales y no perfiles falsos.
- Sospechar de ofertas baratas.
- Utilizar un sistema de seguridad eficiente.
- En caso de pagar con código QR es importante que sea legítimo y no provenga de cuentas sospechosas o ajenas al sitio oficial.

Igualmente, la Superintendencia de Industria y Comercio[59], recomendó:

- Abstenerse de suministrar datos personales frente a estos mensajes falsos enviados ya sea por correo o mensajes a celular.
- Verificar la veracidad de la información con la Entidad.
- Revisar que la información recibida provenga de una empresa ya sea pública o privada, que se encuentre autorizada para recolectar datos personales.

Una opinión distinta a los dos párrafos anteriores sostiene Díaz[60] donde refiere que es importante tener en cuenta las normas, debido a que estas, son las que permiten tomar medidas eficientes de seguridad cuando se hace uso de plataformas de E_commerce. Según el autor las empresas que hacen uso del comercio digital deben tener en cuenta la "ley 1581 de 2012" y el cumplimiento también de la norma "PCI DSS", siendo esta última en la que más se hace referencia, ya que, habla de un marco de buenas prácticas que cubre aspectos de seguridad tan importantes como criptografía en el almacenamiento y transferencia de datos, seguridad perimetral, revisión constante a la plataforma tecnológica en seguridad de infraestructura, autenticación de usuarios, procesos adecuados en control de accesos, a su vez se tiene presente la seguridad en el almacenamiento, procesamiento y transmisión de datos personales de titulares de tarjetas. Con esto se cumplirá la normatividad y se disminuirá los riesgos materializados por pérdida o robo de información.

Por el contrario, el portal de Noticias Caracol[61] afirma que si un negocio vende por internet a través del Marketplace deben tener en cuenta lo siguiente:

- Poner la información completa de los productos como foto, descripción y disponibilidad.
- Tener el precio adecuado por cada uno de los productos.
- Revisar periódicamente las estadísticas de la plataforma digital.

---

[59] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Datos personales y coronavirus covid 19. [Sitio web] [Consulta: 2021] disponible en https://www.sic.gov.co/slider/datos-personales-y-coronavirus-covid-19-

[60] DÍAZ, ORTIZ, Arthus. Nueva norma para la seguridad en las transacciones Eléctricas. Revista Empresarial & Laboral [en linea] [consulta: 2021] Disponible en https://revistaempresarial.com/tecnologia/nueva-norma-para-la-seguridad-en-las-transacciones-electronicas/

[61] NOTICIAS CARACOL. ¿Cómo vender con éxito a través de internet? Estos consejos le pueden ser muy útiles. [Sitio web] [consulta: 2021] Disponible en https://noticias.caracoltv.com/economia/util-y-rapido/como-vender-con-exito-a-traves-de-internet-estos-consejos-le-pueden-ser-muy-utiles

- Asesoría de expertos en estos tipos de comercio.

Así también, el diario EL PAIS[62], también menciona que entre los principales riesgos en el comercio online se encuentra los sitios web falsos, métodos de pago poco fiables y perfiles falsos de vendedores, pero a su vez menciona que los consumidores que hacen uso de las plataformas de comercio electrónico en tiempos de pandemia deben:

- Verificar datos importantes del vendedor o denominación social como datos de contacto, medios de comunicación directa, datos de inscripción en el Registro mercantil.
- Que se tenga una correcta autorización administrativa, donde se tenga un ente de supervisión.
- Tener en cuenta el código de conducta, que se pueda consultar electrónicamente.
- Que el precio del producto este acorde a los impuestos aplicables y al gasto de envió.
- Que se tengan claros los procedimientos de pago, entrega y ejecución.
- Recordatorio de las garantías aplicables.
- Duración del contrato según sea el caso.
- Tener en cuenta el procedimiento de reclamaciones.
- Los costes y plazos de devolución.
- Que exista un derecho de desistimiento.

Con respecto a lo mencionado en párrafos anteriores, se evidencia que las opiniones previas tienen enfoques distintos, pero entre ellas se visibiliza la misma intención, y es, que las empresas y clientes deben tener en cuenta ciertos aspectos seguridad para lograr salvaguardar la protección de sus datos.

Otro aspecto de seguridad a tener presente lo refiere la UNIVERSIDAD DE LIMA[63] esta discute que el comercio electrónico en el extranjero tuvo algunas novedades importantes, ejemplo, la verificación múltiple, la cual se basa de no solo usar una contraseña, sino que el usuario debe usar un token para mejor seguridad, implementar biometrías, mecanismos de voz o huella de voz, lectores de huella digital. Continuando con el tema, se sigue resaltando las medidas que se usan en otros países por ejemplo Google Wallet, donde un usuario realiza una compra haciendo uso de su celular por medio de bluetooth o NFC, donde también se puede programar para usar huella dactilar, digitar código o usar huella de voz. También resalta la instalación de Google Authenticator para mejorar la seguridad y tener así una mejor autenticación.

[62] EL PAIS. Como proteger mis derechos en el comercio electrónico. [Sitio web] [consulta:2021] Disponible en https://elpais.com/economia/2021/04/12/mis_derechos/1618211660_036186.html
[63] UNIVERSIDAD DE LIMA. El 'Boom' del comercio electrónico y sus riesgos. [Sitio web] [consulta:2021] Disponible en https://www.ulima.edu.pe/entrevista/carlos-torres-05-10-2020

De forma cercana, con lo mencionado por la Universidad de Lima, el banco BBVA[64], también recomienda que se debe tener presente una autenticación reforzada de cliente, donde se verifica que el cliente dice ser quien es, esta se basa en que el servicio de pago utilice mínimo dos factores de autenticación distintos. Por ejemplo: Que al realizar la transacción al cliente se le solicite una contraseña, a la vez tenga el celular para efectuar la operación y por último utilice su huella dactilar para entrar a los servicios de su aplicación.

Un aspecto diferente lo expreso la Empresa Sura[65], donde recomendó a las empresas que protegieran los datos personales de sus usuarios de la siguiente manera:

- Dentro de la empresa no todo el personal debe tener acceso a las bases de datos.
- Los datos sensibles deben estar a cargo de una persona especial en el área adecuada.
- Para el tratamiento de datos personales se debe contar siempre con la autorización del titular.
- Tener una política de protección de datos.
- Tener una adecuada gestión de las distintas solicitudes que pueden hacer los clientes sobre sus datos.
- Hacer usos de mecanismos de protección tecnológicos para evitar que los datos sean robados o se pierdan.
- El uso inadecuado de os datos representa un riesgo, se enfrenta a sanciones administrativas y económicas para la empresa.

Finalizando este debate, las empresas tanto nacionales como internacionales al ver la situación mundial de coronavirus, se enfocaron de manera inmediata a buscar diversos aspectos de seguridad para proteger datos personales en plataformas de comercio electrónico. Aquí es importante mencionar que cada empresa tiene un punto de vista diferente para lograr una efectiva seguridad, unas recomendaron estrategias directas para las plataformas E-commerce como implementar software y hardware de prevención de perdida de datos (DLP), otras aplicaron las normas o legislación vigente en sus sistemas digitales, algunas empresas dieron ciertas recomendaciones o consejos de como los consumidores debían salvaguardar sus datos cuando hacen compras por internet, en otra instancia, algunas sugirieron implementar varias medidas de seguridad como usar token, Google Wallet, Google Authenticator, varias preguntas de seguridad, biometrías, códigos de acceso, reconocimiento facial, huella dactilar o de voz.

[64] BBVA. PSD2 y autenticación reforzada: nuevas reglas sobre la verificación de la identidad de los clientes. [Sitio web] [consulta:2021] Disponible en https://www.bbva.com/es/opinion/psd2-y-autenticacion-reforzada-nuevas-reglas-sobre-la-verificacion-de-la-identidad-de-los-clientes/

[65] SURA. ¿Usas bien los datos personales sensibles? [Sitio web] [consulta:2021] Disponible en https://segurossura.com/co/blog/revista-empresas-sura/usas-bien-datos-personales-sensibles/

En conclusión, la revista FORBES[66] menciona que es muy importante contar con soluciones de seguridad y ciberseguridad para proteger la información y el riesgo de fuga de datos refiriendo como ejemplo la empresa Claro. Sostiene que la protección inicial de los datos se basa desde la instalación de un equipo especializado de red y correo, que le permita a la empresa tener un control mayor de las acciones que se realizan alrededor de la misma, donde se pueda validar la navegación web, el correo electrónico, las aplicaciones de mensajería, los archivos a compartir, que todo este auditado y controlado bajo la capa de seguridad en red. Otro aspecto muy importante para tener en cuenta es la protección de los datos donde se debe contar con un agente que controle toda la información almacenada en dispositivos externos recordando a los empleados sobre la confidencialidad y evitar el almacenamiento de la información. Por último, se debe hacer uso del servidor de Descubrimiento para que realice escaneo de conexiones, privilegios de información en las BD, en servidores principales y archivos, de igual manera permisos de acceso, también implementar un bunker de entrada y salida de datos. Por último, las empresas han de implementar consolas centrales que registren los intentos de vulneración a la información, mitigando fraudes y riesgos informáticos.

