UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

REVISIÓN DE LITERATURA SOBRE CIBERSEGURIDAD EN PYMES ENFOCADAS AL COMERCIO ELECTRÓNICO

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: KATHERIN YELENA LOOR PINELA

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Katherin Yelena Loor Pinela con documento de identificación N° 0957793094 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 30 de enero del año 2024

Atentamente,

_____

Katherin Yelena Loor Pinela
0957793094

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Katherin Yelena Loor Pinela con documento de identificación No. 0957793094, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Revisión de literatura sobre ciberseguridad en PYMES enfocadas al comercio electrónico", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 30 de enero del año 2024

Atentamente,

_____

Katherin Yelena Loor Pinela
0957793094

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: REVISIÓN DE LITERATURA SOBRE CIBERSEGURIDAD EN PYMES ENFOCADAS AL COMERCIO ELECTRÓNICO realizado por Katherin Yelena Loor Pinela con documento de identificación N° 0957793094, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 30 de enero del año 2024

Atentamente,

_____

Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo en primer lugar a mi Dios que gracias a su misericordia y bendiciones me ha permitido culminar esta meta tan anhelada.

También dedico a mi Madre, mi Padre, mis Hermanos, quienes siempre me han brindado su apoyo y han confiado en mí incondicionalmente. Además, a mi amada hija Ainhoa quien definitivamente ha sido mi motor y mi fuerza para no rendirme. Mi esposo Jhony quien ha sido una parte importante de compañía y comprensión durante este largo camino.

Finalmente, a mi abuelita porque con sus consejos y palabras de aliento hicieron de mí una mejor persona que no se deja derrotar fácilmente así también acompañándome en cada sueño, meta y proyecto que me plantee.

AGRADECIMIENTO

Agradezco a Dios por ser una parte fundamental en mi vida y quien me ha llenado de sabiduría y fortaleza durante todo este lapso para culminar con éxito este gran paso importante en mi vida para de esta manera poder escalar en el mundo profesional.

A mi familia por todo el apoyo para cumplir con esta meta, a mi tutor el Ing. Joe Llerena Izquierdo por su apoyo, guía y conocimiento brindado en la realización del trabajo de titulación.

A todos mis maestros y a la Universidad Politécnica Salesiana quienes han sido parte de este camino largo para mi crecimiento en el ámbito profesional y personal formándome como una buena cristiana y honrada ciudadana.

RESUMEN

El comercio electrónico se ha desarrollado especialmente en los últimos años debido a la pandemia en donde las PYMES debido a las restricciones y suspensión de sus operaciones presenciales optaron por la adopción del e-commerce.

Los negocios avanzan muy rápido que las organizaciones están expuestas a delitos informáticos asociados a las transacciones de comercio electrónico, por esta razón las PYMEs se ven obligadas a enfocarse en la seguridad y reducir las vulnerabilidades en la información y la protección de datos. El objetivo general en esta investigación es analizar los aspectos fundamentales en los que se basa la ciberseguridad para detectar posibles ciberataques en las PYMES con el objetivo de encontrar soluciones mediante la realización de un análisis exhaustivo de la literatura de los años 2020 hasta 2024. Se utiliza un estudio de tipo cuantitativo y descriptivo, la técnica del mapeo sistemático de acuerdo con el estándar del diagrama de flujo PRISMA para la revisión de literatura relevante. El uso de la técnica del mapeo sistemático obtuvo 30 artículos científicos relevantes, la consideración a resguardar más referenciada es la inseguridad en transacciones y medios de pago, la característica de seguridad más referenciada es la integridad, el ataque más común es el ataque pishing y spear pishing, la solución tecnológica más utilizada es el Blockchain, Cifrado y la Inteligencia Artificial (IA).

Como conclusión a los resultados en este estudio las PYMEs podrán aumentar la confianza y la disposición de los clientes para realizar transacciones en el comercio electrónico.

Palabras claves: ciberseguridad, PYMEs, comercio electrónico.

ABSTRACT

Electronic commerce has developed especially in recent years due to the pandemic where SMEs, due to the restrictions and suspension of their face-to-face operations, choose to adopt electronic commerce.

Businesses advance so quickly that organizations are exposed to computer crimes associated with electronic commerce transactions, for this reason SMEs are forced to focus on security and reduce vulnerabilities in information and data protection. The general objective of this research is to analyze the fundamental aspects on which cybersecurity is based to detect possible cyberattacks in SMEs with the aim of finding solutions by carrying out an exhaustive analysis of the literature from the years 2020 to 2024. It is used a quantitative and descriptive study, the technique of systematic mapping in accordance with the PRISMA flowchart standard for the review of relevant literature. The use of the systematic mapping technique obtained 30 relevant scientific articles, the most referenced consideration to protect is insecurity in transactions and means of payment, the most referenced security characteristic is integrity, the most common attack is the pishing and Spear attack pishing, the most used technological solution is Blockchain, Encryption and Artificial Intelligence (AI).

It is concluded that with the result of this study, SMEs will be able to increase the confidence and willingness of customers to carry out transactions in electronic commerce.

Key words: cybersecurity, SMEs, e-commerce.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Actualmente, las organizaciones que están orientadas hacia el comercio electrónico se enfrentan a varias amenazas una de estas es el software con códigos vulnerables el cual se utiliza para introducir códigos fraudulentos en los procesos de pago con tarjeta de crédito en páginas web (Pérez González, 2021)(Lopez Chila & Andrade Ávila, 2020). Si bien, esto perjudica a los consumidores directamente pero también a la entidad ya que se ve afectada en conjunto a su reputación, procesos y su continuidad en el mercado por la pérdida de fidelidad (Coello Ochoa, 2021)(Miranda Jiménez, 2021). La seguridad tecnológica se ha convertido en un problema importante que limita el desarrollo y la popularidad del comercio electrónico (Terán Villafuerte, 2023)(Mayorga Muñoz, 2022). La integridad, la privacidad, el no repudio y la confidencialidad son dimensiones de seguridad importantes para proteger las transacciones de comercio electrónico contra amenazas a la seguridad (Osman, 2020)(Jamra et al., 2020).

