FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ARTÍCULO DE REVISIÓN

MACHINE LEARNING EN LA SEGURIDAD INFORMÁTICA DE LAS PYMES: UNA REVISIÓN SISTEMÁTICA

AUTORES

LAURO CHINCHAY VASQUEZ (ORCID: 0009-0007-8354-6939)

ALEJANDRO MAGNO TUCTO VALERIO (ORCID: 0000-0002-9218-9394)

ASESOR

DRA. IVONNE SADITH MUSAYON OBLITAS (ORCID: 0000-0002-5877-8857)

LÍNEA DE INVESTIGACIÓN DE PROGRAMA

GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS Y/O SISTEMAS DE INFORMACIÓN

LÍNEA DE ACCIÓN RSU

INDUSTRIA, INNOVACIÓN E INFRAESTRUCTURA

LIMA, PERÚ, NOVIEMBRE DE 2024

Referencia bibliográfica

Tucto Valerio, A. M., & Chinchay Vasquez, L. (2024). *Machine learning en la seguridad informática de las pymes: una revisión sistemática* [Trabajo de investigación, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Alejandro Magno Tucto Valerio
Tipo de documento de identidad	DNI
Número de documento de identidad	72767856
URL de ORCID	https://orcid.org/0000-0002-9218-9394
Datos del autor	
Nombres y apellidos	Lauro Chinchay Vasquez
Tipo de documento de identidad	DNI
Número de documento de identidad	46337365
URL de ORCID	https://orcid.org/0009-0007-8354-6939
Datos del asesor	
Nombres y apellidos	Ivonne Sadith Musayon Oblitas
Tipo de documento de identidad	DNI
Número de documento de identidad	09606289
URL de ORCID	https://orcid.org/0000-0002-5877-8857
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Leonardo Erick Noblecilla Mirano
Tipo de documento	DNI
Número de documento de identidad	42054053
Secretario del jurado	
Nombres y apellidos	Jhony Alex Zárate Bocanegra
Tipo de documento	DNI
Número de documento de identidad	09623461
Vocal del jurado	
Nombres y apellidos	Ivan Carlos Luigi Cappillo Salazar
Tipo de documento	DNI
Número de documento de identidad	10302597
Datos de la investigación	
Título de la investigación	Machine learning en la seguridad informática de las pymes: una revisión sistemática

Línea de investigación Institucional	Ciencia, Tecnología e Innovación
Línea de investigación del Programa	Gestión estratégica de tecnologías y/o sistemas de información
Línea de acción RSU	Industria, innovación e infraestructura
URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#5.02.04

Autónoma
Universidad Autónoma del Perú

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

En la ciudad de Lima, el jurado de sustentación del trabajo de investigación conformado por: el MG. LEONARDO ERICK NOBLECILLA MIRANO como presidente, el MG. JHONY ALEX ZÁRATE BOCANEGRA como secretario y el MG. IVÁN CARLOS LUIGI CAPPILLO SALAZAR como vocal, reunidos en acto público para dictaminar el trabajo de investigación titulado:

MACHINE LEARNING EN LA SEGURIDAD INFORMÁTICA DE LAS PYMES: UNA REVISIÓN SISTEMÁTICA

Presentado por el egresado:
LAURO CHINCHAY VASQUEZ

Para obtener el **Grado académico de bachiller en INGENIERÍA DE SISTEMAS**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado** con una calificación de **Doce (12).**

En fe de lo cual firman los miembros del jurado, el 25 de noviembre del 2024.

PRESIDENTE	**SECRETARIO**	**VOCAL**
MG. LEONARDO ERICK NOBLECILLA MIRANO	MG. JHONY ALEX ZÁRATE BOCANEGRA	MG. IVÁN CARLOS LUIGI CAPPILLO SALAZAR

Autónoma
Universidad Autónoma del Perú

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

En la ciudad de Lima, el jurado de sustentación del trabajo de investigación conformado por: el MG. LEONARDO ERICK NOBLECILLA MIRANO como presidente, el MG. JHONY ALEX ZÁRATE BOCANEGRA como secretario y el MG. IVÁN CARLOS LUIGI CAPPILLO SALAZAR como vocal, reunidos en acto público para dictaminar el trabajo de investigación titulado:

MACHINE LEARNING EN LA SEGURIDAD INFORMÁTICA DE LAS PYMES: UNA REVISIÓN SISTEMÁTICA

Presentado por el egresado:
ALEJANDRO MAGNO TUCTO VALERIO

Para obtener el **Grado académico de bachiller en INGENIERÍA DE SISTEMAS**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado** con una calificación de **Once (11).**

En fe de lo cual firman los miembros del jurado, el 25 de noviembre del 2024.

PRESIDENTE	**SECRETARIO**	**VOCAL**
MG. LEONARDO ERICK NOBLECILLA MIRANO	MG. JHONY ALEX ZÁRATE BOCANEGRA	MG. IVÁN CARLOS LUIGI CAPPILLO SALAZAR

Autónoma
Universidad Autónoma del Perú

ACTA DE APROBACIÓN DE ORIGINALIDAD

Yo IVONNE SADITH MUSAYON OBLITAS docente de la Facultad de Ingeniería y Arquitectura de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Autónoma del Perú, en mi condición de asesora del trabajo de investigación titulado:

MACHINE LEARNING EN LA SEGURIDAD INFORMÁTICA DE LAS PYMES: UNA REVISIÓN SISTEMÁTICA

De los egresados CHINCHAY VASQUEZ LAURO y TUCTO VALERIO ALEJANDRO MAGNO, certifico que el trabajo de investigación tiene un índice de similitud de 10% verificable en el reporte de similitud del software Turnitin que se adjunta.

La suscrita revisó y analizó dicho reporte a lo que concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender el trabajo de investigación cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Autónoma del Perú.

