# Emerging Technologies: a systematic literature review to strengthen cybersecurity

George Danny Anaya Salazar[1]; Verónica Daleska Herrera Lazo[2]; José Julio Bendezú Huaroto[3]; Alan Omar Bermúdez-Cavero[4]; Giany Zegarra Castañeda[5]
[1,2,3,4,5]Universidad Tecnológica del Perú, Perú, *U18308964@utp.edu.pe, U18211947@utp.edu.pe, c25596@utp.edu.pe, c20415@utp.edu.pe, c21953@utp.edu.pe*

***Abstract*– This review aims to identify and collect current knowledge on how technologies such as artificial intelligence, machine learning, blockchain, IoT, and others can strengthen cybersecurity. Method: the PICO strategy and PRISMA diagram were used, 133 relevant articles were selected and analyzed from the SCOPUS database between the years 2019 to April 2024. The methods of this SLR included rigorous inclusion and exclusion criteria to ensure the relevance and quality of the studies analyzed. Results: within the present work the most widely used emerging technologies and their practical applications in cybersecurity are highlighted, identifying significant trends and patterns in the implementation of these technologies. Conclusions: the main current limitations are pointed out, such as the lack of standardization and the need for further empirical research, and key areas for future research are proposed, including the evaluation of the effectiveness of these technologies in different business contexts; this study provides a comprehensive and updated view that can guide both researchers and practitioners in the implementation of cybersecurity strategies based on emerging technologies, offering a solid foundation for improving defenses against increasingly sophisticated cyber threats.***

***Keywords*-- Security, Cybersecurity, Emerging Technologies, Networking, Internet of Things.**

# Tecnologías Emergentes: una revisión sistemática de literatura para fortalecer la ciberseguridad

George Danny Anaya Salazar[1]; Verónica Daleska Herrera Lazo[2]; Alan Omar Bermúdez-Cavero[3]; José Julio Bendezú Huaroto[4]; Giany Zegarra Castañeda[5]
[1,2,3,4,5]*Universidad Tecnológica del Perú, Perú, U18308964*@utp.edu.pe, *U18211947*@utp.edu.pe, c25596@utp.edu.pe, c20415@utp.edu.pe, c21953@utp.edu.pe

***Resumen*– Esta revisión tiene como objetivo identificar y recopilar el conocimiento actual sobre cómo tecnologías como la inteligencia artificial, el aprendizaje automático, blockchain, IoT, y otras, pueden fortalecer la ciberseguridad. Método: se utilizó la estrategia PICO y el diagrama PRISMA, se seleccionaron y analizaron 133 artículos relevantes de la base de datos SCOPUS entre los años 2019 hasta abril de 2024. Los métodos de esta RSL incluyen criterios rigurosos de inclusión y exclusión para garantizar la relevancia y calidad de los estudios analizados. Resultados: dentro del presente trabajo se puede apreciar que se destacan las tecnologías emergentes más utilizadas y sus aplicaciones prácticas en la ciberseguridad, identificando tendencias significativas y patrones en la implementación de estas tecnologías. Conclusiones: se señalan las principales limitaciones actuales, como la falta de estandarización y la necesidad de más investigaciones empíricas, y se proponen áreas clave para futuras investigaciones, incluyendo la evaluación de la eficacia de estas tecnologías en diferentes contextos empresariales; este estudio proporciona una visión integral y actualizada que puede guiar tanto a investigadores como a profesionales en la implementación de estrategias de ciberseguridad basadas en tecnologías emergentes, ofreciendo una base sólida para mejorar las defensas contra amenazas cibernéticas cada vez más sofisticadas.***

***Palabras clave*-- Seguridad, Ciberseguridad, Tecnologías Emergentes, Redes, Internet de las cosas.***

## I. Introducción

A medida que las conexiones digitales y la interdependencia de estas empiezan a volverse más complejas, usadas y generalizadas, aumentan las áreas vulnerables donde pueden llegar a realizarse ciberataques en las organizaciones, por otro lado también los atacantes no autorizados mejoran continuamente sus métodos de ataque, intentando ingresar sin autorización a los sistemas, amenazar los datos y explotar las vulnerabilidades; las organizaciones reconocen estas amenazas y su cambiante naturaleza; como una respuesta a esto las organizaciones han cambiado la dirección de las medidas para la ciberseguridad hacia una dirección más dinámica y predictiva [1]; esta nueva dirección enfocada en esta actualidad de tecnologías emergentes supone una buena opción a la hora de centrarnos en esta necesidad de las organizaciones.

En este contexto, las tecnologías emergentes como la computación en la nube, vehículos automáticos, las nuevas inteligencias artificiales(IA), macro datos, el aprendizaje automático (ML) y los avances en la Ciberseguridad tienen un enorme potencial; estas tecnologías emergentes crean un entorno en el que la ciberseguridad puede ser dinámica y adaptativa; por ello estas tecnologías han surgido como tecnologías clave que pueden ofrecer soluciones innovadoras para fortalecer la ciberseguridad; estas tecnologías prometen no solo mejorar la capacidad de detección y respuesta ante incidentes, sino también predecir y mitigar posibles ataques antes de que ocurran [2][3].

Los ciberataques son un riesgo significativo para las empresas, ya que estas pueden provocar graves problemas; estas pueden incluir un deterioro de la reputación de la empresa, algunos problemas legales que traerían con las autoridades y la perdida de información crítica de la empresa; por ejemplo, un ciberataque exitoso puede interrumpir las operaciones de una empresa o puede llegar a causar el cierre completo de las actividades en una organización; generando así pérdidas financieras significativas mientras duren los ataques en sus sistemas y podría extenderse más allá del tiempo inicial del ataque [4]. Hay algunos métodos ampliamente utilizados para fortalecer la seguridad en las empresas contra ciberataques, donde se destaca la implementación de sistemas de autenticación multifactor (MFA) para garantizar un acceso seguro a los sistemas, la segmentación de redes para limitar el alcance de posibles intrusiones, y la actualización constante de parches de seguridad en software y hardware para reducir vulnerabilidades; pero las empresas también están adoptando tecnologías emergentes como la inteligencia artificial y el aprendizaje automático para mejorar la detección y respuesta a ciberataques; sin embargo, estas tecnologías también presentan nuevas limitantes, como la necesidad de desarrollar algoritmos más robustos y la integración eficaz con sistemas existentes; además, la falta de estandarización en la implementación y adopción de estas tecnologías también limitan su efectividad en la práctica [5].

