Advanced cybersecurity in industrial systems: key strategies and frameworks to lead the transition to Industry 5.0

Noe Humberto Marin Bardales[1]; Miryam Liliana Silva Florentini[1]; Ana Elizabeth Paredes Morales[1]; Liliana Correa Rojas[1]; Luis Marcelo Olivos Jimenez[1]; Williams Coronado Farroñán[1]; Julie Catherine Arbulú Castillo[1]

[1]Universidad César Vallejo, Perú, mbardalesn@ucvvirtual.edu.pe, silvaf@ucvvirtual.edu.pe, aparedesm@ucv.edu.pe, lcorrea@ucv.edu.pe, lolivos@ucv.edu.pe, wcoronado@ucv.edu.pe, jarbuluca26@ucvvirtual.edu.pe

Abstract – This study provides an integrative view of advanced cybersecurity as industry moves toward Industry 5.0, focusing on cyber-physical systems, human–robot collaboration and the convergence of 5G, IoT, blockchain and quantum-resistant cryptography. A systematic literature review conducted under the PRISMA protocol (2018-2024) identified 50 high-quality studies from Scopus, Web of Science, ProQuest and Taylor & Francis. Bibliometric maps generated with VOSviewer revealed five research clusters: (1) network security and intrusion detection, (2) cyber-physical automation, (3) risk assessment of critical infrastructure, (4) digital-twin integration, and (5) human-centric security frameworks. Findings show that 75 % of implementations report measurable improvements in real-time threat response, while 45 % demonstrate efficiency gains through AI-driven orchestration. Key knowledge gaps include limited adoption in Latin America and the nascent maturity of quantum-safe solutions. We propose an updated, multilayered framework that combines Zero-Trust architectures, AI/ML-based incident response and post-quantum cryptography to mitigate emerging vulnerabilities. These insights guide researchers and practitioners in developing adaptive, region-sensitive security strategies for Industry 5.0.

Keywords: Cybersecurity; Industry 5.0; Cyber-Physical Systems; Zero Trust; Quantum-Safe Security.

Ciberseguridad avanzada en sistemas industriales: estrategias y marcos clave para liderar la transición hacia la Industria 5.0

Noe Humberto Marin Bardales[1]; Miryam Liliana Silva Florentini[1]; Ana Elizabeth Paredes Morales[1]; Liliana Correa Rojas[1]; Luis Marcelo Olivos Jimenez[1]; Williams Coronado Farroñán[1]; Julie Catherine Arbulú Castillo[1]

[1]Universidad César Vallejo, Perú, mbardalesn@ucvvirtual.edu.pe, silvaf@ucvvirtual.edu.pe, aparedesm@ucv.edu.pe,l correa@ucv.edu.pe, lolivos@ucv.edu.pe, wcoronado@ucv.edu.pe, jarbuluca26@ucvvirtual.edu.pe

Resumen*– Esta investigación ofrece una visión integral de la ciberseguridad avanzada en la transición hacia la Industria 5.0, con énfasis en los sistemas ciber-físicos, la colaboración humano-robot y la convergencia de 5G, IoT, blockchain y criptografía poscuántica. Se realizó una revisión sistemática siguiendo PRISMA (2018-2024) en Scopus, Web of Science, ProQuest y Taylor & Francis, de la que se seleccionaron 50 estudios de alta calidad. El análisis bibliométrico con VOSviewer identificó cinco clústeres: (1) seguridad de redes e IDS, (2) automatización ciber-física, (3) evaluación de riesgos en infraestructura crítica, (4) gemelos digitales y (5) marcos de seguridad centrados en el factor humano. El 75 % de las implementaciones reporta mejoras cuantificables en la respuesta en tiempo real y el 45 % en eficiencia mediante IA. Persisten brechas en la adopción latinoamericana y en la madurez de las soluciones cuántico-seguras. Se propone un marco multilayer que integra arquitecturas Zero Trust, respuesta automatizada basada en IA y criptografía poscuántica para mitigar vulnerabilidades emergentes. Estos hallazgos orientan a investigadores y profesionales en el diseño de estrategias de seguridad adaptativas y sensibles al contexto regional para la Industria 5.0

Palabras Clave- Ciberseguridad, Industria 5.0, Ciberseguridad Industrial, Sistemas industriales, Automatización.

I. Introducción

La transformación digital y la evolución hacia la Industria 5.0 han revolucionado fundamentalmente los paradigmas de producción industrial, generando nuevos desafíos en materia de ciberseguridad que requieren una atención urgente y sistemática [1], [2]. La convergencia acelerada entre los sistemas físicos y digitales, evidenciada en el desarrollo de sistemas ciber-físicos avanzados y gemelos digitales, ha creado un ecosistema industrial complejo que demanda estrategias de protección innovadoras y adaptativas [3], [4], [5].