Lima, 20 de Enero de 2025

IVONNE SADITH MUSAYON OBLITAS

DNI - 09606289

Machine learning en la seguridad informática de las pymes: una revisión sistemática

Machine learning in computer security of smes: a systematic review

Lauro Chinchay Vasquez [1], Alejandro Magno Tucto Valerio [2]

RESUMEN

Las pequeñas y medianas empresas (PYME) requieren atención urgente ya que el riesgo de los ciberataques es el más evidente en su panorama cibernético. El propósito de este trabajo es la evaluación crítica de la literatura existente centrada en el Machine Learning aplicado a la Protección Cibernética de las pymes. Se revisó un total de ochenta y ocho artículos pertenecientes al periodo de 2020 – 2024, estos fueron extraídos de las bases de datos IEEE Xplore Digital Library, Science Direct, ACM Digital Library y SpringerLink. La metodología incluyó la revisión de la cantidad de estudios sobre la identificación de amenazas, la gestión de riesgos, la protección de recursos, los sistemas de usuarios y la cibercrimen forensics. se identificaron habilidades transferibles mediante el uso de sistemas de Machine Learning e Inteligencia Artificial. Al implementar estas técnicas de IA, las opiniones de los encuestados consideran que las amenazas que enfrentan las pymes son desafíos. Incrementar el uso de Machine Learning, enfocar mejores las medidas de seguridad e introducir nuevos sistemas con el uso de inteligencia artificial. La inteligencia artificial es necesaria no solo para la detección eficaz de nuevas amenazas. Su problema central es conocer las técnicas que pueden ayudar a la integración de bases de datos y la facilitación de conceptos muy variados. Las conclusiones indican que la adopción es vital para consolidar la ciberseguridad en las pymes. Machine Learning se presenta como una solución clave para protegerlas frente al aumento de las amenazas cibernéticas.

[1] Universidad Autónoma del Perú. Orcid 0009-0007-8354-6939. lchinchayv@autonoma.edu.pe

[2] Universidad Autónoma del Perú. Orcid 0000-0002-9218-9394. atuctov@autonoma.edu.pe

Palabras clave: ciberseguridad, machine learning, inteligencia artificial (ia), protección cibernética

ABSTRACT

Small and medium-sized businesses (SMEs) require urgent attention as the risk of cyberattacks is the most evident in their cyber landscape. The purpose of this work is the critical evaluation of the existing literature focused on Machine Learning applied to the Cyber Protection of SMEs. A total of eighty-eight articles belonging to the period 2020 – 2024 were reviewed, these were extracted from the IEEE Xplore Digital Library, Science Direct, ACM Digital Library and SpringerLink databases. The methodology included reviewing the number of studies on threat identification, risk management, resource protection, user systems and cybercrime forensics. Transferable skills were identified through the use of Machine Learning and Artificial Intelligence systems. When implementing these AI techniques, respondents' opinions consider the threats faced by SMEs to be challenges. Increase the use of Machine Learning, better focus security measures and introduce new systems with the use of artificial intelligence. Artificial intelligence is necessary not only for the effective detection of new threats. Its central problem is knowing the techniques that can help the integration of databases and the facilitation of very varied concepts. The conclusions indicate that adoption is vital to consolidate cybersecurity in SMEs. Machine Learning is presented as a key solution to protect them against the increase in cyber threats.

Keywords: cybersecurity, machine learning, artificial intelligence (ai), cyber protection

I. Introducción

Recientemente, los ataques cibernéticos se han constituido como uno de los principales problemas que enfrentan las empresas desde diferentes dimensiones, entre ellas el impacto financiero, el detrimento de su imagen, y la sustracción de datos. Al igual que con cualquier avance tecnológico, aparece un lado más oscuro y busca el eslabón más débil. La protección contra los ataques de virus que los intrusos imponen a las operaciones de estas organizaciones ha hecho que la incorporación del Machine Learning a la ciberseguridad de las PYME sea una práctica efectiva [1]. El crecimiento de la complejidad de los sistemas y aplicaciones va intrínsecamente vinculado con el aumento de las posibilidades de ser víctima de un ciberataque económico [2]. En la lucha por robar o eliminar información empresarial vital, saltarse sitios web en línea e interrumpir el funcionamiento de una organización, se utilizan incluso las técnicas de inserción de malware dentro de los modelos de las redes neuronales [3]. La imperfección en la seguridad de los sistemas, que es constantemente causado por un aumento de complejidad en los ciberataques, ha llevado a las PYME a implantar tecnologías más complejas con el fin de mejorar su nivel de ciberseguridad. Comúnmente, las soluciones como la instalación de cortafuegos o la implementación de sistemas de detección de intrusos han sido los aliados más efectivos [4]. Sin embargo, en la actualidad existe una gran cantidad de ciberataques preferidos que están ocultos dentro de las aplicaciones. Para resolver esta situación y no poner en riesgo la operatividad de una PYME, hay que contar con sistemas SPGSI sostenidos por IA y ML que ayudan a enfrentar los nuevos desafíos, mejorar nuestros métodos de detección y garantizar la defensa contra nuevas amenazas en el sistema de amenazas [5]. Este enfoque de análisis no solo potencia las capacidades de detección y respuesta, sino que también permite a las PYME

implementar una ciberdefensa más sólida y eficaz, logrando el mejor aprovechamiento de los recursos y, en consecuencia, mejorando la resistencia ante ciberataques futuros [6].

Es crucial proteger la información ya que de ello depende la integridad, la confidencialidad y la disponibilidad de todo tipo de datos procesados por las organizaciones, sobre todo, de aquellas que están catalogadas como PYME dependientes de infraestructuras críticas. En relación con el problema destacado anteriormente, uno de los enfoques que se han sugerido es introducir sistemas de aprendizaje automático, que se han visto como una estrategia importante en la detección, clasificación y respuesta a actividades maliciosas, incluyendo APT, que están en aumento y se están volviendo sofisticadas. En los sistemas de control industrial (ICS) empleados por las PYME en sectores estratégicos, el uso de machine learning permite el reconocimiento de Tarea, Técnica, Proceso (TTP) de la alta cibercriminalidad, más allá de los sistemas de seguridad convencionales. Además, estos sistemas permiten los ajustes en línea, disminuyendo así las posibilidades de exposición a las debilidades y aumentando la resiliencia organizacional [7-8]. Utilizando un enfoque del aprendizaje automático como el bosque aleatorio, capaz de detectar amenazas con un 99% de eficacia, las PYME pueden mejorar su postura de seguridad y resistencia a un ciberataque [9]. Las preocupaciones sobre los ciberataques han llevado a grandes establecimientos, predominantemente los más grandes en el sector de la tecnología, a dedicar sus esfuerzos a invertir en IA y aprendizaje automático. Esto tiene un impacto inevitable en la seguridad de las pequeñas y medianas empresas, que es crítico para proteger los datos digitales en la Cuarta Revolución Industrial [10].

