Técnicas de computación utilizadas para prevenir delitos informáticos

Jimmy Intriago-Moreira[1], Leonardo Chancay-García[1]

Jintriago7783@utm.edu.ec, Leonardo.chancay@utm.edu.ec

[1]Universidad Técnica de Manabí, Ciencias Informáticas, Portoviejo, Ecuador

DOI: https://doi.org/10.56124/encriptar.v7i14.003

Resumen

En el marco de la prevención de delitos informáticos en América Latina, se ha realizado una revisión sistemática de la literatura con el propósito de analizar enfoques y hallazgos clave presentes en 24 artículos publicados entre 2018 y 2023. Estos artículos se han clasificado en dos categorías: delitos informáticos y técnicas de prevención. En relación con los delitos informáticos, se investigaron las modalidades existentes y la legislación vigente que los aborda. Por otro lado, en el ámbito de las técnicas de prevención, se examinaron tendencias, efectividad y desafíos relacionados con su implementación. El análisis revela una distribución equilibrada entre ambas categorías, con un 47.37% de los artículos centrados en delitos informáticos y un 52.63% en técnicas de prevención. Este estudio busca proporcionar una comprensión comprehensiva de los aspectos clave en la prevención de delitos informáticos en la región latinoamericana, así como ofrecer una perspectiva sobre las tendencias emergentes y los retos presentes en este campo.

Palabras-clave: delitos informáticos, prevención, técnicas, América Latina, España, revisión sistemática, modalidades, legislación, efectividad, desafíos.

Abstract

Within the framework of the prevention of computer crimes in Latin America, a systematic review of the literature has been carried out with the purpose of analyzing approaches and key findings present in 19 articles published between 2018 and 2023. These articles have been classified into two categories: computer crimes and prevention techniques. In relation to computer crimes, the existing modalities and the current legislation that addresses them were investigated. On the other hand, in the field of prevention techniques, trends, effectiveness and challenges related to their implementation were examined. The analysis reveals a balanced distribution between both categories, with 47.37% of the articles focused on computer crimes and 52.63% on prevention techniques. This study seeks to provide a comprehensive understanding of the key aspects of cybercrime prevention in the Latin American region, as well as offer a perspective on emerging trends and challenges present in this field.

Keywords: computer crimes, prevention, techniques, Latin America, Spain, systematic review, modalities, legislation, effectiveness, challenges.

1. Introducción

La tecnología ha experimentado un crecimiento impresionante a nivel global durante las últimas tres décadas, generando un aumento significativo de conductas delictivas en el ciberespacio. Estas nuevas formas de delincuencia han surgido en respuesta al avance constante de las Tecnologías de la Información y la Comunicación (TIC), las cuales se actualizan continuamente. En consecuencia, es crucial comprender las medidas de protección contra estos delitos informáticos. Según Henao et al. (2022), diversos

sectores han adoptado modelos basados en el aprendizaje automático (machine learning) para mejorar procesos, tomar decisiones y desarrollar herramientas digitales. En los últimos años, este enfoque ha ganado terreno en la ciberseguridad, abarcando aspectos ofensivos, defensivos y éticos. Además, se han creado dispositivos como los Honeypots, diseñados para detectar ataques previamente desconocidos. Estos dispositivos pueden rastrear desde fraudes con tarjetas de crédito hasta el robo de identidades (Armijos, 2018).

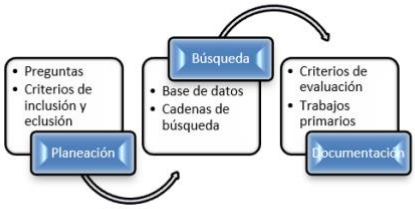
Existen diversas técnicas de computación que pueden emplearse para prevenir delitos informáticos. Según Cruz (2018), algunas características de seguridad clave incluyen el uso de contraseñas robustas, la instalación de software de seguridad, el mantenimiento regular de sistemas informáticos, la gestión de la privacidad en línea y la educación en seguridad informática. Además, los sistemas SIEM (Administración de Eventos e Información de Seguridad) han ganado relevancia como soluciones de seguridad que permiten a las organizaciones identificar amenazas potenciales y vulnerabilidades antes de que afecten sus operaciones. Estos sistemas utilizan inteligencia artificial para automatizar procesos de detección de amenazas y respuesta a incidentes, convirtiéndose en un componente esencial de los Centros de Operaciones de Seguridad (SOC). Este estudio bibliográfico tiene como objetivo recopilar información relevante sobre las diversas técnicas de computación utilizadas en ataques informáticos, centrándose especialmente en aquellas más frecuentes en organizaciones a nivel mundial y en América Latina. A través de este análisis sistemático, se busca profundizar en la comprensión de las amenazas cibernéticas y explorar las estrategias disponibles para hacerles frente en un entorno digital en constante cambio.

2. Metodología de la investigación

La metodología empleada en este estudio se fundamenta en PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), una pauta reconocida en la realización de revisiones sistemáticas y metaanálisis. Para facilitar el proceso, se empleó la herramienta en línea Parsifal (https://parsif.al). El proceso de revisión se estructuró en tres fases fundamentales: Planificación, Realización e Informes (ilustradas en la Figura 1), las cuales se detallan a continuación. Además, esta metodología se aplica para asegurar la integridad y rigor de la revisión sistemática, asegurando la obtención de resultados precisos y confiables. En la fase de Planificación, se delinearon los objetivos, se establecieron los criterios de inclusión y exclusión, y se definió la estrategia de búsqueda. Luego, en la fase de Realización, se

ejecutó la búsqueda en bases de datos académicas, revistas científicas, repositorios institucionales y conferencias. Los artículos fueron seleccionados siguiendo los criterios preestablecidos y se extrajo la información relevante. Finalmente, en la fase de Informes, se presentaron los resultados de manera estructurada y analítica, resaltando los hallazgos clave, tendencias y desafíos identificados. La metodología PRISMA junto con la herramienta Parsifal se combinaron para garantizar la exhaustividad y rigurosidad en cada etapa del proceso de revisión, proporcionando un enfoque confiable y sistemático para la investigación.

Figura 1. Etapas del método aplicado a la revisión sistemática



2.1 Planificación de la revisión

La planificación del proceso de revisión se estructura en función de los objetivos específicos planteados para este estudio. Inicialmente, se definen las palabras clave PICOC (Población, Intervención, Comparación, Resultado, Contexto) para orientar la búsqueda de manera efectiva. Estas palabras clave se presentan en la tabla 1, empleando listas de términos en lugar de sinónimos.

Se formulan cuatro preguntas de investigación (PI) que se relacionan directamente con los objetivos planteados:

- PI1. ¿Cuáles son las técnicas de prevención de delitos informáticos más utilizadas en América Latina y España?
- PI2. ¿Qué información proporcionan los análisis de los artículos acerca de la efectividad de las técnicas de prevención de delitos informáticos implementadas en la región?
- PI3. ¿Cuáles son los principales desafíos y barreras que enfrenta la implementación de las técnicas de prevención de delitos informáticos en América Latina y España?

- PI4. ¿Existen diferencias significativas en las técnicas de prevención utilizadas entre los países de América Latina y España?

Justificación de la inclusión de España:

Dada la naturaleza global del ciberespacio y la interconexión de amenazas cibernéticas, se incluyen estudios y datos provenientes de España para enriquecer la perspectiva general de las técnicas de prevención de delitos informáticos en la región. España comparte similitudes en los desafíos de ciberseguridad y podría aportar valiosa información que complementará la comprensión de las estrategias utilizadas en América Latina. Basándose en las palabras clave, se construyó una cadena de búsqueda base, que se expone a continuación: ("delitos informáticos" OR "ciberdelitos") AND ("técnicas de prevención" OR "medidas de seguridad") AND ("América Latina" OR "Latinoamérica" OR "España").