Existen muchos programas maliciosos cuya amenaza puede o no estar dirigida desde varias fuentes, y existen algunos delincuentes, programadores, piratas informáticos, códigos de virus y más (Mayorga Muñoz, 2022)(Escalante Quimis, 2021)(Villamar Arellano, 2023). Hacer del ciberespacio una inversión continua es esencial para toda empresa comercial porque sigue invirtiendo dinero y adaptándose a todas las innovaciones en este entorno (Coello Ochoa, 2021). Construir un muro de seguridad excepcional para una empresa exitosa puede resultar costoso. Por lo tanto, cualquier empresa que opere debe contar con un departamento de soporte técnico de TI para mantenerse a salvo de las amenazas de ciberseguridad (Al-Bassam & Al-Alawi, 2021)(Falconi Tamayo, 2021).

Con el avance tecnológico, la ciberseguridad es más propensa a nuevos ataques cibernéticos tales como: malware, phishing, robo de credenciales, suplantación de identidad, denegación de servicio, ataque de red de protocolo, etc. (Toala Indio, 2021)(Reinoso Ordóñez, 2021)(Rosero Tejada, 2021). Por este motivo se emplea la revisión de diferentes soluciones para verificar fuentes de datos grandes y erradicar estos altercados, creando una falsa seguridad (Moncayo Ronquillo, 2021).

Las PYMEs se definen globalmente como empresas con un número de empleados de entre 10 y 250 personas. Sin embargo, son un aspecto fundamental tanto para el crecimiento como para la estabilidad de las economías en todo el mundo (Guaranda Lara, 2021). Las pymes no pueden seguir tratando el riesgo de ciberseguridad de esta manera, ya que la cuestión podría

complicarse más (Alahmari & Duncan, 2021). Por eso la investigación en este ámbito es sumamente importante para las PYMEs.

El objetivo general: Analizar los aspectos fundamentales en los que se basa la ciberseguridad para detectar posibles ciberataques en las PYMES con el objetivo de proteger la información sensible y asegurar la disponibilidad de los dispositivos que manejan la información.

Objetivos específicos: 1) Analizar los aspectos en los que se basa la ciberseguridad y que pueden emplearse en PYMES para aumentar la protección de seguridad e impedir ciberataques mediante una revisión de literatura. 2) Determinar los peligros y riesgos subyacentes en las transacciones y compras realizadas en los comercios electrónicos para su categorización e incidencia a través de la revisión de artículos científicos. 3) Evaluar los resultados obtenidos formulando estrategias que permitan mitigar los peligros y riesgos mediante el análisis cuantitativo y descriptivo.

Las pequeñas y medianas empresas son el verdadero campo de batalla de la ciberseguridad debido que se debe proteger los activos de comercio electrónico del acceso, uso, modificación o destrucción no autorizada.

2. REVISIÓN DE LITERATURA

2.1. Ciberseguridad

Las vulnerabilidades, riesgos, amenazas, confidencialidad, integridad, disponibilidad y autenticación son conceptos vinculantes a la seguridad cibernética operativa (Mullet et al., 2021).

Una vulnerabilidad es una debilidad que un atacante puede aprovechar para complicar un sistema. Los defectos pueden estar en programas, sistemas o controles; las vulnerabilidades pueden ser acceso remoto, software y red. Una amenaza se refiere a cualquier incidente que influya en algún tipo de operaciones, activos, personas, negocios o sistemas debido a un acceso no autorizado o una violación de información. El riesgo es el grado en que las amenazas y la probabilidad de que ocurran afectan una actividad, activos, personas o una empresa; en temas de ciberseguridad, el riesgo se manifiesta en propiedades como la pérdida de confidencialidad, integridad, disponibilidad y autenticación. La accesibilidad permite realizar tareas o permite el acceso a recursos, que pueden ser hardware, software o información. La integridad se refiere a mantener la información precisa. Confidencialidad: El derecho para acceder a los datos lo conserva únicamente la persona relevante o el propietario de estos. El acceso de terceros hacia la data es considerado una amenaza. La autenticación es el mantenimiento de los permisos del usuario y el acceso a recursos protegidos, y las amenazas utilizan vulnerabilidades para obtener acceso a recursos o información; El acceso inadecuado es el resultado de una mala configuración y puede causar daños físicos y lógicos.

2.2. Comercio Electrónico

El comercio electrónico, traducido al inglés como e-commerce, se define como una actividad económica que utiliza medios digitales para intercambiar bienes o servicios (Alcívar-Cruz & Llerena-Izquierdo, 2023).Por medio del sitio web, los usuarios tienen la posibilidad de acceder al catálogo y a la información que contenga el producto las 24/7. La razón por la que estas empresas son tan importantes es que ahora las consideran parte de sus planes estratégicos. Las empresas elaboran sus sitios web y perfiles en las redes modernas con el objetivo de influir en una amplia gama de compradores.

Tal es así que (Osman, 2020) estima que “para el 2040 el 95% de las compras serán en línea” que existe un crecimiento de ventas en e-commerce, cuyo cambio en su comportamiento de compra que según las estadísticas son realmente reveladores, de modo que 43% compran en

línea desde la comodidad de su cama, 23% en el lugar de trabajo, 20% desde el baño o en su vehículo, 10% cuando están bajo los efectos del alcohol y 4% de forma accidental.

2.3. Seguridad informática en PYMEs

La seguridad dentro de las pequeñas y medianas empresas es un aspecto importante de las plataformas de comercio electrónico debido que los ciberdelincuentes consideran que este tipo de organizaciones son objetivos atractivos, ya que pueden tener sistemas de seguridad más débiles en comparación con las empresas más grandes (Melendrez-Caicedo & Llerena-Izquierdo, 2022). Mientras algunos piratas informáticos continúan atacando el comercio electrónico y robando información privada de los clientes (Pérez González, 2021). La seguridad del comercio electrónico tiene como objetivo proteger los activos ante el acceso, uso, modificación o ingreso de intrusos. Según (Jamra et al., 2020), existen siete dimensiones de la seguridad del comercio electrónico:

Integridad, comprueba si hay datos no autorizados que se reutilizan sin el permiso del usuario.

No repudio, no niega la venta ni la compra.

Autenticación, garantiza que solo los usuarios con autorización tengan el acceso a la cuenta.