El grado de digitalización de las PYME, bajo el marco de nuevas tecnologías, hace que estas empresas pongan un mayor esfuerzo en mejorar su competitividad y eficiencia. Por otro lado, este avance a su vez ha expandido la vulnerabilidad de estas empresas a un ciberespacio que se evidencia más y más intrincado [11]. Debido a que las PYME funcionan con recursos escasos, están en desventaja en cuanto a mantener un nivel razonable de medidas de mitigación de seguridad para las amenazas cibernéticas y que, en muchos casos, son incluso dirigidas a las fallas de seguridad del código. Así es el caso de la técnica del "Insecurity Refactoring", que consiste en transformar el control sobre ciertas partes del código, limitando la posibilidad de implementar errores durante modificaciones extensas del código. Esto a su vez ha mostrado de alguna manera la lista de posibles variantes de las amenazas que se están volviendo cada vez más diferentes variantes [12].

La protección de la información considerada sensible y sobre los sistemas informáticos es, en consecuencia, de relativa importancia para la operación continua y la confianza del cliente. En relación a lo anterior, la inteligencia artificial (IA) y el aprendizaje automático son herramientas que se pueden emplear con el fin de reforzar la ciberseguridad en las PYME, debido a que permiten detectar y neutralizar las vulnerabilidades de las PYME antes de ser aprovechadas [13]. La inteligencia artificial (IA) y el aprendizaje automático (ML) proporcionan a las PYME de una mejor protección en contra de la amenaza del cibercrimen al considerar que se tiene una mejor detección y respuesta frente a tales ataques. Tal como se acostumbra en la implementación [14]. En el contexto de la ciberseguridad, los sistemas de recomendación pueden ser muy útiles para las pequeñas y medianas empresas en su proceso de toma de decisiones debido a la reducción de la exposición al riesgo; un riesgo como las amenazas del ciberespacio. Asimismo, solucionar estos

problemas tiene relevancia, sobre todo por los retos que representan en términos de privacidad y seguridad de datos de estas tecnologías. Sí, aunque el ML parece atender tales factores, su éxito puede ser relativamente distinto. Para superar esto, un modelo de ciberseguridad cognitiva se propone que ofrece mayor efectividad en la identificación de amenazas al integrar fuentes de información [15-16]. Una consideración crítica que debe tenerse en cuenta al implementar IA y ML es la seguridad de la información y la privacidad. Para que estos sistemas funcionen correctamente, se debe procesar una gran cantidad de información; este aumento en la cantidad de datos críticos también incrementa las posibilidades de ciberataques, así como de violaciones de privacidad [17]. En cuanto a las empresas que manejan estos datos críticos, deben cumplir con los requisitos de las agencias de contraataque que registran la información en un estándar que respalda la privacidad, lo que a su vez presenta otro grado de responsabilidad en lo que respeta a la gestión. de la seguridad de la información [18]. No obstante, la aplicación del Aprendizaje Automático y la IA para la ciberseguridad de las PYME no se lleva a cabo sin algunos problemas y controversias. En lo que respeta a lo que se espera de la literatura disponible en la actualidad, se señalan altos costos de implementación, falta de cualificación del personal y complejidad de los modelos, lo que hace que la justificación de su utilidad en pequeñas empresas con recursos limitados. Sea una propuesta interesante. Además, existen cuestiones morales y de privacidad relacionadas con el despliegue de tales sistemas, que requieren una gran cantidad de datos sensibles [19]. Esto ha provocado una discusión sobre la opacidad y la objetividad de la toma de decisiones automatizada y la eficacia de tales tecnologías para abordar las brechas entre los grandes actores y los pequeños en la industria [20]. La creciente integración de la IA y el ML en el campo de la ciberseguridad

también plantea desafíos éticos en las políticas. Los temas de transparencia y equidad en la automatización de la toma de decisiones son de importancia crítica. Debe haber una disposición de que los sistemas de Inteligencia Artificial, siempre que sean creados, eviten significativamente los sesgos en dichos procesos de toma de decisiones que conduzcan a la creación de malware inteligente [21]. Además, también es muy relevante asegurar que las decisiones tomadas sean tales que puedan ser comunicadas y justificadas a las personas y partes interesadas [22]. Por último, pero no menos importante, la adaptabilidad y escalabilidad tanto de la IA como del ML también son muy importantes en el contexto de la ciberseguridad, ya que permiten el combate directo contra amenazas en evolución. Si bien estos métodos han aumentado la detección de ataques a la red, el foco ha sido más bien mejorar la precisión general en lugar de atacar ataques específicos, creando una necesidad de soluciones más flexibles y dinámicas [23].

Eventualmente, se evaluarán los resultados para valorar qué tan bien funcionan las soluciones de inteligencia artificial propuestas para la ciberseguridad, delinear problemas emergentes y recomendar posibles direcciones para futuras investigaciones.

II. Método

Para investigar la utilización de la inteligencia artificial y el aprendizaje automático en la ciberseguridad de las pequeñas y medianas empresas, se aplicó la metodología PRISMA. Dicho estudio se realizó en las bases de datos académicos como IEEE Xplore, ScienceDirect, ACM Digital Library y SpringerLink, en relación con los ciberataques, vulnerabilidades, medios defensivos y tecnologías IA y ML [24].

Las investigaciones fueron seleccionadas de fuentes publicadas para los períodos de 2020 a 2024, dependiendo de su relevancia, calidad metodológica y validación empírica. Estos datos fueron apreciados ya que contribuyeron al número y la relevancia de la información [25]. La revisión de la literatura se completó de manera bastante exhaustiva, centrándose en la detección de ataques cibernéticos, su mitigación y técnicas de automatización de respuesta. Los datos crudos se agruparon en categorías relevantes con el propósito de presentar la información de manera más clara y organizada, sin perder el enfoque y la claridad de la investigación.