El analizar y sintetizar la información recabada sobre las tecnologías emergentes usadas en el ámbito de la ciberseguridad puede proporcionar una integral de las herramientas disponibles que existen hasta la fecha y su potencial aplicación en los entornos empresariales para poder entender cuales podrán ser beneficiosas; ya que, esta investigación busca identificar qué tecnologías ofrecen los mayores beneficios y cómo pueden implementarse eficazmente para proteger contra amenazas en constante evolución; la protección contra las diferentes y cambiantes amenazas necesitan conocimientos enlazados sobre las

amenazas, vulnerabilidades y mitigación defensiva [6]. Aunque existe una amplia cantidad de publicaciones dirigidas hacia este enfoque, muchas de estas no tienen una visión general y sistemática que permite evaluar de forma completa su relevancia para la ciberseguridad, por ello, buscamos poder dirigir la recopilación en este contexto.

El objetivo de esta revisión sistemática de literatura es identificar y evaluar el estado actual del conocimiento sobre el uso de tecnologías emergentes en la ciberseguridad. Este estudio se propone sintetizar la investigación existente para proporcionar una comprensión integral de las tendencias y oportunidades en la aplicación de tecnologías como la inteligencia artificial, el aprendizaje automático, blockchain, IoT y otras en la protección contra ciberataques.

## II. METODOLOGÍA

La revisión realizada en este estudio se llevó a cabo como una revisión sistemática sin metaanálisis. La estrategia utilizada se basó en el enfoque PICO (Pregunta, Intervención, Comparación y Resultados), donde la pregunta PICO formulada fue: "¿Qué tecnologías emergentes se utilizan en la seguridad cibernética para prevenir ataques en empresas?" Los componentes de PICO, sus palabras clave y sus preguntas fueron definidos de la siguiente manera: el Problema (P) incluyó la pregunta "¿Como se han definido la ciberseguridad?" junto a los términos "Security", "cibersecurity", "Cyber threats", "Vulnerabilities" y "Cyber attacks"; la Intervención (I) incluyo la pregunta "¿Que tecnologías emergentes se han aplicado?" y se centró en los términos "Emerging technologies" y "Advanced technologies"; los Resultados (O) se identificaron con la pregunta "¿Qué niveles de seguridad han obtenido estos métodos y qué limitaciones han presentado?" junto al uso de los términos "Prevention" y "Protection"; y el Contexto (C) se delimitó con la pregunta "¿En qué tipos de empresa se ha investigado?" y los terimnos "Companies", "Organizations" y "Businesses".

La búsqueda sistemática se realizó en la base de datos SCOPUS utilizando la ecuación de búsqueda específica:

"(TITLE-ABS-KEY (security OR cibersecurity OR "Cyber threats" OR "Vulnerabilities" OR "Cyber attacks") AND TITLE-ABS-KEY ("Emerging technologies" OR "Advanced technologies") AND TITLE-ABS-KEY (companies OR organizations OR businesses)) AND PUBYEAR > 2018 AND PUBYEAR < 2025 AND (LIMIT-TO (LANGUAGE, "English")) AND (LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "re") OR LIMIT-TO (DOCTYPE, "ch")) AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI") OR LIMIT-TO (SUBJAREA, "BUSI")) AND (LIMIT-TO (EXACTKEYWORD, "Emerging Technologies") OR LIMIT-TO (EXACTKEYWORD, "Internet Of Things") OR LIMIT-TO (EXACTKEYWORD, "Cybersecurity") OR LIMIT-TO (EXACTKEYWORD, "Network Security") OR LIMIT-TO (EXACTKEYWORD, "Artificial Intelligence") OR LIMIT-TO (EXACTKEYWORD, "Security") OR LIMIT-TO (EXACTKEYWORD, "Cyber Security")) "

Esta se enfocó en excluir artículos publicados antes de 2019 y que no estén escritos en inglés; también se excluyeron trabajos que no son documentos como artículos de revista, capítulos de libros y artículos de conferencia en áreas relacionadas con la informática, la ingeniería y los negocios; y por último se utilizaron palabras clave específicas relacionadas con las tecnologías emergentes y la ciberseguridad para refinar los resultados de la búsqueda.

Tras la aplicación de los criterios de inclusión y exclusión establecidos, se obtuvieron 327 artículos relevantes. El proceso de selección de estudios se realizó siguiendo la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), donde se eliminaron los artículos duplicados y se evaluó el cumplimiento de los criterios de inclusión y exclusión. Finalmente, se seleccionaron 133 artículos que cumplieron con los criterios temáticos de la revisión sistemática, de los cuales 56 fueron recuperados en texto completo para su posterior análisis.

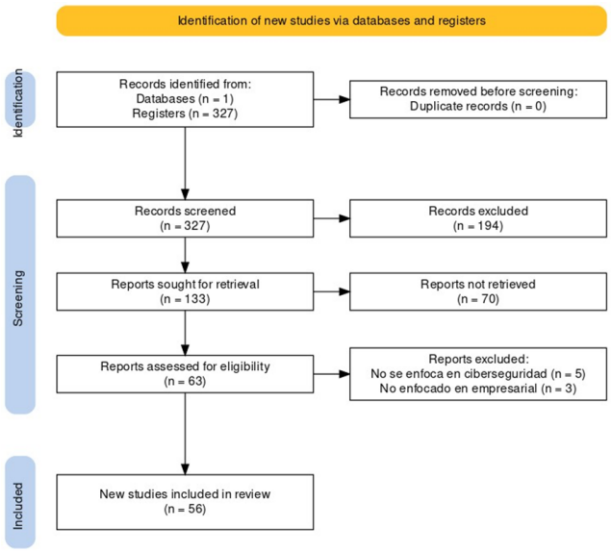


Fig. 1 Diagrama de flujo Prisma

## III. RESULTADOS

Luego de cumplir el paso PRISMA, tenemos los 56 resultados de los cuales podemos estructurar en la cantidad de veces que se usan las tecnologías emergentes en los documentos (ver Figura 2), de los cuales tenemos que las tecnologías que más aparecen son: cloud, blockchain, IoT e IIoT y la IA.