Confidencialidad, se refiere al cifrado y descifrado.

Privacidad, puede controlar los términos bajo los cuales se adquiere y utiliza la información personal.

Disponibilidad, se refiere a la verificación de la eliminación de datos.

Al realizar auditorías, garantiza el almacenamiento de registros y solo las personas autorizadas pueden acceder a la cuenta.

3. METODOLOGÍA

Esta investigación busca los factores de ciberseguridad que se usan en las PYMEs dentro del entorno del comercio electrónico, se utilizará una revisión sistemática de la literatura basada en orientación de soluciones que mitiguen aquellos ataques. La metodología se divide en 3 fases: inicio, Análisis cualitativo y Análisis de resultados, para cada fase se toman acciones durante la investigación como se describe a continuación. ver fig. 1.

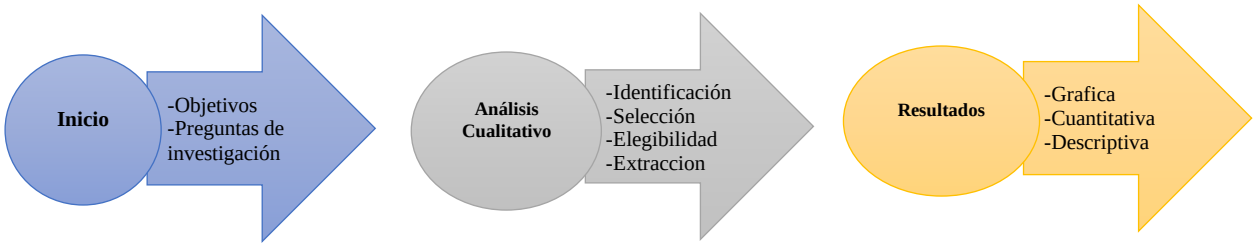


Figura 1. Revisión Sistemática.

1) Inicio: En esta etapa, se determinan los principales objetivos de la revisión sistemática y preguntas relacionadas con el tema o propósito del estudio.

El objetivo general es analizar los aspectos fundamentales en los que se basa la ciberseguridad para detectar posibles ciberataques en las PYMEs con el fin de proteger la información sensible y asegurar la disponibilidad de los dispositivos que manejan la información.

2) Análisis cualitativo: Para comprender a la ciberseguridad con respecto al comercio electrónico la metodología usa el análisis de arriba hacia abajo; conociendo los componentes, estrategias o tecnologías para mejorar la seguridad en las transacciones o medios de pago e identificar la frecuencia de ataques; esta metodología esta compuesta por cuatro actividades: identificación de estudios, selección, análisis de elegibilidad y extracción.

Identificación de estudios:

a) Clasificación: Se eligen artículos de investigaciones desde el año 2020; se usan las bases de datos: IEEE Xplorer y Google Scholar. Las palabras clave de búsqueda son: “(Cibersecurity OR E-commerce OR SMEs)”

b) Criterios de inclusión y exclusión: Los criterios de inclusión son: artículos desde el año 2020, artículos científicos o “articule review”. Artículos en idioma inglés. Los criterios de exclusión son: artículos menores al año 2020, artículos que no correspondan al área de estudio.

Selección: Se desarrolló mediante el proceso de investigación y los artículos fueron seleccionados según criterios.

Análisis de elegibilidad: Se desarrolló mediante el proceso de investigación y se realiza una revisión minuciosa correspondiente a cada artículo elegido.

Extracción: Se desarrolló mediante el proceso de investigación y se realiza extracción de la data correspondiente a cada artículo en una hoja de cálculo; los datos son: Consideraciones a

resguardar, Aspectos básicos de seguridad, Grupo de riesgos, Soluciones encontradas.

3) Análisis de resultados: En esta etapa los datos son tabulados en la hoja de cálculo con el fin de encontrar respuestas a las preguntas de investigación mediante gráficos, datos cuantitativos y descripciones ante las situaciones encontradas.

a. ¿Cuáles son las consideraciones para resguardar dentro de una PYMEs?

b. ¿Cuáles son los aspectos básicos de seguridad?

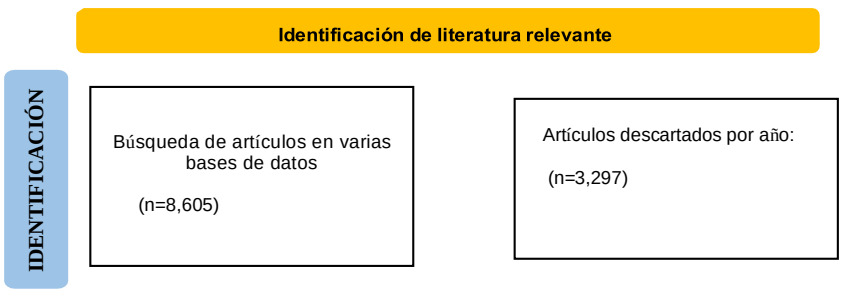
c. ¿Cuáles son los grupos de riesgos predominantes?

d ¿Cuáles son las Soluciones encontradas?

4. RESULTADOS

4.1. Identificación de investigaciones para clasificar las propuestas de ciberseguridad en PYMEs enfocadas al comercio electrónico mediante revisión bibliográfica.

Se empleó la revisión bibliográfica, es decir se examinaron artículos científicos relacionados a soluciones de ciberseguridad en pequeñas o medianas empresas enfocadas al comercio electrónico. El análisis cualitativo se utiliza para ayudar a comprender las cuestiones de ciberseguridad relacionadas con el comercio electrónico se realiza la identificación, selección, análisis de calificación y adquisición; búsqueda de vulnerabilidades, riesgos, amenazas y luego aplicar criterios de exclusión e inclusión. La búsqueda se basa en criterios de inclusión y exclusión dio como resultado 8,605 artículos, después de la revisión sistemática de la literatura se obtuvo 30 artículos, ver Fig. 2, estos artículos responden a los objetivos específicos.