Tabla 1. Palabras clave de PICOC

Término	Palabras clave
Población	delitos informáticos, ciberdelitos
Intervención	técnicas de prevención, medidas de seguridad
Comparación	América Latina, Latinoamérica, España

Los criterios de inclusión y exclusión se detallan en la tabla 2. Los criterios de inclusión determinan la recuperación de artículos publicados en revistas científicas y actas de congresos, entre 2018 y la fecha de diciembre de 2023, en inglés o español. Estos artículos deben contener al menos un resumen en inglés. Por su parte, los criterios de exclusión se enfocan en excluir publicaciones incompletas, no accesibles, no innovadoras o que aborden temas divergentes.

Tabla 2 Criterio de selección

Criterios de inclusión	Criterio de exclusión
Artículos de revistas científicas	Duplicados
Publicados desde 2018 hasta julio 2023	Contenido no accesible
	Otros idiomas distintos a inglés o español
	Temáticas distintas

La evaluación de la calidad de los artículos seleccionados se establece mediante tres preguntas de evaluación de calidad (PEC), cuyos valores ponderados se presentan en la tabla 3. Un artículo se considera apto para la revisión sistemática si obtiene al menos 1,5 puntos en esta evaluación.

Las preguntas de evaluación de calidad (PEC) junto con sus respectivos pesos revisados son los siguientes:

PI1. ¿Cómo ha evolucionado la distribución de estudios sobre ciberdelincuencia en América Latina y España en función del año de publicación y las categorías temáticas? (Peso: 1.0) (Adaptada de RQ1)

PI2. ¿Cuáles son las técnicas de prevención de delitos informáticos más utilizadas en América Latina y España, y cómo se agrupan en términos de eficacia? (Peso: 0.5) (Adaptada de RQ2)

PI3. ¿Cuál es la efectividad de las técnicas de prevención de delitos informáticos implementadas en la región, y qué enfoques específicos han demostrado ser más exitosos? (Peso: 0.5) (Adaptada de RQ3)

PI4. ¿Cuáles son los tipos predominantes de delitos informáticos en América Latina y España, y cómo se distribuyen en categorías temáticas específicas? (Peso: 1.0) (Adaptada de RQ4)

PI5. ¿Cuáles son los propósitos principales de los estudios sobre ciberdelincuencia en la región, y cómo se han enfocado en términos de educación, concienciación, regulaciones y otras áreas? (Peso: 1.0) (Adaptada de RQ5)

PI6. ¿Cómo se han abordado y analizado los diferentes aspectos de la ciberdelincuencia, desde ciberataques y ciberseguridad hasta la evaluación de herramientas y el impacto de los delitos informáticos en América Latina y España? (Peso: 1.0) (Adaptada de RQ6)

Tabla 1. Peso de las respuestas

Definición	Peso
Sí	1.0
Parcial	0.5
No	0.0

Estas preguntas y sus valores ponderados permiten evaluar la calidad y relevancia de los artículos seleccionados para la revisión sistemática de la literatura sobre técnicas de prevención de delitos informáticos en América Latina y España, considerando la presencia de información sobre delitos, tipos de delitos y aspectos técnicos de las técnicas de prevención.

2.2 Realización de la revisión

Para llevar a cabo esta revisión, se optó por explorar diversas bases de datos académicas y científicas especializadas de los delitos en el campo de la informática. Las bases de datos seleccionadas fueron ACM Digital Library, Scielo, Dialnet, Scopus, MDPI. En cada una de estas bases de datos, se ajustaron los parámetros de búsqueda para garantizar una búsqueda exhaustiva y específica en relación con los delitos informáticos en América Latina y España. Se tuvieron en cuenta factores como el rango de años y el tipo de publicación.

2.3 Informe de la revisión

Tras completar la búsqueda en cada base de datos, se realizó una primera selección de artículos siguiendo los criterios de selección establecidos. Estos criterios estuvieron diseñados para incluir estudios relevantes y de calidad en la revisión. Luego, se aplicaron los criterios de calidad a los trabajos seleccionados, utilizando preguntas de evaluación previamente definidas. Una vez completada la evaluación y selección de los artículos, se procedió a la extracción de datos. Esta etapa implicó la recopilación y organización de información relevante de los artículos seleccionados. Los datos extraídos se utilizaron posteriormente para realizar análisis detallados sobre las

técnicas de prevención de delitos informáticos en América Latina y España como se ve en la tabla 4.

Tabla 3. Campos del formulario de extracción de datos

Descripción	Tipo	RQ
Identificación	Número	-
Título	Texto	RQ1
Año de publicación	Número	-
Técnicas de prevención utilizadas	Texto	RQ1
Eficacia de las técnicas	Texto	RQ2
Tipo de delito	Lista (texto)	RQ3
País de desarrollo	Texto	-

3. Resultados

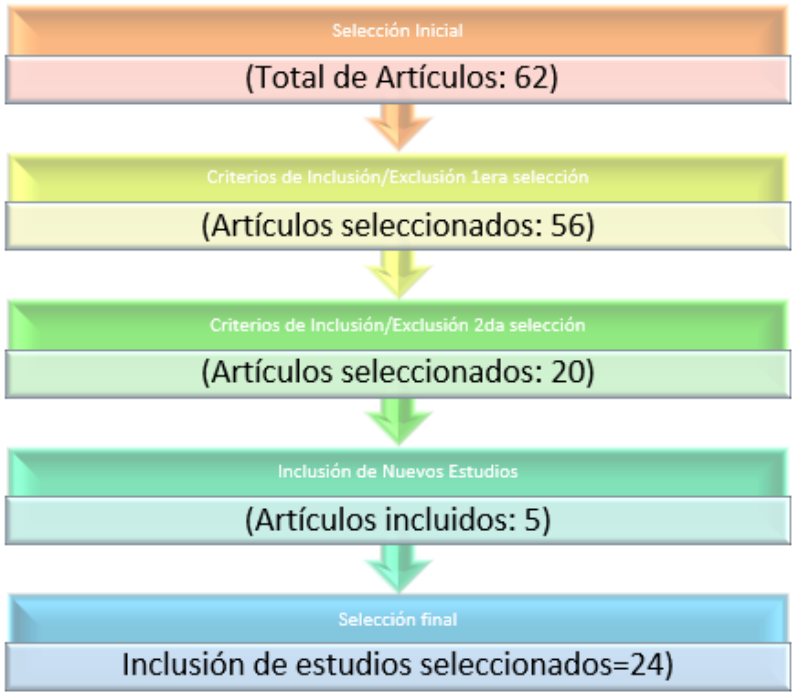
3.1 Selección y extracción de papel

En la tabla 5 se presentan los resultados de la búsqueda realizada en las bases de datos seleccionadas. Se identificó un total de 47 artículos relacionados con el tema de los delitos informáticos. Cada columna indica la cantidad de artículos recuperados y seleccionados en cada base de datos. En la primera selección, se aplicaron criterios de inclusión y exclusión para determinar qué artículos cumplían con los requisitos establecidos en el protocolo de revisión. Posteriormente, se realizó una segunda selección basada en la importancia del tema y el idioma de los artículos. Como resultado de este proceso, se seleccionaron un total de 24 artículos que cumplían todos los criterios de inclusión y exclusión establecidos en la revisión. Es importante destacar que esta tabla refleja el número de artículos recuperados y seleccionados en cada base de datos, lo que proporciona una visión general del alcance de la revisión bibliográfica y la cantidad de estudios considerados en el análisis.

