593 Digital Publisher
CEIT
ISSN 2588-0705

# Soluciones de monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. Revisión de literatura

# Artificial Intelligence-Based Cybersecurity Monitoring Solutions in Industrial Networks: A Literature Review

**Lenin Hernán Cortés-Llanganate** [1]
**Universidad Católica de Cuenca - Ecuador**
**lenin.cortes.11@est.ucacue.edu.ec**

**Andrés Sebastián Quevedo-Sacoto** [2]
**Universidad Católica de Cuenca - Ecuador**
**asquevedos@ucacue.edu.ec**

**doi.org/10.33386/593dp.2024.6.2629**

V9-N6 (nov-dic) 2024, pp 05-17 | Recibido: 02 de julio del 2024 - Aceptado: 10 de agosto del 2024 (2 ronda rev.)

1 ORCID: https://orcid.org/0009-0006-4904-5244
2 ORCID: https://orcid.org/0000-0001-5585-0270

**Cómo citar este artículo en norma APA:A**

Cortés-Llanganate, L., Quevedo-Sacoto, A., (2024). Soluciones de monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. Revisión de literatura. 593 Digital Publisher CEIT, 9(6), 05-17, https://doi.org/10.33386/593dp.2024.6.2629

Descargar para Mendeley y Zotero

# RESUMEN

La convergencia de las tecnologías operativas (OT) con las tecnologías de la informacion (IT) ha incrementado significativamente el riesgo de que las redes industriales sufran ciber ataques. El objetivo del presente artículo ha sido revisar sistemáticamente la literatura existente sobre soluciones de monitoreo de ciberseguridad en redes industriales basadas en inteligencia artificial (IA), con el propósito de identificar los principales fabricantes, soluciones, funcionalidades y sectores industriales en donde aplican esta tecnología. Se ha empleado el método PRISMA para realizar la búsqueda sistemática de documentación que contenga información relevante en los últimos 7 años. Los resultados obtenidos muestran que existen fabricantes como Nozomi Networks, Claroty, Dragos y Darktrace, que poseen soluciones de monitoreo de ciberseguridad basados en IA. Estas soluciones cuentan con funcionalidades como identificación de activos y comunicaciones, análisis de comportamiento, gestión de vulnerabilidades e inteligencia de amenazas. También se identifica que estas tecnologías estan siendo aplicadas en diferentes sectores industriales, como el energético, petróleo y gas, agua y saneamiento entre otros. Se concluye que la adopción de este tipo de tecnologías es de vital importancia para la detección más rápida y precisa de amenazas cibernéticas en las infraestructuras críticas, por lo cual es importante seguir invirtiendo en el desarrollo y aplicación de este tipo de soluciones.

**Palabras claves:** ciberseguridad industrial, inteligencia artificial, monitoreo de ciberseguridad, redes industriales, sistema de detección de intrusiones.

# ABSTRACT

The convergence of operational technologies (OT) with information technologies (IT) has significantly increased the risk of industrial networks suffering from cyber-attacks. The objective of this article has been to systematically review the existing literature on cybersecurity monitoring solutions in industrial networks based on artificial intelligence (AI), with the purpose of identifying the main manufacturers, solutions, functionalities, and industrial sectors where this technology is applied. The PRISMA method has been used to conduct a systematic search for documentation containing relevant information in the last 7 years. The results obtained show that there are manufacturers such as Nozomi Networks, Claroty, Dragos, and Darktrace, which have AI-based cybersecurity monitoring solutions. These solutions have functionalities such as asset and communication identification, behavior analysis, vulnerability management, and threat intelligence. It is also identified that these technologies are being applied in different industrial sectors, such as energy, oil and gas, water and sanitation, among others. It is concluded that the adoption of these type of technologies is of vital importance for the faster and more accurate detection of cyber threats in critical infrastructures, which is why it is important to continue investing in the development and application of these solutions.

**Keywords:** industrial cybersecurity, artificial intelligence, cybersecurity monitoring, industrial networks, intrusion detection system.

593 Digital Publisher CEIT ISSN 2588-0705

## Introducción

En el mundo actual la interconexión de sistemas es algo inevitable, por lo cual las redes industriales se han vuelto cada vez más susceptibles a amenazas cibernéticas. Estas redes son fundamentales para el funcionamiento eficiente y seguro de infraestructuras críticas, como plantas de energía, sistemas de agua, manufactura, petróleo y gas, entre otras se enfrentan desafíos únicos de ciberseguridad.

Los sistemas SCADA (Supervisory Control and Data Acquisition), sistemas de control industrial ICS, son componentes esenciales de las redes industriales, que proporcionan control y monitoreo de procesos críticos (Nankya et al., 2023), estas redes son consideradas como redes de Tecnología Operativa (OT).

La integración de las redes tradicionales de TI y las tecnologías operacionales (OT) se ha incrementado en todos los sectores de las infraestructuras críticas, impulsada por la Industria 4.0 y el Internet de las Cosas Industrial (IIoT) para mejorar la eficiencia industrial (Alotaibi, 2023). Esta convergencia es esencial para la seguridad y la toma de decisiones en tiempo real (Berindei et al., 2023). Pues según (Boye & Onate, 2023) el mundo interconectado actual es muy vulnerable a ciberataques y la industria está tomando cada vez más medidas de ciberseguridad para salvaguardar sus sistemas y datos.