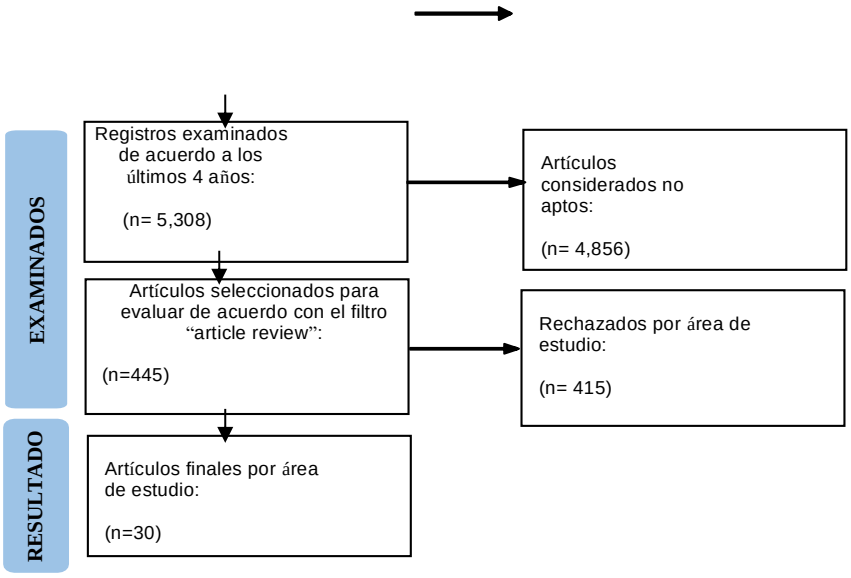


Figura 2. PRISMA para la selección de literatura relevante

Al extraer o separar datos en el libro de excel el cual contiene cuatro grupos y se describen a continuación. El primer grupo esta denominado como Consideraciones a resguardar conformado por: Inseguridad en transacciones y medios de pago, Inseguridad en el intercambio de información, Inseguridad en las redes internas de las PYMES. El segundo grupo esta denominado como Aspectos básicos de seguridad conformado por: Confidencialidad, Integridad, Disponibilidad y Autenticación. El tercer grupo esta denominado Grupo de riesgos conformado por: Ataques de ransomware, Ataques a la cadena de suministro, Filtración y piratería de datos, malware, Ataques de phishing y spear phishing, Ataques de denegación de servicio (DoS). El cuarto grupo esta denominado Soluciones encontradas conformado por: Computación en la nube, Blockchain, Firewalls, Software antivirus, Cifrado, Auditorias periódicas, Inteligencia artificial, Big Data y Capacitaciones a empleados.

La tabla 1 expone los 30 artículos que se utilizaron para la extracción de datos.

Repositorios	**Artículos Científicos**	**Cant.**

IEEE	(Wang et al., 2020), (Zawaideh et al., 2023), (Alahmari & Duncan, 2021),(Wang et al., 2020),(Y. Li & Li, 2020),(Al-Bassam & Al-Alawi, 2021), (Surya et al., 2023),(Huang, 2022),(M. Li et al., 2021),(Shen et al., 2023),(Jamra et al., 2020),(Sun et al., 2023),(Jain et al., 2022),(Bhatt & Gupta, 2021),(Mike et al., 2023),(Marican et al., 2023),(Wiafe et al., 2020),(Ozkan-Ozay et al., 2024),(Al-Khater et al., 2020)	19
GOOGLE	(Tzoneva et al., 2021),(Wan Asri et al., 2020),(Zhang et al., 2020),(Ebrahimi, 2021), (Ruiz & others, 2021), (Gull et al., 2023),(Badotra et al., 2021),(Osita et al., 2022), (Wylde et al., 2022),(Poehlmann et al., 2021), (Ubaidah et al., 2023)	11
	Total literatura relevante	30

Fuente: Autor.

Estos 30 artículos relacionados indican algunas características bibliográficas a considerar, el 63% de artículos (19 documentos) son de IEEE, el 37% de artículos (11 documentos) son de GOOGLE SCHOLAR, ver Fig. 3.

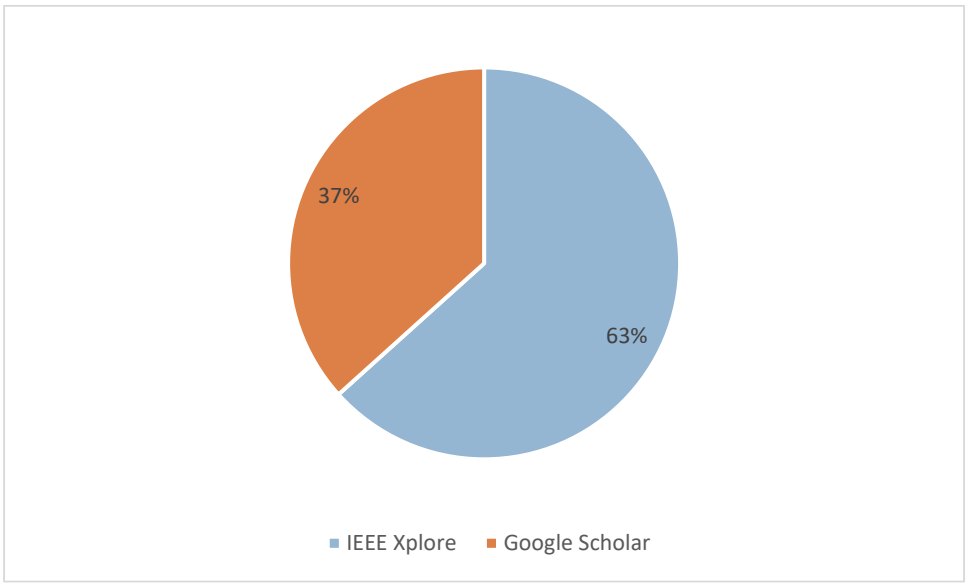


Figura 3. Bases de datos de publicaciones

4.2. Determinación de los grupos de ataques y las soluciones existentes de ciberseguridad en PYMEs enfocadas al comercio electrónico mediante la revisión científica.

A partir de estos 30 artículos obtenidos de la revisión bibliográfica se obtuvieron las soluciones y respuestas hacia las preguntas de investigación determinándose diferentes porcentajes ante las: Consideraciones a resguardar, Aspectos básicos de seguridad, Grupo de riesgos, Soluciones encontradas.

a. ¿Cuáles son las consideraciones para resguardar dentro de una PYMEs?