Tabla 5 Documentos recuperados y seleccionados

Base de datos	Cantidad	1ra selección	2ª selección
ACM Digital Library	13	13	0
Scielo	10	8	2
Dialnet	23	23	17
Scopus	1	1	1
MDPI	15	11	4
Total	62	56	24

Figura 2 Diagrama Prisma



La información recopilada se sintetiza en la Tabla 6, donde también se identifica la columna correspondiente a cada pregunta de investigación (RQ).

Tabla 4 Datos extraídos de artículos seleccionados

Id	Estudio (RQ1)	País	Año	Técnicas de prevención utilizadas (RQ2)	Eficacia de las técnicas (RQ3)	Tipo de delito (RQ4)	Propósito del estudio (RQ5)	Enfoque de análisis (RQ6)
1	Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú	Perú	(2022)	Información para planes de prevención del delito	Sí	Ciberdelito	Conciencia y educación	Impacto en la educación
2	Criminología en las redes sociales: Un estudio realizado en la escuela CESUVER a nivel secundaria a través de la campaña	México	(2022)	Información para planes de prevención del delito	No	Delitos informáticos en redes sociales	Regulaciones y análisis	Evaluación legislativa
3	Diagnóstico de utilización de Redes sociales: factor de riesgo para el adolescente	México	(2018)	Información para planes de prevención del delito	No	Delitos informáticos en redes sociales	Uso de redes y delitos	Relación con redes sociales
4	Conocimiento e identificación del cyberbullying por	Argentina	(2018)	Información para planes de prevención del	No	Cyberbullying	Educación y concienciación	Impacto en la educación

	parte de docentes de Buenos Aires			delito				
5	Adolescentes frente a los riesgos en el uso de las TIC	Perú	(2020)	Información para planes de prevención del delito	No	Riesgos en el uso de las TIC	Estrategias de protección	Comportamiento de adolescentes
6	La cibercriminalidad sexual juvenil como nueva forma de delincuencia	México	(2021)	Información para planes de prevención del delito	No	Cibercriminalidad sexual juvenil	Delincuencia juvenil	Enfoque en jóvenes delincuentes
7	Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman	Colombia	(2020)	Filtro Kalman	Sí	Ciberataques en sistemas industriales SCADA	Técnicas predictivas	Enfoque en ciberataques
8	Análisis y caracterización de conjuntos de datos para detección de intrusiones	Cuba	(2020)	Conjuntos de datos	No	Detección de intrusiones	Evaluación de datos	Enfoque en conjuntos de datos
9	Análisis comparativo de variables utilizadas en redes distribuidas zigbee para detección de intrusiones desde dispositivos finales en una red de vehículos autónomos no tripulados	España	(2022)	Variables en redes zigbee	No	Detección de intrusiones en vehículos autónomos	Variables y detección	Comparativa de variables
10	Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio	Perú	(2022)	Snort, Suricata	No	Detección de sondeos de redes y ataques de denegación de servicio	Evaluación de herramientas	Eficacia de herramientas
11	Suricata como detector de intrusos para la seguridad en redes de datos empresariales	Cuba	(2022)	Suricata	No	Detección de intrusos en redes empresariales	Uso de Suricata en redes	Enfoque en seguridad empresarial
12	Evaluación del rendimiento de honeypot en redes telemáticas.	Venezuela	(2022)	Honeypot	No	Rendimiento de honeypots en redes telemáticas	Evaluación de rendimiento de honeypots	Análisis de rendimiento
13	Estudio exploratorio de las estrategias para la protección a las redes empresariales de las infecciones ransomware	Ecuador	(2020)	Estrategias de protección	No	Protección contra infecciones ransomware en redes empresariales	Estrategias de protección en ransomware	Análisis de estrategias
14	Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim	Ecuador	(2022)	Alienvault Ossim	No	Sistemas centralizados de seguridad informática	Evaluación de sistemas con Alienvault Ossim	Análisis de herramientas
15	Técnica de protección para credenciales de autenticación en	Colombia	(2018)	Técnica de protección de credenciales	No	Ataques phishing en redes sociales y correo electrónico	Protección contra ataques phishing	Análisis de técnicas

	redes sociales y correo electrónico ante ataques phishing							
16	Patrones en el orden de los clics y su influencia en la debilidad de las claves en la Técnica de Autenticación Gráfica Passpoints	Cuba	(2019)	Patrones de clics, Autenticación Gráfica Passpoints	No	Debilidad de claves en Autenticación Gráfica Passpoints	Análisis de patrones en autenticación	Enfoque en autenticación
17	CMS y LMS vulnerables a ataques de sus administradores de bases de datos.	Cuba	(2018)	Información para planes de prevención del delito	No	Vulnerabilidades en CMS y LMS	Ataques internos en sistemas	Análisis de vulnerabilidades
18	Desafíos de Seguridad en Redes 5G	Costa Rica	(2019)	Información para planes de prevención del delito	No	Desafíos de seguridad en redes 5G	Identificar desafíos de seguridad en la implementación de redes 5G	Análisis de desafíos y barreras en la implementación
19	Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos	Chile	(2018)	Delito de fraude informático aspecto legal	No	Elementos criminológicos en análisis jurídico-penal de delitos informáticos	Explorar elementos criminológicos en el análisis jurídico-penal de delitos informáticos	lisis de aspectos criminológicos en el ámbito jurídico-penal
20	El delito de fraude informático: Concepto y delimitación	Chile	(2020)	Delito de fraude informático aspecto legal	No	Delito de fraude informático	Definir y delimitar el delito de fraude informático en el ámbito legal	Análisis del concepto y delimitación del fraude informático en el marco legal
21	Detección de ciberataques en mensajes de redes sociales basada en redes neuronales convolucionales y técnicas de PNL	México	(2023)	Enfoque en la detección de ciberataques en lugar de técnicas de prevención	Si Detectar y clasificar ciberataques	Ciberataques en mensajes de redes sociales	Detectar y clasificar ciberataques	Análisis de procesamiento de lenguaje natural y arquitectura de redes neuronales convolucionales
22	Técnicas de aprendizaje automático para predecir ataques de phishing en redes Blockchain: un estudio comparativo	España	(2023)	Técnicas	Si	Ataques de phishing en redes Blockchain	Comparativa de técnicas de aprendizaje automático	Análisis de eficacia en la predicción de ataques de phishing en entornos Blockchain
23	Análisis de información digital en dispositivos de almacenamiento mediante técnicas de procesamiento del lenguaje natural supervisadas y no supervisadas	España	(2023)	Técnicas de procesamiento del lenguaje natural supervisadas y no supervisadas	Si	Análisis de información digital en dispositivos de almacenamiento	Explorar técnicas de procesamiento del lenguaje natural	Enfoque en análisis de información digital en dispositivos de almacenamiento
24	Integración de detectores de ataques basados en aprendizaje automático en ejercicios defensivos de una gama cibernética 5G	España	(2022)	Aprendizaje automático para detectores de ataques	Si	Detección de ataques en ejercicios defensivos cibernéticos 5G	Integración de aprendizaje automático en ejercicios defensivos	Análisis de integración de detectores en ejercicios cibernéticos 5G

3.2 Análisis de datos

Dentro de esta subsección, se abordan de manera individual los campos de datos relacionados con cada una de las preguntas de investigación (RQ).

3.2.1. RQ1: Análisis de Estudios Identificados

La distribución de los estudios analizados, basados en el año de publicación y las categorías temáticas, proporciona una perspectiva esclarecedora sobre las tendencias en el ámbito de la ciberdelincuencia en América Latina y España. Esta distribución se presenta visualmente en la Figura 2. Se destaca un crecimiento constante en los años recientes, en contraste con los primeros períodos de estudio. Los trabajos se han agrupado en alrededor de 4 o 5 categorías temáticas principales, las cuales se han definido en función de los objetivos y enfoques de cada estudio. Además, en la Figura 2 se muestra la distribución de los trabajos según su país de origen. En este sentido, resalta los países que sobresalen en cuanto a la producción de artículos sobre ciberdelincuencia. Esto indica un marcado interés de las naciones por abordar los desafíos de este fenómeno. Así mismo, como los países de la región y España han desempeñado un papel relevante en la generación y difusión del conocimiento en esta área.