6.3 EXPLICACIÓN DE LAS ESTRATEGIAS DE SEGURIDAD MÁS IMPLEMENTADAS POR LAS MIPYMES EN UN ENTORNO E-COMMERCE PARA PREVENIR LAS FUGAS DE INFORMACIÓN.

Durante los tiempos de pandemia las empresas se valieron de varias estrategias que les permita prevenir las fugas de información en sus entornos e-commerce. Según la Organización Mundial del Comercio señala algunas de las estrategias implementadas como la contribución de formulación de políticas, mejorar el desarrollo de las plataformas de comercio, incluir mecanismos de control, prever el uso de certificados electrónico (normatividad) y desarrollar un ámbito de confianza en los consumidores.

Argumentando lo anterior, Según Access Now[67] en 2020 recomienda que las empresas implementen la siguiente estrategia para la protección de datos como:
Usar los derechos y principios de privacidad de datos: Consiste en Minimizar y limitar la recopilación y almacenamiento de datos, haciendo referencia de que la pandemia de COVID 19 no sea un pretexto para recopilar gran cantidad de datos innecesarios. Por otro lado, se debe limitar el acceso a dichos datos solamente a quienes requieran esta información, estos datos se deben almacenar de manera

[66] FORBES. Seguridad de la información en tiempos de pandemia. Revista Forbes Advertorial. [en linea] [consulta:2021] Disponible en https://forbes.co/2020/04/28/tecnologia/seguridad-de-la-informacion-en-tiempos-de-pandemia/

[67] ACCESS NOW. Recomendaciones para la protección de la privacidad y los datos en la lucha contra el COVID-19. [en linea] [Consulta: 2021] disponible en https://www.accessnow.org/cms/assets/uploads/2020/04/Recomendaciones-para-la-proteccio%CC%81n-de-la-privacidad-y-los-datos-en-la-lucha-contra-el-COVID-19.pdf

confiable y segura en bases de datos separadas.

Del mismo modo Cataldo[68] en la plataforma de pacto global red Colombia consolida que la información que las empresas tienen influencia permanezca protegida y que el derecho privacidad tenga prioridad en la entidad. Esto se logra usando como estrategia un riguroso apego a las normas que actualmente tratan sobre la protección de los datos, así mismo luchar para que no se vulneren los derechos humanos en proveedores, trabajadores y clientes logrando así, garantizar los derechos de cada uno de los involucrados.

Además, las MiPymes implementaron como estrategia para proteger a sus clientes en las plataformas E-commerce, divulgar consejos en diferentes medios de comunicación, de la forma en como los usuarios debían de proteger su información confidencial cuando hacen uso de sus plataformas de comercio electrónico. También, sugerían a sus clientes por estos medios de comunicación ingresar directamente a su página oficial, que toda compra o adquisición se hiciera usando una red privada o de casa y no redes públicas.

De acuerdo con el párrafo anterior, el Portal de Noticias Caracol[69], menciona estrategias que deben tener los televidentes para salvaguardar su información confidencial en plataformas de comercio electrónico, entre estas: Someterse al derecho de decidir qué información compartir, al igual reservarse de dar información que es de carácter sensible o discriminatoria como preferencias sensuales, credo religioso, historia clínica, dirección política, información de ámbito personal o familiar. También sugiere que se debe leer detenidamente la política de privacidad de cada plataforma electrónica y que, a pesar de todo, se tiene el derecho de conocer que hay en las bases de datos, actualizar la información, que se excluya algún dato y que sea rectificada.

Es importante destacar que las empresas usaron como estrategia, publicar en su página oficial o plataformas de comercio digital, banners de información o mensajes recordando a los usuarios, estrategias que les permite proteger sus datos personales, como, por ejemplo: Usar contraseñas seguras, cuando se realice cualquier tipo de transacción hacerla desde su equipo personal, no guardar contraseñas en el navegador, cambiar la contraseña constantemente, no solicitar ayudas de terceros, conectarse desde una red privada, contar con antivirus actualizado, leer las políticas de privacidad.

[68] CATALDO, Marcelo. Empresa y privacidad el dilema de la protección de datos en pandemia. [Sitio web] [Consulta: 2021] disponible en https://www.pactoglobal-colombia.org/blog/nuestras-voces/empresa-y-privacidad-el-dilema-de-la-proteccion-de-datos-en-pandemia.html

[69] NOTICIAS CARACOL. Cuidado con los datos personales. [Sitio web] [Consulta: 2021] disponible en https://www.facebook.com/NoticiasCaracol/videos/2203956366321618/

De igual modo, en el sitio oficial del ministerio de telecomunicaciones[70] se da a conocer unas estrategias para proteger la información personal, que fueron conocidas en la conferencia del día internacional de protección de datos personales. Donde se propone que se use una normatividad robusta, también se resalta que cada persona debe velar por la seguridad de sus propios datos, al igual de los que le rodean. Por otro lado, se señala que la huella digital es una herramienta importante que ayuda a evitar los ciberataques. Finalmente, se menciona el uso y creación de nuevas herramientas donde se salvaguarde la identidad personal y un análisis de datos.

Del mismo modo, la plataforma de mercado libre[71] en la nueva declaración de privacidad que hizo el 28 de junio de 2021, propone las siguientes medidas para detectar y prevenir, delitos y abusos que concierne a la seguridad de los datos personales:

- Implementar acciones y herramientas de prevención de delitos y fraudes con relación a la plataforma.
- Poner en marcha un modelo de algoritmo, para detectar y prevenir el fraude.
- Informar a los miembros de Brand Protection Program sobre la información de aquellos vendedores que han sido denunciados para que se puedan ejercer los derechos del cliente.

Continuando con el tema, también es importante mencionar que cada cliente, usuario o internauta es responsable de tomar sus propias estrategias para salvaguardar y proteger sus datos personales. Las organizaciones que velan por la seguridad y protección de datos personales, en sus sitios oficiales o plataformas e-commerce publicaron estrategias que debía implementar cada persona a la hora de realizar cualquier operación o transacción por internet. Con relación a lo anterior, la Superintendencia de industria y Comercio[72] en su página oficial público en cuanto al tratamiento de datos, la importancia de garantizar el principio de veracidad o calidad, principio de circulación y acceso restringido, principio de finalidad y principio de seguridad, en este último sugiere adoptar medidas estrictas de seguridad para evitar acceso no autorizado, perdida, consulta, adulteración o fraude de los datos personales.
Por otro lado, el Ministerio de las Tecnologías de la información y las

[70] MINISTERIO DE TELECOMUNICACIONES. Varias medidas para proteger los datos personales durante la COVID-19 fueron conocidas en conferencia. [Sitio web] [Consulta: 2021] disponible en https://www.telecomunicaciones.gob.ec/varias-medidas-para-proteger-los-datos-personales-durante-la-covid-19-fueron-conocidas-en-conferencia/

[71] MERCADO LIBRE. Declaración de privacidad y confidencialidad de la información de Mercado Libre. [Sitio web] [Consulta: 2021] disponible en https://www.mercadolibre.com.co/privacidad/declaracion-privacidad/1.1

[72] SUPERINTENDENCIA INDUSTRIA Y COMERCIO. Datos personales y Coronavirus COVID 19: Recolección y uso de datos en casos de urgencia médica o sanitaria. [Sitio web] [Consulta: 2021] disponible en https://www.mercadolibre.com.co/privacidad/declaracion-privacidad/1.1

comunicaciones[73] (MinTIC) propone como estrategia para salvaguardar la información de los usuarios, la implementación del modelo de seguridad y privacidad de la información (MSPI) el cual permite preservar el buen uso, la confidencialidad, disponibilidad, integridad y privacidad de los datos. Con la adopción de este modelo se busca promover mejores prácticas de seguridad de la información dentro de la organización.

Por último, se resalta una estrategia que involucra muchas de las estrategias mencionadas anteriormente, esta estrategia se basa en las soluciones DLP (Data Loss Prevention**)** que actualmente la empresa claro, Evotec, la revista Forbes e it Digital Security, el instituto nacional de ciberseguridad, Interempresas y entre muchas más, resaltan en sus sitios oficiales la importancia de implementar herramientas DLP para prevenir la perdida de datos o fuga de información. Según Interempresas[74] cita a Bitglass una compañía de seguridad total en la nube donde señala que muchas empresas actualmente usan aun herramientas como firewall, monitoreo y cifrado de red que ya no son estrategias adecuadas, como lo son las soluciones DLP.