El primer grupo llamado Consideraciones a resguardar presenta: la inseguridad en transacciones y medios de pago 47%, la inseguridad en el intercambio de información 27% y la inseguridad en las redes internas de las PYMEs 27%, ver figura 4.

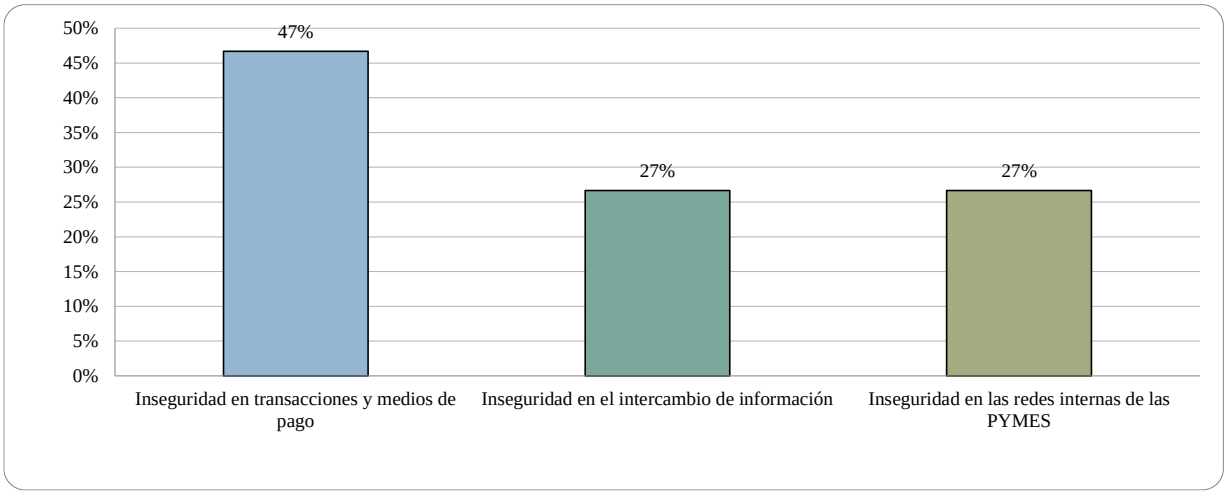


Figura 4. Consideraciones para resguardar.

b. ¿Cuáles son los aspectos básicos de seguridad?

El segundo grupo denominado Aspectos básicos de seguridad muestra: la confidencialidad 23%, la integridad 40%, la disponibilidad 17% y la autenticación 20%, ver figura 5.

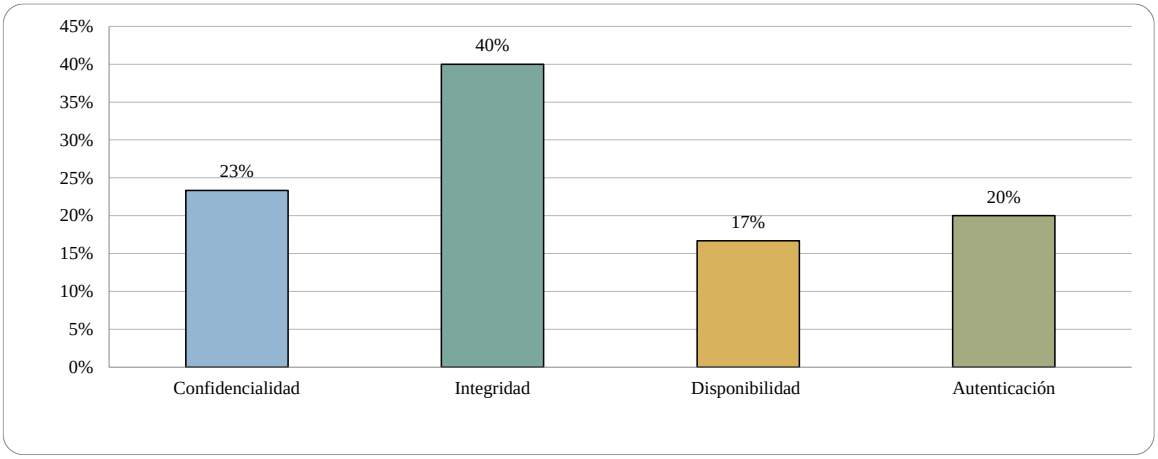


Figura 5. Aspectos básicos de seguridad

c. ¿Cuáles son los grupos de riesgos predominantes?

El tercer grupo llamado Grupo de ataques presenta: Ataques de ransomware 10%, ataques a la cadena de suministro 3%, Filtración y piratería de datos 17%, malware 20%, Ataques pishing o spear pishing 30%, Ataques de denegación de servicio (DOS) 13%, ver figura 6.

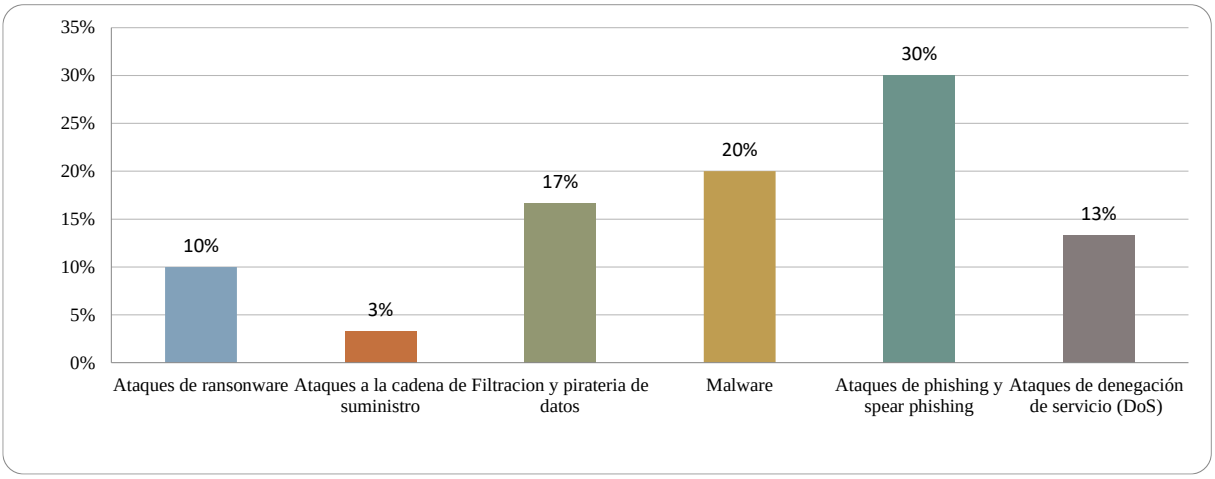


Figura 6. Grupo de riesgos.

d. ¿Cuáles son las Soluciones encontradas?