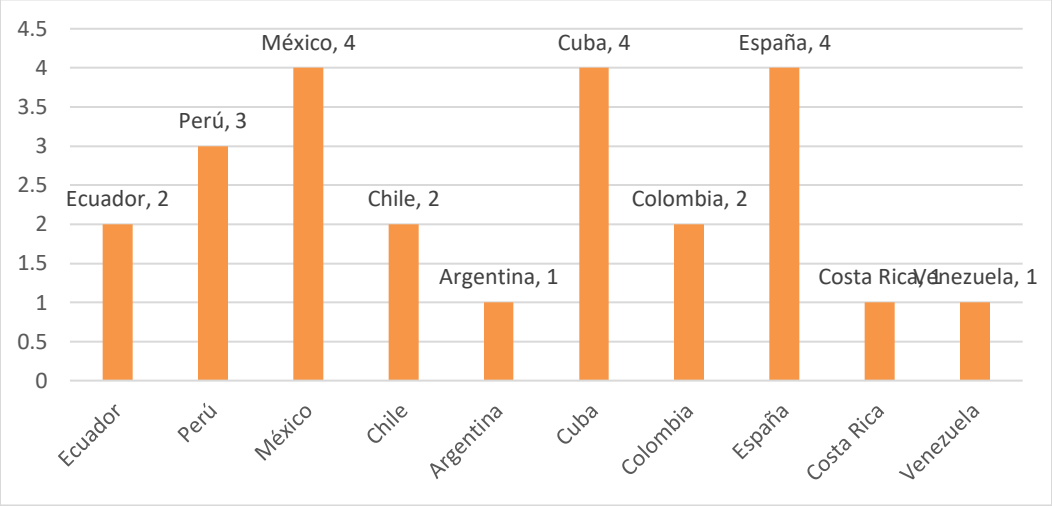


Figura 1 **-** Distribución de artículos por país de origen

3.2.2. RQ2: Técnicas de prevención utilizadas

Agrupando las técnicas de prevención utilizadas (RQ2) en pocos grupos y calculando los porcentajes de cada grupo, así como los artículos referenciados en cada uno de ellos, obtenemos la siguiente tabla:

Tabla 5. Distribución de Técnicas de Prevención Utilizadas (RQ2)

Técnica de Prevención	%	Artículos Referenciados
Información para Planes de Prevención del Delito	33%	1, 2, 3, 4, 5, 6, 17, 18
Detección y Prevención Técnica	42%	7, 8, 9, 10, 11,12,14,21,23,24
Estrategias de Protección	8%	13, 19
Técnicas de Autenticación	8%	15, 16
Aspectos Legales y Jurídicos	4%	20
Estrategias innovadoras	4%	22

En la tabla 7 se presenta una distribución de las técnicas de prevención utilizadas en los estudios analizados, agrupadas en diferentes categorías. El grupo con mayor porcentaje es delitos como "Información para Planes de Prevención del Delito" con un 33%, que abarca la mayoría de los artículos. Luego, “Detección y Prevención Técnica”, con un 42%. Con un 9% también se encuentran “Estrategias de Protección” y “Técnicas de Autenticación”. Y finalmente “Aspectos Legales y Jurídicos” con el 4%. Estas técnicas reflejan el enfoque diverso de los estudios en relación con las estrategias de prevención de delitos informáticos en América Latina y España. Las técnicas de prevención y detección utilizadas en los estudios muestran una variedad de enfoques para abordar la problemática de los delitos informáticos en América Latina y España. A continuación, se detallan estas técnicas y por qué se utilizan:

- Información para planes de prevención del delito: Esta técnica se basa en recopilar y analizar información relevante sobre delitos informáticos en la región. Los estudios utilizan esta técnica para comprender la naturaleza de los delitos y desarrollar estrategias de prevención efectivas y basadas en evidencia.
  Detección y Prevención Técnica: Se encuentra a) Filtro Kalman y técnicas de predicción de ciberataques: Este método permite anticipar comportamientos anómalos y tomar medidas preventivas (Quiroz et al., 2020)(Quiroz et al., 2020). Además, el artículo 23 propone métodos respaldados por inteligencia artificial y procesamiento de lenguaje natural para analizar y clasificar automáticamente información en dispositivos de almacenamiento digital, contribuyendo así a la prevención del cibercrimen. b) Variables en redes Zigbee para detección de intrusiones: Los estudios que analizan redes Zigbee distribuidas se centran en evaluar variables para identificar intrusiones y mejorar la seguridad en sistemas autónomos (Pola et al., 2022). c) Herramientas de detección de intrusiones (Snort, Suricata): Estas herramientas son ampliamente utilizadas y se evalúan en estudios para mejorar la detección de ataques y vulnerabilidades, contribuyendo así a fortalecer los sistemas de prevención. d) Técnica de Honeypot: Se emplea la creación de sistemas o servicios falsos para atraer a posibles atacantes y recopilar

información sobre sus métodos. Los estudios que utilizan honeypots evalúan tácticas de ataque y comportamientos maliciosos para fortalecer la prevención.

- Estrategias de Protección: Esta técnica engloba diversos métodos y enfoques para proteger sistemas y datos de amenazas informáticas. Los estudios pueden analizar estrategias específicas, como protección contra ransomware, y evaluar su eficacia.
- Técnica de Protección de Credenciales: Estudios que se centran en proteger credenciales de autenticación utilizan esta técnica. Evalúan métodos para prevenir ataques de phishing y robo de contraseñas en redes sociales y correo electrónico.
- Patrones de Clics, Autenticación Gráfica Passpoints: Esta técnica se enfoca en analizar patrones de clics y su influencia en la seguridad de la autenticación gráfica. Los estudios evalúan cómo los patrones pueden ser explotados y proponen medidas para mejorar la seguridad.
- Detección de ciberataques en mensajes de redes sociales utilizando técnicas de procesamiento de lenguaje natural (NLP) y una arquitectura de red neuronal convolucional (CNN). El enfoque se centra en detectar y clasificar cuatro tipos de ciberataques en mensajes de redes sociales, que incluyen malware, phishing, spam y ataques de bots. Un aspecto destacado es que el análisis se realiza sin depender de características específicas de una red social particular.
- Estrategias innovadoras: Se encuentra información para la prevención de ataques cibernéticos, específicamente explorando el uso de tecnologías blockchain. La estrategia detalla cómo las características descentralizadas e inmutables de la cadena de bloques pueden ser aprovechadas para fortalecer la seguridad cibernética. Algunas de las áreas específicas cubiertas incluyen la autenticación descentralizada, la integridad de datos y la resistencia a ataques de manipulación. La inclusión de este estudio en el análisis resalta la diversidad de enfoques y la continua evolución de las estrategias de prevención en España..

La presencia de estas diversas técnicas refleja la amplitud de enfoques que los estudios en América Latina han adoptado para abordar los desafíos de la prevención de delitos informáticos. Cada técnica aborda una faceta particular de la ciberseguridad, y en conjunto contribuyen a un panorama más completo de las estrategias de prevención en la región.