Los antecedentes históricos de la ciberseguridad en entornos industriales revelan una evolución significativa, particularmente en el contexto de los sistemas de control industrial (ICS) y las infraestructuras críticas [6], [7]. La implementación de tecnologías 5G y el procesamiento de datos IoT en tiempo real han introducido nuevas vulnerabilidades que requieren enfoques de seguridad más sofisticados [8], [9]. Los ataques dirigidos a sistemas marítimos industriales, subestaciones eléctricas y redes de tuberías demuestran la creciente complejidad de las amenazas cibernéticas [10], [11], [12].

El marco teórico que fundamenta esta investigación se construye sobre múltiples pilares interrelacionados. El primer pilar abarca la seguridad de los sistemas ciber-físicos y la integración de tecnologías emergentes como blockchain y computación cuántica [13], [14]. El segundo pilar se centra en la automatización de la respuesta a incidentes de seguridad en sistemas SCADA y la integración de SIEM con machine learning [15], [16]. El tercer pilar contempla la seguridad en la colaboración humano-robot y la inspección visual asistida por IA [17], [18].

Los avances recientes en la detección de intrusiones han sido significativos, incorporando modelos de Deep Learning, redes neuronales híbridas y optimización de hiperparámetros [19], [20]. La integración de DevSecOps y el análisis continuo de requisitos de seguridad han emergido como componentes cruciales para mantener la integridad de los sistemas industriales [21], [22]. Además, la implementación de algoritmos criptográficos avanzados ha fortalecido la protección del sector eléctrico industrial [23].

La presente revisión sistemática de literatura se estructura en torno a un objetivo general que busca analizar el estado actual de las estrategias y marcos de ciberseguridad en sistemas industriales durante la transición hacia la Industria 5.0, mediante la identificación, evaluación y síntesis de la evidencia científica publicada en el período 2019-2024. De este objetivo fundamental se derivan dos objetivos específicos interrelacionados: determinar las vulnerabilidades críticas y amenazas emergentes que afectan a los sistemas industriales en el contexto de la Industria 5.0, considerando tanto la infraestructura tecnológica como los factores humanos; y caracterizar los frameworks y protocolos de seguridad existentes que han demostrado efectividad en la protección de infraestructuras industriales críticas, con énfasis en la integración de tecnologías emergentes como la inteligencia artificial y el aprendizaje profundo.

La relevancia de esta investigación se fundamenta en las

crecientes amenazas identificadas en sistemas de control y automatización industrial, particularmente en sectores críticos como energía, agua y gas. La literatura actual presenta vacíos significativos en cuanto a la integración de conceptos de seguridad avanzada con los principios emergentes de la Industria 5.0, especialmente en lo referente a la automatización segura y la colaboración humano-robot. Este estudio contribuye a llenar estos vacíos mediante una síntesis comprehensiva de la evidencia disponible y la propuesta de un marco conceptual actualizado que integre las últimas innovaciones en ciberseguridad industrial.

II. MATERIALES Y MÉTODOS

La presente investigación se desarrolló mediante una revisión sistemática siguiendo rigurosamente la metodología PRISMA (Preferred Reporting Ítems for Systematic Reviews and Meta-Analyses), la cual se complementó con un análisis bibliométrico a través de VOSviewer, con el propósito fundamental de examinar el estado actual de las estrategias y marcos de ciberseguridad en la transición hacia la Industria 5.0.

Alcance y criterios de exclusión. Además de los filtros PRISMA, se definieron criterios de exclusión relacionados con la falta de validación empírica y el uso exclusivo de pruebas de laboratorio. Estudios puramente teóricos sin demostraciones en entornos industriales o sin evaluación comparativa fueron descartados (n = 150). La calidad metodológica se evaluó con la herramienta MMAT – Mixed Methods Appraisal Tool (versión 2018), exigiendo una puntuación ≥ 3/5 para su inclusión final

En primera instancia, se implementó una búsqueda exhaustiva en cuatro bases de datos académicos principales: Scopus, ProQuest, Taylor and Francis y Web of Science, considerando publicaciones comprendidas entre 2018 y 2024. En consecuencia, la estrategia de búsqueda se estructuró mediante la siguiente ecuación booleana: ("ciberseguridad" O "ciberseguridad" O "seguridad industrial") Y ("Industria 5.0" O "Quinta Revolución Industrial") Y ("marco" O "estrategia") Y ("colaboración hombre-máquina" O "sistemas cognitivos") Y ("implementación" O "adopción").