De los 56 artículos revisados, se tomaron en cuenta 10 tecnologías emergentes que fueron usadas para la ciber seguridad, de los cuales algunos artículos abordan varios de estas tecnologías; por otro lado, hay artículos que no abordan ninguna de estas o la abordan, pero no la ocupan para la ciberseguridad. Según la tabla mostrada (ver Figura 2) se pueden apreciar los artículos que fueron usados para la

elaboración de esta RSL, ya que estas muestran un “SI” en la tecnología ocupada, mientras que los “-” muestra que no se tiene relación.

| REFERENCIA | TECNOLOGIAS EMERGENTES | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | CLOUD | IoT e IIoT | BLOCKCHAIN | IA | CRYPTOGRAFIA | QR | RECONOCIMIENTO FACIAL | CNN | EDR | S. AUTOMATIZACION |
| Al-Aqrabi, Lane, Hill [8] | SI | SI | - | - | - | - | - | - | - | - |
| Ahmed, Elahi, Abrar, Aslam, Khalid, Habib [33] | - | - | - | - | - | - | - | - | - | - |
| Alisher, Uddin, Afzal [44] | - | - | - | - | - | - | - | - | - | - |
| Alneyadi, Normalini [25] | - | - | - | - | - | - | - | - | - | SI |
| AlQadheeb, Bhattacharyya, Perl [26] | - | - | - | - | - | - | - | - | - | SI |
| Arunkumar, Kousalya [45] | - | - | - | - | - | - | - | - | - | - |
| Aslan, Aktuğ, Ozkan-Okay, Yilmaz, Akin [5] | SI | - | SI | SI | SI | - | - | - | - | - |
| Bagheri, Bendavid, Safkhani, Rostampour [10] | - | - | - | - | SI | - | - | - | - | - |
| Bamhdi [34] | - | - | - | - | - | - | - | - | - | - |
| Bansal, Gupta, Mathur [9] | - | - | - | - | SI | - | - | - | - | - |
| Bhutta et al [11] | - | SI | - | - | - | - | - | - | - | - |
| Butt [35] | - | - | - | - | - | - | - | - | - | - |
| Corallo, Lazoi, Lezzi, Pontrandolfo [36] | - | - | - | - | - | - | - | - | - | - |
| Chatziamanetoglou, Rantos [1] | - | - | - | - | - | - | - | - | - | - |
| Daim, Lai, Yalcin, Alsoubie, Kumar [37] | - | - | - | - | - | - | - | - | - | - |
| Da Silva, Silva, Neto, Lemos, Neto, Esposito [6] | SI | - | - | - | - | - | - | - | - | - |
| Dhirani, Mukhtiar, Chowdhry, Newe [2] | - | - | - | - | - | - | - | - | - | - |
| Domínguez, De Jesús Mateo Sanguino [38] | - | - | - | - | - | - | - | - | - | - |
| Fatima-tuz-Zahra, Jhanjhi, Brohi, Malik [12] | - | - | - | SI | - | - | - | - | - | - |
| Ghimire, Rawat, Liu, Li [39] | - | - | - | - | - | - | - | - | - | - |
| Guo, Yang, Tan [40] | - | - | - | - | - | - | - | - | - | - |
| Hassija, Chamola, Gupta, Jain, Guizani [41] | - | - | - | - | - | - | - | - | - | - |
| Hussain, Kumar [46] | - | - | - | - | - | - | - | - | - | - |
| Javed Butt, Abbod, Lors, Jahankhani, Jamal, Kumar [42] | - | - | - | - | - | - | - | - | - | - |
| Kahtan, Abdulhak, Al-Ahmad, Alzoubi [43] | - | - | - | - | - | - | - | - | - | - |
| Kaja, Shaout, Ma [24] | - | - | - | SI | - | - | - | - | - | - |
| Khan, Sohail, Nazir, Hussain, Shah, Ali [13] | - | - | - | SI | - | SI | - | - | - | - |
| Kashyap, Rana, Kansal, Walia [7] | SI | SI | - | - | - | - | - | - | - | - |
| Kosmowski, Piesik, Piesik, Śliwiński [27] | - | - | - | - | - | - | - | - | - | - |
| Kumar, Kumar, Agarwal [14] | - | - | - | - | - | - | SI | - | - | - |
| Kumar, Bhamu, Sangwan [47] | - | - | - | - | - | - | - | - | - | - |
| Li, Dong, Wang [28] | - | - | - | - | - | - | - | - | - | - |
| Lilhore et al [15] | - | - | - | - | - | - | - | SI | - | - |
| Li, Zhao, Min, Qi, Liu [16] | - | SI | - | - | SI | - | - | - | - | - |
| Lodha, Pillai, Solanki, Sahasrabudhe, Jarali [17] | - | - | SI | - | - | - | - | - | - | - |
| Maamar, Benahmed [18] | - | - | - | SI | - | - | - | - | - | - |
| Mannayee, Ramanathan [19] | SI | SI | SI | - | - | - | - | - | - | - |
| Martell, Cueto, Vela, Torres, Reátegui, Alejandría[20] | - | - | - | - | - | - | - | - | SI | - |
| Mtetwa, Tarwireyi, Adigun [48] | - | - | - | - | - | - | - | - | - | - |
| Muheidat, Patel, Tammisetty, Tawalbeh, Tawalbeh [49] | - | - | - | - | - | - | - | - | - | - |
| Mujinga [29] | SI | - | - | - | - | - | - | - | - | - |
| Mustapha, Vaicondam, Jahanzeb, Usmanovich, Yusof [23] | - | SI | - | SI | - | - | - | - | - | - |
| Pandey, Arora, Arora, Goyal, Gera, Yadav [50] | - | - | - | - | - | - | - | - | - | - |
| Paraskevas [51] | - | - | - | - | - | - | - | - | - | - |
| Rawat [30] | - | - | SI | - | - | - | - | - | - | - |
| Saeed, Altamimi, Alkayyal, Alshehri, Alabbad [52] | - | - | - | - | - | - | - | - | - | - |
| Samtani, Raff, Anderson [4] | - | - | - | - | - | - | - | - | - | - |
| Sarker, Yunus, Deraman [53] | - | - | - | - | - | - | - | - | - | - |
| Seng, Al-Ameen, Wright [54] | - | - | - | - | - | - | - | - | - | - |
| Shahzad, Zhang [55] | - | - | - | - | - | - | - | - | - | - |
| Shi, Liu, Zhang, Zhang [56] | - | - | - | - | - | - | - | - | - | - |
| Tabassum, Alyas, Hamid, Saleem, Malik [57] | - | - | - | - | - | - | - | - | - | - |
| Thombre [21] | - | - | - | SI | - | - | - | - | - | - |
| Toussaint, Krima, Panetto [3] | - | - | - | - | - | - | - | - | - | - |
| Tseng, Wong, Otoum, Aloqaily, Othman [58] | - | - | - | - | - | - | - | - | - | - |
| Haddaway, Page, Pritchard, McGuinness [59] | - | - | - | - | - | - | - | - | - | - |
| Varjovi, Babaie [60] | - | - | - | - | - | - | - | - | - | - |
| Voutilainen, Kari [22] | - | - | SI | - | - | - | - | - | - | - |
| Zhang, Chen, Li [61] | - | - | - | - | - | - | - | - | - | - |
| Zhang, Xu, Liu, Lu, Xu, Tao [32] | - | - | SI | - | - | - | - | - | - | - |