3.2.3. RQ3: Análisis de la eficacia de las técnicas

En la RQ3 "Análisis de la eficacia de las Técnicas" se observa una variedad de enfoques en los estudios de ciberdelincuencia en América Latina. Algunos estudios no proporcionan información específica sobre la eficacia de las técnicas empleadas, sino que se centran en describir el problema en cuestión. Por ejemplo, los artículos 2, 3, 4, 17 y 18 se enfocan principalmente en la descripción y análisis de los delitos informáticos y sus implicaciones, sin ofrecer datos sobre la eficacia de las técnicas utilizadas. Por otro lado, los estudios que evalúan la eficacia de las técnicas de

prevención en ciberseguridad son el artículo 1, habla totalmente de la eficacia y el artículo 7 (filtro Kalman, técnica predictiva). En el artículo 22 se analiza la eficacia de las técnicas basadas en blockchain para prevenir y mitigar delitos informáticos en la región. Es importante destacar que la mayoría de los trabajos no brindan información detallada sobre la eficacia de las técnicas, centrando su atención en la comprensión y el análisis de los problemas relacionados con la ciberdelincuencia en la región y España. En el artículo 23 contribuye al panorama de la ciberseguridad al explorar la eficacia de las técnicas de procesamiento del lenguaje natural en el análisis de información digital, ofreciendo así una perspectiva valiosa para mejorar las estrategias de prevención y detección de amenazas en dispositivos de almacenamiento. El artículo 24, "Integración de detectores de ataques basados en aprendizaje automático en ejercicios defensivos de una gama cibernética 5G," presenta una contribución valiosa al analizar la eficacia de la integración de modelos de aprendizaje automático en ejercicios defensivos. Este artículo se destaca al abordar específicamente la aplicación práctica de técnicas de aprendizaje automático para detectar y mitigar amenazas en entornos de redes 5G. Al presentar casos de uso concretos, como la detección de ataques DoH y cryptomining, proporciona información valiosa sobre la efectividad de estas técnicas en situaciones realistas. La propuesta de utilizar Redes Generativas Adversarias (GANs) para generar tráfico sintético también muestra una consideración innovadora para mejorar la preparación contra amenazas futuras. Este enfoque detallado en la eficacia práctica de las técnicas hace que sea una contribución destacada en el análisis de la eficacia de las técnicas de ciberseguridad.

3.2.4. RQ4: Tipo de delito

La tabla 8 se presenta una descripción de los tipos de delito abordados en los artículos analizados, así como el porcentaje de distribución de los artículos en cada categoría y los números de los artículos referenciados en cada grupo. A continuación, se ofrece una descripción de cada grupo: a) Delitos Informáticos en Redes Sociales (8%): Esta categoría se enfoca en delitos informáticos relacionados con el uso de redes sociales. Los artículos referenciados son el artículo 2, que explora la criminología en las redes sociales, el artículo 3, que realiza un diagnóstico de la utilización de redes sociales como factor de riesgo para adolescentes. b) Detección de intrusiones y ataques (15%): Esta categoría se concentra en la detección de intrusiones y ataques informáticos. Los artículos referenciados son el artículo 8, que analiza conjuntos de datos para la detección de intrusiones, los artículos 9, 11, que se centran en la detección de intrusiones desde diferentes perspectivas. c) Evaluación de herramientas y tecnologías (19%): En esta categoría se evalúan diversas herramientas y tecnologías en el ámbito de la ciberseguridad. Los artículos referenciados 10,12,13,14 evalúan herramientas para la detección de sondeos y ataques de denegación de servicio, el artículo 12 evalúa el rendimiento de honeypots en redes telemáticas, y los artículos 13 y 14, que exploran estrategias y sistemas de protección. d) Técnicas de protección contra amenazas y

riesgos (9%): Aquí se tratan estrategias de protección contra amenazas y riesgos informáticos. Los artículos referenciados 15 y 16 proponen técnicas de protección para credenciales de autenticación y patrones en autenticación Gráfica Passpoints ante ataques phishing. El artículo referenciado es el artículo 16, que analiza patrones en el orden de los clics y su influencia en la debilidad de las claves. La siguiente tabla proporciona una visión detallada de cómo se distribuyen los artículos en diferentes tipos de delitos relacionados con aspectos técnicos y tecnológicos en el ámbito de la ciberdelincuencia.

Tabla 6. Tipo de delito

Tipo de Delito	%	Artículos Referenciados
Conocimiento sobre tipo de delito	23%	1,4,5,6,19,20
Delitos Informáticos en Redes Sociales	8%	2, 3
Detección de intrusiones y ataques	15%	8, 9, 11,24
Evaluación de herramientas y tecnologías	19%	10, 12, 13,14
Detección de Ciberataques	4%	21
Predecir ataques de phishing en redes blockchain	4%	22
Técnicas predictivas	4%	7
Prevención de delitos	8%	17,18
Técnicas de protección contra amenazas y riesgos	8 %	15,16
Delitos abordados con Machine Learning e Inteligencia Artificial	8%	23,24

3.2.5. RQ5: Propósito del estudio

La tabla 9 presenta un análisis detallado de los propósitos de los estudios relacionados con la ciberdelincuencia en América Latina y España. Cada fila de la tabla representa una clasificación del propósito de estudio, se muestra el porcentaje y los artículos de cada clasificación.

Tabla 7. Propósito del estudio

Propósito del Estudio	%	Artículos
Información para planes de prevención del delito	29%	1, 3, 4, 6, 7, 17, 18
Educación y concienciación	8%	4, 15
Regulaciones y análisis	4%	2
Estrategias de protección	13%	5, 8,13
Delincuencia juvenil	4%	6
Evaluación de herramientas	8%	10, 14
Uso de redes y delitos	4%	3
Identificar desafíos de seguridad en la implementación de redes 5G	4%	18
Explorar elementos criminológicos en el análisis jurídico-penal de delitos informáticos	4%	19
Definir y delimitar el delito de fraude informático en el ámbito legal	4%	20
Detección de Ciberataques	0%	0
Predicción de ataques de phishing	0%	0
Evaluación de herramientas con Machine Learning e IA	17%	21,22,23,24

El propósito del estudio (RQ5) es el enfoque principal de esta descripción y análisis. Aquí se resumen los hallazgos clave:

a) Información para planes de prevención del delito (29%): Se observa que la mayoría de los estudios se centran en proporcionar datos para desarrollar estrategias de prevención de delitos informáticos. b) Educación y concienciación (9%): Algunos estudios abordan la educación y concienciación sobre delitos informáticos, especialmente entre jóvenes y educadores. c) Regulaciones y análisis (4%): Un pequeño porcentaje de estudios analiza la eficacia de las regulaciones existentes en la lucha contra los delitos informáticos, así como su implementación en la región. d) Estrategias de protección (13%): Se desarrollan y analizan estrategias específicas de protección contra delitos informáticos, tanto tecnológicas como prácticas. e) Delincuencia juvenil (5%): Se estudia la participación de los jóvenes en actividades delictivas en línea. f) Evaluación de herramientas (8%): Se evalúa la eficacia de herramientas específicas utilizadas en la prevención de delitos informáticos, incluyendo herramientas de detección, seguridad y protección. g) Uso de redes y delitos (4%): Algunos estudios investigan cómo los delincuentes utilizan las redes y su relación con los delitos informáticos. h) Desafíos de seguridad en redes 5G (5%): Se centran en los desafíos específicos de seguridad que surgen con la implementación de redes 5G y cómo protegerlas de amenazas cibernéticas. i) Elementos criminológicos en análisis jurídico-penal (5%): Se exploran aspectos criminológicos en el análisis jurídico-penal de los delitos informáticos. j) Definición y delimitación del fraude informático (4%): Se

centran en definir y delimitar el delito de fraude informático en el ámbito legal. k) Evaluación de herramientas con machine learning e IA (17%): Se evalúan diversas técnicas, métodos y estrategias basadas en machine learning e IA para prevenir ciberataques. Esto incluye el análisis de redes sociales y la predicción de ataques en Blockchain. En el Artículo 21 en la "Detección de ciberataques en mensajes de redes sociales basada en redes neuronales convolucionales y técnicas de PNL (Procesamiento de Lenguaje Natural)." Este artículo claramente implica el uso de redes neuronales convolucionales y técnicas de PNL, lo cual está relacionado con Machine Learning y procesamiento de lenguaje natural. Se lo analiza en el Artículo 22 haciendo uso de técnicas de aprendizaje automático para predecir ataques de phishing en redes Blockchain. En el Artículo 23 al involucrar técnicas de procesamiento de lenguaje natural, lo cual está relacionado con la inteligencia artificial. Así mismo con el Artículo 24 hacia la integración de detectores de ataques basados en aprendizaje automático.