El cuarto grupo denominado Soluciones encontradas muestra: Computación en la nube en 10%, Blockchain 17%, Firewalls 10%, Software antivirus 10%, Cifrado 17%, Auditorias periódicas 7%, Inteligencia artificial 17%, Big Data 7% y Capacitaciones a empleados 7% ver figura 7.

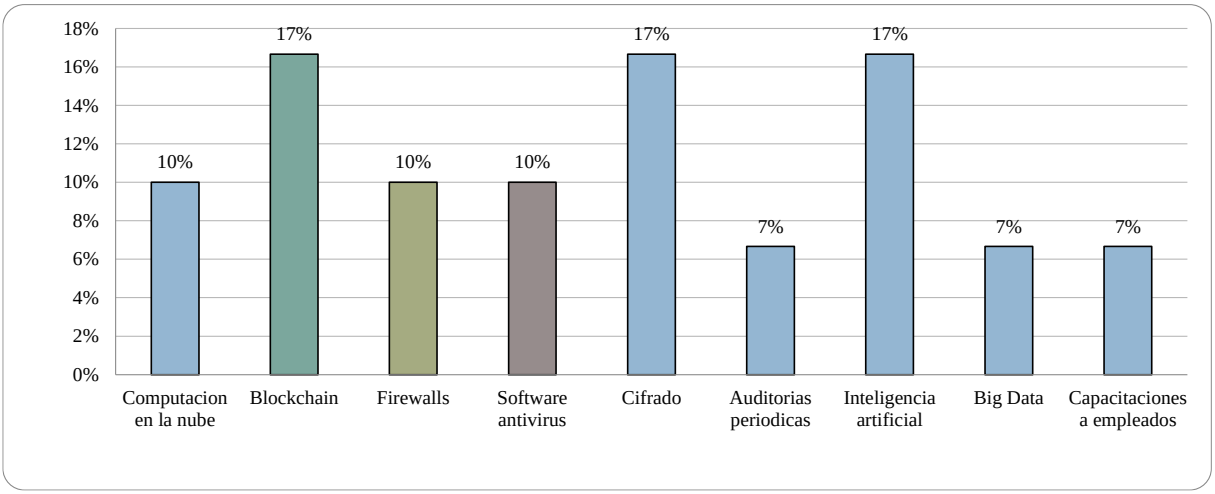


Figura 7. Soluciones encontradas

4.3. Análisis de resultados para conocer las soluciones de ciberseguridad en PYMEs enfocadas al comercio electrónico de los artículos científicos mediante el análisis cuantitativo y descriptivo.

Con base en la recopilación y tabulación de datos, cada conjunto de datos se obtiene de la siguiente manera:

La consideración para resguardar más referenciada es la inseguridad en transacciones y medios de pago, es decir que estas investigaciones intentan minimizar los fraudes existentes en los sistemas los cuales pueden ser usados por personas maliciosas y sobrepasar la seguridad; es decir 47% (14 artículos) referencia la inseguridad en transacciones y medios de pago.

El aspecto de seguridad más referenciado es la integridad, los artículos tratan de maximizarlos para que los datos o la información que los clientes utilizan cuando compran en línea deben permanecer iguales o no modificarse. Este principio es importante porque compartir o cambiar los datos de los clientes puede provocar una pérdida de confianza en la seguridad y la integridad del comercio electrónico; es decir 40% (12 artículos) referencian la integridad.

El grupo de ataque que predomina es el ataque pishing o spear pishing, estos artículos intentan minimizar la filtración de la data y minimizar estos problemas, ya que el vínculo entre el phishing y estos problemas es en muchos casos directo, ya que la mayoría de los ataques de ransomware y robo de credenciales comienzan con un intento de phishing exitoso, es decir un 30% (9 artículos) menciona el ataque pishing.

La solución tecnológica más usada se tiene al blockchain, cifrado e inteligencia artificial, es decir que los artículos nombran a estas 3 tecnologías debido que trabajando en conjunto el

blockchain ayuda a la IA a escalar para proporcionar información más procesable, gestionar el consumo de datos y el intercambio de modelos, y crear una economía de datos transparente y confiable.; es decir 17% (5 artículos) utilizaron estas tecnologías.

La figura 8 presentan los 30 artículos tabulados en la hoja de cálculo, para cada característica mencionada en las columnas y que se encuentren en el documento se marca con 1, por cada columna se obtiene la sumatoria, el valor del porcentaje se obtiene dividiendo la sumatoria de la columna para los 30 artículos.

Articulos		Consideraciones a resguardar			Aspectos básicos de seguridad				Grupo de riesgos						Soluciones encontradas								
Item	Año de publicación	Seguridad en transacciones y medios de pago	Seguridad en el intercambio de información	Seguridad en las redes internas de las PYMES	Confidencialidad	Integridad	Disponibilidad	Autenticación	Ataques de ransonware	Ataques a la cadena de suministro	Filtracion y pirateria de datos	Malware	Ataques de phishing y spear phishing	Ataques de denegación de servicio (DoS)	Computacion en la nube	Blockchain	Firewalls	Software antivirus	Cifrado	Auditorias periodicas	Inteligencia artificial	Big Data	Capacitaciones a empleados
1	2023	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
2	2023	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0
3	2021	1	0	0	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0
4	2020	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
5	2020	0	1	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
6	2021	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0
7	2023	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
8	2022	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0
9	2021	0	0	1	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
10	2023	0	1	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
11	2021	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
12	2020	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
13	2020	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
14	2021	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
15	2021	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
16	2023	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
17	2021	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0
18	2020	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
19	2022	0	1	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
20	2022	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
21	2023	0	1	0	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
22	2021	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
23	2022	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
24	2021	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
25	2023	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
26	2023	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
27	2020	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
28	2024	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0
29	2020	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
30	2023	1	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1
	Resultado	14	8	8	7	12	5	6	3	1	5	6	9	4	3	5	3	3	5	2	5	2	2
	Porcentaje	47%	27%	27%	23%	40%	17%	20%	10%	3%	17%	20%	30%	13%	10%	17%	10%	10%	17%	7%	17%	7%	7%

Figura 8. Revisión literaria.