Fig. 2 Uso de la tecnología emergente en los artículos

Solo 13 de los trabajos contiene un tipo de empresa donde se aplica. El tipo de empresa más popular fueron las empresas industriales y de servicios aplicadas en 4 artículos cada uno (ver Figura 3).

Las tecnologías usadas en los trabajos revisados presentan limitaciones que como se muestra (ver Figura 4), las que más limitaciones presentaron fueron la IA y el Cloud siendo que el sistema de detección y respuesta y el CNN no presentaron estas limitaciones.

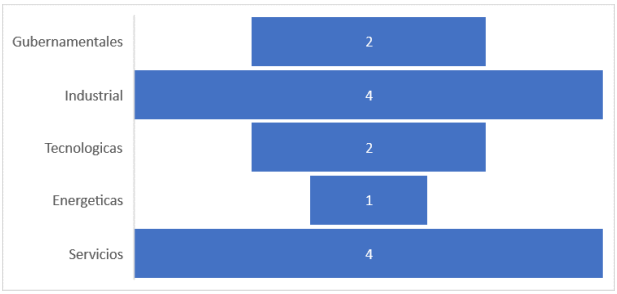


Fig. 3 Empresas aplicadas en los trabajos

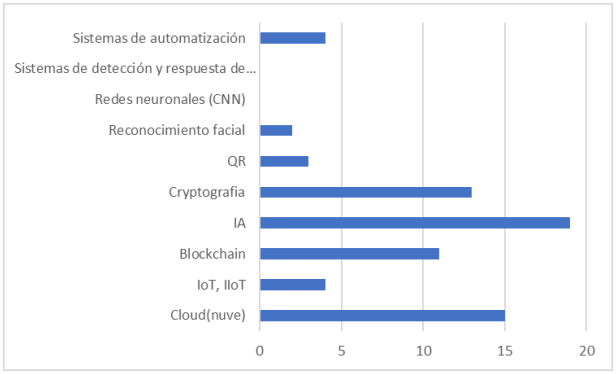


Fig. 4 Cantidad de limitantes que se presentaron por tecnología emergente aplicada.

En base a las tecnologías emergentes revisadas (ver Figura 2); veremos el desempeño, las limitantes y el funcionamiento.

***Cloud***: En el área de almacenamiento en la nube, los artículos mencionan que las plataformas de computación en la nube ofrecen una serie de beneficios críticos para las empresas. Estas plataformas garantizan una seguridad avanzada de los datos, aseguran una alta disponibilidad, permiten una recuperación de datos eficiente, proporcionan escalabilidad y facilitan la gestión proactiva de amenazas [7].

En esta área, se exhibe un enfoque para la mitigación de DDoS, donde se usa la arquitectura multicapa compuesta de capa de nieve y capa de nube, donde las primeras proporcionan la infraestructura para mitigar ataques y las segundas para definir las políticas de mitigación global [8]. Por otro lado, se presenta también una arquitectura IoT basado en la nube donde el cual se basa en diferentes capas [9]: Capa de aplicación (Application), Capa de red (Network), Capa de percepción (Perception). Donde las capas funcionan en comunicación entre sí, pero a la vez siendo independientes.

***IoT e IIoT***: Se expone un protocolo de autenticación, el cual se enfoca en escenarios que involucran aplicaciones de IoT y análisis de datos accesibles mediante nubes de IoT, donde participantes de diversos niveles de seguridad requieren acceso a servicios de análisis distribuidos gestionados por una entidad confiable [9].

***Blockchain***: Se destacan artículos los cuales abordan las investigaciones de la tecnología blockchain donde se menciona que facilita la validación de la coherencia de los datos y la detección de ataques complejos, [7]. Además, los

estudios indican que los sistemas blockchain son considerados seguros debido a su uso de criptografía asimétrica; de esta forma de cifrado implica la existencia de un conjunto de claves públicas, accesibles para cualquiera, y otro conjunto de claves privadas, que solo el propietario puede ver [10].