(Pochmara & Świetlicka, 2024) manifiesta que el equipamiento de muchas empresas funciona con sistemas heredados los cuales carecen de funciones de seguridad, con lo cual la integración de estos sistemas en la Industria 4.0 requiere la inclusión de ciberseguridad. Según (Schmitt, 2023) la detección precisa y oportuna de ciber amenazas, mediante el uso de sistemas y algoritmos basados en IA, es de vital importancia en la resiliencia de los sistemas de ciberseguridad.

El presente artículo de revisión se compone de cinco secciones, incluida la introducción, y está organizado de la siguiente manera: la sección 2 describe la metodología utilizada para seleccionar la literatura sobre ciberseguridad en redes industriales basadas en Inteligencia Artificial. La sección 3 proporciona una revisión de la literatura y resultados obtenidos. La sección 4 comprende la discusión. Finalmente, la sección 5 detalla las conclusiones.

Para la presente investigación se formularon preguntas de investigación generadas acorde al tema de estudio, en este caso en particular soluciones de monitoreo ciberseguridad en redes industriales. Para llevar a cabo la investigación fue necesario responder las siguientes preguntas: ¿Qué fabricantes de soluciones de monitoreo de ciberseguridad especializados en redes industriales existen?, ¿Cuáles son las principales funcionalidades que debe tener una solución de monitoreo de ciberseguridad especializada en redes industriales basada en IA?, ¿En qué sectores de la industria se podría aplicar esta tecnología?

## Método

Antes de realizar la revisión bibliográfica, se siguieron las reglas del método PRISMA (Page et al., 2021), el cual fundamenta su metodología en la revisión de bases de datos y artículos de libre acceso de fuentes como: Web of science, Scopus y Google Academic. Se establecieron parámetros clave, tales como preguntas de investigación, búsqueda de documentos, selección de artículos y finalmente la obtención de datos, con el objetivo de encontrar la información más relevante y actualizada posible, lo cual permita la elaboración de un documento científico de excelente calidad.

Las **búsqueda**s de información se realizaron entre enero de 2024 y mayo de 2024. Se utilizaron las siguientes palabras clave y términos de búsqueda: ‘Artificial Intelligence’, ‘Machine Learning’, ‘Deep Learning’, ‘AI’, ‘ML’, ‘DL’, ‘Cybersecurity’, ‘Threats’, ‘IoT’, ‘ICS’, ‘OT’, ‘SCADA’, ‘Industry 4.0’, ‘Industry 5.0’, ‘Detection’, ‘Monitor’, ‘Monitoring’, ‘Intrusion detection’, ‘IDS’ e ‘Artificial Intelligence’.

Las estrategias de búsqueda combinaron **términos utilizando operadores booleanos como AND y OR.** Se utilizaron las siguientes 2 cadenas de búsqueda: Cadena 1 = *"('industrial' OR 'OT') AND 'cybersecurity' AND 'monitoring'"*; Cadena 2 = *"('Artificial Intelligence' OR 'Machine Learning' OR 'Deep Learning' OR 'AI' OR 'ML' OR 'DL') AND ('Cybersecurity' OR 'Threats') AND ('IoT' OR 'ICS' OR 'OT' OR 'SCADA' OR 'Industry 4.0' OR 'Industry 5.0') AND ('Detection' OR 'Monitor' OR 'Monitoring')"*; cadenas que fueron empleadas para asegurar una búsqueda exhaustiva y específica.

Se llevó a cabo una búsqueda bibliográfica sin restricción de años, con el fin de recopilar toda la información verificada y publicada tras varios años de estudio en el ámbito del monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. Considerando enfoques mencionados anteriormente, se eliminaron artículos repetidos y se filtró la información limitándola a los últimos 7 años, con el objetivo de tener los datos más recientes en la literatura científica sobre este tema.

Se realizó un filtró por relevancia de publicación, de los artículos obtenidos se identificó las tecnologías que cumplen con el criterio de ser especializada en redes industriales y que cuenta con IA. Posterior se obtuvo de forma manual información técnica más detallada de esas tecnologías, con el fin de obtener un análisis más completo. Al final se obtuvieron 26 documentos que abordan las preguntas de investigación planteadas.

En la Tabla 1 se detalla el procedimiento empleado para la selección y descarte de información obtenida de los documentos revisados, para lo cual se establecieron parámetros basados en la metodología PRISMA, como se ilustra en la Figura 1.