Estos resultados reflejan la diversidad de enfoques y prioridades en la investigación sobre ciberdelincuencia en América Latina, destacando un interés significativo en la prevención y la educación para abordar efectivamente las amenazas cibernéticas en la región.

RQ6: Enfoque de análisis

Los estudios se han centrado en diversos aspectos, desde la evaluación de técnicas de prevención y su eficacia, hasta la exploración de tipos específicos de delitos informáticos y sus impactos. La tabla 10 resume estos enfoques de análisis, indicando el porcentaje de estudios que se han dedicado a cada uno, junto con los artículos de referencia correspondientes. Este análisis temático subraya la riqueza y diversidad de la investigación en ciberdelincuencia en América Latina, contribuyendo así a una comprensión más profunda de esta problemática en constante evolución.

Tabla 8. Enfoque de análisis

Enfoque de Análisis	%	Artículos Referenciados
Ciberataques	21%	7, 15, 16, 17, 18
Ciberseguridad	13%	8, 13, 14
Educación y Concienciación	8%	4, 5
Herramientas de Detección	21%	3,9,10, 11, 12
Impacto	4%	1
Ámbito Jurídico-Penal	13%	2,19, 20
Comportamiento Delictivo	4%	6
Evaluación de herramientas con Machine Learning e IA	17%	21,22,23,24

El enfoque de análisis en los estudios sobre ciberdelincuencia en América Latina muestra una amplia variedad de intereses y objetivos. El análisis de ciberataques es el enfoque más prominente, representando el 21% de los estudios. Estos estudios se centran en la investigación de patrones de ataques y sus consecuencias, lo que refleja la necesidad de comprender mejor las tácticas de los ciberdelincuentes para prevenir futuros ataques (Artículos: 7, 15, 16, 17, 18). Un enfoque igualmente relevante es la ciberseguridad, también con un 13%. Estos estudios analizan medidas y estrategias para proteger sistemas y redes de amenazas cibernéticas, contribuyendo a mejorar la resistencia de las infraestructuras tecnológicas ante posibles ataques (Artículos: 8, 13, 14). La educación y la concienciación juegan un papel importante, constituyendo el 8% de los enfoques. Estos estudios se centran en analizar estrategias educativas para prevenir la ciberdelincuencia, reconociendo la importancia de informar y empoderar a las personas para tomar decisiones seguras en línea (Artículos: 4, 5). El enfoque en herramientas de detección representa el 21% de los estudios. Estos análisis buscan evaluar la eficacia de las herramientas tecnológicas utilizadas para detectar y mitigar amenazas cibernéticas (Artículos: 3,9,10, 11, 12). El impacto de los delitos informáticos también es explorado, constituyendo el 4%. Este estudio analiza las repercusiones de los ciberataques en diferentes ámbitos, desde la educación hasta la seguridad industrial (Artículos: 1). Los enfoques como el ámbito jurídico-penal y el comportamiento delictivo representan el 13%, y 4% respectivamente. Los estudios en el ámbito jurídico-penal exploran las implicaciones legales de los delitos informáticos (Artículos: 2,19, 20), mientras que los estudios sobre comportamiento delictivo se centran en entender las motivaciones y métodos de los ciberdelincuentes (Artículo: 6). Los enfoques restantes representan el 17% sobre la Evaluación de las herramientas con Machine Learning e IA. Este enfoque se refiere al estudio y la evaluación de herramientas de ciberseguridad utilizando tecnologías avanzadas como Machine Learning (Aprendizaje Automático) e Inteligencia Artificial (IA). . La evaluación de estas herramientas incluye la identificación de patrones de comportamiento malicioso, la detección de amenazas en tiempo real y el desarrollo de sistemas más avanzados y adaptativos para hacer frente a la evolución constante de las amenazas cibernéticas (Artículos: 21, 22, 23, 24).

En conjunto, estos enfoques de análisis reflejan la diversidad y amplitud de la investigación sobre ciberdelincuencia en América Latina, abordando desde aspectos técnicos y de seguridad hasta consideraciones legales y sociales.

Aporte de la RSL: Evaluación de novedad y aporte

Comparativa de enfoques en investigación de Ciberseguridad: España y Latinoamérica

Enfoque avanzado de España en IA: Los estudios provenientes de España muestran un claro énfasis en el uso de técnicas avanzadas de Inteligencia Artificial (IA) y aprendizaje automático. Se mencionan algoritmos como árboles de decisión, bosques aleatorios y XGBoost, indicando un nivel más elevado de sofisticación en comparación con algunos estudios latinoamericanos.

Diversidad de enfoques en Latinoamérica: Los estudios de Latinoamérica abarcan una variedad de temas, desde legislación hasta concienciación educativa y evaluación de herramientas específicas. Se observa una diversidad de enfoques, lo que refleja la complejidad y amplitud de los desafíos en ciberseguridad que enfrenta la región.

Énfasis en aspectos legales en Latinoamérica: Algunos estudios latinoamericanos se centran en aspectos legales, como la evaluación legislativa y elementos criminológicos en el análisis jurídico-penal de los delitos informáticos. Esto sugiere una preocupación por abordar los problemas desde una perspectiva legal y regulatoria.

Diferencias en recursos y enfoques específicos: Las diferencias podrían atribuirse a factores como la disponibilidad de recursos y la especialización de los investigadores en cada región. Mientras España se destaca en el uso de técnicas más avanzadas como machine learning e IA, algunos estudios latinoamericanos adoptan enfoques específicos según las necesidades locales.

Estos hallazgos proporcionan una visión general de las tendencias observadas en la investigación sobre ciberseguridad en España y Latinoamérica, destacando tanto similitudes como diferencias en los enfoques y prioridades de investigación.

¿Qué tiene de nuevo una revisión específica del trabajo aplicado en América Latina y la diferencia que hay con España? La revisión específica del trabajo aplicado en América Latina y su comparación con España revela contribuciones únicas y diferencias significativas en la investigación sobre ciberseguridad. En el contexto latinoamericano, se observa una variedad de enfoques que abarcan desde aspectos legales y criminológicos hasta educación y concienciación. Este énfasis diversificado refleja la complejidad de los desafíos en ciberseguridad que enfrenta la región. Por otro lado, España sobresale por la aplicación de técnicas avanzadas de inteligencia artificial y aprendizaje automático en la prevención y detección de ciberdelincuencia, destacando un nivel de sofisticación más alto en sus investigaciones.

¿Cuáles son las diferencias en relación con otras obras similares existentes (incluso de otras regiones)? En comparación con otras obras similares, tanto de

América Latina como de otras regiones, la revisión evidencia las particularidades de los enfoques adoptados. Mientras que otros estudios pueden centrarse en aspectos específicos como legislación, análisis criminológicos o evaluaciones legislativas, la investigación en España se destaca por su amplia diversidad de estrategias, con un claro énfasis en la aplicación de herramientas avanzadas basadas en inteligencia artificial. Esta distinción sitúa a la investigación española en la vanguardia de la innovación en la lucha contra la ciberdelincuencia, proporcionando una perspectiva valiosa y única en comparación con obras similares de otras regiones.