Asimismo; se aborda un sistema de salud basado en blockchain que abarca a pacientes, médicos, farmacias y compañías de seguros [11]; con el cual se logró obtener mayor seguridad y control de los datos médicos por parte de los pacientes. También la reducción de fraudes en el sistema de salud y una mejora en la integración y el intercambio de información entre los diferentes actores del sistema.

En base a las investigaciones de V. Se desarrolló un marco SDFRM basado en blockchain para mejorar la gestión segura y distribuida de recursos en entornos de Industria 4.0. En este entorno se utiliza contratos inteligentes en la blockchain para mejorar el acceso y la gestión distribuida y dinámica de los recursos compartidos, así como la preservación de la privacidad [12]. Esto demostró ser eficaz en términos de seguridad, privacidad, rendimiento y resistencia a ataques, lo que lo convierte en una solución prometedora para mejorar la ciberseguridad en entornos de Industria 4.0 e IoT.

***IA***: Para el área de la inteligencia artificial los artículos dan a conocer un marco que utiliza aprendizaje automático para detectar ataques de rango y agujeros de gusano; el ataque de rango es específico de RPL (protocolo de enrutamiento para redes de baja pérdida y con pérdidas), mientras que el agujero de gusano se hereda de las WSN (sensor de redes inalámbricas); el objetivo al diseñar este modelo es mitigar los efectos de los ataques combinados que ocurren en una red IoT basada en RPL [13].

Se propuso un modelo híbrido que combina K-means y red neuronal profunda (Deep Neural Network, DNN) para la detección de anomalías relacionadas con el robo de electricidad en sistemas AMI (Advanced Metering Infrastructure) [14]. La aplicación de este modelo hibrido en la ciberseguridad podría:

Permitir modelar patrones normales de algún proceso en las empresas.

Usar el modelo DNN para detectar desviaciones en el patrón y clasificar a los clientes como normales o anormales (maliciosos).

También se aborda el uso de aprendizaje automático para categorizar documentos confidenciales, junto a una interfaz de usuario del administrador para crear y administrar políticas; y un componente del lado del cliente que intercepta y bloquea la transferencia de archivos confidenciales a través de USB; puede ayudar a las pequeñas y medianas organizaciones a proteger sus datos confidenciales de manera efectiva y sencilla [15]. Ya que estas se encargan del bloqueo de atacantes externos por medio de los equipos de la empresa, y usar la IA para poder analizar correctamente todos los intentos y así saber cómo actuar en otro momento.

Por otro lado, en el aprendizaje automático, se plantea un modelo de ML (machine learning) personalizado utilizando datos proporcionados por NCSC-FI (National Cyber Security Centre Finland) y consultas dirigidas al conjunto de datos preconfigurado de IBM Watson Discovery News [16]. En [16], Voutilainen et al. (2020) refiere en la primera solución, el modelo de ML creado utilizando los datos proporcionados por NCSC-FI pudo encontrar nueva información relevante de los documentos y en la segunda solución, utilizando el conjunto de datos preconfigurado de IBM Watson Discovery News, las consultas realizadas pudieron proporcionar una imagen general casi en tiempo real sobre el fenómeno de "big game hunting".

Se propuso un sistema de detección de intrusos de dos etapas basado en algoritmos de aprendizaje automático. Se señala la primera etapa donde utiliza K-Means para detectar ataques, y la segunda etapa utiliza varios algoritmos de aprendizaje supervisado para clasificar los ataques. En esta etapa se usaron cuatro algoritmos diferentes: J48, Random Forest, Adaptive Boosting y Naive Bayes [17]. Con los cuales se pudieron clasificar varios ataques, pero se identificó que el algoritmo Naive Bayes es el que más problemas tuvo al detectar ataques.

***Criptografía***: Para esta área los artículos hacen notar formas para mantener la privacidad de la comunicación personal y restringirla únicamente a los destinatarios deseados, por eso se recurre a la criptografía. Las claves podrían ser superadas mediante un ataque de fuerza bruta; lo importante es utilizar una clave lo suficientemente larga como para que un ataque de este tipo requiera una cantidad significativa de poder de procesamiento [18].

Por otro lado, el artículo de Bagheri et al. [19] presenta un protocolo mejorado denominado PPSG, específicamente diseñado para redes inteligentes. Este protocolo integra características físicas no clonables (Physical Unclonable Function, PUF) junto con un componente de criptografía de curva elíptica (Elliptic curve cryptography, ECC) para mitigar las vulnerabilidades.

Li et al. [20] mencionan que dentro de la criptografía se encuentra el cifrado; donde se propuso y desarrolló un esquema ligero de preservación de la privacidad basado en cifrado homomórfico para el IIoT [20]. Y al dividir los cálculos en una parte fija y una dinámica se permitió que los dispositivos IIoT de recursos limitados pudieran realizar operaciones sobre datos cifrados. También se propone soluciones como el cifrado avanzado, autenticación biométrica y detección de anomalías impulsada por IA [21].

***Quick Response (código de respuesta rápida, QR)***: Para el QR el artículo de Khan et al. [22] describen un entorno FIN-TECH donde los usuarios pueden limitar las transacciones móviles a través de sistemas automatizados de remitentes en lugar de depender de fuentes manuales; de esta manera se puede solicitar que se asignen privilegios exclusivamente a mis dispositivos personales; y así, si alguien intenta acceder a la información necesaria, no podrá utilizar mi cuenta.

***Reconocimiento facial***: Para este reconocimiento presentan un estudio para los dispositivos de seguridad ya sea en hogares u oficinas. El estudio señala un sistema de reconocimiento facial basado en IoT que utiliza una Raspberry

Pi, una cámara, un módulo GSM (Sistema Global de Comunicaciones Móviles) y una base de datos de rostros autorizados para brindar seguridad en hogares, oficinas y ciudades inteligentes [23]; de esta manera presentar datos biométricos para que los dispositivos puedan estar seguros.