En la Figura 1, se observa un diagrama de flujo de las actividades a realizar.

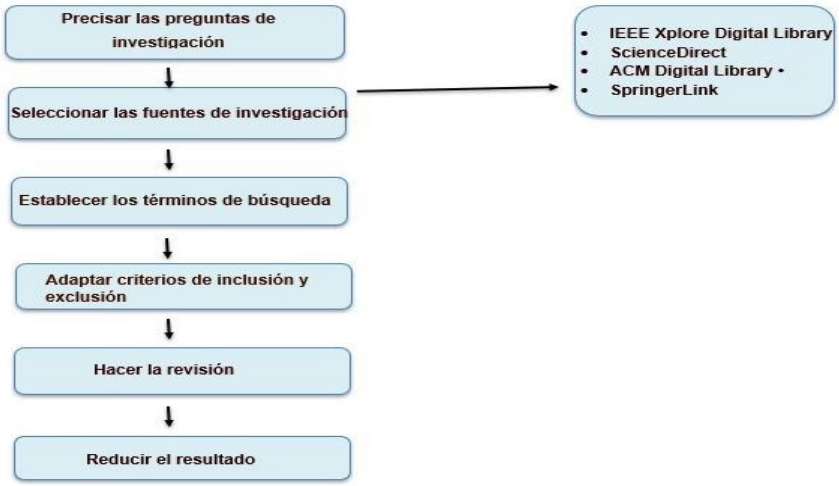

Figura.1. Diagrama de Flujo SRL

III. Análisis e integración de la información

A. Fuentes donde se realizó la Búsqueda

Se aplicó la técnica de búsqueda documental en 4 bibliotecas selectivas y con ello se logró recuperar 88 textos: 50 en la base de ScienceDirect, 30 en la base de IEEE Xplore Digital Library, 6 en la base de ACM Digital Library y 2 en SpringerLink. El análisis global fue dirigido a estudios sobre las dificultades de la detección de ciberseguridad en sistemas de procesamiento [26].

En la figura 2, muestra el diagrama del proceso de búsqueda y análisis.

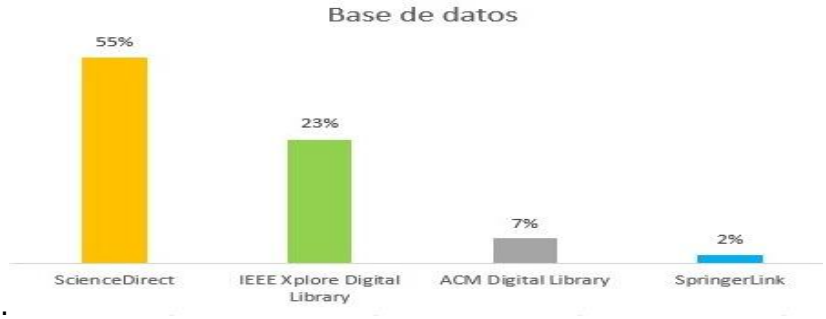

Figura.2. Base de Datos

Se encontraron las fuentes de procedencia de ScienceDirect y IEEE Xplore Digital Library.

B. Términos de Búsqueda

TABLA I. ECUACIÓN DE BÚSQUEDA

Base de Datos	Ecuación
IEEE Xplore, ScienceDirect, ACM Digital Library, SpringerLink	Fórmula de búsqueda: "Inteligencia Artificial" OR "Machine Learning" AND "Seguridad Informática" AND "Pymes"

C. Criterios de Inclusión y Exclusión Preguntas de la Investigación

Para esta investigación se plantearon 5 preguntas, tal como se observa en la tabla II.

TABLA II. PREGUNTAS DE INVESTIGACIÓN

Preguntas de la Investigación	Motivación
P-01: ¿La IA y el machine learning se utilizan en la detección y planeación de trata de ciberseguridad informática?	IA y ML encienden la lucha contra los comportamientos anómalos, siendo capaces de desplegar sistemas de detección de amenazas en tiempo real. La IA, las redes neuronales, la inteligencia computacional y el aprendizaje automático hacen posible que los sistemas operen de

Preguntas de la Investigación	Motivación
	manera autónoma y se autoconfiguren y se resuelvan problemas sin intervención humana [27].
P-02: ¿Qué técnicas se emplean en la actualidad para la detección y prevención de trata de la ciberseguridad informática?	Actualmente, se utilizan técnicas como el análisis de comportamiento, firmas digitales, algoritmos de detección de intrusiones y análisis de tráfico de red para identificar y prevenir riesgos. [28]
P-03: ¿Las empresas utilizan la inteligencia artificial y el machine learning para mejorar la gestión de riesgos y la toma de decisiones en materia de seguridad informática?	Las empresas utilizan IA y ML para analizar grandes volúmenes de datos, detectar patrones anómalos y tomar decisiones informadas en tiempo real, mejorando la gestión de riesgos y la seguridad [29]
P-04: ¿Cuáles obstáculos y restricciones surgen al implementar soluciones fundamentadas en inteligencia artificial y aprendizaje automático en el contexto de la seguridad informática de las empresas?	Los desafíos incluyen la falta de datos representativos, la transparencia de los modelos, la necesidad de actualizaciones constantes y las consideraciones éticas y legales sobre la privacidad [30]
P-05: ¿Cuántos artículos sobre la evaluación de rendimientos y la calidad en la arquitectura basada en IA aplicados en la ciberseguridad se publicaron por año en el periodo de 2020 a 2024?	La elaboración de la tabla permite medir el volumen anual de artículos sobre el tema evaluación del rendimiento y la evaluación de la calidad de arquitecturas de IA en ciberseguridad, en el periodo 2020 a 2024.

D. Fuentes de búsqueda

Se establecieron los siguientes criterios, como se detalla en la Tabla III.