5. DISCUSIÓN

Los 30 artículos seleccionados por el método PRISMA respondieron satisfactoriamente a las preguntas de investigación. La revisión sistemática aplicada ayuda a estructurar el documento volviéndolo comprensible para que los futuros investigadores de ciberseguridad en PYMEs enfocadas al comercio electrónico puedan obtener orientación adicional sobre el grupo de ataques y las soluciones tecnológicas.

En los 30 artículos seleccionados se verifica que el grupo de ataque mas predominante es el Pishing o spear pishing, seguido del malware, considerando que el ataque menos referenciado es el ataque a la cadena de suministro debido que al hablar de este ataque ya lo encontramos inmerso en el malware ya que un atacante puede apuntar a un proveedor de servicios de ciberseguridad y agregar código malicioso (o malware) a su software, que luego puede insertarse en las actualizaciones del sistema destinadas a los clientes del proveedor. Cuando los clientes descargan actualizaciones creyendo que provienen de una fuente confiable, el malware puede brindar a los atacantes acceso a los sistemas y la información de esos clientes.

La solución principal más referenciada son el blockchain, el cifrado y la Inteligencia artificial en 17%, el aspecto de seguridad mas referenciado es las Integridad en 40%, las consideraciones a resguardar predominan la inseguridad en transacciones y medios de pago en 47%.

La seguridad de las transacciones es un aspecto muy valioso ya que es la principal preocupación de los clientes potenciales en línea y la preocupación por parte de las pymes son los costos de estas soluciones tecnológicas por lo cual deben hacer un esfuerzo para obtenerlas debido que con el pasar del tiempo el Internet se introduce cada vez más en nuestro diario vivir, el comercio electrónico se convertirá en un actor importante en la economía dentro de los próximos años.

6. CONCLUSIÓN

El rápido crecimiento del comercio electrónico ha restructurado la manera en que las pequeñas y medianas empresas hacen negocios, permitiéndoles ingresar a los mercados globales y abrir nuevas oportunidades de crecimiento. Sin embargo, esta transformación digital también expone a las pymes a mayores amenazas a la ciberseguridad que pueden dañar sus datos, su integridad financiera y su reputación.

El objetivo general de esta investigación es analizar los aspectos fundamentales en los que se basa la ciberseguridad para detectar posibles ciberataques en las PYMEs con el objetivo de proteger la información sensible y asegurar la disponibilidad de los dispositivos que manejan la información, brindando una visión desde las consideraciones de inseguridad a resguardar, el aspecto de seguridad predominante, el grupo de ataque más común y la solución tecnológica más utilizada. Se encontraron un total de 22 características, que se enumeraron en una hoja de cálculo y respondieron a las preguntas de la investigación.

Muchos recursos están dedicados al fraude cibernético, el robo de identidad, la interceptación de mensajes, la privacidad, el abuso de datos personales y más. Esta investigación presenta algunos escenarios en los que puede existir un riesgo cibernético identificando una cantidad considerable de posibles ciberataques y vulnerabilidades.

De acuerdo con la revisión sistemática, la ciberseguridad se puede resguardar mediante el Blockchain, cifrado y la IA ya que bajo este esquema se puede preservar la privacidad de los usuarios tomando los datos en tiempo real bajo esquemas de seguridad aceptables de esta forma ayudando a proteger los datos confidenciales de su organización y reduzca eficazmente los problemas de fuga de datos.

7. REFERENCIAS

Al-Bassam, S. A., & Al-Alawi, A. I. (2021). Cybersecurity Risks on Health Sector Social Media: Systematic Literature Review. *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 1–9. https://doi.org/10.1109/ICDABI53623.2021.9655909

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*, *8*, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

Alahmari, A. A., & Duncan, R. A. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–6. https://doi.org/10.1109/ECAI52376.2021.9515166

Alcívar-Cruz, B., & Llerena-Izquierdo, J. (2023). After-Sales and Customer Loyalty Strategies for Fixed Internet Through the Implementation of Virtual Assistance in the Ecuadorian Context. In V. Robles-Bykbaev, J. Mula, & G. Reynoso-Meza (Eds.), *Intelligent Technologies: Design and Applications for Society* (pp. 139–149). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-24327-1_12

Badotra, S., Sundas, A., & others. (2021). A systematic review on security of E-commerce systems. *International Journal of Applied Science and Engineering*, *18*(2), 1–19.

Bhatt, A., & Gupta, H. (2021). Emerging Trends and Application Area of Cyber Security. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–4. https://doi.org/10.1109/ICRITO51393.2021.9596403

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

Ebrahimi, M. (2021). *AI-Enabled Cybersecurity Analytics: Detecting and Defending against Cyber Threats*. The University of Arizona.

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

Falconi Tamayo, L. F. (2021). *Desarrollo e implementación de una aplicación Web para la Gestión de Boletería de Vilaró Microteatro Restaurante*. https://dspace.ups.edu.ec/handle/123456789/20292

Guaranda Lara, S. N. (2021). *Modelo de gestión para el alineamiento de estrategias corporativas en pymes mediante las tecnologías de la información y comunicación*. http://dspace.ups.edu.ec/handle/123456789/20911

Gull, H., Alabbad, D. A., Saqib, M., Iqbal, S. Z., Nasir, T., Saeed, S., & Almuhaideb, A. M. (2023). E-commerce and cybersecurity challenges: Recent advances and future trends. *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, 91–111.

