REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS

Volumen 2, Número 4
Octubre-Diciembre 2025

Edición Trimestral

CROSSREF PREFIX DOI: 10.71112

ISSN: 3061-7812, www.omniscens.com

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 2, Número 4
octubre-diciembre 2025

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

Contacto principal: admin@omniscens.com

Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 2, Núm. 4, octubre-diciembre 2025, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: https://www.omniscens.com, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 octubre 2025.

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 2, Número 4, 2025, octubre-diciembre

DOI: https://doi.org/10.71112/4mvx1985

MACHINE LEARNING APLICADO EN LA SEGURIDAD INFORMÁTICA

MACHINE LEARNING APPLICATED IN CYBERSECURITY

Raymond Pérez Meza

Costa Rica

DOI: https://doi.org/10.71112/4mvx1985

Machine Learning aplicado en la seguridad informática

Machine Learning applicated in cybersecurity

Raymond Pérez Meza

Raymond.perez.meza@una.cr

https://orcid.org/0000-0003-4932-7840

Universidad de Costa Rica

Costa Rica

RESUMEN

El Machine Learning en la actualidad es una de las tecnologías y/o herramientas más utilizadas, sin embargo, en muy pocas ocasiones se logra identificar su utilidad e importancia. El propósito de este trabajo es identificar como el ML está siendo utilizado actualmente en el campo de la ciberseguridad, esto a partir de un análisis bibliográfico en el cual se logró evidenciar cada una de las utilidades del ML, aplicado en mecanismos de seguridad de los datos, sistemas de información y en diversas áreas relacionadas con la seguridad informática. Los resultados obtenidos son evidencia de como el ML está presente en mecanismos de seguridad en dispositivos de Internet de las Cosas (IoT), Sistemas de Detección de Intrusiones (IDS), análisis de sitios web, detección de fraudes bancarios e Industria 4.0, prácticamente en cada tecnología que utilizamos.

Palabras clave: aprendizaje máquina; ciberseguridad; seguridad informática; detección de intrusiones; internet de las cosas

DOI: https://doi.org/10.71112/4mvx1985

ABSTRACT

Machine Learning (ML) has become one of the most widely used technologies and tools today; however, its utility and significance are often overlooked. The purpose of this research is to examine how ML is currently being applied in the field of cybersecurity through a comprehensive literature review. This analysis highlights the various applications of ML in data security mechanisms, information systems, and multiple domains related to information security. The findings demonstrate that ML plays a critical role in security mechanisms for Internet of Things (IoT) devices, Intrusion Detection Systems (IDS), website analysis, banking fraud detection, and Industry 4.0—essentially permeating nearly every technology we use.

Keywords: machine learning; cybersecurity; computer security; intrusion detection; internet of things

Recibido: 1 de noviembre 2025 | Aceptado: 4 de diciembre 2025 | Publicado: 5 de diciembre 2025

INTRODUCCIÓN

Cuando se habla del mundo de la ciberseguridad en la actualidad, se debe tener claridad que ante el avance tecnológico y en la sociedad de la información en la que nos encontramos, día a día salen noticias, cuestionamientos y demás situaciones ligadas a que tan segura esta la información actualmente o que tan seguros estamos nosotros como ciudadanos en esta sociedad que se encuentra hiper conectada.

Como punto fundamental de partida, en primera instancia, es importante hacer una breve diferenciación entre el Machine Learning y la Inteligencia Artificial (IA), puesto que de manera normal pueden ser considerado lo mismo. En resumidas cuentas, se podría diferenciar de manera simple, donde el ML está centrado en sistemas que aprenden de los datos, mientras

que la IA permite que los sistemas realicen tareas de manera autónoma. (Forero & Bennasar, 2024)

Puntualmente hablando del machine learning, el “aprendizaje máquina” como podría ser conceptualizado a crecido y es un tema de actualidad. La mayor parte de la población a escuchado del alcance de los robots, maquinas inteligentes y todas estas tecnologías actuales, sin embargo muy pocas personas se han puesto a analizar como esto podría afectarnos en la actualidad, más allá del temor básico de la suplantación de los humanos en el ámbito laboral por los robots, sino como esas tecnologías existentes, basada en el machine learning están siendo utilizadas con fines lícitos e ilícitos y una gran parte de la población no se ha dado cuenta que ya está utilizando estas tecnologías.