TABLA III. CRITERIOS DE ARTÍCULOS PRE - CRITERIOS

Criterios		
Inclusión	I-01	Estudios que se centren en la aplicación de la inteligencia artificial y el machine learning en la seguridad informática de las empresas.
	I-02	Estudios que presenten resultados empíricos y datos cuantitativos sobre la eficacia de la I.A y el M.L en la seguridad informática.
	I-03	Estudios publicados en foros o revistas científicas y conferencias reconocidas en el área de la seguridad informática.
	I-04	Estudios publicados en los últimos 5 años para que aseguremos la actualidad y la veracidad de la información.
	I-05	Artículos escritos en inglés, español y portugués.
Exclusión	E-01	Estudios que no abordan la aplicación de la I.A y M.L en la ciberseguridad de las empresas.
	E-02	Estudios que no presenten resultados empíricos o datos cuantitativos sobre la eficacia de la aplicación I.A y M.L. en la seguridad informática.

Criterios		
	E-03	Estudios que no sean publicados en foros o revistas no calificadas ni que tengan valor en el área de la seguridad.
	E-04	Estudios publicados hace más de 5 años que no aseguran la actualidad de la información.
	E-05	Los artículos de investigación están escritos en inglés, español y portugués.

E. Sintetizar el Resultado

Se analizaron los 45 artículos seleccionados, tal como se observa en la tabla IV.

TABLA IV. CANTIDAD DE ARTÍCULOS POST - CRITERIOS

Base de Datos	Pre - Criterios	Excluidos	Incluidos	Porcentaje (%)
ScienceDirect	50	31	18	54%
IEEE Xplore Digital Library	30	10	20	34%
ACM Digital Library	6	2	4	7%
SpringerLink	2	0	2	5%
Total	88	43	45	100%

F. RESULTADOS

La Revisión Sistemática de Literatura responde a las preguntas planteadas.

P-01: ¿La IA y el machine learning se utilizan en la detección y planeación de trata de ciberseguridad informática?

En el caso de nuestro trabajo de investigación, se da la necesidad de trabajar con volúmenes grandes de información para detectar actividades inusuales y vulnerabilidades en tiempo real. Las técnicas de IA y aprendizaje automático (ML) son muy útiles para la ciberseguridad, ya que mejoran la detección de riesgos y la mitigación de riesgos. El software de mejora genera en tiempo real sobre patrones anómalos, lo cual es crucial para la identificación de nuevas amenazas, al mismo tiempo proteger entornos únicos, aumentando la eficiencia de la protección. [31-32]

P-02: ¿Qué técnicas se emplean en la actualidad para la detección y prevención de trata de la ciberseguridad informática?

Hoy en día, el aprendizaje automático es una tecnología madura que ha encontrado muchos usos en el sistema big data, cuya premisa es la seguridad de la información. Estas herramientas son útiles al tratar con datos que tienen una amplia gama de variaciones, así como con la búsqueda de amenazas que crecen rápidamente. Si se utiliza aprendizaje automático para el desarrollo de sistemas de detección de intrusos, entonces estos sistemas podrán identificar acciones peligrosas y adaptarse para contrarrestar varios tipos nuevos de ataques. [33-34]

P-03: ¿Las empresas utilizan la I. A y M.L para mejorar la gestión de riesgos y la toma de decisiones en materia de seguridad informática?

Hoy en día, las organizaciones utilizan IA y ML para optimizar la gestión de riesgos y tomar decisiones relativas a la seguridad. Tal tecnología se involucra en el análisis de inmensas cantidades de datos para incluso anticipar una amenaza. El aprendizaje ayuda en la inteligencia de amenazas en un entorno colaborativo, mientras que los sistemas de detección de intrusiones construidos sobre ML garantizan protección en tiempo real. La ciberseguridad se ha integrado la IA y el ML en el mundo que ve rápidamente hacia la conectividad. [35-36]

P-04: ¿Cuáles obstáculos y restricciones surgen al implementar soluciones fundamentadas en inteligencia artificial y aprendizaje automático en el contexto de la seguridad informática de las empresas?

La IA y el aprendizaje automático tienen un potencial impresionante como herramientas esenciales en la ciberseguridad para las organizaciones empresariales, sin embargo, hay obstáculos significativos que deben superarse, entre ellos la complejidad técnica, el costo elevado, la falta de suficientes conjuntos de datos etiquetados, la necesidad de actualizaciones permanentes para la nueva amenaza,

etc. Estos desafíos resultan ser aún más perjudiciales para las pequeñas y medianas empresas en las economías emergentes, donde la presión entre problemas éticos, infraestructurales y capacidades humanas. Además, busca solucionar estos problemas y fortalecer los niveles de ciberseguridad [37-38].

P-05: ¿Cuántos artículos sobre la evaluación de rendimientos y la calidad en la arquitectura basada en IA aplicados en la ciberseguridad se publicaron por año en el periodo de 2020 a 2024?

Se creó una tabla para registrar los artículos (2020-2024) sobre la evaluación de la arquitectura IA en ciberseguridad, mostrada en la Tabla V.

TABLA V. ARTÍCULOS POR AÑO

Base de Datos	Cantidad	Artículos/ años
ScienceDirect	19	[2] 2024, [3] 2022, [6] 2021, [10] 2023, [14] 2023, [16] 2024, [17] 2021, [23] 2021, [25] 2023, [28] 2024, [30] 2024, [31] 2024, [32] 2023, [33] 2023, [34] 2024, [35] 2021, [36] 2024, [37] 2024, [38] 2022
IEEE Xplore	20	[1] 2021, [4] 2023, [5] 2020, [7] 2021, [8] 2024, [9] 2023, [12] 2021, [18] 2024, [20] 2021, [21] 2022, [22] 2023, [26] 2023, [27] 2020, [39] 2023, [40] 2022, [42] 2023, [43] 2023, [44] 2024, [45] 2024, [13] 2020
ACM Digital Library	4	[11] 2023, [19] 2024, [41] 2022, [29] 2021
SpringerLink	2	[15] 2023, [24] 2024
Total	45	

En la Figura 3 se observa la cantidad de artículos encontrados por año.