Comparativas RSL - Tendencias y diferencias en ciberseguridad: La revisión sistemática de la literatura (RSL) titulada "Revisión Sistemática de la Literatura relacionada con ciberseguridad apoyada con Análisis de Big Data para actividades de Red Team" aborda el periodo 2017-2021 en el ámbito de la ciberseguridad, utilizando técnicas de big data respaldadas por análisis de Red Team (Quezada & León , 2022). Los resultados de esta RSL revelan varias anomalías de ciberseguridad, destacando Phishing, Ataques de Red, Malware e Ingeniería Social como las más prevalentes. En términos de métodos y técnicas, ambas revisiones resaltan la relevancia del Machine Learning (ML) y Deep Learning (DL) para la detección de amenazas cibernéticas. Comparando esta RSL desarrollada se destaca el enfoque en América Latina y España, en donde se revela una mayor diversidad de objetivos y enfoques. En este sentido es una RSL general que se centra en una taxonomía que abarca temas desde el análisis jurídico-penal de los delitos informáticos hasta la concienciación y educación en ciberdelitos. En este sentido, la RSL desarrollada en este trabajo está más enfocada en la diversidad de enfoques, destacando la necesidad de una estrategia multidisciplinaria que aborde la ciberdelincuencia desde perspectivas legales, educativas y tecnológicas. La revisión sistemática de la literatura (RSL) titulada "Comparativa de Estrategias en la Detección de Ransomware: Revisión Sistemática y Análisis Integral" se centra en estudios exhaustivos sobre técnicas de detección de ransomware mediante Machine Learning (ML). La revisión sistemática esta basada en la metodología de Barbara Kitchenham, que explora algoritmos y herramientas de software (Cumbicus et al., 2022). La investigación destaca Random Forest (RF), Decision Tree (DT), Long Short-Term Memory (LSTM), Support Vector Machine Learning (SVM), y Deep Neural Network (DNN), con énfasis en RF (23%) y herramientas como Cuckoo Sandbox y Weka Framework. Se menciona que el Random Forest (RF) brinda el mejor rendimiento (23%) y también destaca Decision Tree (DT) (14%) y Long Short-Term Memory (LSTM) (9%). Esta RSL tiene un enfoque en algoritmos y herramientas específicas de ML, la RSL ofrece insights valiosos sobre las estrategias que han demostrado ser efectivas. La identificación de Random Forest, Decision Tree y Long Short-Term Memory como los más utilizados, junto con Cuckoo Sandbox y Weka Framework, proporciona una base sólida para la implementación. Las conclusiones obtenidas en el trabajo resaltan la alta prevalencia de Random Forest y la eficacia de ML para la detección temprana de ransomware, fortaleciendo la solidez y la aplicabilidad de los resultados.

4. Conclusiones

Este estudio exhaustivo ha proporcionado un análisis profundo de las estrategias y técnicas de prevención de delitos informáticos en el contexto de América Latina, basándose en una revisión sistemática de la literatura. Las conclusiones extraídas a partir de esta revisión destacan varios puntos clave. En primer lugar, se ha observado un incremento notable en el interés por abordar la ciberdelincuencia en la región latinoamericana, lo que se refleja en la creciente cantidad de publicaciones académicas en los últimos años. Este aumento refleja la creciente conciencia sobre la importancia de la seguridad cibernética en la región y la necesidad de abordar este problema de manera más integral.

Con relación a las técnicas de prevención, la revisión de la literatura ha permitido identificar una amplia gama de enfoques empleados en los estudios analizados. Estos enfoques comprenden desde estrategias orientadas a la protección de la seguridad en redes sociales hasta técnicas avanzadas de detección de intrusiones y análisis detallado de vulnerabilidades. Esta diversidad de enfoques pone de manifiesto la considerable amplitud y complejidad de la ciberdelincuencia en América Latina. Este fenómeno delictivo se manifiesta en diversas formas y se adapta constantemente a nuevas estrategias, lo que hace imperativo el desarrollo de soluciones de seguridad igualmente variadas y multifacéticas. La respuesta efectiva a la ciberdelincuencia en la región demanda una combinación de estrategias que aborden tanto la prevención como la detección de amenazas, así como la mitigación de sus efectos, para brindar una defensa completa y adecuada contra los riesgos cibernéticos en constante evolución.

Sin embargo, se debe destacar que la eficacia de estas técnicas de prevención no se aborda de manera exhaustiva en la mayoría de los estudios. A pesar de que algunos artículos proporcionan evaluaciones de eficacia, la mayoría se centra en la descripción de los desafíos y riesgos asociados con la ciberdelincuencia, más que en la efectividad de las soluciones propuestas. Esto sugiere una oportunidad de investigación para futuros estudios que se centren en evaluar de manera más rigurosa y detallada la eficacia de las medidas de prevención específicas en el contexto latinoamericano. En cuanto al propósito de los estudios analizados, se ha constatado una amplia diversidad de objetivos que demuestran la riqueza y complejidad del campo de la ciberdelincuencia en América Latina. Entre los objetivos identificados se destacan el análisis jurídico-penal de los delitos informáticos, que busca comprender y abordar desde una perspectiva legal las distintas facetas de la ciberdelincuencia. Esta línea de investigación es fundamental para la definición de marcos legales adecuados y la aplicación de sanciones pertinentes en casos de delitos informáticos.

Además, se ha encontrado un enfoque importante en la concienciación y educación en torno a los ciberdelitos. Estos esfuerzos buscan informar y preparar a individuos y organizaciones para reconocer y prevenir amenazas cibernéticas, promoviendo

prácticas seguras en el uso de la tecnología. Este enfoque educativo es esencial para empoderar a la sociedad en la protección de sus activos digitales y la promoción de una cultura de seguridad cibernética. Asimismo, otros estudios se han orientado hacia el análisis de aspectos tecnológicos y estrategias específicas de protección. Estos investigan y proponen soluciones técnicas y tecnológicas para prevenir y mitigar los delitos informáticos, destacando la importancia de la innovación y la implementación efectiva de herramientas de seguridad.

La diversidad de objetivos en los estudios resalta la necesidad de abordar la ciberdelincuencia desde múltiples perspectivas complementarias, que van desde el ámbito legal hasta el educativo y tecnológico. Esta variedad de enfoques contribuye a una comprensión integral de los desafíos y soluciones en el campo de la seguridad cibernética en América Latina, subrayando la importancia de un enfoque multidisciplinario y colaborativo para abordar eficazmente esta problemática en constante evolución. Los resultados de esta revisión de la literatura resaltan la necesidad de un enfoque multidisciplinario y colaborativo para abordar la ciberdelincuencia en América Latina. La colaboración entre expertos en seguridad cibernética, investigadores legales y educadores es esencial para desarrollar estrategias efectivas de prevención y mitigación. Además, se destaca la importancia de llevar a cabo evaluaciones continuas y exhaustivas de la eficacia de las técnicas de prevención para garantizar un enfoque basado en evidencia en la lucha contra la ciberdelincuencia en la región. Esta revisión de la literatura ofrece una visión integral de los esfuerzos actuales y las áreas de enfoque en la prevención de la ciberdelincuencia en América Latina, aunque también señala la necesidad de continuar investigando y adaptándose a los desafíos en constante evolución en este campo.

Agradecimientos

Los autores agradecen al grupo de investigación Tecnologías Aplicadas a la Producción y los Servicios (TAPS) y al Facultad de Ciencias Informáticas, de la Universidad Técnica de Manabí.