Ahora bien, acá es donde se plantea como el machine learning está siendo utilizado en el ámbito propio de la ciberseguridad, como eras herramientas, algoritmos y demás tecnologías son utilizadas tanto para proteger los datos, para analizarlos así como para facilitar ciertas labores que los seres humanos tendríamos que dedicar muchos tiempo para hacerlo, pero más allá de esos fines lícitos, estas tecnologías también son utilizadas para realizar diversos tipos de ataques, fraudes cibernéticos y demás actividades ilícitas, y todos y cada uno de nosotros estas a expensas.

Es por ello por lo que se plantea evidenciar, como está siendo utilizado el machine learning para proteger, prevenir y brindar soluciones eficientes en el ámbito de la ciberseguridad.

METODOLOGÍA

Antecedentes:

En la actualidad la protección de la información en las organizaciones es fundamental, pues ésta representa un activo de alto valor para las empresas que requiere de una atención

especial para garantizar la disponibilidad, confidencialidad e integridad de esta. El machine learning tiene más de 25 años en la industria, a pesar de tratarse de trayectoria relativamente extensa, su aplicabilidad a la seguridad es nueva y se encuentra en auge.

Según (Gómez et al., 2014) la revisión manual sigue siendo la metodología más confiable para hacer pruebas de seguridad, sin embargo, la tecnología de machine learning hace un aporte a los hackers éticos en el proceso de revisión, mostrándole archivos interesantes para que les den prioridad. Las herramientas automáticas y la tecnología no están para reemplazar el trabajo de estos hackers éticos, sino para complementarlos y ayudarlos.

Existen diversos estudios qué indican la aplicabilidad del machine learning en la seguridad, de los cuales exponen que el propósito del machine learning es el desarrollo de programas informáticos que tengan la capacidad de desplegar funciones inteligentes, similares a las del cerebro humano. También expresan la utilización del machine learning en casas de campañas para atribuir el ataque. Además, se verifica si un conjunto de los ataques recibidos coincide con otros en común y la coordinación de la prevención sea más breve y eficaz. (Vilone & Longo, 2021)

En síntesis, a pesar de que el machine learning aplicado a la seguridad es una necesidad, los trabajos realizados sobre esta temática apuntan que a pesar de que es evidente la necesidad y que ya existen las herramientas, estas prácticas no están siendo utilizadas, porque las empresas desconocen como adquirir o utilizarlas para un bien organizacional. Esto evidencia que el desconocimiento de como emplear estos recursos es igual o mayor la afectación a lo que puede provocar un ataque de seguridad.

Esta investigación utiliza el estudio bibliográfico documental como base, éste puede ser aplicada a cualquier tema de investigación para determinar la relevancia e importancia de este y asegurar la originalidad de una investigación. Además, permite que otros investigadores

consulten las fuentes bibliográficas citadas, pudiendo entender y quizá continuar el trabajo realizado.(Gómez et al., 2014)

Se revisaron recursos digitales que provee la Universidad de Costa Rica con sus respectivas fuentes bibliográficas con el fin de identificar las principales iniciativas del machine learning en el área de la seguridad. Las librerías digitales seleccionadas fueron:

- EBSCOhost: AcademicSearch Ultimate
- Access Engineering
- ProquestOneAcademic
- JSTOR AAF Art &Sciences X
- Springer eBooks: Informatica

El uso de estas bases brindó la posibilidad de tener contextos sobre diferentes investigaciones previas en el área propia de la investigación lo cual es fundamental en un estudio.

RESULTADOS

A continuación, se detallan los resultados obtenidos dentro de las búsquedas en los recursos digitales que provee la Universidad a fin de identificar las principales iniciativas del machine learning en el área de la seguridad.

Entre las palabras claves que se utilizaron para obtener los criterios de búsquedas fueron machine learning en la ciberseguridad, Inteligencia artificial, Deep learning, Ciberseguridad, Boosting Machine, Deep Neuronal Network, machine learning in cybersecurity. Dichos resultados en estas librerías mencionadas ya antes, se logra obtener con gran valía 20 documentos, de los cuales tienen fecha de publicación comprendidas entre los años 2017 y 2024.