Concluyendo con este objetivo, como se viene analizando en pandemia muchas de las empresas que hacen uso del comercio electrónico eligen soluciones DLP como estrategia qué posibilita la corrección y prevención de fuga de información, aunque en el mercado existen varias soluciones DLP, todas con llevan al mismo objetivo salvaguardar la información. Además, esta estrategia DLP previene perdidas o fugas de información a través de las distintas salidas o vectores como correo, mensajería instantánea, internet, capturas de pantalla, almacenamiento en la nube, móviles USB, control de archivos, unidades de red, impresión, aplicaciones, entre otros. Es importante resaltar que este tipo de estrategia implementa controles para prevenir riesgos y la mayoría de las empresas la usan para prevenir fugas de información. Asimismo, la revista it Digital security en 2019 cita la encuesta realizada por Garther que el 50% de las empresas tienen como estrategia la implementación de alguna forma DLP integrada, una cifra que en los últimos años ha venido creciendo.

[73] MINTIC. Fortalecimiento de la gestión TI en el estado. [Sitio web] [Consulta: 2021] disponible en https://mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/ .

[74] INTEREMPRESAS. Solo el 31% de las empresas usan soluciones de DLP pese a que las fugas de datos son su principal preocupación. [Sitio web] [Consulta: 2021] disponible en https://www.interempresas.net/Ciberseguridad/Articulos/319652-Solo-31-por-ciento-empresas-usan-soluciones-DLP-pese-fugas-datos-son-principal.html

6.4 COMPARACIÓN DE LA ESTRATEGIA DE SEGURIDAD PARA PREVENCIÓN Y PROTECCIÓN DE PÉRDIDA DE DATOS MÁS APROPIADA EN LAS MIPYMES CUANDO USAN PLATAFORMAS E-COMMERCE.

De acuerdo con el análisis que se viene adelantando en la presente monografía, se puede comparar como las diferentes estrategias que implementaron las MiPymes cuando usan plataformas E-commerce en tiempos de COVID 19 permiten salvaguardar la información, posibilitándoles seguir creciendo en el mercado y lo más importante, velar por la protección de datos de sus clientes. Se evidencia que empresas importantes del sector como evoTec, hacen uso de las soluciones DLP a comparación de otras estrategias que hay actualmente en el mercado o que se mencionaron en el objetivo anterior. Debido a que, este tipo de soluciones DLP tienen gran auge para evitar la fuga y perdida de información, logrando asegurar la información sensible de los clientes, una mejor reputación y sigan permaneciendo protegidas en el mercado.

Una de las estrategias expuestas en pandemia refiere a que **'el usuario es responsable de la protección de sus datos y de una normatividad robusta**' no es tan apropiada cuando hay empresas que necesitan recopilar una gran cantidad de información de los consumidores para poder vender, sobre todo las empresas que promocionan servicios. En cambio, la estrategia que propone EvoTec[75] donde afirma que lo más apropiado es la "implementación de software y hardware de prevención de perdida de datos" (DLP), donde asegura que es una solución de seguridad que incluye protección al navegador, firewalls, antivirus, protección probada online ante amenazas, entre otros. Siendo una de las mejores herramientas que alerta, monitoriza y es clave contra la perdida de información.

Otra de las estrategias en pandemia, se basa en que '**la mayoría de las empresas divulgaron en sus sitios web oficiales una serie de consejos a los usuarios sobre cómo deben proteger sus datos personales cuando hacen uso del comercio online**' aunque fue una buena estrategia que la mayoría de MiPymes implementaron, para enseñarle a los usuarios a evitar ataques cibernéticos, no se considera como una gran estrategia, debido a que, muchos usuarios desconocen sobre técnicas efectivas de seguridad informática. Comparativamente con EvoTec, la revista Forbes[76] sostiene que es importante que las empresas que usan plataformas de comercio digital cuenten con estrategias de seguridad, como lo son las soluciones DLP, similar a como implementa la empresa Claro, ya que es una estrategia, que ofrece soluciones de seguridad en la web, correo electrónico, servidores de archivos, monitoreo de red, dispositivos extraíbles y protección en el acceso a aplicaciones.

[75] EVOTEC. Prevención de fuga de información/ Data Loss Prevention (DLP) [Sitio web] [Consulta: 2021] disponible en https://www.evotec.es/prevencion-de-fuga-de-informacion-dlp/
[76] FORBES. Op. cit., p. 1.

Con relación a lo anterior, sostiene que el primer paso para implementar este tipo de solución DLP es instalando un equipo especializado de correo y de red que controle en un 360, las actividades que realizan los empleados incluso en el teletrabajo, donde se valida la navegación web, uso de archivos compartidos, aplicaciones de mensajería instantánea, usabilidad de correo electrónico, que todo este auditado y controlado bajo la capa de seguridad en red. Como segundo paso, instalación de un agente que controle todo almacenamiento de datos de dispositivos externos como CDs, USB, sistemas de impresiones, discos duros, enviando alertas a los funcionarios de la organización, recordando de la confidencialidad y el no almacenamiento de información. Como tercer paso, se debe contar con un servidor de descubrimiento que este escaneando privilegios y permisos de acceso a información en las bases de datos, escaneo a servidores y archivos principales, escaneo a conexiones, escaneo de entrada y salida de datos, permitiendo salvaguardar la información general de la empresa. Por último, la estrategia DLP debe contar con una consola principal de administración, que permita tener un registro de los intentos de vulneración a la información, que mitigue el fraude y riesgo informático en la empresa. De manera similar, la revista it Digital Security[77], manifiesta que en los últimos años se ha venido incrementando la demanda de soluciones DLP, siendo una estrategia importante para proteger el flujo de datos en uso, en reposo y en movimiento. A su vez, que las soluciones DLP permiten analizar los diferentes medios o canales en donde se ve, se transporta o se almacena la información, también contribuye a concretar políticas que refuercen la prevención de perdida de datos.

De igual forma, la empresa ITConnect[78] afirma que las organizaciones en tiempos de pandemia deben contar con un robusto sistema DLP que este bien configurado, que informe que aplicaciones se usan en el teletrabajo, al igual, muestre que datos se están accediendo, modificando, almacenando o eliminando. Por otro lado, que sea un sistema que brinde la capacidad de bloquear accesos a cierta información y permita a las empresas saber dónde está su información confidencial, quien accede a ella, donde se está compartiendo y en qué momento. Por el contrario, otra estrategia que se recomendó implementar en tiempos de Covid 19 fue el 'modelo de seguridad y privacidad de la información' (MSPI) que busca promover mejores prácticas de seguridad de la información dentro de una organización, pero no es una estrategia pensada para todos debido a que va dirigida prácticamente a profesionales o funcionarios que trabajen en el área de tecnología.

[77] IT DIGITAL SECURITY. DLP, o como prevenir la fuga de datos. [Sitio web] [Consulta: 2021] disponible en https://www.itdigitalsecurity.es/reportajes/2019/01/dlp-o-como-prevenir-la-fuga-de-datos

[78] IT CONNECT. COVID 19: DLP y seguridad de la información en estos tiempos. [Sitio web] [Consulta: 2021] disponible en https://itconnect.lat/portal/2020/04/01/covid-000019/

No obstante, las MiPymes que pusieron en marcha la estrategia 'apego a las normas que velan por la protección de datos' siendo una buena iniciativa y guía, pero tiene su defecto, ya que, la mayoría de los usuarios no hacen acato a la legislación, por desconocimiento o porque sinceramente no las ponen en práctica. Sin embargo, según la empresa Endpoint Protector[79] manifiesta que cualquier tipo de empresa debe implementar estrategias de protección de datos, no solo por cumplir una normatividad sino para evitar filtrado o perdida de datos que pueda dejar severas consecuencias en la reputación o estado financiero de la empresa. De Igual manera, refiere que las empresas deben usar herramientas DLP como parte esencial para la protección de datos, adaptándose a los esfuerzos y necesidades que se deben cubrir, logrando así, el cumplimiento de las nuevas regulaciones de protección de datos como CCPA (Ley de privacidad del consumidor de california) o GDPR (Reglamento General de Protección de Datos). La implementacion de esta estrategia de seguridad ayuda a las MiPymes que usan plataformas de comercio digital a encontrar, controlar y supervisar los datos sensibles que viajan dentro y fuera de la red. Ahora bien, en tiempos de pandemia el uso del comercio electrónico creció, obligando a que muchas de las MiPymes usen herramientas DLP para lograr, identificar y supervisar los datos confidenciales, como, por ejemplo, descubriendo como es la transferencia de la información en la red, que vulnerabilidades o malas prácticas de seguridad en el manejo de datos se puede presentar. Asimismo, una ventaja más de esta estrategia DLP es ser multiplataforma, ayuda que la empresa tenga menos gastos, ya que se puede controlar todo desde un mismo panel de control. Al igual, establece políticas y reglas preconfiguradas que son aplicables a toda la red de la organización, bloqueando transferencias de datos confidenciales a través de medios que son altamente inseguros (mensajería, aplicaciones, servicios en la nube, el compartido de archivos, entre otros.) También limita el acceso a datos confidenciales de personas no autorizadas, logrando que la empresa sea la única que pueda autorizar en función individual, grupal o por departamentos permitiendo cifrar o eliminar los datos que se encuentran en dispositivos no autorizados. Además, esta estrategia también permite que se controle puertos USB, periféricos en dispositivos logrando que solo se permita el acceso de dispositivos que se encuentren en la lista blanca y es importante destacar que los archivos transferidos por USB son cifrados automáticamente. Finalmente sugiere, que se tenga configurada una política de trabajo remoto DLP, con el fin de que las herramientas DLP funcionen fuera de la red de la empresa o en equipos que estén conectados o no, asumiendo la protección de la información sin importar en donde se encuentre el equipo. Del mismo modo, propone que las empresas eduquen a los empleados en seguridad de datos y en soluciones DLP, con el propósito de que los empleados no eludan políticas, denuncien problemas, eviten realizar malas prácticas de seguridad, corrijan errores y así de esta manera, las empresas que usan

[79] ENDPOINT PROTECTOR. Las mejores Prácticas de prevención de perdida de datos. [Sitio web] [Consulta: 2021] disponible en https://www.endpointprotector.es/blog/las-mejores-practicas-de-prevencion-de-perdida-de-datos/

plataformas de comercio electrónico en pandemia podrán garantizar la, integridad, confidencialidad, disponibilidad y protección de los datos.