***Convolutional Neural Network (red neuronal convolucional, CNN)***: Para este tipo de redes el artículo menciona que la seguridad cibernética se ha convertido en una prioridad crítica debido a la interconexión de dispositivos y sistemas. El estudio expone un modelo híbrido de detección de intrusiones (HIDM) que utiliza un CNN-LSTM optimizado y transferencia de aprendizaje para mejorar el desempeño en la detección de ataques en redes de Industria 4.0 [24]. Al integrar estas técnicas, el modelo se busca mejorar significativamente la precisión y eficacia en la detección de ataques, adaptándose así a las demandas y desafíos únicos de la infraestructura de Industria 4.0.

***Endpoint Detection and Response (detección y respuesta de puntos finales, EDR):*** Para esta área los artículos mencionan que el protocolo de autenticación está diseñado para escenarios de aplicaciones de IoT y análisis de datos que se acceden a través de nubes de IoT. Se evidencia en los artículos que, en estos casos, los participantes de diferentes niveles de seguridad necesitan acceder a servicios de análisis distribuidos mediante una entidad confiable central [25].

Por otro lado, se sugiere tener estrategias más amplias como la adopción de arquitecturas de datos escalables, el uso de técnicas avanzadas de análisis de datos y el fortalecimiento de la gobernanza de datos en las organizaciones [26]. Ya que el estudio indica que el marco de seguridad propuesto demostró ser confiable y capaz de manejar con éxito ataques maliciosos, logrando así un equilibrio adecuado entre seguridad, eficiencia y capacidad de respuesta ante amenazas.

***Sistemas de automatización***: En estos sistemas en los artículos se presenta un marco integrado de gestión de la continuidad del negocio que incluye aspectos de seguridad funcional y ciberseguridad. Además, se sugieren mejoras en la configuración de los subsistemas de sensores para reducir la probabilidad de operación espuria de los sistemas relacionados con la seguridad [27]. Esto permite abordar de manera sistemática las vulnerabilidades que podrían afectar la confiabilidad, seguridad y seguridad de la planta industrial, mejorando su resiliencia; con el fin de segmentar el sistema informático industrial y la red para distinguir las zonas de seguridad y diseñar una zona desmilitarizada (DMZ). Por otro lado, también mejorar la resiliencia y seguridad de la red informática hospitalaria al proporcionar una mejor evaluación y gestión de los riesgos de seguridad. Así optimizar el diseño y desarrollo de los sistemas de información [28].

En los trabajos donde se abordan los sistemas de automatización las limitantes fueron: las dificultades en la aplicación de parches de software en sistemas y redes OT debido a la heterogeneidad de los dispositivos de diferentes proveedores, y la complejidad de los sistemas y redes TIC y OT que los hace susceptibles a fallas y vulnerables a ciberataques.

La mayoría de los estudios entre 2019 y 2020 no tuvieron una tasa de detección de ataques, pero son 5 los estudios que muestran estos datos (ver Figura 5), aquí se nota que en la mayoría los estudios en IA son los que proporcionan mayores porcentajes de detección de ataques; siendo que el único estudio en Blockchain tuvo una tasa baja de detección.

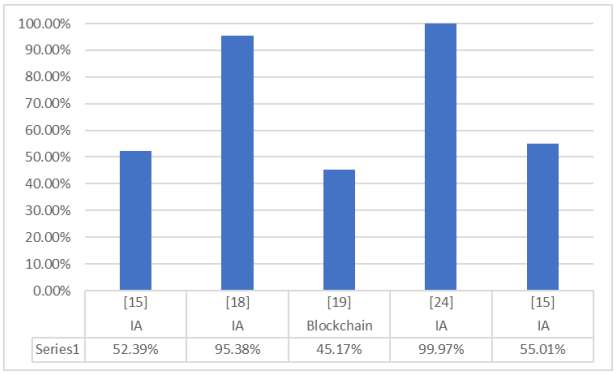


Fig. 5 Tasa de detección de ataques

## IV. DISCUSIÓN

En este estudio de revisión, se evaluó el uso de tecnologías emergentes en la ciberseguridad, destacando que las más utilizadas fueron la computación en la nube (Cloud), blockchain, Internet de las Cosas (IoT) e Internet de las Cosas Industriales (IIoT), y la inteligencia artificial (IA). Estas tecnologías demuestran un gran potencial para mejorar la ciberseguridad, aunque también enfrentan desafíos y limitaciones significativas.

La aplicación de IA y el ML en ciberseguridad está mostrando un avance significativo en la detección de ataques y la protección de sistemas críticos. Las investigaciones recientes han demostrado la efectividad de estos enfoques en varios contextos. Además, con el trabajo realizado por A. Maamar y K. Benahmed se ha logrado identificar anomalías en sistemas de medición avanzada (AMI) mediante modelos híbridos que combinan algoritmos de clustering y redes neuronales profundas [14], y mediante el estudio de Thombre, se ha desarrollado un sistema eficaz para la protección de datos confidenciales en pequeñas y medianas empresas (PYMEs) [15]. En contraste con lo mencionado en el estudio de Verma, concluye que es valioso considerar que la IA no es la medida determinante para todos los problemas de ciberseguridad. La detección mediante esta tecnología ofrece capacidades avanzadas de identificación de amenazas y respuesta a incidentes, pero también conduce a otros riesgos, como ataques adversariales y la explotación de algoritmos de IA. Estos desafíos resaltan que, aunque las herramientas basadas en IA representan un avance crucial en la lucha contra las amenazas cibernéticas, no son infalibles [29].

La computación en la nube es reconocida por sus beneficios en seguridad avanzada de datos, alta disponibilidad, recuperación eficiente de datos, escalabilidad y gestión proactiva de amenazas; no obstante, enfrenta desafíos como la

latencia y la dependencia de la conectividad a internet. Ejemplos destacados incluyen la propuesta de Da Silva et al. [8] para mitigar ataques DDoS utilizando una arquitectura multicapa; además, se presentaron arquitecturas IoT basadas en la nube que utilizan diferentes capas para garantizar una comunicación eficiente y segura [9].