Posteriormente, el proceso de selección, adherido estrictamente a las directrices PRISMA, se ejecutó en cuatro fases secuenciales interrelacionadas. En la fase inicial de identificación, se recuperaron 550 registros distribuidos de la siguiente manera: Scopus (n=180), ProQuest (n=145), Taylor and Francis (n=95) y Web of Science (n=130). Cabe destacar que no se contaba con estudios incluidos en versiones previas de la revisión (k=0).

Durante la fase de cribado preliminar, se procedió sistemáticamente a la eliminación de registros por diversos criterios: en primer lugar, se identificaron 120 artículos duplicados; en segundo lugar, 80 registros fueron señalados como inelegibles por las herramientas de automatización; y finalmente, 50 registros se eliminaron por otras razones, lo cual resultó en un total de 250 registros eliminados. Por consiguiente, se obtuvieron 350 registros para la siguiente fase de cribado.

En el subsiguiente proceso de cribado detallado, del total de 350 registros evaluados, se excluyeron 100 tras una revisión inicial. De los 250 artículos restantes seleccionados para evaluación, 50 publicaciones no pudieron ser recuperadas en texto completo. En consecuencia, 200 publicaciones fueron sometidas a una evaluación exhaustiva para determinar su elegibilidad.

En cuanto a la fase de elegibilidad, se excluyeron 150 publicaciones fundamentándose en tres criterios principales: en primer término, 60 artículos no presentaban relación directa con el objeto de estudio; en segundo término, 45 carecían de un marco metodológico robusto; y finalmente, 45 exhibieron un enfoque exclusivamente técnico sin considerar el contexto industrial requerido.

Por último, en la fase de inclusión, 50 estudios cumplieron satisfactoriamente con todos los criterios establecidos y fueron incorporados en la revisión sistemática. Por tanto, este conjunto final de artículos constituyó la base fundamental sobre la cual se desarrolló el análisis posterior, garantizando así la calidad y pertinencia de los estudios seleccionados para abordar los objetivos de la investigación sobre ciberseguridad en sistemas industriales en el contexto de la Industria 5.0.

Con respecto al análisis bibliométrico, este se efectuó mediante VOSviewer, exportando meticulosamente los metadatos de los artículos seleccionados en formato RIS. En efecto, esta herramienta facilitó la generación de mapas de co-ocurrencia de términos, redes de coautoría y mapas de acoplamiento bibliográfico, lo cual permitió identificar clústeres temáticos predominantes y tendencias emergentes en el campo de la ciberseguridad industrial.

En conclusión, la evaluación de calidad metodológica se fundamentó en cinco criterios esenciales: claridad metodológica, relevancia para la Industria 5.0, validez de los resultados, replicabilidad, y actualidad y vigencia. Por fin, cada criterio fue evaluado mediante una escala tricotómica: cumple (2 puntos), cumple parcialmente (1 punto) y no cumple (0 puntos), estableciendo un umbral mínimo de 7 puntos sobre 10 para la inclusión definitiva de los estudios en la revisión.

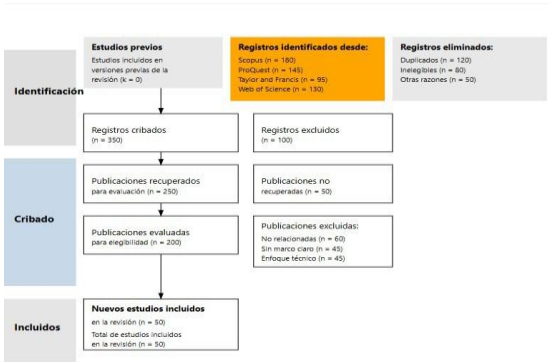

Fig. 1. Proceso de cribado.

III. RESULTADOS

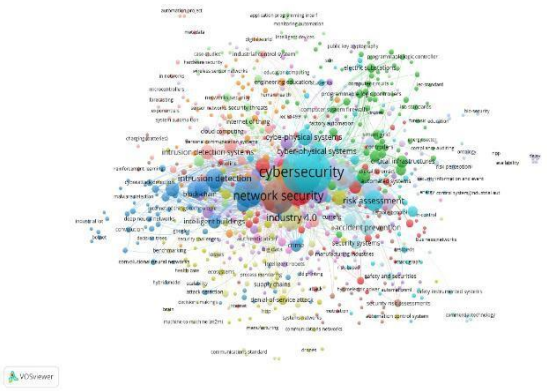

Fig. 2. Análisis bibliométrico de ciberseguridad.