Referencias

Andrade , L. (2022). Criminología en las redes sociales: Un estudio realizado en la escuela. *Archivos de Criminología, Seguridad Privada y Criminalística,*(29), 43-74. https://dialnet.unirioja.es/servlet/articulo?codigo=8333919

Armijos, J. (2018). *Honeypot como herramienta de prevención de ciberataques*. http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-1212_CampoverdeArmijosJI

Castellanos , O., & García, M. (2020). Análisis y caracterización de conjuntos de datos para detección de intrusiones. *Serie Científica de la Universidad de las Ciencias Informáticas,,* *13*(4), 39-52. https://dialnet.unirioja.es/servlet/articulo?codigo=8590270

Coyac , J., Sidorov , G., Aguirre , E., & Hernández, G. (2023). Detección de ciberataques en mensajes de redes sociales basada en redes neuronales convolucionales y técnicas de PNL. *Mach. Learn. Knowl. Extr., 5*(3), 1132-1148. https://doi.org/https://doi.org/10.3390/make5030058

Cruz, J. (2018). *Implementación de una herramienta SIEM (Security Information and Event Management) en una empresa de seguros*. https://alicia.concytec.gob.pe/vufind/Record/UTPD_c903375fe44f585050b24552744526e0

Cumbicus, O., Ludeña, P., & Neyra , L. (2022). Técnicas de Machine Learning para la Detección de Ransomware: Revisión Sistemática de Literatura. https://doi.org/https://doi.org/10.5281/zenodo.7373655

Díaz, J., Mejías, A., & Arteaga, F. (2001). Aplicación de los filtros de Kalman a sistemas de control. https://www.redalyc.org/pdf/707/70780105.pdf

Domínguez, A., Sepúlveda, J., & Núñez, Y. (2018). CMS y LMS vulnerables a ataques de sus administradores de bases de datos. *Revista de Arquitectura e Ingeniería, 12*(2). https://dialnet.unirioja.es/descarga/articulo/6548141.pdf

Ferruzola , E., Bermeo , O., & Arévalo , L. (2022). Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim. *Ecuadorian Science Journal,* *6*(1), 23-31. https://dialnet.unirioja.es/servlet/articulo?codigo=8470898

González , C. (2019). Desafíos de Seguridad en Redes 5G. *Revista Technology Inside*, 36-45. https://dialnet.unirioja.es/servlet/articulo?codigo=8856330

Henao, B., Prada, J., Pérez, A., Bernal, S., Gaviria, J., Ramírez, A., & Navarro, A. (2022). *Ciberseguridad: los datos tienen la respuesta.*

Joshi , K., Bhatt, C., Shah , K., Parmar , D., Corchado , J., Bruno , A., & Mazzeo , L. (29 de julio de 2023). Técnicas de aprendizaje automático para predecir ataques de phishing en redes Blockchain: un estudio comparativo. *16*(8), 366. https://doi.org/https://doi.org/10.3390/a16080366

Lanzillotti, A., & Korman, G. (septiembre de 2018). Conocimiento e identificación del cyberbullying por parte de docentes de Buenos Aires. *Revista mexicana de investigación educativa,* *23*(78).

https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-66662018000300817

Lorusso, G., & Rios, C. (2022). Evaluación del rendimiento de honeypot en redes telemáticas. *Revista Electrónica de Estudios Telemáticos, 21*(1), 26-45. https://ojs.urbe.edu/index.php/telematique/article/view/3832/5283

Martínez , L., Sandoval, A., & García, L. (2023). Análisis de información digital en dispositivos de almacenamiento mediante técnicas de procesamiento del lenguaje natural supervisadas y no supervisadas. *Future Internet , 15*(5), 155. https://doi.org/https://doi.org/10.3390/fi15050155

Mayer, L. (junio de 2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis , 24*(1). https://doi.org/http://dx.doi.org/10.4067/S0718-00122018000100159

Mayer, L., & Oliver , G. (junio de 2020). El delito de fraude informático: Concepto y delimitación. *Rev. chil. derecho tecnol., 9*(1). https://doi.org/http://dx.doi.org/10.5354/0719-2584.2020.53447

Mozo, A., Pastor, A., Karamchandani, A., Cal, L., Rivera, D., & Moreno, J. (2022). Integración de detectores de ataques basados en aprendizaje automático en ejercicios defensivos de una gama cibernética 5G. *Appl. Sci. , 12*(20), 10349. https://doi.org/https://doi.org/10.3390/app122010349

Navarro-Cardoso, F., & Montesdeoca , D. (31 de julio de 2021). La cibercriminalidad sexual juvenil como nueva forma de delincuencia. *Revista Penal México, 10*(19), 37-58. https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/453

Noreña , P., & Calderón , S. (2018). Técnica de protección para credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing. *Publicaciones e Investigación, 12*(2). https://dialnet.unirioja.es/servlet/articulo?codigo=8660137

Orosco , J., & Pomasunco, R. (8 de junio de 2020). Adolescentes frente a los riesgos en el uso de las TIC. *Revista Electrónica de Investigación Educativa, 22*. https://doi.org/https://doi.org/10.24320/redie.2020.22.e17.2298

Pacheco, B., Lozano, J., & González, N. (2018). Diagnóstico de utilización de Redes sociales: factor de riesgo para el adolescente. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 8*(16). https://doi.org/https://doi.org/10.23913/ride.v8i16.334

Perdigón, R. (2022). Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio. *Revista científica de sistemas e informática, 2*(2), 21-33. https://dialnet.unirioja.es/servlet/articulo?codigo=8719009

Perdigón, R. (2022). Suricata como detector de intrusos para la seguridad en redes de datos empresariales. *Ciencia UNEMI, 15*(39), 15-39. https://doi.org/https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

Pola, E., López, M., González, J., González, N., Mujica, D., & Santamaría, G. (2022). Analisis comparativo de variables utilizadas en redes distribuidas zigbee para detección de intrusiones desde dispositivos finales en una red de vehículos autónomos no tripulados. https://dialnet.unirioja.es/servlet/articulo?codigo=8661169

Pola, E., López, M., González, J., González, N., Mújica, D., & Santamaría, G. (2022). Análisis comparativo de variables utilizadas en redes distribuidas zigbee para detección de intrusiones desde dispositivos finales en una red de vehículos autónomos no tripulados. *Revista DYNA, 97*(6). https://dialnet.unirioja.es/servlet/articulo?codigo=8661169

Quezada , B., & León , D. (2022). Revisión sistemática de la literatura relacionada con ciberseguridad apoyada con análisis de Big Data para actividades de Red Team. http://dspace.ups.edu.ec/handle/123456789/23322

Quiroz , S., Zapata , J., & Vargas , H. (2020). Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman. *23*(48), 249-267. https://dialnet.unirioja.es/servlet/articulo?codigo=7833456

Quiroz , S., Zapata , J., & Vargas , H. (2020). Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman. http://dx.doi.org/10.22430/22565337.1586

Ramirez, E., Norabuena, R., Toledo, R., & Henostroza, P. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. *Revista Científica General José María Córdova, 20*(37), 209–224. https://doi.org/https://doi.org/10.21830/19006586.791

Rodríguez , O., Legón, C., Socorro, R., & Navarro, P. (julio de 2019). Patrones en el orden de los clics y su influencia en la debilidad de las claves en la Técnica de Autenticación Gráfica Passpoints. *Serie Científica de la Universidad de las Ciencias Informáticas, 12*(7), 37-47. https://dialnet.unirioja.es/servlet/articulo?codigo=8590186

Vivanco, D., Bolaños , F., & Angulo, N. (2020). Estudio exploratorio de las estrategias para la protección a las redes empresariales de las infecciones ransomware. *Revista Científica Multidisciplinaria Arbitrada "YACHASUN", 4*(7). https://dialnet.unirioja.es/servlet/articulo?codigo=8377825