Huang, G. (2022). Research on e-commerce security in data and cloud computing environment. *2022 International Conference on Artificial Intelligence in Everything (AIE)*, 482–487. https://doi.org/10.1109/AIE57029.2022.00098

Jain, M., Sinha, A., Agrawal, A., & Yadav, N. (2022). Cyber security: Current threats, challenges, and prevention methods. *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 1–9. https://doi.org/10.1109/ICACCM56405.2022.10009154

Jamra, R. K., Anggorojati, B., Kautsarina, Sensuse, D. I., & Suryono, R. R. (2020). Systematic Review of Issues and Solutions for Security in E-commerce. *2020 International*

Conference on Electrical Engineering and Informatics (ICELTICs), 1–5. https://doi.org/10.1109/ICELTICs50595.2020.9315437

Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Alazab, M. (2021). Anonymous and Verifiable Reputation System for E-Commerce Platforms Based on Blockchain. *IEEE Transactions on Network and Service Management*, *18*(4), 4434–4449. https://doi.org/10.1109/TNSM.2021.3098439

Li, Y., & Li, J. (2020). Risk Management of E-Commerce Security in Cloud Computing Environment. *2020 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, 787–790. https://doi.org/10.1109/ICMTMA50254.2020.00172

Lopez Chila, R. D., & Andrade Ávila, A. E. (2020). *E-commerce, Rival o Aliado para las Comercializadoras Textiles de Guayaquil*. E-Commerce, Rival or Ally for the Textile Marketers of Guayaquil; Editorial Abya-Yala. https://pure.ups.edu.ec/en/publications/e-commerce-rival-or-ally-for-the-textile-marketers-of-guayaquil

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*, 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Mayorga Muñoz, C. J. (2022). *Amenazas en el espacio cibernético con incidencia en la información de entidades públicas y privadas*.

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Mike, N., Krén, E., & Kecskeméti, T. (2023). Information Security among SMEs in Hungary - An Overview. *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, 1521–1525. https://doi.org/10.23919/MIPRO57284.2023.10159886

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Mullet, V., Sondi, P., & Ramat, E. (2021). A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access*, *9*, 23235–23263. https://doi.org/10.1109/ACCESS.2021.3056650

Osita, G. C., Chisom, C. D., Okoronkwo, M. C., Esther, U. N., & Vanessa, N. C. (2022). Application of Emerging Technologies in Mitigation of e-Commerce Security Challenges. *CCU J. Sci*, *2*, 2734–3766.

Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*.

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*.

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021). The organizational cybersecurity success factors: an exhaustive literature review. *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*, 377–395. https://doi.org/https://doi.org/10.1007/978-3-030-71017-0_27

Reinoso Ordóñez, L. A. (2021). *Desarrollo de sistema informático para la gestión de pagos de cuotas de los residentes de la Urbanización Belo Horizonte*. https://dspace.ups.edu.ec/handle/123456789/20332

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los*

canales electrónicos: Un mapeo sistemático.

Ruiz, R. de S., & others. (2021). *Novel approaches to applied cybersecurity in privacy, encryption, security systems, web credentials, and education*. London Metropolitan University.

Shen, H., Wu, G., Xia, Z., Susilo, W., & Zhang, M. (2023). A Privacy-Preserving and Verifiable Statistical Analysis Scheme for an E-Commerce Platform. *IEEE Transactions on Information Forensics and Security*, *18*, 2637–2652. https://doi.org/10.1109/TIFS.2023.3269669

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys \& Tutorials*. https://doi.org/10.1109/COMST.2023.3273282

Surya, S., Jagtap, S. R., Ramnarayan, R., Priyadarshini, M., Ibrahim, R. K., & Alazzam, M. B. (2023). Protecting Online Transactions: A Cybersecurity Solution Model. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2630–2634. https://doi.org/10.1109/ICACITE57410.2023.10183282

Terán Villafuerte, B. J. (2023). *Análisis de delitos informáticos relevantes en organizaciones gubernamentales de Latinoamérica*.

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*.

Tzoneva, M., Forney, K. J., Keel, P. K., Walker, M., Thornton, L., De Choudhury, M., Teevan, J., Bulik, C. M., Levinson, C. A., Zerwas, S., Halliwell, E., Shen, C., Wasylkiw, L., & Williamson, M. E. (2015). Cybersecurity and Small to Medium Business. In *Sex Roles* (Vol. 23, Issue 5, pp. 269–282). https://doi.org/10.1016/j.jadohealth.2015.04.026

Ubaidah, S., Faqiani, N., Afiq, M. I., & Abd Aziz, N. E. (2023). Emerging Trends in Cybersecurity: Issues in Cybersecurity During Covid-19 Pandemic. *Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023*, 102.

Villamar Arellano, D. A. (2023). *Estrategias de prevención frente a los ciberataques en la Unidad Educativa Luis Alfredo Noboa Icaza*.

Wan Asri, Azman Che Mat, Engku Ahmad, Spenkuch, J. L., Wahab, A. R. A., Lewis, M. K., Hassan, M. K., Shariff, K., Syariah, D. I. A., Schmidt, U., Tennyson, S., Yang, H. K., & Shen, C. (2004). A Comparative Study of Consumer Trust in Major Digital Trade Agreements. In *Jurnal Pengurusan* (Vol. 23, pp. 269–282). https://doi.org/10.1016/j.jadohealth.2015.04.026

Wang, M., Ding, Z., Zhao, P., Yu, W., & Jiang, C. (2020). A Dynamic Data Slice Approach to the Vulnerability Analysis of E-Commerce Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(10), 3598–3612. https://doi.org/10.1109/TSMC.2018.2862387

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, *8*, 146598–146612. https://doi.org/10.1109/ACCESS.2020.3013145

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: a review. *SN Computer Science*, *3*(2), 127.

Zawaideh, F. H., Abu-Ulbeh, W., Mjlae, S. A., El-Ebiary, Y. A. B., Al Moaiad, Y., & Das, S. (2023). Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce. *2023 International Conference on Computer Science and Emerging Technologies (CSET)*, 1–7. https://doi.org/10.1109/CSET58993.2023.10346628

Zhang, S.-X., Zhang, Q.-Q., Liu, Y.-S., Yan, X.-T., Zhang, B., Xing, C., Zhao, J.-L., & Ying, G.-G. (2020). Reliance on Technology and the Increased Cybersecurity Vulnerabilities It

Poses to Our Transportation Industry. In *Science of the Total Environment* (Vol. 712, Issues 0048–9697).