Partiendo de los resultados de estas búsquedas de nuestro interés, 10 documentos fueron publicados en el idioma de inglés. El restante (15) en español.

De estos 10 escritos en ingles 5 fueron artículos de investigación, 5 entradas de diario (Journal) y un artículo de tipo editorial en el que se detallan los avances recientes del machine learning en el área de la ciberseguridad.

Cabe destacar que los centros de investigación de estos documentos en inglés pertenecen a Department OF Intelligent Mechatronics Engineering, Sejong University, Seoul, 05006, Korea, así mismo a Enginyeria Informatica, Escola D'enginyeria (Ee), Universitat Aut ` Onoma De Barcelona.

Las entradas de diario son parte de www.journals.elsevier.com, Fundación I+D DEL Software Libre (Fidesol), Granada (Spain) como también de un sitio alemán llamado Springer-Verlag Gmbh Germany, PART OF Springer Nature. Como también el editorial le pertenece al sitio www.wiley.com.

De los restantes 15 artículos en idioma español, a diferencia de los documentos en inglés, no hay entradas de diario, más si 5 editoriales. Uno para el sitio mexicano www.nexos.com.mx, otro para el observatorio de la ciberseguridad en América latina y el caribe, observatoriociberseguridad.org/ y por último que le pertenece a la Universidad ICESI - Cali, Colombia

Siendo así el restante de escritos que pertenecen a investigaciones de universidades a continuación detalladas:

- Pontificia Universidad Católica del Ecuador Sede Ambato, (Ecuador)
- Centro de Investigación en Matemáticas, Unidad Zacatecas, México
- Real Instituto Elcano - Madrid España
- Universitat Oberta de Catalunya
- Universidad Católica del Ecuador

- Universidad Industrial de Santander, Colombia.

Todos estos artículos se concentran sus publicaciones entre los años 2019-2020-2022-2023-2024, en donde el año 2020 se concentra la mayoría de estos.

Sin incluir el editorial del observatorio de la ciberseguridad en América latina y el caribe, el promedio de páginas de todos los restantes 19 documentos es de 25 hojas por artículo, obviando que son los documentos de investigación quienes se llevan el rubro más grueso de documentación debido a sus alcances. El editorial por sí solo consta de 204 páginas.

Se identificaron 49 autores en todos los escritos de estos una entrada de diario en ingles llamada Intelligent Detection and Recovery from cyberattacks cuenta con 7 autores luego dos investigaciones, una del año 2018 y otra del año 2020 con 5 autores, consecuente a eso los documentos cuentan con 2 o un autor.

DISCUSIÓN

Los documentos investigados, tiene como eje principal el uso del machine learning y su aplicación en el ámbito de la ciberseguridad, aplicada en diferentes ámbitos e industrias, de los cuales serán considerados a continuación:

El creciente auge de tecnologías relacionadas con el Internet de las Cosas, IoT, ha permitido que la ciberseguridad sea uno de los principales factores a analizar, donde han creado sistemas de modelado para detección de ataque cibernéticos basado en sensores inalámbricos más comunes y utilizados en el IoT. (Haider et al., 2020).

Además, el machine learning es utilizado en sistemas de detección de intrusiones, conocido como “Intrusion Detection Systems (IDS)”. Se puede identificar uno de los más importantes usos del machine learning en la actualidad. Estos sirven como defensas de ciberseguridad el cual, mediante el aprendizaje automático, aporta protección en sistemas de control industriales. (Anthi et al., 2021).

Asimismo, se logró identificar que empresas dedicadas a brindar soluciones de aplicativos antivirus han notado que se los ataques conocidos como phishing; (dichos ataques utilizan él envió de correo electrónicos que parecen fuentes de confianza como bancos, compañías y demás, pero en realidad son correos manipulados para solicitar información confidenciar al receptor). Ante este tipo de ataques, se han utilizado técnicas de machine learning para la detección de sitios web, redes sociales y correos electrónicos fraudulentos. (Dueñas, 2020).