En la tabla 1, se hace una comparación de las similitudes, diferencias, funcionabilidad, utilidad, ventajas y desventajas de cada una de las estrategias, para lograr mostrar la estrategia de seguridad para prevención y protección de pérdida de datos más apropiada en las MiPymes cuando usan plataformas e-commerce.

Tabla 1. Comparación de la estrategia DLP con las demás estrategias implementadas por las MiPymes en pandemia.

ESTRATEGIAS PARA LA PREVENCIÓN Y PROTECCIÓN DE PERDIDA DE DATOS.					
Comparación	**Implementar las soluciones de prevención de perdida de datos (DLP)**	**Las MiPymes divulgaron en sus sitios oficiales una serie de consejos y recomendaciones para sus usuarios, sobre cómo proteger sus datos personales cuando hacen uso del comercio online.**	**Modelo de seguridad y privacidad de la información (MSPI)**	**Apego a las normas que velan por la protección de datos.**	**El usuario es responsable de la protección de sus datos y de una normatividad robusta.**
Semejanzas	Proteger los datos y evitar accesos no autorizados, cuidando aquella información sensible que se encuentran en red, en herramientas, dispositivos, servidores, plataformas E-commerce o en cualquier parte del sistema de información.	Concientizar a sus usuarios la importancia de proteger sus datos personales, dando a conocer técnicas de ataque que usan los ciberdelincuentes y a su vez, brindar recomendaciones para salvaguardar su información.	Es una estrategia del gobierno colombiano, que tiene como objetivo la transparencia de los datos, adaptando buenas prácticas de seguridad de la información en entidades del sector público.	Tiene como propósito regular el tratamiento de los datos personales refiriendo el motivo, su tratamiento y uso, que las empresas o cualquier persona le piensa dar a los mismos, con el fin de realizar un seguimiento legal.	Que el mismo usuario se haga responsable de sus propios datos, que sea consiente a donde y a quien se los quiere compartir, siendo él mismo desde su propia autonomía el que acepte términos y condiciones sobre el tratamiento de sus datos personales.
	Es una estrategia pensada para todo tipo de empresa y usuario. La estrategia beneficia a todo tipo de empresa – clientes.	Es una estrategia implementada por la mayoría de las empresas. La estrategia beneficia sobre todo a los usuarios que tienen conocimientos base en técnicas de seguridad informática.	Es una estrategia pensada para el sector público. La estrategia beneficia únicamente a entidades del sector público. No tiene costo, pero su implementación depende de un	Estrategia que obliga a todas las empresas a velar por la protección de los datos personales. La estrategia beneficia a empresas y clientes que conocen la normatividad y las ponen en práctica. No tiene costo, pero si se requiere de un	Estrategia pensada únicamente para los usuarios. La estrategia beneficia únicamente a los usuarios que tienen cierto nivel de conocimiento en técnicas sobre la protección de datos.

Diferencias	Tiene un costo su implementación entre $25 a $90 dólares por año y por usuario.	El costo depende del sitio o medio web que se utilice para publicar la información.	profesional en el área TI.	experto en el tema para capacitar a todo el personal.	No tiene costo, pero si el usuario quiere tener más conocimiento en el tema, debe capacitarse en cursos relacionados con seguridad informática, que por lo general tienen algún costo.
Funcionabilidad.	Realiza un análisis de los datos a nivel contextual previniendo y protegiendo a la empresa - usuario sobre la perdida de información.	El administrador de la página web coloca todas las recomendaciones o consejos para que los usuarios que visiten la página las pongan en práctica.	El profesional TI en la empresa implementa el Modelo de Seguridad y Privacidad de la Información con el fin de incrementar la transparencia de la gestión pública	La implementa todo tipo de empresa sin importar si son públicas o privadas, para garantizar la protección de los datos personales.	El usuario se vale de sus propias técnicas de seguridad para proteger sus datos personales.
Utilidad	Esta estrategia la usaron la empresa Claro, Trend Micro, evoTec, Symantec, Intel Security, Endpoint Protector, Kaspersky Lab, etc.	Esta estrategia la implementaron Mercado Libre, superintendencia de industria y comercio, Access Now, El portal de Noticias caracol, Claro, ESET, Sura, BBVA, etc.	Las empresas del sector público, alcaldías, gobernaciones, entre otras.	Las empresas y usuarios que conocen la normatividad.	Los usuarios que tienen previos conocimientos en técnicas de ciberseguridad
	Según Letslaw[80] las ventajas de la estrategia DLP son: En la empresa se puede implementar soluciones DLP tanto al Software como al hardware. Permite la reducción de amenazas.	Todo tipo de empresa la puede implementar en su página o sitio web oficial. Todos los usuarios que ingresen al sitio web oficial de la empresa o plataforma de comercio electrónico pueden darse por enterados de las recomendaciones o consejos para proteger sus datos personales.	Según MINTIC[81] las ventajas del modelo MSPI son: Las empresas del sector publico garantizan la transparencia de sus datos. Suministra una serie de guías que permiten abordar cada una de las fases del modelo. Determina necesidades de la	Todo tipo de empresa la debe tener en cuenta para la protección de datos personales. Derecho a la protección de los datos. Está disponible para todos tanto para empresa y usuario. No tiene costo. Obliga a las empresas a	La empresa no se hace responsable por las malas prácticas ejercidas por los usuarios. El usuario es autónomo de brindar su información personal a la hora de adquirir productos o servicios. Es una estrategia que se puede implementar en tiempo inmediato si el usuario tiene

[80] LETSLAW. Que es la Prevención de Perdida de Datos o DLP. [Sitio web] [Consulta: 25 de mayo de 2022] disponible en https://letslaw.es/prevencion-de-perdida-de-datos/
[81] MINTIC. Op. cit.

	Garantiza la protección de los datos.	Es una estrategia que se puede implementar en tiempo inmediato.	empresa, requisitos de seguridad, procesos, estructura todo con el fin de garantizar la confiabilidad,	responder por la pérdida de datos personales.	conocimientos en seguridad informática.
Ventajas	Da cumplimiento a la normatividad vigente de protección de datos personales.	No tiene costo implementarla.	integridad y disponibilidad d ellos activos de información.	Los usuarios conocen diferentes medidas para proteger sus datos.	
	Evita multas por perdida de datos.		Promueve el uso de buenas prácticas de seguridad de la información.	Es una estrategia que se puede implementar en tiempo inmediato.	
	Ofrece soluciones de detección para prevenir perdida de datos en el correo electrónico, en los dispositivos de almacenamiento estén o no conectados, en la red y en la nube, donde garantiza que todo este monitoreado y protegido.				
	Permite que la empresa tenga inventarios y evaluaciones de sus datos.				
	Logra que la empresa tenga una clasificación de sus datos.				
	Implementación de políticas de gestión de los datos.				
	Implementa un solo programa global DLP para monitorear todo el sistema de la empresa.				
	Formar a los empleados.				