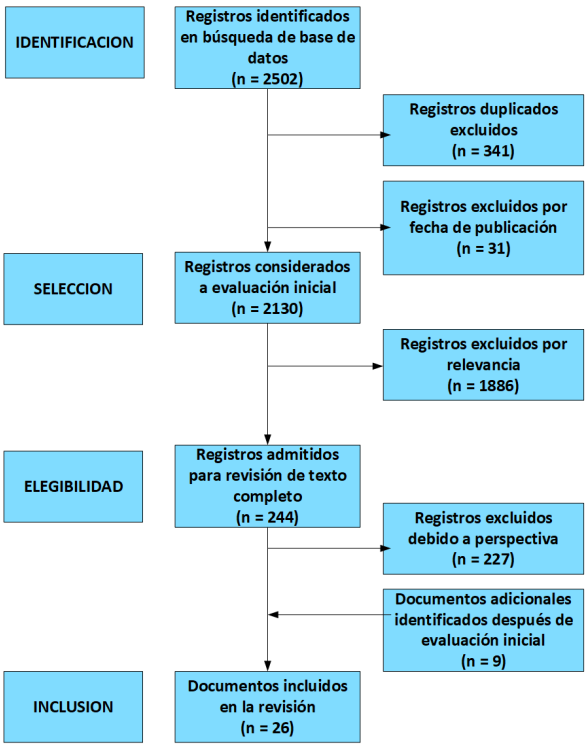
**Tabla 1**

*Criterios de inclusión y exclusión*

| N° | Inclusión | Exclusión |
|---|---|---|
| C1 | Artículos relacionados con Ciberseguridad en redes industriales | Tesis |
| C2 | Artículos publicados en los últimos 7 años. | Artículos no relacionados con ciberseguridad en redes industriales. |
| C3 | Artículos relacionados con OT, ICS, SCADA e IIOT | Revisar artículos |
| C4 | Artículos relacionados con Inteligencia artificial, Machine Learning, Deep Learning, AI, ML, DL, Industria 4.0, Industria 5.0 y Detección de intrusiones | Revisar artículos |
| C5 | Libros, datasheets, estudios de mercado y reportes técnicos relacionados con las soluciones de ciberseguridad basadas en IA especializadas en ciberseguridad encontradas en los artículos revisados. | Revisar documentos |
| C6 | Normativas de ciberseguridad utilizadas en redes industriales | Revisar documentos |

**Figura 1**

*Diagrama de flujo del proceso de selección de documentos*




Luego de analizar los documentos se consideraron varios aspectos como los tipos de soluciones de ciberseguridad, las marcas, las funcionalidades de las soluciones de

ciberseguridad basadas en IA y los sectores industriales en los cuales aplican este tipo de soluciones. Esto conllevó a la obtención de 26 documentos entre artículos científicos, datasheets de soluciones especializadas, estudios de mercado, libros, normativas de ciberseguridad para redes industriales y reportes técnicos, los cuales se detallan en la Tabla 2 detallados cronológicamente por su fecha de publicación, de los cuales se ha extraído la información en función de las preguntas de investigación.

Ver Tabla 2.

**Resultados**

A continuación se proporciona una revisión de las principales tecnologías de ciberseguridad identificadas en la literatura. Estas soluciones desempeñan un papel crucial en la protección de las redes industriales, las mismas que brindan capas adicionales de defensa contra las amenazas cibernéticas.

*Firewall.* - Los firewalls son una de las primeras líneas de defensa en la ciberseguridad, están diseñados para filtrar el tráfico y controlar el acceso a los recursos de red (Stouffer et al., 2023). En una red industrial generalmente se implementa entre la convergencia de la red Empresarial y la DMZ industrial, para proporcionar un control de acceso y monitoreo de tráfico que cursa da DMZ (Berindei et al., 2023). Entre los fabricantes que han realizado adaptaciones de su firewall para que operen en redes industriales se tiene a Fortinet (Rubio et al., 2019) y Palo Alto (Thielemann & Voster, 2023).

*IDS (Intrusion Detection System).* - Los IDS se emplean para escanear y analizar el tráfico de red, y en caso de detectar algún comportamiento sospechoso alerta (Soliman et al., 2023). El monitoreo de red en redes industriales se realiza mediante la captura y análisis pasivo del tráfico, lo cual es crucial para monitorear redes y detectar problemas de seguridad de manera oportuna (Alotaibi, 2023), los datos del tráfico de la red que fueron recopilados localmente se reenvían a un motor de análisis de datos centralizado (Houmb et al., 2023), en este caso un IDS. Existen dos tipos de IDS, los basados en firmas y los basados en anomalías (Rubio et al., 2019).

Los IDS basados en firmas utilizan un patrón que corresponde a la identificación de una amenaza específica conocida, dentro de las soluciones basadas en firmas, se incluye fabricantes como Cisco con su solución Snort y Suricata desarrollada por OISF (Bécue et al., 2021), las cuales se tratan de soluciones de IT adaptadas a entornos industriales mediante firmas de ataques escritas para redes OT.

Por otro lado se tienen los IDS basados en anomalías, los cuales incorporan algoritmos de detección basados en Inteligencia Artificial y Machine Learning (IA/ML), permitiendo identificar actividades maliciosas dentro de la red (Schmitt, 2023).

Existen autores que proponen la creación de un IDS especializado en entornos industriales basados en IA/ML, (Soliman et al., 2023) plantea un IDS basado en Deep Learning, (Ye & Zhao, 2022) propone en IDS con Aprendizaje Semi-Auto-Supervisado, mientras (Alkahtani & Aldhyani, 2022) sugiere un IDS basado en Machine Learning y Deep Learning, (Mubarak et al., 2022) manifiesta que la aplicación de técnicas de Machine Learning son estrategias prometedoras para mejorar la detección de soluciones de ciberseguridad en ataques a sistemas industriales.

Es importante destacar que en la actualidad ya existen soluciones IDS comerciales que utilizan inteligencia artificial especializadas en redes industriales. Entre los principales fabricantes que tienen soluciones IDS especializadas en redes industriales se encuentran Nozomi Networks, Darktrace (Rubio et al., 2019), Dragos y Claroty (Hurd & Mccarty, 2017).