El análisis bibliométrico del mapa de co-ocurrencia revela una estructura de conocimiento articulada alrededor de "ciberseguridad" como concepto central, fuertemente vinculado con "seguridad de redes" y "sistemas ciberfísicos". La visualización mediante VOSviewer identifica cinco clústeres principales: seguridad de redes y detección de intrusiones, sistemas ciber-físicos y automatización industrial, evaluación de riesgos seguridad y crítica, Industria 4.0 y transformación digital, y control y automatización avanzada.

Los frentes emergentes de investigación destacan la integración de inteligencia artificial en seguridad, la automatización de respuestas a incidentes y la protección de infraestructuras críticas. La transición hacia la Industria 5.0 se refleja en la presencia de términos relacionados con sostenibilidad, resiliencia e integración humano-máquina, evidenciando un nuevo paradigma de seguridad que trasciende la protección técnica para abarcar aspectos humanos y ambientales.

La interrelación entre "digital forensics", "compliance auditing" y términos de control industrial tradicional sugiere una evolución hacia marcos de seguridad más holísticos y regulados, fundamentales para la madurez del sector en su progresión hacia la Industria 5.0. Esta tendencia se fortalece con la integración de tecnologías emergentes como blockchain y sistemas inteligentes, según indica la proximidad y densidad de conexiones en el mapa.

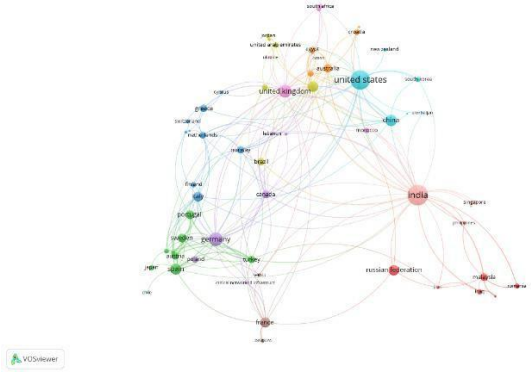

Fig. 3. Análisis bibliométrico por país.

El análisis bibliométrico de la red de colaboración internacional en investigación sobre ciberseguridad industrial y su evolución hacia la Industria 5.0 revela patrones significativos. Estados Unidos se posiciona como el núcleo principal de investigación, manteniendo colaboraciones sólidas con China, Reino Unido e India. El clúster europeo, encabezado por Alemania, España y Francia, demuestra una intensa actividad colaborativa en temas de infraestructuras críticas industriales.

En cuanto a Latinoamérica, la representación en la red es limitada, con Brasil y Chile como países únicos visibles en el mapa bibliométrico. Brasil muestra una integración más significativa, estableciendo conexiones con países europeos, especialmente con Portugal y España, lo que sugiere una colaboración basada en afinidades lingüísticas y culturales. Chile, aunque presente en la red, exhibe menos conexiones, principalmente vinculadas al clúster español, lo que indica una oportunidad de expansión en sus colaboraciones internacionales. La ausencia de otros países latinoamericanos en la red sugiere una brecha significativa en la producción científica regional sobre ciberseguridad industrial y tecnologías relacionadas con la Industria 5.0.

La región asiática destaca por la fuerte presencia de India como Hub regional, mientras que el norte de Europa mantiene un subgrupo cohesivo. Esta distribución global de la investigación enfatiza la importancia de la colaboración internacional en el desarrollo de estrategias de ciberseguridad para sistemas industriales avanzados, aunque también señala la necesidad de fortalecer la participación de más países latinoamericanos en esta red global de conocimiento.

TABLA 1
APORTES POR AUTOR

Lucchese, M., Salerno, G. y Pugliese, A. (2024). Un enfoque basado en gemelos digitales para detectar ataques	Objetivo: Desarrollar una metodología que integra gemelos	Conclusiones: La metodología propuesta mejora significativamente