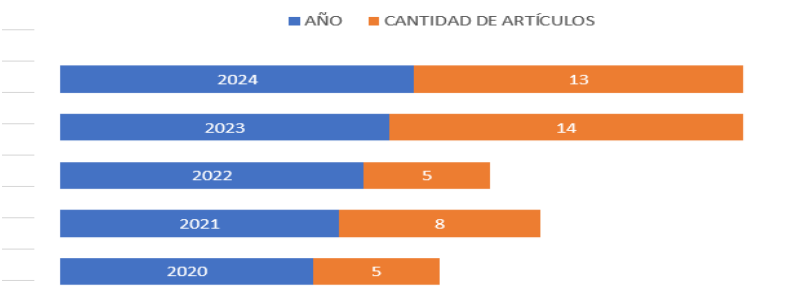

Fig.3. Cantidad de artículos por año

G. DISCUSIÓN

Los agentes inteligentes que se encuentran dentro de las definiciones de Inteligencia Artificial y los parámetros de aprendizaje automático (ML) han demostrado ser eficaces en la mejora de la gestión de pedidos al agilizar procesos y permitir decisiones en tiempo real [39][40]. Este trabajo confirma que, comparable a otras investigaciones, la automatización de actividades rutinarias ayuda en gran medida a atender solicitudes en tiempos más cortos ya reducir problemas operativos, y, en consecuencia, aumenta la productividad [41][42].

Una diferencia importante en relación con las investigaciones anteriores es que, además de apuntar a la previsión de la demanda, nuestra solución incluye también la asignación automatizada de activos. Esto agrega un valor adicional, ya que hay un gran número de estudios que se centran exclusivamente en la modelización predictiva sin tal aplicación, la cual es muy importante para mejorar la gestión empresarial en general [43].

Además, como ocurrió en otros estudios, hubo dificultades con la implementación de estas tecnologías, especialmente en las Pequeñas y Medianas Empresas. Entre las principales barreras se expresan el alto costo de implementación y la necesidad de capacitar a las personas en las competencias tecnológicas requeridas para garantizar el uso adecuado del sistema [44]. Sin embargo, estos problemas limitan la utilización completa de herramientas basadas en IA. Las aplicaciones de IA ofrecen ventajas increíbles, pero no todas pueden ser explotadas debido a tales limitaciones.

Finalmente, este artículo destaca la necesidad de enfrentar los problemas éticos relacionados con la privacidad de los datos y la transparencia algorítmica para infundir confianza en los usuarios con respecto al uso responsable de tales tecnologías [45].

IV. Conclusiones

En esta revisión se ha demostrado que la IA y el ML no solo son eficaces en la administración de la tecnología y la planificación de la seguridad, sino también en el análisis de datos masivos e integración de contramedidas nuevas.

Métodos modernos como sistemas automáticos de detección de intrusiones o incluso el aprendizaje federado mejoran el nivel de ciberseguridad porque permiten a las organizaciones cooperar sin recurrir a la violación de la privacidad, lo que a su vez mejora las defensas contra amenazas emergentes.

En el mundo de los negocios, la IA y el ML actúan como instrumentos que mejoran la gestión de riesgos y la toma de decisiones, ya que pueden identificar patrones inusuales y reaccionar instantáneamente a ciberataques, lo cual es muy importante en el contexto de una sociedad. digital e interconectada. Sin embargo, estas tecnologías no están en uso generalizado porque son costosas, requieren ciertas características técnicas complejas y emplean personal altamente calificado, lo que plantea desafíos principalmente para las pequeñas y medianas empresas, que también tienen problemas con infraestructura y recursos. Es importante resolver estos problemas para que su uso sea mucho más generalizado de lo que es en la actualidad.

Por último, en la bibliografía se destacaron más de 100 publicaciones y la investigación se realizó entre los años 2020 a 2024 aprehendiendo la tendencia en el activismo en las investigaciones en IA en Ciberseguridad.

Referencias

[1] M. M. A. Mutalib, Z. Zainol, y M. H. M. Halip, "Mitigating malware threats at small medium enterprise (SME) organisation: A review and framework", en *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, 2021. https://doi.org/10.1109/ICRAIE52900.2021.9703991

[2] Moutaz Alazab, Ruba Abu Khurma, Maribel García-Arenas, Vansh Jatana, Ali Baydoun, Robertas Damaševičius, “Enhanced threat intelligence framework for advanced cybersecurity resilience”, Egyptian Informatics Journal, Volume 27, 2024, 100521, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2024.100521

[3] Z. Wang, C. Liu, X. Cui, J. Yin, y X. Wang, "EvilModel 2.0: Bringing Neural Network Models into Malware Attacks", Computers & Security, vol. 102, p. 102807, 2022. DOI: https://doi.org/10.1016/j.cose.2022.102807

[4] A. R. Amran, A. Ibrahim Zaki Ahmad Lutfi, A. Saad, A. N. Hilman Ahmad Jaafar and S. Mohamad, "Development of Secured Network Design for Small Enterprise Server," 2023 International Conference on Engineering Technology and Technopreneurship (ICE2T), Kuala Lumpur, Malaysia, 2023, pp. 251-255, DOI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10540511&isnumber=10540460

[5] M. I. Khan, S. Tanwar and A. Rana, "The Need for Information Security Management for SMEs," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020, pp. 328-332, DOI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9337108&isnmber=9337061

[6] O. Yurekten y M. Demirci, "Citadel: Cyber threat intelligence assisted defense system for software-defined networks", Computer Networks, vol. 197, p. 108013, 2021. DOI: https://doi.org/10.1016/j.comnet.2021.108013

[7] KA Ubaidillah, SI Hisham, F. Ernawan, G. Badshah y E. Suharto, "Sistema de detección de intrusiones que utiliza una red neuronal profunda basada en autocodificador para la ciberseguridad de las PYME", 2021 5th International Conference on Informatics and Computational Sciences (ICICoS) , Semarang, Indonesia, 2021, págs. 210-215, DOI: 10.1109/ICICoS53627.2021.9651851

[8] S. Moiz, A. Majid, A. Basit, M. Ebrahim, AA Abro y M. Naeem, "Seguridad y detección de amenazas mediante la implementación de Wazuh basada en la nube", 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) , Tandojam, Pakistán, 2024, págs. 1-5, DOI: 10.1109/KHI-HTC60760.2024.10482206