Nozomi Networks es una compañía suiza fundada en 2013, que desarrollo la solución Scada Guardian especializada en redes industriales, la cual incluye un IDS de red basado tanto en firmas como en anomalías, cuenta con soporte

**Tabla 2**
*Obtención de datos*

| N° | Título | Autor(es) o Entidad | Año de Publicación | Fuente | Relevancia (PI1, PI2, PI3) | Tipo de documento |
|---|---|---|---|---|---|---|
| 1 | Solution Overview Claroty Continuous Threat Detection | Claroty | 2024 | Claroty web portal | PI2 | Datasheet |
| 2 | Darktrace/OT The Most Comprehensive Prevention, Detection, and Response Solution Purpose Built for Critical Infrastructures | Darktrace | 2024 | Darktrace web portal | PI2 | Datasheet |
| 3 | OT CYBERSECURITY THE 2023 YEAR IN REVIEW | Dragos, inc. | 2024 | Dragos web portal | PI3 | Reporte Técnico |
| 4 | Overview Nozomi Networks Platform | Nozomi Networks | 2024 | Nozomi Networks web portal | PI2 | Datasheet |
| 5 | Cybersecurity of Industrial Systems—A 2023 Report | Pochmara, J., & Świetlicka, A. | 2024 | Scopus | PI2, PI3 | Articulo científico |
| 6 | A Survey on Industrial Internet of Things Security: Requirements; Attacks; AI-Based Solutions; and Edge Computing Opportunities | Alotaibi, B. | 2023 | Web of science | PI1, PI3 | Articulo científico |
| 7 | THE CYBER SECURITY PARADIGM IN INDUSTRY 4.0 | Berindei, A.-M., Ilie, C., & Florentina, B. | 2023 | Scopus | PI1 | Articulo científico |
| 8 | Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems | Boye, F., & Onate, T. | 2023 | Google Academic | PI3 | Articulo científico |
| 9 | A Comprehensive Guide to OT Security | Darktrace | 2023 | Darktrace web portal | PI3 | Reporte Técnico |
| 10 | Datasheet Dragos Platform | Dragos, inc. | 2023 | Dragos web portal | PI2 | Datasheet |
| 11 | Intelligent Risk-Based Cybersecurity Protection for Industrial Systems Control: A Feasibility Study | Houmb, S. H., Iversen, F., Ewald, R., Faer-aas, E., & Asa, E. | 2023 | Web of science | PI1, PI3 | Articulo científico |
| 12 | Securing Industrial Control Systems Components Cyber Threats; and Machine Learning-Driven Defense Strategies | Nankya, M., Chataut, R., & Akl, R. | 2023 | Scopus | PI1, PI2, PI3 | Articulo científico |
| 13 | Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection | Schmitt, M. | 2023 | Scopus | PI1, PI3 | Articulo científico |
| 14 | Deep learning-based intrusion detection approach for securing industrial Internet of Things | Soliman, S., Oudah, W., & Aljuhani, A. | 2023 | Web of science | PI1, PI3 | Articulo científico |
| 15 | Guide to Industrial Control Systems (ICS) Security | Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. | 2023 | NIST web portal | PI1, PI2, PI3 | Normativa de ciberseguridad para el sector industrial |
| 16 | Market Guide for CPS Protection Platforms | Thielemann, K., & Voster, W. | 2023 | Claroty web portal | PI1, PI2, PI3 | Estudio de mercado |
| 17 | Cyber Security for Next-Generation Computing Technologies | Ullah Khan, I., Ouaissa, M., Ouaissa, M., Abou El Houda, Z., & Fazal Ijaz, M. | 2023 | Google Academic | PI1 | Libro |
| 18 | Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector | Alghassab, M. | 2022 | Web of science | PI3 | Articulo científico |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems | Alkahtani, H., & Aldhyani, T. H. H. | 2022 | Web of science | PI1, PI3 | Articulo científico |
| 20 | Industrial Datasets with ICS Testbed and Attack Detection Using Machine Learning Techniques | Mubarak, S., Habaebi, M. H., Islam, M. R., Balla, A., Tahir, M., Elsheikh, E. A. A., & Suliman, F. M. | 2022 | Web of science | PI1, PI2 | Articulo científico |
| 21 | Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning | Muhammad, A. R., Sukarno, P., & Wardana, A. | 2022 | Scopus | PI1, PI2 | Articulo científico |
| 22 | A Semi-Self-Supervised Intrusion Detection System for Multilevel Industrial Cyber Protection | Ye, F., & Zhao, W. | 2022 | Web of science | PI1 | Articulo científico |
| 23 | A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology | Zhang, S., Liu, Y., & Yang, D. | 2022 | Web of science | PI1, PI3 | Articulo científico |
| 24 | Artificial intelligence, cyberthreats and Industry 4.0: challenges and opportunities | Bécue, A., Praça, I., & Gama, J. | 2021 | Google Academic | PI1, PI2, PI3 | Articulo científico |
| 25 | Current cyber-defense trends in industrial control systems | Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. | 2019 | Google Academic | PI1, PI3 | Articulo científico |
| 26 | A Survey of Security Tools for the Industrial Control System Environment | Hurd, C., & McCarty, M. | 2017 | Google Academic | PI1 | Articulo científico |

para una gran cantidad de protocolos OT e IT (Bécue et al., 2021).