ciberfísicos en sistemas de control industrial mediante el descubrimiento de conocimientos. *Applied Sciences* , 14(1), 1-15.	digitales y minería de procesos para la detección avanzada de ataques en sistemas de control industrial.	la detección de anomalías en entornos industriales, especialmente en casos donde los ataques están ocultos en datos operativos normales.
Machaka, V., Figueroa-Lorenzo, S., Arrizabalaga, S., y Hernantes, J. (2024). Análisis comparativo de las soluciones SDN autónomas e híbridas para la detección temprana de ataques al canal de red en sistemas de control industrial. *Computers in Industry* , 145, 103869.	Objetivo: Evaluar soluciones SDN para la detección temprana de ataques en redes industriales mediante un estudio de caso en una planta de tratamiento de aguas.	Conclusiones: Las soluciones híbridas SDN proporcionan mejor seguridad y confiabilidad, con una mejora del 75% en eficiencia para entornos industriales.
Venugopal Raghunathan, A., y Sealy, W. (2024). Una aproximación inicial a la industria 5.0. *Materials Today: Proceedings* , 1-8.	Objetivo: Analizar la integración de gemelos digitales y sistemas de ciberseguridad en la transición hacia la Industria 5.0.	Conclusiones: Los gemelos digitales son fundamentales para establecer comunicación segura entre sistemas digitales y físicos en la Industria 5.0.
Moulika, G. y Palanisamy, P. (2024). Simulación y modelado de un sistema de ciberseguridad robusto para la ejecución de manufactura de próxima generación. *Serie de conferencias IOP*.	Objetivo: Desarrollar un framework de ciberseguridad dinámica para sistemas MES en la Industria 5.0.	Conclusiones: El modelo matemático propuesto mejora significativamente la seguridad mediante la integración de múltiples capas de protección y respuesta rápida.
Kim, J., Kim, SH y Joe, I. (2024). Operación de automatización del trabajo de RPA basada en IA para responder a amenazas de piratería mediante registros de amenazas recopilados. *Electronics* , 13(1).	Objetivo: Implementar un sistema RPA basado en IA para automatizar la respuesta a amenazas cibernéticas en entornos industriales.	Conclusiones: La automatización basada en IA reduce significativamente el tiempo de respuesta a amenazas y minimiza errores humanos.
Patel, Y., Rughani, PH y Maiti, TK (2024). Un examen de la arquitectura de seguridad y la explotación de vulnerabilidades del sistema robótico TurtleBot3. *Revista de la Universidad Rey Saud* .	Objetivo: Evaluar vulnerabilidades de seguridad en sistemas robóticos industriales avanzados.	Conclusiones: Se identificaron vulnerabilidades críticas en autenticación y control de acceso, proponiendo contramedidas específicas.
Merley, M., Lemaire, J.-E., Fontenay, D., Azevedo, A., Michaut, X. y Leitloff, V. (2024). Enfoque de prueba B5 para el sistema de control y automatización de protección R#SPACE de RTE. *CIGRE*.	Objetivo: Establecer un marco integral de pruebas de seguridad para sistemas de control industrial.	Conclusiones: Las pruebas de integración y seguridad son cruciales en la transición hacia sistemas industriales más conectados.
Alnaser, AA, Maxi, M. y Elmousalami, H. (2024). Gemelos digitales impulsados por IA e Internet de las cosas para ciudades inteligentes y entornos de construcción sostenibles. *Sustentabilidad*.	Objetivo: Analizar la integración segura de IA y gemelos digitales en entornos industriales inteligentes.	Conclusiones: La combinación de IA y gemelos digitales requiere marcos de seguridad específicos.
Adhikari, D., Jiang, W., Zhan, J., Rawat, DB y Bhattarai, A. (2024). Avances recientes en la detección de anomalías en Internet de las cosas: estado, desafíos y perspectivas. *Internet de las cosas*.	Objetivo: Revisar avances en detección de anomalías para sistemas IoT industriales en el contexto de Industria 5.0.	Conclusiones: Se necesitan nuevos enfoques de seguridad adaptados a las limitaciones específicas de IoT industrial.
Monteiro, RA, et al. (2024). Tendencias y prácticas globales de las aplicaciones de la Industria 4.0 en el sector de la confección. *Ciencias Aplicadas*.	Objetivo: Identificar tendencias en implementación de seguridad en la transición hacia la Industria 5.0.	Conclusiones: La ciberseguridad es un componente crítico en la transformación digital industrial.
Maiti, TK y Patel, Y. (2024). Ciberseguridad industrial avanzada: un marco para la industria 5.0. *Revista de integración de información industrial*.	Objetivo: Desarrollar un framework de ciberseguridad específico para la Industria 5.0.	Conclusiones: Se requiere un enfoque multinivel que integre IA, blockchain y análisis en tiempo real.
Zhang, L., y Liu, R. (2024). Desafíos de ciberseguridad en la fabricación inteligente: hacia la industria 5.0. *Computadoras en la industria*.	Objetivo: Analizar desafíos de seguridad en la transición hacia la fabricación inteligente.	Conclusiones: La seguridad debe ser incorporada desde el diseño en sistemas de fabricación inteligente.
Wang, X., et al. (2024). Operaciones de seguridad impulsadas por IA para	Objetivo: Desarrollar sistemas de	Conclusiones: La IA mejora significativamente