En el ámbito del IoT e IIoT, se propusieron protocolos de autenticación enfocados en escenarios que involucran aplicaciones de IoT y análisis de datos accesibles mediante nubes de IoT. Estos protocolos aseguran el acceso seguro a servicios de análisis distribuidos, gestionados por una entidad confiable; sin embargo, tanto IoT e IIoT al ser implementadas en entornos empresariales, presentan desafíos significativos relacionados con la interoperabilidad entre dispositivos de diferentes fabricantes; por ende aquí aparece la necesidad de estándares más robustos que permitan una integración más fluida, especialmente en sectores donde la heterogeneidad tecnológica es alta; además, esta falta de comunicación limita el potencial de estas tecnologías para trabajar en conjunto y mejorar las capacidades de ciberseguridad a nivel organizacional [9].

Estudios como los de Bhutta et al, [10] y Lodha et al [11] confirman el papel crucial de la blockchain en la protección de datos; del mismo modo, también mencionamos los trabajos de Voutilainen et al [16] y Kaja et al [17], donde estos destacan la efectividad del aprendizaje automático (Machine learning) en la detección de intrusiones; con ello la consistencia de estos resultados en esta RSL valida la importancia de estas tecnologías para la ciberseguridad empresarial.

En los estudios relacionados a los sectores específicos; a pesar de que solo 13 de los estudios revisados detallan tipos de empresas, las aplicaciones en industrias específicas, como el sector salud con blockchain y la industria 4.0 con contratos inteligentes, destacan el potencial de estas tecnologías para resolver problemas únicos [11], [12]; sin embargo, los datos también revelan que estos enfoques aún están limitados por la falta de casos de éxito documentados en otras industrias, lo que sugiere un área clave para futuras investigaciones.

## V. CONCLUSIÓN

Esta revisión sistemática de la literatura tenía como objetivo identificar y evaluar las tecnologías emergentes utilizadas en la ciberseguridad para prevenir ataques; en esta RSL obtuvimos hallazgos los cuales demuestran que la adopción de tecnologías como la IA, blockchain, computación en la nube, criptografía e IoT/IIoT que al ser aplicadas ayudaron en la prevención de ataques y en la mejora de la ciberseguridad.

Los hallazgos se obtuvieron en las tecnologías buscadas como la computación en la nube, en los artículos revisados destacan su capacidad para ofrecer seguridad avanzada, alta disponibilidad y recuperación eficiente de datos, estas capacidades son cruciales para las empresas en la gestión proactiva de amenazas cibernéticas; en cuanto a IoT e IIoT, se identificaron protocolos de autenticación y arquitecturas basadas en la nube que mejoran la seguridad mediante la segmentación y la gestión de datos distribuidos; también la tecnología blockchain ha mostrado su potencial en la validación de datos y la detección de ataques complejos, con aplicaciones específicas en la salud y la industria 4.0, asegurando la privacidad y el control de los datos mediante contratos inteligentes y criptografía asimétrica; la inteligencia artificial (IA) ha emergido como herramientas crítica en la detección y mitigación de ciberataques, con aplicaciones que van desde la detección de anomalías en infraestructuras críticas hasta la protección de datos confidenciales en pequeñas y medianas empresas; la criptografía, incluyendo el cifrado homomórfico y las claves basadas en ADN, se ha resaltado por su capacidad para mantener la privacidad de las comunicaciones y asegurar los datos en entornos industriales; las tecnologías de reconocimiento facial y códigos QR están mejorando significativamente la seguridad en el acceso y la autenticación de usuarios, mientras que las Redes Neuronales Convolucionales (CNN) y los sistemas de detección y respuesta de endpoints (EDR) están optimizando la detección de intrusiones y la respuesta a incidentes; finalmente, los sistemas de automatización están siendo integrados para gestionar la continuidad del negocio y mejorar la resiliencia de las infraestructuras críticas frente a ciberataques.

Esta revisión sistemática de la literatura contribuye a lo existente al proporcionar una visión consolidada y actualizada de las tecnologías emergentes en la ciberseguridad empresarial; al sintetizar los resultados de estudios recientes, este trabajo ofrece una base sólida para futuras investigaciones y prácticas en el campo de la ciberseguridad.

Para futuras investigaciones consideramos que se deberían enfocar en realizar estudios sobre la implementación práctica de estas tecnologías en diferentes industrias, como también es recomendable explorar estrategias para superar las barreras de adopción y realizar metaanálisis para obtener una comprensión más profunda de la efectividad de cada tecnología; consideramos que una dirección de investigación futura prometedora es la evaluación de la relación costo-beneficio en la implementación de tecnologías como la criptografía homomórfica en entornos de recursos limitados, también se sugiere el investigar nuevas tecnologías emergentes, su potencial impacto en la ciberseguridad empresarial y el cómo pueden integrarse en infraestructuras críticas para aumentar la resiliencia frente a ciberataques.

## REFERENCIAS


[1] D. Chatziamanetoglou y K. Rantos, «Cyber Threat Intelligence on Blockchain: A Systematic Literature Review», Computers, vol. 13, n.o 3, p. 60, feb. 2024, doi: 10.3390/computers13030060.

[2] [2] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, y T. Newe, «Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review», Sensors, vol. 23, n.o 3, p. 1151, ene. 2023, doi: 10.3390/s23031151.

[3] [3] K.-K. R. Choo, «The cyber threat landscape: Challenges and future research directions», Computers & Security, vol. 30, n.o 8, pp. 719-731, nov. 2011, doi: 10.1016/j.cose.2011.08.004.