Darktrace es una compañía inglesa (Thielemann & Voster, 2023), la cual entre sus soluciones cuenta con Darktrace/OT, solución dedicada a redes OT, el sistema emplea algoritmos de auto aprendizaje para detectar y responder a ciber amenazas en redes industriales en tiempo real (Ullah Khan et al., 2023).

Dragos es una compañía estadounidense (Thielemann & Voster, 2023), se especializa en ciberseguridad para entornos OT con su Dragos Platform, la cual ofrece capacidades IDS para detectar y responder a ciberataques en tiempo real (Hurd & Mccarty, 2017).

Finalmente, se tiene a Claroty, una empresa israelí fundada en el 2016, su solución Continuous Threat Detection (CTD), realiza la detección de anomalías de red basado en (modelos deterministas y de comportamiento) (Bécue et al., 2021).

*IPS (Intrusion Prevention System)*. - Los Sistemas de Prevención de Intrusiones (IPS) detectan una actividad intrusiva e intentan detener la dicha actividad (Stouffer et al., 2023), esta inspección de tráfico es en línea y no de forma pasiva, por lo cual es importante que el IPS previo a su despliegue sea validado que no interrumpe tráfico legítimo de la red industrial (Nankya et al., 2023). Los IPS funcionan con firmas que detectan ataques conocidos, algunos fabricantes como Cisco con su solución Firepower o Fortinet con su modulo IPS dentro de su firewall Fortigate han incluido firmas de seguridad para reconocer ataques en protocolos OT (Bécue et al., 2021).

*SIEM (Security Information and Event Management*). - Las soluciones (SIEM) son soluciones del mundo TI utilizadas para monitorear, analizar y correlacionar eventos a partir de logs de equipamiento como IDS, IPS, Firewall, aplicaciones, etc, con el fin de detectar intentos de intrusión (Stouffer et al., 2023). Según (Muhammad et al., 2022) el SIEM también se utiliza para realizar monitoreo en tiempo real de varios IDS, indica también que Splunk es uno de los fabricantes de SIEM, mientras (Hurd & Mccarty, 2017) indica que el fabricante AlienVault combina potentes capacidades (SIEM) y de gestión de logs con herramientas de seguridad para brindar un monitoreo de seguridad centralizado.

*Honeypot.* - Según (Zhang et al., 2022) además del IDS, el honeypot es otra solución que permite detectar ataques e intrusiones

desconocidos, el mismo se define como un "sistema de información cuyo valor consiste en el uso no autorizado o ilícito de dicho recurso", el honeypot es un engaño planificado para actuar como un señuelo, el cual pueda ser investigado, atacado o comprometido. (Rubio et al., 2019) manifiesta que en el mercado actual, una de las principales plataformas de detección basadas en honeypots es ThreatMatrix del fabricante Attivo Networks, que es capaz de detectar intrusiones en tiempo real en sistemas ICS/SCADA e incluso entornos IoT.

Dentro de las principales funcionalidades que debe tiene una solución de monitoreo de ciberseguridad especializada en redes industriales basadas en IA se detalla las siguientes:

*Descubrimiento y gestión de activos existentes*. - Permite contar con un inventario de activos del hardware, software e infraestructura (Nankya et al., 2023), posibilitando contar información de inventario de todos los componentes de la red OT (Mubarak et al., 2022), esta funcionalidad es soportada por los fabricantes Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023) y Darktrace (Darktrace ©, 2024).

*Identificación de comunicaciones de activos*. - Permite determinar los diferentes protocolos que están siendo utilizados por los activos para comunicarse dentro de la red (Nankya et al., 2023), los fabricantes Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023) y Darktrace (Darktrace ©, 2024) incluyen esta característica.

*Inteligencia de amenazas*. - Según (Thielemann & Voster, 2023) la mayoría de las soluciones de ciberseguridad incluyen indicadores de compromiso (IoC), detecciones basadas en firmas e informes alineados con el marco MITRE ATT&CK para OT. El uso de IA en ciberseguridad busca conseguir la detección avanzada de amenazas, superando la seguridad tradicional que intenta seguir el ritmo de las tácticas cambiantes de los ciberdelincuentes (Pochmara & Świetlicka, 2024). Fabricantes como Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023) y Darktrace (Darktrace ©, 2024) cuentan con dicha funcionalidad dentro de sus soluciones.

*Detección de anomalías*. - La detección de anomalías utiliza técnicas de aprendizaje automático, lo cual permite detectar un comportamiento sospechoso similar a un ciberataque (Muhammad et al., 2022). Según (Bécue et al., 2021) detección de anomalías consiste en comparar las actividades observadas versus las definiciones establecidas de lo que se considera normal, con el objetivo de identificar posibles desviaciones significativas. Esta funcionalidad es propia de soluciones como Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023) y Darktrace (Darktrace ©, 2024) al estar basadas en Inteligencia Artificial.

*Riesgo y Gestión de vulnerabilidades*. - Las vulnerabilidades son debilidades en los sistemas de información, procedimientos, controles o implementaciones del sistema que pueden ser explotados por una amenaza (Stouffer et al., 2023). Según (Thielemann & Voster, 2023) existen soluciones que pueden correlacionar el descubrimiento de activos con bases de datos de vulnerabilidades, permitiendo así priorizar las amenazas conocidas, detectando aplicaciones inseguras y password por defecto, ofrecen posibles remediaciones de mitigación y dan seguimiento de acciones mediante tickets. Esta característica es soportada por los fabricantes Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023) y Darktrace (Darktrace ©, 2024) al estar basadas en Inteligencia Artificial.