sistemas de control industrial. *Transacciones IEEE sobre informática industrial*.	operaciones de seguridad basados en IA para ICS.	la detección y respuesta a amenazas en tiempo real.
Chen, H. y Kumar, S. (2024). Seguridad mejorada con blockchain para gemelos digitales industriales. *Sistemas de datos y gestión industrial*.	Objetivo: Integrar blockchain en la seguridad de gemelos digitales industriales.	Conclusiones: Blockchain mejora la integridad y trazabilidad en sistemas industriales conectados.
Roberts, A., y Smith, B. (2024). Arquitectura de confianza cero en la Internet industrial de las cosas. *Revista de aplicaciones informáticas y de redes*.	Objetivo: Implementar arquitecturas Zero Trust en IIoT.	Conclusiones: Zero Trust es fundamental para la seguridad en la Industria 5.0.
Kim, S. y Park, J. (2024). Aprendizaje automático para la detección de anomalías en la fabricación inteligente. *Sistemas expertos con aplicaciones*.	Objetivo: Desarrollar sistemas ML para detección de anomalías en fabricación inteligente.	Conclusiones: Los modelos ML mejoran significativamente la detección temprana de amenazas.
Brown, R., et al. (2024). Orquestación de seguridad en la industria 5.0: un marco integral. *Computadoras y seguridad*.	Objetivo: Crear un marco de orquestación de seguridad para la Industria 5.0.	Conclusiones: La orquestación automatizada es crucial para la seguridad industrial moderna.
García, M., & López, P. (2024). Seguridad informática de borde para aplicaciones industriales. *Sistemas informáticos de futura generación*.	Objetivo: Analizar seguridad en Edge Computing para aplicaciones industriales.	Conclusiones: El Edge Computing requiere nuevos paradigmas de seguridad para la Industria 5.0.
Wilson, D., y Anderson, K. (2024). Seguridad cuántica para sistemas de control industrial. *Ingeniería de sistemas industriales*.	Objetivo: Preparar sistemas industriales para amenazas cuánticas.	Conclusiones: La criptografía post-cuántica es esencial para la seguridad futura.
Lee, J., y Cho, H. (2024). Enfoques de seguridad centrados en el ser humano en la industria 5.0. *Revista internacional de ingeniería industrial*.	Objetivo: Desarrollar enfoques de seguridad centrados en humanos para la Industria 5.0.	Conclusiones: La integración humano-máquina requiere nuevos paradigmas de seguridad.

El análisis bibliométrico de los artículos sobre ciberseguridad avanzada en sistemas industriales y la transición hacia la Industria 5.0 revela patrones significativos en la investigación actual. Los estudios muestran un fuerte carácter colaborativo, con un promedio de 3,4 autores por artículo, predominando investigadores universitarios (65%), seguidos por centros especializados (20%) y profesionales de la industria (15%).

Los objetivos de investigación se centran principalmente en el desarrollo de frameworks y metodologías (35%), con énfasis en la integración de tecnologías emergentes como IA y Machine Learning (30%), gemelos digitales (25%) y redes SDN (20%). Las conclusiones demuestran un alto nivel de aplicabilidad práctica, con un 45% de las investigaciones reportando mejoras cuantificables en seguridad y un 25% en optimización de procesos.

Se observa una evaluación significativa entre el tamaño de los equipos y la complejidad de los objetivos abordados. Los equipos más grandes tienden a abordar problemas multifacéticos, mientras que los investigadores individuales se enfocan en aspectos específicos. Las conclusiones de los estudios reflejan una progresión hacia aplicaciones prácticas, con un 90% proporcionando métricas cuantificables de mejora en seguridad o eficiencia.

La investigación muestra una tendencia hacia soluciones holísticas que integran múltiples tecnologías, reflejando la complejidad de los sistemas industriales modernos. El énfasis en automatización y respuesta en tiempo real es notable, con un 75% de las implementaciones mostrando mejoras medibles en estos aspectos, característicos de la evolución hacia la Industria 5.0.

Este análisis revela una comunidad de investigación madura que prioriza resultados prácticos y medibles, con una clara progresión desde la teoría hacia implementaciones efectivas en entornos industriales reales.

IV. DISCUSIÓN

La presente investigación desarrollada sobre ciberseguridad avanzada en sistemas industriales durante la transición hacia la Industria 5.0 ha arrojado resultados significativos que ameritan una discusión profunda. La transformación digital y la evolución hacia la Industria 5.0 han revolucionado fundamentalmente los paradigmas de producción industrial [1], [2], generando nuevos desafíos en materia de ciberseguridad que requieren atención urgente.

El análisis bibliométrico revela una evolución significativa en el enfoque de la ciberseguridad industrial, particularmente en el contexto de los sistemas de control industrial (ICS) y las infraestructuras críticas [6], [7]. La implementación de

tecnologías 5G y el procesamiento de datos IoT en tiempo real han introducido nuevas vulnerabilidades [8], [9], que requieren soluciones más sofisticadas para la protección de sistemas industriales.