	Confianza por parte de los consumidores. Evita perdidas económicas en las MiPymes por perdida de datos.				
Desventajas	Es una estrategia que no se puede implementar de manera inmediata por lo que se debe tener previamente un análisis y una respectiva clasificación de los datos. Tiene costo. Dificultad para proteger los datos almacenados en la nube o en dispositivos personales, cuando se implementa el teletrabajo.	Solo son recomendaciones que las empresas dan, más no garantizan que se eviten ataques al hardware y al software tanto de la empresa como de los usuarios. No todos los usuarios que visitan el sitio web comprenderán y pondrán en práctica las recomendaciones o consejos sobre protección de perdida de datos. Las empresas no están garantizando la protección de los datos, si no implementan una protección en tiempo real tanto al hardware como al software. Desconfianza por parte de los usuarios, debido a que no se le garantiza la protección de sus datos personales.	Solo se puede implementar en entidades del sector público. Solo la pueden implementar profesionales en TI. La mayoría de las empresas la desconocen. Es una estrategia que se puede implementar no a corto plazo, si no, a mediano o largo plazo, hasta que el profesional en el área tenga organizado su plan operativo. Se debe usar mucha documentación para lograr su implementación. Se debe pagar periódicamente a un profesional para estar realizando seguimiento al MSPI.	Solo es una normatividad que las empresas deben cumplir, más no garantiza que se eviten ataques al hardware y al software tanto de la empresa como de los usuarios. Es una estrategia que no se puede implementar de manera inmediata cuando la empresa o el usuario no tiene conocimiento sobre la legislación vigente de protección de datos personales. Desconfianza por parte de los usuarios, debido a que la empresa no le garantiza 100% la protección de sus datos personales.	Es una estrategia que tendría éxito solo en los usuarios que tienen previos conocimientos en temas de ciberseguridad. La mayoría de las empresas no la ven como buena estrategia porque ponen en riesgo su reputación, son propensas a millonarias pérdidas económicas, por lo general los usuarios por falta de experticia en el tema no se hacen responsables. Es una estrategia que no se puede implementar de manera inmediata cuando el usuario no tiene conocimientos en temas de ciberseguridad. El usuario debe hacer cursos o estudiar para ser profesional en áreas de seguridad informática, lo cual le generan gastos para él. Desconfianza por parte de los usuarios, debido a que la empresa le asume toda su responsabilidad en caso de presentar pérdida de datos.

Fuente: Autor

Concluyendo este objetivo, se observa en la tabla comparativa y en el análisis que se viene desarrollando que la estrategia más apropiada, recomendada, con mayores ventajas y puesta en marcha por varias de las empresas para fortalecer la seguridad en sus plataformas de E-commerce en tiempos de pandemia, se centra en las soluciones DLP, considerándola como una estrategia eficiente que contribuye a las MiPymes a salvaguardar la información tanto de sí mismas como de sus

clientes, logrando su integridad, disponibilidad y confidencialidad. Es importante destacar que hay varias empresas que velan por proteger este activo tan importante, que es la información y que, del mismo modo, usan y recomiendan como estrategia las “soluciones de prevención de perdida de datos DLP” como la empresa ‘Symantec’, ‘Claro’, ’Endpoint’ ‘Protector’, ‘Trend Micro’, ‘Intel Security’, ‘evoTec’, ‘Kaspersky Lab’ y entre otras.

7 CONCLUSIONES

Después de realizar el análisis conceptual a los mecanismos de seguridad para protección de perdida de datos ofrecidos por las plataformas de comercio electrónico, se establece que las estrategias de seguridad que implantaron muchas de las MiPymes en tiempos de pandemia no garantizaban del todo la protección de datos o no lograban evitar la fuga de información; sin embargo, durante el presente análisis se pudo evidenciar que las empresas necesitan fortalecer más su estrategia de seguridad. Por lo que la implementación de software y hardware de prevención de perdida de datos DLP se convierte en una estrategia importante para evitar la fuga y perdida de datos, logrando en las MiPymes una mejor prevención y protección de su información.

Se pudo evidenciar que la mayoría de las MiPymes en tiempos de pandemia no estaban preparas en técnicas de seguridad informática, por esta razón sufrieron diferentes ataques cibernéticos en sus sitios oficiales o plataformas de comercio digital, entre los ataques cibernéticos más frecuentados se encuentra la suplantación de identidad, el phishing, ramsonware, los fraudes a medios de pago, el smishing, el pharming y la propagación e infección por código malicioso, entre otros.

Muchas de las micro, pequeñas y medianas empresas, subsanaron varios riesgos informáticos aconsejando a sus consumidores por medio de sus paginas oficiales, sobre la importancia de proteger sus datos personales cuando se hace uso del comercio online, entre los consejos más enunciados se encuentran: realizar toda transacción en la misma plataforma de comercio electrónico, no compartir datos sensibles por medios externos de la plataforma, siempre verificar la autenticidad y legalidad de la página, no hacer descargas de archivos sospechosos, verificar que la tienda virtual o plataforma en caso de Colombia este vigilada por la superintendencia de industria y comercio, verificar la reputación del vendedor o el consumidor, evitar hacer transferencias por medios externos, mantener actualizado el sistema operativo, el navegador, el antivirus, la plataforma E-commerce, las aplicaciones y por último, siempre denunciar cualquier incidente informático.

Cada MiPyme tiene un punto de vista diferente para lograr una efectiva seguridad de datos, unas recomendaron estrategias directas para las plataformas E-commerce como implementar software y hardware de prevención de perdida de datos (DLP), otras aplicaron las normas o legislación vigente en sus sistemas digitales, algunas empresas dieron ciertas recomendaciones o consejos de como los consumidores debían salvaguardar sus datos cuando hacen compras por internet, en otra instancia, algunas sugirieron implementar varias medidas de seguridad como usar token, Google Wallet, Google Authenticator, varias preguntas

de seguridad, biometrías, códigos de acceso, reconocimiento facial, huella dactilar o de voz.

Muchas de las estrategias que usaron las empresas en tiempos de Covid 19, para protección de perdida de datos en sus plataformas de comercio electrónico, se basan en derechos de privacidad de datos, el apego a la legislación y normas de protección de datos, divulgar consejos en sitios oficiales a sus consumidores sobre recomendaciones para el cuidado de datos sensibles, al igual que el usuario es responsable de velar por la protección de sus propios datos personales, implementación del modelo de seguridad y privacidad de la información y por ultimo el mas recomendado usar herramientas de ciberseguridad, como implementar software y hardware de prevención de pérdidas de datos (DLP).

Todas las estrategias de seguridad para la protección de datos en plataformas de E-commerce, buscan siempre prevenir la perdida de la información, no obstante, estas pueden ser atacadas por ciberdelincuentes, para obtener cualquier tipo de información confidencial, al igual controlar el tráfico de datos en la red o el servidor. En consecuencia, la seguridad, en el entorno de las plataformas de comercio electrónico, es un tema que siempre debe ser tenido en cuenta por las empresas, que a pesar de las estrategias y políticas de seguridad que se plantean, no son suficientes para combatir la diversidad de riesgos y delitos que se pueden presentar.

En este sentido, la elección de una buena estrategia de seguridad como las soluciones DLP, es una decisión que está basada de acuerdo con los objetivos de seguridad que tiene las MiPymes cuando usan plataformas E-commerce esto va acorde según su estructura, costo y seguridad. Por ello, la implementación de esta estrategia debe estar basada en argumentos de investigación, análisis, documentación y en conocimiento de profesionales.

Por último, la estrategia DLP prevención de la perdida de datos, se convierte en un elemento fundamental para detectar vulnerabilidades, amenazas o riesgos que atentan contra la seguridad de las empresas que usan plataformas de comercio electrónico. A su vez propone controles, alternativas o políticas que corroboren con la protección de los datos. En este aspecto la monografía que se viene desarrollando ha tenido como énfasis buscar una estrategia que vele por la seguridad de la información en las empresas que usan plataformas de comercio digital. Mediante este análisis y de acuerdo con los riesgos de seguridad más presentados se ha elegido las soluciones DLP como la mejor estrategia de seguridad, debido a su amplia cobertura de seguridad que puede generar dentro de la empresa, su fácil implementación, al igual, la que mayor sobresale en el mercado y como la más seleccionada por las empresas de hoy en día.

8 RECOMENDACIONES

Una vez ha finalizado esta investigación monográfica, en la cual se ha establecido mecanismos importantes para la elección de una buena estrategia de seguridad en el contexto de las MiPymes cuando usan plataformas de comercio electrónico, se recomienda que:

- Empresas tanto como consumidores sean responsables de velar por el cuidado de los datos sensibles, de la misma manera, tener en cuenta estrategias como el uso de derechos de privacidad de datos, herramientas cibernéticas de prevención de perdida de datos como las soluciones (DLP), poner en práctica la legislación y normatividad que vela por la protección de datos personales y por último, aceptar los consejos y recomendaciones que hacen diferentes empresas o expertos en el tema para salvaguardarse de ataques y riesgos cibernéticos.

- Las MiPymes deben analizar de manera periódica sus técnicas aplicadas de seguridad informática para comprobar si efectivamente están aportando a salvaguardar los datos sensibles de sus consumidores cuando hacen uso de las plataformas de comercio electrónico. Al igual, es importante que comparen estrategias que están de punta en el mercado, como la estrategia basada en soluciones DLP que se propone en esta monografía, la cual, es elegida de acuerdo con la investigación documentada que se hizo, teniendo en cuenta las diferentes bases de datos, demostrando que es una de la más recomendadas por empresas nacionales e internacionales en tiempos de pandemia.