[9] SY Yi, MM Singh, GC Sodhy y T. Jabar, "Generación de huellas dactilares para la detección de amenazas persistentes avanzadas (APT) mediante técnicas de aprendizaje automático", 13.ª Conferencia internacional sobre tecnología de la información en Asia (CITA) de 2023 , Kota Samarahan, Malasia, 2023, págs. 31-36, DOI: 10.1109/CITA58204.2023.10262639

[10] M. Imran, H. U. R. Siddiqui, A. Raza, M. A. Raza, F. Rustam, y I. Ashraf, "A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems", Computers & Security, vol. 123, p. 103445, 2023. DOI: https://doi.org/10.1016/j.cose.2023.103445

[11] G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. B. Rapa, A. V. Grammatopoulos, y F. Di Franco, "The role of machine learning in cybersecurity",

Digital Threats: Research and Practice, vol. 4, no. 1, p. 8, 2023. DOI: https://doi.org/10.1145/3545574

[12] A. Emer, M. Unterhofer y E. Rauch, "Un modelo de evaluación de la ciberseguridad para pequeñas y medianas empresas", en IEEE Engineering Management Review , vol. 49, núm. 2, págs. 98-109, 1 segundo trimestre, junio de 2021, DOI: 10.1109/EMR.2021.3078077

[13] Serna Valdivia, E. Jhordany, y Mejía Miranda, J."Propuesta de un Agente Inteligente para el Manejo y Mitigación de Riesgos de Ciberseguridad en Entornos IoT," en 2020 9th International Conference On Software Process Improvement (CIMPS), Mazatlán, Sinaloa, México, 2020, pp. 158-158. DOI: http://doi.org/10.1109/CIMPS52057.2020.9390153

[14] Marc Schmitt, Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection, Journal of Industrial Information Integration, Volume 36, 2023, 100520, ISSN 2452-414X, DOI: https://doi.org/10.1016/j.jii.2023.100520

[15] L. Ferreira, D. C. Silva, y M. U. Itzazelaia, "Sistemas de recomendación en ciberseguridad", Knowledge and Information Systems, vol. 65, pp. 5523-5559, 2023. DOI: https://doi.org/10.1007/s10115-023-01906-6

[16] L. Liu, Z. Sajid, C. Kravaris, y F. Khan, "Detection and analysis of cybersecurity challenges for processing systems", Process Safety and Environmental Protection, vol. 185, pp. 1061-1071, 2024. DOI: https://doi.org/10.1016/j.psep.2024.03.088

[17] Y. Jiang y Y. Atif, "A selective ensemble model for cognitive cybersecurity analysis", Journal of Network and Computer Applications, vol. 184, p. 103210, 2021. DOI: https://doi.org/10.1016/j.jnca.2021.103210

[18] GM Kumar y D. Hemanand, "Desarrollo de un modelo robusto de seguridad de datos para mantener la integridad de la información mediante inteligencia artificial y leyes cibernéticas", Conferencia internacional de 2024 sobre sistemas inteligentes para la ciberseguridad (ISCS) , Gurugram, India, 2024, págs. 1-7, DOI: 10.1109/ISCS61804.2024.10581024

[19] J. Ghadermazi, A. Shah, y S. Jajodia, "A machine learning and optimization framework for efficient alert management in a cybersecurity operations center", Digital Threats, vol. 5, no. 2, p. 19, 2024. DOI: https://doi.org/10.1145/3644393

[20] J. P. S. Piest, M. -E. Iacob, M. van Sinderen, M. Gemmink and B. Goossens, "A Reinforcement Learning Platform for Small and Medium-sized Enterprises in Logistics," 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Gold Coast, Australia, 2021, pp. 289-298, DOI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9626344&isnumber=9626200

[21] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, y R. Ahmad, "Machine Learning and Deep Learning Approaches for Cybersecurity: A Review", IEEE Xplore, 2022. DOI: https://doi.org/10.1109/ICRAIE52900.2021.9712274

[22] A. Pawlicka, M. Pawlicki, R. Kozik and M. Choraś, "The Need for Practical Legal and Ethical Guidelines for Explainable AI-based Network Intrusion Detection

Systems," 2023 IEEE International Conference on Data Mining Workshops (ICDMW), Shanghai, China, 2023, pp. 253-261, DOI: 10.1109/ICDMW60847.2023.00038

[23] A. S. Ayesha y D. D. Manivannan, "Intrusion detection based on Machine Learning techniques in computer networks", Internet of Things, vol. 16, p. 100462, 2021. DOI: https://doi.org/10.1016/j.iot.2021.100462

[24] C. Nobles, "The weaponization of artificial intelligence in cybersecurity: A systematic review", Procedia Computer Science, vol. 239, pp. 547-555, 2024. DOI: https://doi.org/10.1016/j.procs.2024.06.206

[25] T. Sowmya y E. A. Mary Anita, "A comprehensive review of AI-based intrusion detection systems", Measurement: Sensors, vol. 28, p. 100827, 2023. DOI: https://doi.org/10.1016/j.measen.2023.100827

[26] C. N. Fleron, J. K. Jørgensen, O. Kulyk, y E. Paja, "Towards a Basic Security Framework for SMEs – Results From an Investigation of Cybersecurity Challenges in Denmark", IEEE 31st International Requirements Engineering Conference Workshops (REW), Hannover, Germany, 2023, pp. 230-233. DOI: https://doi.org/10.1109/REW57809.2023.00046

[27] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, y M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade", IEEE Access, vol. 8, pp. 222310-222354, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3041951

[28] T. Yang, Y. Qiao, y B. Lee, "Towards trustworthy cybersecurity operations using Bayesian deep learning to improve uncertainty quantification of anomaly

detection", Computers & Security, vol. 144, p. 103909, 2024. DOI: https://doi.org/10.1016/j.cose.2024.103909

[29] L. Ashiku y C. Dagli, "Network intrusion detection system using deep learning", Procedia Computer Science, vol. 185, pp. 239-247, 2021. DOI: https://doi.org/10.1016/j.procs.2021.05.025

[30] A. Anderson, A. Ahmad, y S. Chang, "Case-based learning for cybersecurity leaders: A systematic review and research agenda", Information & Management, vol. 61, no. 7, p. 104015, 2024. DOI: https://doi.org/10.1016/j.im.2024.104015