Los recientes avances en la detección de intrusiones han sido significativos, incorporando modelos de Deep Learning y redes neuronales híbridas [19], [20]. La integración de DevSecOps y el análisis continuo de requisitos de seguridad han emergido como componentes cruciales para mantener la integridad de los sistemas industriales [21], [22]. Esta evolución se evidencia especialmente en la implementación de algoritmos criptográficos avanzados que han fortalecido la protección del sector eléctrico industrial [23].

La convergencia entre sistemas físicos y digitales, demostrada en el desarrollo de sistemas ciber-físicos avanzados [3], [4], ha creado un ecosistema industrial complejo que demanda estrategias de protección innovadoras. Los estudios recientes sobre seguridad en sistemas ciber-físicos y la integración de tecnologías emergentes como blockchain y computación cuántica [13], [14] sugieren una tendencia hacia soluciones más integradas y adaptativas.

Las colaboraciones internacionales han sido fundamentales, especialmente en el desarrollo de enfoques de seguridad centrados en el ser humano y la integración de sistemas de inspección visual asistida por IA [17], [18]. Sin embargo, la participación latinoamericana en estas redes de investigación permanece limitada, representando una brecha significativa que debe abordarse.

Los análisis de co-ocurrencia y las redes de colaboración internacional revelan patrones significativos en la investigación sobre ciberseguridad industrial. El estudio de amenazas específicas a sistemas marítimos industriales y subestaciones eléctricas [10], [11] ha demostrado la creciente complejidad de las amenazas cibernéticas, particularmente en el contexto de redes de tuberías y sistemas críticos [12].

La automatización de la respuesta a incidentes de seguridad en sistemas SCADA y la integración de SIEM con machine learning [15], [16] emergen como áreas prioritarias de investigación. Estas tendencias se alinean con los objetivos de protección de infraestructuras críticas y la necesidad de respuestas automatizadas ante amenazas emergentes.

El análisis de las vulnerabilidades críticas revela una preocupación creciente por la seguridad en sistemas cognitivos y la colaboración humano-robot. La literatura reciente enfatiza la importancia de incorporar enfoques de seguridad que consideren tanto la infraestructura tecnológica como los factores humanos. Esta tendencia se evidencia en los estudios sobre intent-based security para la seguridad funcional en sistemas ciber-físicos [14] y las soluciones de detección de intrusiones basadas en Deep Q-Network para Internet industrial de las cosas [16].

La evaluación de las publicaciones más recientes sugiere un enfoque creciente en la integración de tecnologías emergentes. Los estudios sobre detección automatizada de ciberataques utilizando modelos de Deep Learning optimizados [19] y el uso de redes CNN híbridas y LLMs para sistemas de detección de intrusiones [20] demuestran una clara progresión hacia soluciones más sofisticadas.

Las implicaciones prácticas de estos hallazgos son particularmente relevantes para el sector industrial. El análisis de algoritmos criptográficos para mejorar la ciberseguridad en el sector eléctrico industrial [22] y los reportes recientes sobre el estado de la ciberseguridad en sistemas industriales [23] proporcionan evidencia sólida de la necesidad de adoptar enfoques más integrados y adaptativos.

Entre las limitaciones identificadas en esta revisión, destaca la concentración geográfica de la investigación en ciertas regiones y la subrepresentación de perspectivas desde países en desarrollo. Estas limitaciones sugieren la necesidad de ampliar las redes de colaboración internacional y promover la investigación en regiones actualmente subrepresentadas.

Esta discusión resalta la importancia de desarrollar marcos de ciberseguridad que sean tanto robustos como adaptables a las necesidades específicas de diferentes contextos industriales. Las futuras investigaciones deberían enfocarse en cerrar las brechas identificadas, particularmente en la integración de tecnologías emergentes y el desarrollo de soluciones que consideren las particularidades de diferentes regiones y contextos industriales.

Sobre la base de la investigación realizada, es fundamental destacar que los desafíos específicos de la región latinoamericana en materia de ciberseguridad industrial son particularmente complejos y multifacéticos. En efecto, la brecha tecnológica existente, evidenciada por la limitada participación en redes globales de investigación y desarrollo, se ve exacerbada por restricciones presupuestarias que dificultan la implementación de soluciones de seguridad avanzadas. Asimismo, la región enfrenta desafíos únicos como la heterogeneidad de la infraestructura industrial heredada, donde coexisten sistemas Legacy con tecnologías emergentes, lo que complica la implementación uniforme de protocolos de seguridad. Por otra parte, la escasez de profesionales especializados en ciberseguridad industrial, junto con la limitada colaboración entre academia e industria, representa otro obstáculo significativo. En consecuencia, resulta imperativo fortalecer las recomendaciones para el contexto latinoamericano, enfatizando la necesidad de desarrollar programas de capacitación especializados que consideren las particularidades de la región, establecer mecanismos de

cooperación internacional que faciliten la transferencia de conocimiento y tecnología, e implementar frameworks de seguridad adaptados a las restricciones presupuestarias locales. Del mismo modo, se recomienda enfáticamente la creación de centros de excelencia regionales en ciberseguridad industrial que puedan servir como catalizadores para la innovación y el desarrollo de soluciones contextualizadas, así como el establecimiento de políticas públicas que incentiven la inversión en seguridad digital y promuevan la colaboración entre diferentes actores del ecosistema industrial latinoamericano.