- Es importante que las MiPymes prioricen la seguridad de la información como un activo importante dentro de la organización, dado que las empresas que hacen uso de las plataformas de comercio electrónico son más susceptibles ataques cibernéticos, riesgos y amenazas.

- Las pequeñas y medianas empresas deben capacitar por lo menos una vez al año a sus empleados en temas de seguridad informática; Por otro lado, colocar en sus sitios web información para el usuario sobre la protección de perdida de datos.

- Realizar constantemente auditorias de seguridad informática a las plataformas E-commerce que brindan servicios en las MiPymes en tiempos de pandemia, para detectar en tiempo real posibles riesgos y así fortalecer sus políticas de seguridad.

9 BIBLIOGRAFÍA

ACCESS NOW. Recomendaciones para la protección de la privacidad y los datos en la lucha contra el COVID-19. [en linea] [Consulta: 2021]. Disponible en https://www.accessnow.org/cms/assets/uploads/2020/04/Recomendaciones-para-la-proteccio%CC%81n-de-la-privacidad-y-los-datos-en-la-lucha-contra-el-COVID-19.pdf

gACIS. Crece el E-Commerce aumenta las estafas y los incidentes informáticos. [Sitio web] [consulta:2021]. Disponible en: https://acis.org.co/portal/content/noticiasdelsector/eset-crece-el-ecommerce-aumentan-las-estafas-y-los-incidentes-de-seguridad

ACOSTA ARGOTE, C. Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. [Artículo] [consulta: 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

ÁLAMO CERRILLO, R. La economía digital y el comercio electrónico: su incidencia en el sistema tributario. Dykinson. (pp. 21) [Libro] [Consulta: 2016] PASCUAL, S. I. Comercio electrónico. Mc Graw Hill Education. (pp.16) [sitio web] [s.f]. Disponible en: http://www.ebooks724.com.bibliotecavirtual.unad.edu.co/?il=5357&pg=1

NARVAEZ CHINGAL, M.Y; ORTEGA MEZA, L. S. Importancia del comercio electrónico en la actualidad. *Travesía Emprendedora*, vol. 4, no 1, (p. 36-38) [Artículo] [Consulta: 2020]. Disponible en: http://editorial.umariana.edu.co/revistas/index.php/travesiaemprendedora/article/view/2480/2745 ESPITIA

ZULUAGA, L.M. Comercio electrónico en Colombia: Un mercado pionero amenazado por los gigantes del e-commerce. (pp.19) [Trabajo de grado] [Consulta: 29 de noviembre de 2019]. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/47241/Trabajo%20de%20Grado%20FINAL%20CORREGIDA.pdf?sequence=1&isAllowed=y

JIMÉNEZ, Y. J. Comercio electrónico ventajas y desventajas. 2019. (pp. 10-11) [Proyecto de Grado] [consulta: noviembre 2019]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/16999/3/2019_Comercio_electronico_ventajas.pdf VEGA

CLEMENTE, V. Comercio electrónico y protección de datos. Revista de Estudios Económicos y Empresariales, (pp. 213-214) [Libro] [consulta: 2021].

ESPARZA CRUZ, Nelly. El comercio electrónico en el Ecuador. Ecuador [en Linea] [consulta: 2021]. Disponible en: https://revistas.utb.edu.ec/index.php/sr/article/view/119/pdf

ATALAYAR. Aumenta la ciberdelincuencia durante la pandemia de la COVID-19. [Sitio web] [consulta: 11 de abril 2021] Disponible en: https://atalayar.com/content/aumenta-la-ciberdelincuencia-durante-la-pandemia-de-la-covid-19

BBVA. PSD2 y autenticación reforzada: nuevas reglas sobre la verificación de la identidad de los clientes. [Sitio web] [consulta:2021] Disponible en https://www.bbva.com/es/opinion/psd2-y-autenticacion-reforzada-nuevas-reglas-sobre-la-verificacion-de-la-identidad-de-los-clientes/

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO. Que la pandemia no sea excusa para descuidar la ciberseguridad de su organización. [Sitio web] [consulta:2021] Disponible en: https://www.ccce.org.co/noticias/que-la-pandemia-no-sea-excusa-para-descuidar-la-ciberseguridad-de-su-organizacion/

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Ciberseguridad en entornos cotidianos; estudio del cibercrimen 2020. [Sitio web] [consulta:2021] Disponible en: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020/

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del Cibercrimen en Colombia 2019-2020. [Sitio web] [consulta:2021] Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CANDANOZA, E. El comercio electrónico en tiempos de pandemia. Editorial La República S.A.S. (p.20) [Tesis] [consulta:2021] Disponible en: http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1279_FusarioRJ.pdf

CATALDO, Marcelo. Empresa y privacidad el dilema de la protección de datos en pandemia. [Sitio web] [Consulta: 2021] disponible en https://www.pactoglobal-colombia.org/blog/nuestras-voces/empresa-y-privacidad-el-dilema-de-la-proteccion-de-datos-en-pandemia.html

CERVERA, Carlos; Comercio electrónico: compras y pagos disparados en Colombia en medio de la pandemia. [Sitio web] Actualicese.com. [Consulta:15 de mayo 2020] Disponible en: https://actualicese.com/comercio-electronico-compras-y-pagos-disparados-en-colombia-en-medio-de-la-pandemia/

CLARO. Lo que debes saber de las compras por internet. [Sitio web] [consulta: 29 de mayo 2020] Disponible en: https://www.claro.com.co/institucional/compras-por-internet/

COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 590. Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Bogotá: El Congreso. 2000.

COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY ESTATUTARIA 1581 DE 2012. Reglamentada parcialmente por el decreto nacional 1377 de 2013. [Sitio web] [consulta: 2021] Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

DIARIO OFICIAL DE LA UNIÓN EUROPEA. Reglamento (ue) 2016/679 del parlamento europeo y del consejo. [Sitio web] [consulta:2021]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

DÍAZ, ORTIZ, Arthus. Nueva norma para la seguridad en las transacciones Eléctricas. Revista Empresarial & Laboral [en linea] [consulta: 2021]. Disponible en https://revistaempresarial.com/tecnologia/nueva-norma-para-la-seguridad-en-las-transacciones-electronicas/

EL PAIS. Como proteger mis derechos en el comercio electrónico. [Sitio web] [consulta:2021]. Disponible en: https://elpais.com/economia/2021/04/12/mis_derechos/1618211660_036186.html

EL TIEMPO. Así están suplantando sitios web de comercio electrónico. Casa Editorial NIT. 860.001.022-7. [Sitio web] [consulta: 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/tacticas-de-suplantacion-de-sitios-web-de-comercio-electronico-578204

ENDPOINT PROTECTOR. Las mejores Prácticas de prevención de perdida de datos. [Sitio web] [Consulta: 2021]. Disponible en: https://www.endpointprotector.es/blog/las-mejores-practicas-de-prevencion-de-perdida-de-datos/

EQUIPO HEALTH&BENEFITS. Ecommerce: riesgos a los que se enfrentan los vendedores en internet. Willis Towers Watson Update. [Sitio web] [consulta: 2021]. Disponible en: https://willistowerswatsonupdate.es/ciberseguridad/e-commerce-riesgos-enfrentan-e-vendedores/

ESET. Crece el Ecommerce y aumentan las estafas y los incidentes de seguridad. [Sitio web] [consulta:2021] Disponible en https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

EVOTEC. Prevención de fuga de información/ Data Loss Prevention (DLP) [Sitio web] [Consulta: 2021] Disponible en https://www.evotec.es/prevencion-de-fuga-de-informacion-dlp/

IT DIGITAL SECURITY. DLP, como prevenir la fuga de datos. [Sitio web] [Consulta: 2021]. Disponible en https://www.itdigitalsecurity.es/reportajes/2019/01/dlp-o-como-prevenir-la-fuga-de-datos

FALCONES ESTRADA, J. Estándares de seguridad y confidencialidad de la información aplicables al e-commerce [Sitio web] [consulta:2021]. Disponible en: https://repositorio.pucese.edu.ec/bitstream/123456789/1502/1/FALCONES%20ESTRADA%20JAHIRO.pdf

FERAPONTOV. A. Consejos sobre transacciones y seguridad en eBay. [Sitio web] [consulta: 30 de septiembre 2020]. Disponible en: https://latam.kaspersky.com/blog/secure-ebay-trade/20194/

FORBES. Seguridad de la información en tiempos de pandemia. Revista Forbes Advertorial. [en linea] [consulta:2021] Disponible en https://forbes.co/2020/04/28/tecnologia/seguridad-de-la-informacion-en-tiempos-de-pandemia/

FTC. Libro de datos de Consumer Sentinel Network 2020. [Sitio web] [consulta: febrero 2021]. Disponible en: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020

GOMEZ RESTREPO, C. Seguridad, pilar para el auge del e-commerce. [Sitio web] [consulta: 4 de septiembre de 2021]. Disponible en: https://www.larepublica.co/internet-economy/seguridad-pilar-para-el-auge-del-e-commerce-3227286