[31] M. Macas, C. Wu, y W. Fuertes, "Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems", Expert Systems with Applications, vol. 238, p. 122223, 2024. DOI: https://doi.org/10.1016/j.eswa.2023.122223

[32] O. Alshaikh, S. Parkinson, y S. Khan, "Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach", Computers & Security, vol. 103, p. 103694, 2024. DOI: https://doi.org/10.1016/j.cose.2023.103694

[33] Marc Schmitt, Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection, Journal of Industrial Information Integration, Volume 36, 2023, DOI: https://doi.org/10.1016/j.jii.2023.100520

[34] M. F. Arroyabe, C. F. A. Arranz, I. F. Arroyabe, y J. C. Fernandez de Arroyabe, "Exploring the economic role of cybersecurity in SMEs: A case study of the

UK", Technology in Society, p. 102670, 2024. DOI: https://doi.org/10.1016/j.techsoc.2024.102670

[35] Claudio A. Ardagna, Valerio Bellandi, Ernesto Damiani, Michele Bezzi, Cedric Hebert, Big Data Analytics-as-a-Service: Bridging the gap between security experts and data scientists, Computers & Electrical Engineering, Volume 93, 2021, DOI: https://doi.org/10.1016/j.compeleceng.2021.107215

[36] M. F. Arroyabe, C. F. A. Arranz, I. Fernandez de Arroyabe, y J. C. Fernandez de Arroyabe, "The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges", Technological Forecasting and Social Change, p. 123051, 2024. DOI: https://doi.org/10.1016/j.techfore.2023.123051

[37] Alladean Chidukwani, Sebastian Zander, Polychronis Koutsakis, Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications, Computers & Security, Volume 145, 2024, DOI: https://doi.org/10.1016/j.cose.2024.104026

[38] J. P. Tamvada, S. Narula, D. Audretsch, H. Puppala, y A. Kumar, "Adopting new technology is a distant dream? The risks of implementing Industry 4.0 in emerging economy SMEs", Technological Forecasting and Social Change, p. 122088, 2022. DOI: https://doi.org/10.1016/j.techfore.2022.122088

[39] Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash, Chaminda Hewage, Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales, International Journal of Information Management Data Insights, Volume 3, Issue 2, 2023, DOI: https://doi.org/10.1016/j.jjimei.2023.100191

[40] T. Singano, H. Ngejane, C. Mudau, L. Ndlovu and M. Tyukala, "ML-Based Security Analytics in South African SMEs: A Review and Classification," 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2023, pp. 1-6, doi: 10.1109/ICECET58911.2023.10389479. DOI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10389479&isnumber=10389181

[41] O. Odukoya, "The Transformative Impact of Cloud Computing on Small and Medium-sized Enterprises (SMEs): A Comprehensive Analysis", en 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), 2024, pp. 1-5. DOI: https://doi.org/10.1109/SmartNets61466.2024.10577703

[42] J. P. S. Piest, M.-E. Iacob, M. van Sinderen, M. Gemmink, y B. Goossens, "A reinforcement learning platform for small and medium-sized enterprises in logistics", en 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), 2021, pp. 289-298. DOI: https://doi.org/10.1109/EDOCW52865.2021.00060

[43] A. Emer, M. Unterhofer, y E. Rauch, "A cybersecurity assessment model for small and medium-sized enterprises", IEEE Engineering Management Review, vol. 49, no. 2, pp. 98-109, 2021. DOI: https://doi.org/10.1109/EMR.2021.3078077

[44] F. H. Zawaideh, W. Abu-Ulbeh, S. A. Mjlae, Y. A. B. El-Ebiary, Y. Al Moaiad, y S. Das, "Blockchain solution for SMEs cybersecurity threats in e-commerce", en 2023 International Conference on Computer Science and Emerging

Technologies (CSET), 2023, pp. 1-7. DOI: https://doi.org/10.1109/CSET58993.2023.10346628

[45] N. Mmango y T. Gundu, "Cyber resilience in the entrepreneurial environment: A framework for enhancing cybersecurity awareness in SMEs", en 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2023, pp. 1-6. DOI: https://doi.org/10.1109/ICECET58911.2023.10389226

Anexos

Declaración jurada de autoría

Este documento define los compromisos recíprocos de los miembros firmantes y constituye una Declaración jurada de carácter legal, para el desarrollo en autoría del trabajo de investigación (Artículo de revisión) para la obtención del grado académico (Bachiller). Nosotros, declaramos que hemos sido informados sobre las condiciones para el desarrollo del trabajo de investigación (Artículo de revisión), que conduce al grado académico profesional, las cuales comprenden lo siguiente:

1. El trabajo se desarrollará de forma equitativa, donde los coautores participan de igual manera en todo el proceso de su desarrollo.

2. El proceso de solicitud para el grado académico, debe de realizarse en conjunto, si uno de los autores está ausente no se podrá iniciar el proceso.

3. En caso de incumplimiento de los compromisos incluidos en este documento, las partes lo tienen que poner en conocimiento al director de Escuela.

4. Se podrá generar algunas excepciones en las cuales el autor está imposibilitado para desarrollar el proceso para optar el grado académico a lo cual podrá ceder los derechos de autor patrimoniales de forma permanente al otro autor o autores. Estos casos se darán de acuerdo a la siguiente tabla:

CASO	CESIÓN DE DERECHOS DE AUTOR PATRIMONIAL
Muerte de uno de los autores o uno de los autores no se matricula en la asignatura.	Se activa la cesión de derechos de autor patrimonial permanente de forma inmediata, al otro autor o autores que quedan.
Traslado de un autor a otra institución.	
Uno de los autores desistió abandonar el trabajo (por cualquier otro caso no contemplado anteriormente).	

Los firmantes, estudiantes de la facultad Ingeniería y Arquitectura, escuela de Ingeniería de Sistemas, conscientes en todos sus actos firman el presente documento.

APELLIDOS Y NOMBRES	DNI	FIRMA	HUELLA DIGITAL
Lauro Chinchay Vasquez	46337365		
Tucto Valerio Alejandro Magno	72767856		

Lima, 17 de Julio del 2024