Otra área indagada es en la cual usan algoritmos de machine learning para detección de malware en dispositivos con sistema operativo de dispositivos móviles como lo es Android. Es importante recordar que el malware es un programa informático el cual puede tener algún código malicioso el cual podría poner en riesgo los datos de aplicativos, así como de los dueños de los dispositivos. (Navarro et al., 2018).

También se evidencia que el machine learning es propuesto para ser utilizado con la finalidad de evitar ataques en sitios gubernamentales, debido a que en la actualidad es muy común que existan ataque dirigidos a hacer robo de información así como para hacer que los sitios simplemente dejen de funcionar, para ello se promueve el uso de Machine learning para hacer identificación de archivos llamados “LOGS” en los de accesos en los diferentes servidores web de cada una las entidades gubernamentales. (Pérez et al., 2020).

Una de las áreas también analizadas es el uso de fuentes abiertas, las cuales son una rama de la ciber inteligencia, la cual sirve para obtener y analizar información de posibles problemas y ayudará a apoyar la evaluación de riesgos con la finalidad de prevenir afectación con datos críticos. Está ambientado en Colombia en donde hacen recolección de datos e información usando fuentes abiertas, y donde hacen uso de herramientas de machine learning en el apoyo y protección de los datos. (Pinto et al., 2018).

Con el creciente uso de las tecnologías de información y comunicación, muchos ámbitos de la sociedad han cambiado, incluyendo los negocios, y en la actualidad existen gran cantidad em pequeñas y medianas empresas PYMES las cuales han ingresado a usar las TICs como nicho para poder seguir adelante con sus negocios. Pues existen iniciativas en las cuales mediante algoritmos y machine learning buscan optimizar y detectar a tiempo ataques, y no solo eso, sino que estas mismas herramientas previenen y ayudan a recuperarse los ataques, generando una seguridad proactiva. (Lopez et al., 2020).

Se pudo identificar también, que, en los artículos analizados, se usa también el machine learning en el ámbito bancario, donde algoritmos se encargan de analizar las amenazas a través de patrones los cuales pueden identificar cuando se pueda estar realizando un fraude con tarjetas bancarias. Evidenciando como de manera automatizada se pueden dar seguimiento a procesos y a partir de eso, mejorar la seguridad en un ámbito en el cual el factor económico es fundamental. Acá también se hace uso de sistemas de detección de intrusos. (Fernández, 2019).

Se evidencia también que la aparición de sistemas de autenticación de usuarios basada en biometría, es cada vez más utilizada, donde los algoritmos machine learning (ML) son vulnerables a los ataques tanto en las fases de entrenamiento como en las de prueba, lo que generalmente conduce a el rendimiento disminuye y las brechas de seguridad, por ende se le da gran énfasis a la creación de nuevos mecanismos y algoritmos que ayuden a generar mayor seguridad en diferentes dispositivos, desde los personales hasta los empresariales, considerando la gran cantidad de datos existentes y que se expone constantemente en internet. (Dasgupta et al., 2020).

Otro factor interesante identificado en la investigación es que el machine learning, está siendo usado en muchas áreas e industrias, como ya ha sido mencionado, sin embargo, en la actualidad el clustering ha tenido un gran auge. Se entiende por clustering la utilización de

múltiples equipos de cómputos físicos, los cuales, mediante aplicativos de software y configuraciones, permiten que todos esos equipos o computadoras trabajen como si fueran “una sola” esto gracias a la virtualización. Entonces acá el ML, permite hacer una consideración de muchos modernos y factores para identificar la cantidad de procesamiento de los equipos y en algoritmos de seguridad en los estos.(Martínez et al., 2019).

Otro ámbito analizado es el que el machine learning se ha convertido en una herramienta bastante poderosa y utilizada por parte de los investigadores y desarrolladores de software, siendo de gran utilidad y brindando seguridad informática. Una de esas herramientas analizadas fue la denominada “THE GAN ZOO” que es una herramienta Open Source, con una gran comunidad que da soporte, siendo esta una herramienta que permite realizar gran cantidad de test de seguridad y penetración en sistemas. Esto hace que el uso del machine learning ahorre dicho tiempo a los desarrolladores en las tareas antes citadas. (Flores, 2020).