Las soluciones de ciberseguridad basadas en IA se aplican en una amplia gama de sectores industriales, según (Darktrace ©, 2023), (Zhang et al., 2022), (Rubio et al., 2019), (Houmb et al., 2023), (Thielemann & Voster, 2023), (Schmitt, 2023), y (Alghassab, 2022) los sectores en los que aplica son energía, manufactura, transporte, agua y saneamiento, petróleo y gas, (Alotaibi,

593 Digital Publisher CEIT ISSN 2588-0705

2023), (Boye & Onate, 2023) y (Bécue et al., 2021) incluyen al sector automotriz y salud, (Soliman et al., 2023) agrega a IIoT, (Alkahtani & Aldhyani, 2022) referencia al sector alimenticio, el sector químico y farmacéutico es mencionado por (Stouffer et al., 2023), el sector minero es referido por (Dragos ©, 2024) y finalmente el sector nuclear tal como lo indica (Nankya et al., 2023).

## Discusión

La tabla 3 mapea las principales tecnologías y funcionalidades de ciberseguridad identificadas en la literatura, las mismas se agrupan en tres secciones: Tecnologías de ciberseguridad, funcionalidades clave de soluciones basadas en IA y sectores industriales de aplicación. Se detallan las tecnologías utilizadas, como firewalls, IDS, IPS, etc., las funcionalidades clave, como la detección de anomalías e inteligencia de amenazas, y los sectores industriales en los que se aplican estas soluciones. La tabla proporciona una visión general de las herramientas y estrategias utilizadas para proteger redes industriales, destacando tanto las tecnologías tradicionales como las basadas en inteligencia artificial.

Ver Tabla 3.

Los resultados de esta revisión de literatura demuestran que a pesar de que en las redes industriales existen soluciones tradicionales de ciberseguridad del mundo IT como Firewall, IDS, IPS, SIEM, etc., las cuales se han ido adaptando al mundo OT. Sin embargo, el empleo de soluciones de monitoreo de ciberseguridad basadas en IA es una tendencia creciente, lo cual permite la protección de redes industriales. En el mercado existen fabricantes líderes, especializados en ciberseguridad industrial que han desarrollado plataformas robustas, las cuales no solo detectan y responden a amenazas en tiempo real, sino que también proporcionan la detección de anomalías, mejorando de esta forma la visibilidad de ciberseguridad en la red (Thielemann & Voster, 2023).

Los fabricantes Darktrace, Nozomi Networks, Claroty y Dragos incluyen en sus soluciones IDS funcionalidades que permiten tener una visibilidad completa de todo lo que sucede en la red industrial desde el punto de vista de la ciberseguridad, al contar con características como descubrimiento y gestión de activos existentes, identificación de comunicaciones de activos, inteligencia de amenazas, detección de anomalías y riesgo y Gestión de vulnerabilidades (Claroty ©, 2024), (Nozomi Networks ©, 2024), (Dragos ©, 2023) y (Darktrace ©, 2024), lo cual le permite al personal de ciberseguridad la toma oportuna de decisiones al momento de enfrentarse a un incidente de ciberseguridad industrial.

En lo referente a inteligencia de amenazas los fabricantes Nozomi Networks, Dragos y Claroty cuentan con una arquitectura hibrida entre análisis comportamental basado en IA y firmas de seguridad, lo cual mejora la eficacia de la identificación de amenazas en la red industrial, mientras la solución Darktrace no hace uso de firmas y únicamente utiliza análisis comportamental basado en IA para realizar dicha detección (Darktrace ©, 2023).

Los estudios de casos reales y las evaluaciones empíricas destacan la eficacia de estas soluciones en la detección de amenazas (Mubarak et al., 2022), (Schmitt, 2023). La literatura también enfatiza en la importancia de las colaboraciones y estándares internacionales para mejorar la ciberseguridad en las redes industriales (Hurd & Mccarty, 2017), (Dragos ©, 2024).

Los sectores a los cuales puede aplicarse este tipo de tecnología son muy diversos, entre los sectores más comunes se encuentran el energético, agua y saneamiento, petróleo y gas, transporte y manufactura (Thielemann & Voster, 2023).

## Conclusiones

Las soluciones de monitoreo de ciberseguridad especializadas en redes industriales basadas en IA brindan una visibilidad adecuada en este tipo de entornos. Entre los fabricantes que cuentan con este tipo