[4] M. Toussaint, S. Krima, y H. Panetto, «Industry 4.0 data security: a cybersecurity frameworks review», Journal Of Industrial Information Integration, vol. 39, p. 100604, may 2024, doi: 10.1016/j.jii.2024.100604.
[5] M. Conti, A. Dehghantanha, K. Franke, y S. Watson, «Internet of Things security and forensics: Challenges and opportunities», Future Generation Computer Systems, vol. 78, pp. 544-546, ene. 2018, doi: 10.1016/j.future.2017.07.060.
[6] S. Samtani, E. Raff, y H. Anderson, «Applied Machine Learning for Information Security», Digital Threats, mar. 2024, doi: 10.1145/3652029.kumarseng
[7] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, y E. Akin, «A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions», Electronics, vol. 12, n.o 6, p. 1333, mar. 2023, doi: 10.3390/electronics12061333.
[8] F. S. D. Da Silva, E. Silva, E. P. Neto, M. o. O. Lemos, A. J. V. Neto, y F. Esposito, «A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios», Sensors, vol. 20, n.o 11, p. 3078, may 2020, doi: 10.3390/s20113078.
[9] N. Kashyap, A. Rana, V. Kansal, y H. Walia, «Improve cloud based IoT Architecture layer Security - A literature review», 2021 International Conference On Computing, Communication, And Intelligent Systems (ICCCIS), feb. 2021, doi: 10.1109/icccis51004.2021.9397146.
[10] M. N. M. Bhutta et al., «A Survey on Blockchain Technology: Evolution, Architecture and Security», IEEE Access, vol. 9, pp. 61048-61073, ene. 2021, doi: 10.1109/access.2021.3072849.
[11] G. Lodha, M. Pillai, A. Solanki, S. Sahasrabudhe, y A. Jarali, «Healthcare System Using Blockchain», ICICCS, may 2021, doi: 10.1109/iciccs51141.2021.9432157.
[12] V. Mannayee y T. Ramanathan, «An Efficient SDFRM Security System for Blockchain Based Internet of Things», Intelligent Automation And Soft Computing/Intelligent Automation & Soft Computing, vol. 35, n.o 2, pp. 1545-1563, ene. 2023, doi: 10.32604/iasc.2023.027675.
[13] N. Fatima-Tuz-Zahra, N. Jhanjhi, S. N. Brohi, y N. A. Malik, «Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning», MACS, dic. 2019, doi: 10.1109/macs48846.2019.9024821.
[14] A. Maamar y K. Benahmed, «A Hybrid Model for Anomalies Detection in AMI System Combining K-means Clustering and Deep Neural Network», Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 60, n.o 1, pp. 15-39, ene. 2019, doi: 10.32604/cmc.2019.06497.
[15] S. Thombre, «Freeware Solution for Preventing Data Leakage by Insider for Windows Framework», 2020 International Conference On Computational Performance Evaluation (ComPE), jul. 2020, doi: 10.1109/compe49325.2020.9200160.
[16] J. Voutilainen y M. Kari, «Strategic Cyber Threat Intelligence: Building the Situational Picture with Emerging Technologies», ECCWS, jun. 2020, doi: 10.34190/ews.20.030.
[17] N. Kaja, A. Shaout, y D. Ma, «An intelligent intrusion detection system», Applied Intelligence, vol. 49, n.o 9, pp. 3235-3247, mar. 2019, doi: 10.1007/s10489-019-01436-1.
[18] M. Bansal, S. Gupta, y S. Mathur, «Comparison of ECC and RSA Algorithm with DNA Encoding for IoT Security», ICICT, ene. 2021, doi: 10.1109/icict50816.2021.9358591.
[19] N. Bagheri, Y. Bendavid, M. Safkhani, y S. Rostampour, «Smart Grid Security: A PUF-Based Authentication and Key Agreement Protocol», Future Internet, vol. 16, n.o 1, p. 9, dic. 2023, doi: 10.3390/fi16010009.
[20] S. Li, S. Zhao, G. Min, L. Qi, y G. Liu, «Lightweight Privacy-Preserving Scheme Using Homomorphic Encryption in Industrial Internet of Things», IEEE Internet Of Things Journal, vol. 9, n.o 16, pp. 14542-14550, ago. 2022, doi: 10.1109/jiot.2021.3066427.
[21] N. I. Mustapha, Y. Vaicondam, N. A. Jahanzeb, N. B. A. Usmanovich, y S. H. B. Yusof, «Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem», International Journal Of Interactive Mobile Technologies, vol. 17, n.o 22, pp. 100-116, nov. 2023, doi: 10.3991/ijim.v17i22.45261.
[22] H. U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, y F. Ali, «Role of authentication factors in Fin-tech mobile transaction security», Journal Of Big Data, vol. 10, n.o 1, sep. 2023, doi: 10.1186/s40537-023-00807-3.
[23] A. Kumar, P. S. Kumar, y R. Agarwal, «A Face Recognition Method in the IoT for Security Appliances in Smart Homes, offices and Cities», ICCMC, mar. 2019, doi: 10.1109/iccmc.2019.8819790.
[24] U. K. Lilhore et al., «HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning», Sensors, vol. 23, n.o 18, p. 7856, sep. 2023, doi: 10.3390/s23187856.
[25] H. Al-Aqrabi, P. Lane, y R. Hill, «Performance Evaluation of Multiparty Authentication in 5G IIoT Environments», en Communications in computer and information science, 2019, pp. 169-184. doi: 10.1007/978-981-15-1925-3_13.
[26] K. Martell, R. Cueto-Orbe, S. L. Vela-Del-Aguila, J. I. Torres-Manrique, K. Reátegui-Villacorta, y C. A. Alejandría-Castro, «Business Management in the Information Age: Use of Systems, Data Processing and Scalability for Organizational Efficiency», ICST Transactions On Scalable Information Systems, mar. 2024, doi: 10.4108/eetsis.5408.
[27] M. R. M. A. H. Alneyadi y M. K. Normalini, «Factors Influencing User's Intention to Adopt AI-Based Cybersecurity Systems in the UAE», Interdisciplinary Journal Of Information, Knowledge, And Management, vol. 18, pp. 459-486, ene. 2023, doi: 10.28945/5166.
[28] A. AlQadheeb, S. Bhattacharyya, y S. Perl, «Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior», Array, vol. 14, p. 100146, jul. 2022, doi: 10.1016/j.array.2022.100146.
[29] Dr. R. Verma, "Cybersecurity Challenges in the Era of Digital Transformation," in Transdisciplinary Threads Creating the Future through Multidisciplinary Research, vol. 1, pp. 9-10, January 2024, Infinity Publication Pvt. Ltd. Ltd. Ltd. doi: 10.25215/9392917848.20.