Se puede también analizar dentro de los usos del ML que es aplicable en múltiples áreas, y se logró identificar en la documentación investigada como está siendo usado en la prevención de procesos de infraestructura. Cuando se habla de infraestructura, se referencian todos los equipos presentes en las empresas o las organizaciones desde equipos de cómputo, así como dispositivos de redes y comunicaciones de datos, entre muchos otros. (Cando & Medina, 2021)

Se evidencia qué, en la actualidad, la seguridad informática o ciber seguridad ha tenido un gran auge o se ha logrado identificar que es importante prestarle atención a la seguridad de los datos, de los equipos, de las aplicaciones, de los datos personales. Es acá donde se pude ver reflejado que los métodos tradicionales de seguridad han cambiado y que es importante poder crear, sistemas, aplicativos, algoritmos que se encarguen de monitorear entornos, que tengan capacidad de análisis y de generar respuestas ante necesidades específicas, creando así un surgimiento importante de métodos basados en machine learning. Donde se debe tener

un conocimiento de los ataques que han sucedido, de tal manera que no vuelvan a pasar y en caso de que vuelvan a intentar atacar de esa manera, ya exista el precedente y se pueda prevenir dichos ataques. (Martínez et al., 2019).

Como parte del análisis también se logró identificar, que hay múltiples iniciativas donde diferentes autores han desarrollado algoritmos de ML para ayudar en el ámbito educativo, propiamente a los educadores, esto mediando técnicas inteligentes que se aplican en el análisis de cantidades grandes de datos, propiciando un apoyo para combatir aquellos problemas dinámicos presentes en la educación. (Duzhin & Gustafsson, 2018).

Con la evolución de la industria, y propiamente en la actualidad donde la industria 4.0 toma auge y donde los procesos han sido automatizados, y donde muchos robots realizan trabajos mecanizados y son supervisados por sistemas de inteligencia artificial, aplicativos de software, es importante poder tener asegurados esos sistemas, de tal manera que no existan intromisiones o ataques que puedan destruir algún proceso de manufactura. Es importante recordar que grandes industrias como la automotriz, o la de logísticas de entrega de mercancías, utilizan robots a cargo de realizar dichas labores y si no están seguras en cualquier momento pueden tener grandes pérdidas. Por ende, el machine learning tiene un valor importante en esta industria 4.0 donde se han tomado las precauciones del caso y ya se usan sistemas automatizados basados en ML, para brindar protección a los sistemas y servicios interconectados. (Rozo Florelva, 2020).

Otro de los factores considerados es el crecimiento o la popularidad del Internet de las cosas (IoT), lo cual hace que las redes crezcan de manera exponencial dando como resultado que las especificaciones, necesidades de conexión, varíen; es acá donde los datos que se comparten en la red sean mayores y la capacidad de análisis de volúmenes de datos sean considerables, para ello se entrenan modelos de ML que permitan aprender a desempeñar el papel de defensa de los datos, a través de estrategias de defensas rápidas y sólidas, siendo

este otro campo en el cual el ML es empleado propiamente en la ciberseguridad. (Ramírez et al., 2023).

CONCLUSIONES

El machine learning en la actualidad está siendo muy utilizado en diferentes ámbitos como puedo ser evidenciado con anterioridad. Hay que analizarlo desde múltiples aristas, desde los cuales se puede ver que la seguridad informática ha tenido muchos cambios, y donde se ve que ha evolucionado a sistemas automatizados los cuales mediante algoritmos no solo encuentran o dejan visibles ataques cibernéticos, sino que los sistemas están aprendiendo con generando capacidades de prevención de esos incidentes, y no solo eso, sino que permiten reponerse de muchos ataques que se llevan a cabo.

Una gran área en la cual el Machine Learning tiene un gran potencial, actualmente, es en el creciente uso de mecanismos de IoT, donde miles de millones de dispositivos están siendo conectados a la red y por ende las amenazas son más crecientes con más atacantes al asecho.

Por eso el machine learning, juega un papel importante y donde está siendo utilizado en detección de programas con intensiones maliciosa, y se crean sistemas de detección de intromisiones, y donde los algoritmos usados están constantemente en aprendizaje.

Declaración de conflicto de interés

El autor declara no tener ningún conflicto de interés relacionado con esta investigación.