**Tabla 3**

*Mapeo categórico de hallazgos en literatura*

| **Tecnologías de ciberseguridad** | |
|---|---|
| **Tecnología** | **Tema relevante** |
| Firewall | - Filtrado de tráfico y control de acceso (Stouffer et al., 2023)<br>- Implementación entre red empresarial y DMZ industrial (Berindei et al., 2023)<br>- Fabricantes: Fortinet, Palo Alto (Rubio et al., 2019; Thielemann & Voster, 2023) |
| IDS | - Detección de comportamientos sospechosos en tráfico (Soliman et al., 2023; Alotaibi, 2023; Houmb et al., 2023)<br>- IDS basados en firmas Cisco Snort, Suricata (Bécue et al., 2021) e IDS basados en anomalías (Rubio et al., 2019; Schmitt, 2023)<br>- Propuestas de IDS para entornos industriales: Machine learning (Alkahtani & Aldhyani; Mubarak et al., 2022); Deep Learning (Soliman et al., 2023; Mubarak et al., 2022) y Aprendizaje Semi-Auto-Supervisado (Alkahtani & Aldhyani, 2022)<br>- Fabricantes: Nozomi Networks (Rubio et al., 2019; Bécue et al., 2021), Darktrace (Rubio et al., 2019; Thielemann & Voster, 2023; Ullah Khan et al., 2023), Dragos (Thielemann & Voster, 2023; Ullah Khan et al., 2023), Claroty (Bécue et al., 2021; Hurd & Mccarty, 2017) |
| IPS | - Detección y prevención de intrusiones (Stouffer et al., 2023)<br>- Consideraciones de implementación (Nankya et al., 2023)<br>- Fabricantes: Cisco Firepower, Fortinet Fortigate (Bécue et al., 2021) |
| SIEM | - Monitoreo, análisis y correlación de eventos de seguridad (Stouffer et al., 2023)<br>- Fabricantes: Splunk, AlienVault (Muhammad et al., 2022; Hurd & Mccarty, 2017) |
| Honeypot | - Detección de ataques desconocidos, actuando como señuelo (Zhang et al., 2022)<br>- Fabricante: Attivo Networks (Rubio et al., 2019) |
| **Funcionalidades clave de las soluciones basadas en IA** | |
| **Funcionalidad** | **Tema relevante** |
| Descubrimiento y gestión de activos | - Inventario de activos de hardware, software e infraestructura (Nankya et al., 2023; Mubarak et al., 2022)<br>- Fabricantes: Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023), Darktrace (Darktrace ©, 2024) |
| Identificación de comunicaciones de activos | - Determinación de protocolos de comunicación en la red (Nankya et al., 2023)<br>- Fabricantes: Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023), Darktrace (Darktrace ©, 2024) |
| Inteligencia de amenazas | - Detección avanzada de amenazas utilizando indicadores de compromiso y análisis basados en IA (Thielemann & Voster, 2023; Pochmara & Świetlicka, 2024)<br>- Fabricantes: Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023), Darktrace (Darktrace ©, 2024) |
| Detección de anomalías | - Detección de comportamientos sospechosos mediante aprendizaje automático (Muhammad et al., 2022) y comportamiento fuera de lo normal (Bécue et al., 2021)<br>- Fabricantes: Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023), Darktrace (Darktrace ©, 2024) |
| Riesgo y gestión de vulnerabilidades | - Identificación y gestión de vulnerabilidades en sistemas de información (Stouffer et al., 2023; Thielemann & Voster, 2023)<br>- Fabricantes: Claroty (Claroty ©, 2024), Nozomi Networks (Nozomi Networks ©, 2024), Dragos (Dragos ©, 2023), Darktrace (Darktrace ©, 2024) |
| **Sectores industriales de aplicación** | |
| **Sector** | **Autor** |
| Energía, manufactura, transporte, agua y saneamiento, petróleo y gas | (Darktrace ©, 2023; Zhang et al., 2022; Rubio et al., 2019; Houmb et al., 2023; Thielemann & Voster, 2023; Schmitt, 2023) |
| Automotriz y salud | (Alotaibi, 2023; Boye & Onate, 2023; Bécue et al., 2021 |
| IIOT | (Soliman et al., 2023) |
| Alimenticio | (Alkahtani & Aldhyani, 2022) |
| Químico y farmacéutico | (Stouffer et al., 2023) |
| Minero | (Dragos ©, 2024) |
| Nuclear | (Nankya et al., 2023) |

de soluciones se encuentra Nozomi Networks con su solución Scada Guardian, Claroty con su solución Continuous Threat Detection (CTD), Dragos cuenta con su solución Dragos Platform y finalmente a Darktrace con su solución Darktrace/OT.

Las soluciones anteriormente detalladas cuentan con funcionalidades comunes, entre las cuales se detallan la identificación de activos de red y sus comunicaciones, así como la detección de vulnerabilidades, anomalías y amenazas observadas dentro de la red.

Es importante mencionar que a pesar de que existen fabricantes especializados en soluciones de ciberseguridad industrial basadas en IA, la academia continúa proponiendo investigaciones de este tipo de soluciones, por lo cual, sin duda alguna en los próximos años se observará la incorporación de nuevas soluciones que se sumen a complementar la ciberseguridad en ambientes industriales.

Entre los sectores industriales que más se han beneficiado del uso de este tipo de tecnología están el energético, manufactura, transporte, salud, agua y saneamiento, así como petróleo y gas, sin embargo, esta tecnología se puede aplicar en cualquier sector que haga uso de infraestructura OT. Es necesario que las empresas industriales inviertan en este tipo de tecnologías, lo cual les permita estar preparados para enfrentar las amenazas cibernéticas, las cuales cada vez son más sofisticadas y difíciles de detectar.

El presente estudio se centró en literatura en inglés, debido a que la mayoría de las publicaciones más recientes y de alta calidad en ciberseguridad, especialmente en redes industriales, se encuentran disponibles en este idioma. Esto incluye revistas de renombre y conferencias internacionales, lo que facilita el acceso a los desarrollos más avanzados y actualizados en el campo y permite de esta forma la estandarización de la terminología utilizada. Sin embargo, se reconoce la posible exclusión de investigaciones valiosas en otros idiomas. Para futuros trabajos, se recomienda incluir artículos existentes en otros idiomas ya sea mediante traducciones automáticas o colaboraciones con investigadores multilingües para una revisión más exhaustiva.