GÓMEZ, F. L., y FERNÁNDEZ, R. P. P. Cómo implantar un sgsi según une-en iso/iec 27001 y su aplicación en el esquema nacional de seguridad. (p.90 - 125) [Sitio web] [consulta:2021]. Disponible en https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/reader.action?docID=5486388

INFOSECURITY. Los ciberataques más costosos en la industria del e-Commerce. [Sitio web] [consulta: 21 de abril de 2021]. Disponible en: https://www.infosecuritymexico.com/es/blog/los-ciberataques-mas-costosos-en-la-industria-del-eCommerce.html

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? España: CIBER. [Sitio web] [consulta:2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vsvulnerabilidad-sabes-se-diferencian

INTEREMPRESAS. Solo el 31% de las empresas usan soluciones de DLP pese a que las fugas de datos son su principal preocupación. [Sitio web] [Consulta: 2021] disponible en https://www.interempresas.net/Ciberseguridad/Articulos/319652-Solo-31-por-ciento-empresas-usan-soluciones-DLP-pese-fugas-datos-son-principal.html

IT CONNECT. COVID 19: DLP y seguridad de la información en estos tiempos. [Sitio web] [Consulta: 2021]. Disponible en https://itconnect.lat/portal/2020/04/01/covid-000019/

KPGM. Riesgos del e-commerce a raíz de COVID-19. Cárdenas Dosal, S.C., Sociedad civil mexicana. [Sitio web] [consulta: 2021]. Disponible en: https://home.kpmg/mx/es/home/tendencias/2021/01/riesgos-del-e-commerce-a-raiz-de-covid-19.html

LA NACION. [Sitio web]. Ciberdelitos: durante la pandemia hubo más del doble de denuncias que en los tres años previos. [Consulta: 08 de febrero 2021]. Disponible en: https://www.lanacion.com.ar/seguridad/ciberdelito-nid2593717/

LETSLAW. Que es la Prevención de Perdida de Datos o DLP. [Sitio web] [Consulta: 25 de mayo de 2022]. Disponible en https://letslaw.es/prevencion-de-perdida-de-datos/

MATA. Ransomware en tiempos de pandemia. [Sitio web] [consulta: s.f]. Disponible en: https://madata.com/ransomware-en-tiempos-de-pandemia/

MERCADO LIBRE. Consejos para cuidar la seguridad de tus transacciones online. [Sitio web] [consulta: julio 2021]. Disponible en: https://www.mercadolibre.com.pe/institucional/comunicamos/noticias/consejos-para-cuidar-la-seguridad-de-tus-transacciones-online

MERCADO LIBRE. Declaración de privacidad y confidencialidad de la información de Mercado Libre. [Sitio web] [Consulta: 2021]. Disponible en https://www.mercadolibre.com.co/privacidad/declaracion-privacidad/1.1

MINISTERIO DE TECNOLOGIA DE LA INFORMACIÓN Y LAS COMUNICACIONES. RESOLUCIÓN NÚMERO 002256 DE 06 de NOVIEMBRE DE 2020. [Sitio web] [consulta:2021]. Disponible en: https://www.mintic.gov.co/portal/715/articles-2627_politica_seguridad_privacidad_informacion_resolucion_2256_2020.pdf

MINISTERIO DE TELECOMUNICACIONES. Varias medidas para proteger los datos personales durante la COVID-19 fueron conocidas en conferencia. [Sitio web] [Consulta: 2021]. Disponible en https://www.telecomunicaciones.gob.ec/varias-medidas-para-proteger-los-datos-personales-durante-la-covid-19-fueron-conocidas-en-conferencia/

MINTIC. Fortalecimiento de la gestión TI en el estado. [Sitio web] [Consulta: 2021]. Disponible en https://mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/ .

NOTICIAS CARACOL. ¿Cómo vender con éxito a través de internet? Estos consejos le pueden ser muy útiles. [Sitio web] [consulta: 2021]. Disponible en https://noticias.caracoltv.com/economia/util-y-rapido/como-vender-con-exito-a-traves-de-internet-estos-consejos-le-pueden-ser-muy-utiles

NOTICIAS CARACOL. Comercio electrónico en Colombia creció exponencialmente y también lo hicieron las quejas. Caracol. [Sitio web] [consulta: 2021]. Disponible en: https://noticias.caracoltv.com/actualidad/al-pie-de-la-letra/comercio-electronico-en-colombia-crecio-exponencialmente-y-tambien-lo-hicieron-las-quejas

NOTICIAS CARACOL. Cuidado con los datos personales. [Sitio web] [Consulta: 2021]. Disponible en: https://www.facebook.com/NoticiasCaracol/videos/2203956366321618/

OECD. Recommendation of the Council on Consumer Protection in E-Commerce, OECD Publishing, Paris. [Sitio web] [Consulta: 2021]. Disponible en: https://doi.org/10.1787/9789264255258-en.

OMS. Información básica sobre la COVID-19. [Sitio web] [consulta:2021] Disponible en: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19

PINZÓN PARADA, I. Gestión del riesgo en seguridad informática. Universidad Piloto de Colombia. [Sitio web] [consulta: 2021].

PORTAFOLIO. Delitos informáticos, la otra pandemia en tiempos de coronavirus. [Sitio web] [consulta:2021]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

RIBAGORDA, Arturo. Seguridad y comercio en el web. Universidad Carlos III de Madrid. España [en linea][consulta:2020]. Disponible en: https://revistasic.com/revista41/pdf_41/SIC_41_bibliografia.PDF

LABODIA, BONASTRE, José. Seguridad en el comercio electrónico. (pp.108-109). [en linea] [s.f]. Disponible en: https://www.acta.es/medios/articulos/ergonomia_y_seguridad/014105.pdf

FUSARIO, R. J. Vulnerabilidades en la seguridad de las transacciones interactivas de comercio electrónico a través de la web. (pp. 81-86). [Libro] [consulta:2021].

OBSERVATORIO LEGISLATIVO CELE. (2019). [Sitio web] [consulta:2021]. Disponible en: https://observatoriolegislativocele.com/colombia-ley-de-proteccion-de-datos-personales-2012/pdf?sequence=6&isAllowed=y

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de datos personales. [Sitio web] [consulta:2021]. Disponible en: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

SICE. Comercio Electrónico/Legislación Nacional - Colombia. [Sitio web] [consulta:2021]. Disponible en: http://www.sice.oas.org/e-comm/legislation/col2.asp

GONZALES, Carolina. Los datos personales en días de comercio electrónico.

Editorial La República S.A.S. [Libro] [consulta:2021]. Disponible en: https://www.asuntoslegales.com.co/consultorio/los-datos-personales-en-dias-de-comercio-electronico-3007397

Noticias: Con la “nueva normalidad”, los delitos informáticos se multiplicaron en el país, pero pueden contrarrestarse con inversiones en seguridad digital. [Sitio web] [consulta:2021]. Disponible en: https://www.ccce.org.co/noticias/con-la-nueva-normalidad-los-delitos-informaticos-se-multiplicaron-en-el-pais-pero-pueden-contrarrestarse-con-inversiones-en-seguridad-digital/

SIGNIFICADOS. Significado de Vulnerabilidad. [Sitio web] [consulta:2021]. Disponible en: https://www.significados.com/vulnerabilidad/

RODRÍGUEZ, K; ORTIZ, Olga; QUIROZ, Alicia; y PARRALES, Maria. El e-commerce y las Mipymes en tiempos de Covid-19. [en línea]. 2020, noviembre,05 [Consultado 05 de mayo 2021]. Disponible en: http://w.revistaespacios.com/a20v41n42/a20v41n42p09.pdf

SEMANA. Usuarios no están satisfechos con beneficios a cambio de sus datos. Revista Semana. [en linea] [consulta:2021]. Disponible en https://www.semana.com/empresas/articulo/uso-de-datos-personales-por-parte-de-las-empresas-no-agrada-a-usuarios/296775/

SERRANO, Javier. Revista de Economía Plataformas De Comercio Electrónico E Internacionalización Empresarial. Información Comercial Española [en línea] España [Consulta:30 de abril 2020]. Disponible en: https://doi-org.bibliotecavirtual.unad.edu.co/10.32796/ice.2020.913.6987

SKIBA, K. La pandemia resulta terreno fértil para los ladrones de identidad. [Articulo] [consulta: 6 de febrero de 2021]. Disponible en: https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2021/ladrones-de-identidad-aumentan-en-la-pandemia.html

STATISTA. Los intentos de phishing en tiempos de COVID-19. [Artículo] [consulta: 2020] Disponible en: https://es.statista.com/grafico/18427/intentos-de-phishing-durante-la-pandemia/ SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Datos personales y coronavirus covid 19. [Sitio web] [Consulta: 2021] disponible en https://www.sic.gov.co/slider/datos-personales-y-coronavirus-covid-19-

SUPERINTENDENCIA INDUSTRIA Y COMERCIO. Datos personales y Coronavirus COVID 19: Recolección y uso de datos en casos de urgencia médica o sanitaria. [Sitio web] [Consulta: 2021] disponible en https://www.mercadolibre.com.co/privacidad/declaracion-privacidad/1.1

SURA. ¿Usas bien los datos personales sensibles? [Sitio web] [consulta:2021]. Disponible en: https://segurossura.com/co/blog/revista-empresas-sura/usas-bien-datos-personales-sensibles/

TIRADO RÍOS, N. R. Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. Revista Publicando [Sitio web] [consulta: 2021].