Declaración de contribución a la autoría

Raymond Alejandro Pérez Meza: conceptualización, curación de datos, análisis formal, adquisición de fondos, investigación, metodología, administración del proyecto, recursos,

software, supervisión, validación, visualización, redacción del borrador original, revisión y edición de la redacción.

Declaración de uso de inteligencia artificial

El autor no utilizó inteligencia artificial en ninguna parte del manuscrito.

REFERENCIAS

Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102717

Cando, M., & Medina, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. *3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, *10*(1), 17–41. https://doi.org/10.17993/3ctic.2021.101.17-41

Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine learning in cybersecurity: a comprehensive survey. *Journal of Defense Modeling and Simulation*. https://doi.org/10.1177/1548512920951275

Dueñas, J. (2020). *Aplicación de técnicas de machine learning a la ciberseguridad: Aprendizaje supervisado para la detección de amenazas web mediante clasificación basada en árboles de decisión.* https://openaccess.uoc.edu/items/f49ea127-88ab-47b9-96a4-53194b502e96#page=1

Duzhin, F., & Gustafsson, A. (2018). Machine learning-based app for self-evaluation of teacher-specific instructional style and tools. *Education Sciences*, *8*(1). https://doi.org/10.3390/educsci8010007

Fernández, A. (2019). *Machine Learning en Ciberseguridad*. https://openaccess.uoc.edu/server/api/core/bitstreams/957679da-ab99-4016-b962-225e8823445f/content

Flores, C. (2020). *Inteligencia Artificial, Machine Learning, Deep Learning aplicados a la Ciberseguridad*. https://ojs.umsa.bo/index.php/inf_fcpn_pgi/article/view/96

Forero, W., & Bennasar, F. (2024). Técnicas y aplicaciones del Machine Learning e Inteligencia Artificial en educación: una revisión sistemática. *RIED-Revista Iberoamericana de Educacion a Distancia*, *27*(1), 209–253. https://doi.org/10.5944/ried.27.1.37491

Gómez, E., Fernando, D., Aponte, G., & Betancourt, L. (2014). Literature review methodology for scientific and information management, through its structuring and systematization Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización. *DYNA*, *81*(184), 158–163. http://dyna.medellin.unal.edu.co/

Haider, A., Adnan, M., Rehman, A., Ur, M., & Seok Hyung. (2020). A real-time sequential deep extreme learning machine cybersecurity intrusion detection system. *Computers, Materials and Continua*, *66*(2), 1785–1798. https://doi.org/10.32604/cmc.2020.013910

Lopez, M., Lombardo, J., López, M., Alba, C., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 55. https://doi.org/10.9781/ijimai.2020.08.003

Martínez, J., Iglesias, C., & García, P. J. (2019). Review: machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

Navarro, A., Urcuqui, C., García, M., & Osorio, J. L. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos*. Universidad Icesi. https://doi.org/10.18046/EUI/ee.4.2018

Pérez, M., Rial, G., Sotelo, R., & Gurméndez, M. (2020). Clasificador de logs de acceso para detección de incidentes de ciberseguridad. *Memoria Investigaciones En Ingeniería*, *18*. https://doi.org/10.36561/ing.18.7

Pinto, R., Hernández, M., Pinzón, C., Díaz, D., & García, J. (2018). Open source intelligence (OSINT) in a colombian context and sentiment analysis. *Revista Vínculos*, *15*(2), 195–214. https://doi.org/10.14483/2322939x.13504

Ramírez, D., Garcés, L., Doria, T., Franco, S., Valencia, A., Rodríguez, P., & Espinoza, J. (2023). Tendencias investigativas en el uso de Machine Learning en la ciberseguridad. *Iberian Journal of Information Systems and Technologies*. https://www.proquest.com/openview/c9bf3f3b2192c011f0620adce0649ab3/1?pq-origsite=gscholar&cbl=1006393

Rozo Florelva. (2020). Revisión de las tecnologías presentes en la industria 4.0. *Revista UIS Ingenierías*, *19*(2), 177–191. https://doi.org/10.18273/revuin.v19n2-2020019

Vilone, G., & Longo, L. (2021). Classification of Explainable Artificial Intelligence Methods through Their Output Formats. *Machine Learning and Knowledge Extraction*, *3*(3), 615–661. https://doi.org/10.3390/make3030032