Finalmente a partir de la presente investigación se puede desprender posibles estudios como: estudios comparativos de las soluciones de monitoreo de ciberseguridad industrial en diferentes entornos industriales, así como la integración de soluciones de ciberseguridad basadas en IA con terceros, lo cual puede complementar estas soluciones para que en base a la visibilidad que proveen, puedan interactuar con otras soluciones de ciberseguridad como Firewalls, EDR, SIEM, etc., ampliando de esta manera la cobertura de ciberseguridad en redes industriales.

**Referencias bibliográficas**

Alghassab, M. (2022). Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. Energies, 15(1). https://doi.org/10.3390/en15010218.

Alkahtani, H., & Aldhyani, T. H. H. (2022). Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems. Electronics (Switzerland), 11(11). https://doi.org/10.3390/electronics11111717

Alotaibi, B. (2023). A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. In Sensors (Vol. 23, Issue 17). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s23177470

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Artificial Intelligence Review, 54(5), 3849–3886. https://doi.org/10.1007/s10462-020-09942-2

Berindei, A.-M., Ilie, C., & Florentina, B. (2023). The Cyber Security Paradigm in Industry 4.0. In International Journal of

Mechatronics and Applied Mechanics (Issue 13)

Boye, F., & Onate, T. (2023). Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems. Internet of Things and Cloud Computing. https://doi.org/10.11648/j.iotcc.20231101.11

Claroty ©. (2024). SOLUTION OVERVIEW Claroty Continuous Threat Detection. https://web-assets.claroty.com/resource-downloads/ctd-overview-2024.pdf

Darktrace ©. (2023). A Comprehensive Guide to OT Security. https://cdn.prod.website-files.com/626ff4d25aca2edf4325ff97/6557cf544fbbb42fd1bbd84c_A%20Comprehensive%20Guide%20to%20OT%20Security.pdf

Darktrace ©. (2024). Darktrace/OT The Most Comprehensive Prevention, Detection, and Response Solution Purpose Built for Critical Infrastructures. https://darktrace.com/es/resources/ot-solution-brief

Dragos ©. (2023). Datasheet Dragos Platform. https://www.dragos.com/wp-content/uploads/2021/07/Dragos-Platform-Datasheet-2.pdf

Dragos ©. (2024). OT CYBERSECURITY THE 2023 YEAR IN REVIEW. https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf?hsLang=en

Houmb, S. H., Iversen, F., Ewald, R., Faeraas, E., & Asa, E. (2023). Intelligent Risk-Based Cybersecurity Protection for Industrial Systems Control-A Feasibility Study. In SPE Journal (Vol. 3272). http://onepetro.org/SJ/article-pdf/28/06/3272/3333567/spe-217430-pa.pdf/1

Hurd, C. M., & Mccarty, M. V. (2017). A Survey of Security Tools for the Industrial Control System Environment. http://www.inl.gov

Mubarak, S., Habaebi, M. H., Islam, M. R., Balla, A., Tahir, M., Elsheikh, E. A. A., & Suliman, F. M. (2022). Industrial datasets with ICS testbed and attack detection using machine learning techniques. Intelligent Automation and Soft Computing, 31(3), 1345–1360. https://doi.org/10.32604/IASC.2022.020801

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2022). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. Procedia Computer Science, 217, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339

Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. In Sensors (Basel, Switzerland) (Vol. 23, Issue 21). https://doi.org/10.3390/s23218840

Nozomi Networks ©. (2024). Overview Nozomi Networks Platform. https://cdn.prod.website-files.com/645a4534705010e2cb244f50/65b121e2e08c0ab6e6b0278d_Nozomi-Networks-Platform-Overview.pdf

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. In The BMJ (Vol. 372). BMJ Publishing Group. https://doi.org/10.1136/bmj.n71

Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of Industrial Systems—A 2023 Report. Electronics (Switzerland), 13(7). https://doi.org/10.3390/electronics13071191

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. Computers and Security, 87. https://doi.org/10.1016/j.cose.2019.06.015

593 Digital Publisher CEIT ISSN 2588-0705

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

Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Engineering Journal, 81, 371–383. https://doi.org/10.1016/j.aej.2023.09.023

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) security. https://doi.org/10.6028/NIST.SP.800-82r3

Thielemann, K., & Voster, W. (2023). Market Guide for CPS Protection Platforms. https://www.gartner.com/doc/reprints?id=1-2EDW-F9AQ&ct=230705&st=sb

Ullah Khan, I., Ouaissa, M., Ouaissa, M., Abou El Houda, Z., & Fazal Ijaz, M. (2023). Cyber Security for Next-Generation Computing Technologies. CRC Press. https://doi.org/10.1201/9781003404361

Ye, F., & Zhao, W. (2022). A Semi-Self-Supervised Intrusion Detection System for Multilevel Industrial Cyber Protection. Computational Intelligence and Neuroscience, 2022. https://doi.org/10.1155/2022/4043309

Zhang, S., Liu, Y., & Yang, D. (2022). A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology. International Journal of Digital Crime and Forensics, 14(2), 1–20. https://doi.org/10.4018/ijdcf.302874