UNIVERSIDAD DE LIMA. El 'Boom' del comercio electrónico y sus riesgos. [Sitio web] [consulta:2021]. Disponible en https://www.ulima.edu.pe/entrevista/carlos-torres-05-10-2020

VILLAR ESTRADA, S. S. El obligado y acelerado desarrollo del e-commerce en el Perú durante la pandemia COVID-19: Cuando el miedo y la necesidad superaron la falta de confianza. [Articulo] [Consulta: 20 de agosto 2020] Disponible en: http://www.itaiusesto.com/wp-content/uploads/2020/11/El-obligado-y-acelerado-desarrollo-del-e-commerce-en-el-Per%C3%BA-durante-la-pandemia-COVID-19-Silvia-Villar.pdf

VISA. Capítulo 2 Dominio, Plataforma y Hosting. Plataformas e-commerce. Seminario visa e-commerce. [Sitio web] [consulta: 2021]. Disponible en: https://visaempresarial.com/Content/pdf/seminarios/Capitulo2/Tema/PlataformasEcommerce.pdf

Fecha de Realización:	09/07/2022
Programa:	Especialización en seguridad informática.
Línea de Investigación:	Infraestructura Tecnológica y seguridad en redes.
Título:	Análisis de la seguridad para protección de pérdida de datos en las plataformas e-commerce utilizadas por las MiPymes en tiempo de pandemia.
Autor(es):	Martínez Peña Eduin Yamith.
Palabras Claves:	Comercio electrónico, ciberdelitos, MiPymes, plataforma E-commerce, seguridad de la información,
Descripción:	Por medio de este estudio monográfico se desarrolló un análisis conceptual de las MiPymes enfatizándose en la seguridad para protección de datos en las plataformas de comercio electrónico en tiempos de covid 19. En primera medida, se realizó un estudio a diferentes masas documentales sobre la seguridad que se implementó en las plataformas de E-commerce. A su vez, se desarrolló una metodología de compilación, mediante la cual se analizó información sobre la protección de datos en los sistemas de comercio digital, donde se pudo encontrar elementos de vulnerabilidad, incidentes informáticos, denegación de servicio, suplantación de identidad, alteración o interceptación de datos y entre otros factores, con el fin de analizar los mecanismos enfocados en la seguridad de las plataformas de E-commerce, que fueron utilizadas por las pequeñas MiPymes. Este análisis permitió tener una mejor idea de cómo operaban las MiPymes en la protección de datos en sus sistemas de compra y ventas por internet, buscando nuevas estrategias de seguridad y la forma en cómo se enfrentaron a la seguridad de E-commerce. En este contexto, la presente monografía busca ser un referente para analizar la situación de las MiPymes en momentos de pandemia, en aspectos de seguridad, mostrando los resultados obtenidos de seguridad en protección de perdida de datos en plataformas de E-commerce durante la crisis mundial de coronavirus.

Fuente bibliográfica más destacada: Para el desarrollo de la presente monografía se consultaron 75 fuentes bibliográficas, acontinuación, se relacionan algunas: CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO. Que la pandemia no sea excusa para descuidar la ciberseguridad de su organización. [Sitio web] [consulta:2021] Disponible en: https://www.ccce.org.co/noticias/que-la-pandemia-no-sea-excusa-para-descuidar-la-ciberseguridad-de-su-organizacion/ CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Ciberseguridad en entornos cotidianos; estudio del cibercrimen 2020. [Sitio web] [consulta:2021] Disponible en: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020/ FORBES. Seguridad de la información en tiempos de pandemia. Revista Forbes Advertorial. [en linea] [consulta:2021] Disponible en https://forbes.co/2020/04/28/tecnologia/seguridad-de-la-informacion-en-tiempos-de-pandemia/ ENDPOINT PROTECTOR. Las mejores Prácticas de prevención de perdida de datos. [Sitio web] [Consulta: 2021] disponible en https://www.endpointprotector.es/blog/las-mejores-practicas-de-prevencion-de-perdida-de-datos/	
Contenido del documento:	Introducción. Definición del problema. Justificación. Objetivos. Marco referencial. Diseño metodológico. Desarrollo de los objetivos. Conclusiones. Recomendaciones. Bibliografía.
Marco Metodológico:	La actual monografía se desarrolló bajo tipo compilación, en modo descriptivo, por medio de la cual se analizó diferentes fuentes bibliográficas, sobre la seguridad para protección de pérdida de datos en las plataformas E-commerce utilizada por las MiPymes en tiempo de pandemia, en donde se encontraron los principales riesgos de seguridad, también se compararon las estrategias de seguridad más apropiadas para prevención y protección de pérdida de datos que implementaron las MiPymes cuando usan plataformas E-Commerce. En este aspecto, se tomó como fuente de consulta, diferentes artículos investigativos y teóricos que hablan del tema, los cuales centran su estudio en la seguridad y protección de datos en tiempos de covid 19 y las diferentes

	estrategias de seguridad para la protección de datos en plataformas de comercio digital. Para la recolección de la información se hizo un rastreo a diferentes fuentes bibliográficas usando como referente las siguientes variables: - Riesgos de seguridad en las plataformas de comercio electrónico. - Aspectos de seguridad más usados por las MiPymes para proteger los datos de sus clientes por medio de las plataformas E-commerce. - Estrategia de seguridad para prevención y protección de pérdida de datos. Las fuentes de recolección de información que se utilizó en primera medida son fuentes primarias como libros, artículos, prensa y grabaciones audiovisuales, la mayoría de información se consultó en la biblioteca de la UNAD y en sitios oficiales de instituciones reconocidas. Como segunda medida, las fuentes de recolección secundaria como revistas indexadas, trabajos de investigación de grado, publicaciones científicas, material cargado en los repositorios de universidades o plataformas académicas.
Conceptos adquiridos:	Se identificaron los ataques y riesgos de seguridad que más afrontaron las MiPymes en tiempos de pandemia siendo la suplantación de identidad, el phishing y el ransomware los delitos informáticos de mayor ocasión. A lo largo del desarrollo de la monografía, se muestra como varios autores, medios de comunicación y empresas, propusieron diferentes estrategias en pandemia para protección de datos personales cuando se hace uso de plataformas de comercio electrónico. De acuerdo con el estudio realizado las MiPymes deben priorizar la seguridad de la información como un activo importante dentro de la organización, dado que las empresas que hacen uso de las plataformas de comercio electrónico son más susceptibles ataques cibernéticos En la investigación se tiene como resultado que las MiPymes deben analizar de manera periódica sus técnicas aplicadas de seguridad informática para comprobar si efectivamente están aportando a salvaguardar los datos

	sensibles de sus consumidores cuando hacen uso de las plataformas de comercio electrónico. Al igual, es importante que comparen estrategias que están de punta en el mercado, como la estrategia basada en soluciones DLP que se propone en esta monografía, la cual, es elegida de acuerdo con la investigación documentada que se hizo, teniendo en cuenta las diferentes bases de datos, demostrando que es una de las estrategias más recomendadas por empresas nacionales e internacionales en tiempos de pandemia.
Conclusiones:	Se pudo evidenciar que la mayoría de las MiPymes en tiempos de pandemia no estaban preparas en técnicas de seguridad informática, por esta razón sufrieron diferentes ataques cibernéticos en sus sitios oficiales o plataformas de comercio digital, entre los ataques cibernéticos más frecuentados se encuentra la suplantación de identidad, el phishing, ramsonware, los fraudes a medios de pago, el smishing, el pharming y la propagación e infección por código malicioso, entre otros. Todas las estrategias de seguridad para la protección de datos en plataformas de E-commerce, buscan siempre prevenir la perdida de la información, no obstante, estas pueden ser atacadas por ciberdelincuentes, para obtener cualquier tipo de información confidencial, al igual controlar el tráfico de datos en la red o el servidor. En consecuencia, la seguridad, en el entorno de las plataformas de comercio electrónico, es un tema que siempre debe ser tenido en cuenta por las empresas, que a pesar de las estrategias y políticas de seguridad que se plantean, no son suficientes para combatir la diversidad de riesgos y delitos que se pueden presentar. La estrategia DLP prevención de la perdida de datos, se convierte en un elemento fundamental para detectar vulnerabilidades, amenazas o riesgos que atentan contra la seguridad de las empresas que usan plataformas de comercio electrónico. A su vez propone controles, alternativas o políticas que corroboren con la protección de los datos.