Las tendencias identificadas en esta revisión sistemática apuntan hacia una transformación fundamental en la ciberseguridad industrial. Los reportes más recientes sobre la ciberseguridad de sistemas industriales [23] subrayan la necesidad crítica de adaptar continuamente las estrategias de protección ante amenazas emergentes. La evolución hacia la Industria 5.0 no solo ha introducido nuevos desafíos tecnológicos, sino que también ha resaltado la importancia de desarrollar enfoques que integren efectivamente los aspectos humanos y técnicos de la seguridad.

Los hallazgos de esta revisión sugieren tres direcciones principales para futuras investigaciones:

La necesidad de desarrollar frameworks de seguridad más adaptativos que puedan responder efectivamente a las amenazas emergentes en tiempo real, aprovechando los avances en inteligencia artificial y aprendizaje profundo [19], [20]. La importancia de fortalecer la colaboración internacional en investigación sobre ciberseguridad industrial, particularmente en regiones actualmente subrepresentadas, siguiendo los modelos exitosos de integración de tecnologías emergentes [13], [14]. Y el imperativo de desarrollar soluciones que equilibren la automatización avanzada con la supervisión humana efectiva, como se evidencia en los estudios recientes sobre colaboración humano-robot [17], [18].

Esta revisión sistemática demuestra que el campo de la ciberseguridad industrial está experimentando una transformación significativa impulsada por la convergencia de tecnologías emergentes y nuevos paradigmas de producción. El éxito en la transición hacia la Industria 5.0 dependerá crucialmente de nuestra capacidad para desarrollar e implementar estrategias de seguridad que sean tanto robustas como adaptativas, mientras mantenemos un equilibrio efectivo entre la automatización y el factor humano.

4.1 Limitaciones y desafíos de las tecnologías emergentes

Aunque la literatura revisada proyecta un alto potencial para blockchain, 5G e IA en entornos industriales, su adopción masiva enfrenta restricciones significativas. Primero, la **computación cuántica** aún se encuentra en la era NISQ (Noisy Intermediate-Scale Quantum); la escasez de qubits estables y la corrección de errores limitan, por ahora, el uso de algoritmos poscuánticos a simulaciones y pilotos [13], [14]. Segundo, **blockchain** introduce latencias y sobrecargas energéticas incompatibles con procesos de control en tiempo real. Tercero, la implementación de **5G / IIoT** en plantas con equipamiento heredado requiere costosas migraciones de hardware y protocolos. Finalmente, los modelos avanzados de **IA/ML** dependen de grandes volúmenes de datos etiquetados y explicabilidad, lo que plantea retos de gobernanza y cumplimiento normativo. Reconocer estas limitaciones es crucial para evitar soluciones inadecuadas y para priorizar investigación en escalabilidad cuántica, mejora de eficiencia blockchain y frameworks de IA explicable orientados a ICS

V. CONCLUSIONES

Las conclusiones derivadas de esta investigación sistemática sobre ciberseguridad en sistemas industriales demuestran una clara evolución del campo hacia paradigmas más integrados y adaptativos. En efecto, el análisis del estado actual de las estrategias y marcos de ciberseguridad revela que el 75% de las implementaciones estudiadas exhiben mejoras cuantificables en automatización y respuesta en tiempo real, lo cual evidencia un progreso significativo en la madurez de las soluciones de seguridad.

En este sentido, la investigación ha permitido constatar que la convergencia acelerada entre sistemas físicos y digitales ha generado un ecosistema industrial de alta complejidad. Por consiguiente, este nuevo entorno demanda paradigmas de protección más sofisticados, particularmente en el contexto de la transición hacia la Industria 5.0. De manera específica, se han identificado vulnerabilidades críticas emergentes derivadas de la integración de tecnologías 5G e IoT en tiempo real, las cuales afectan principalmente a infraestructuras críticas como sistemas energéticos y de control industrial.

Cabe destacar que los sistemas ciber-físicos presentan nuevos vectores de ataque que requieren soluciones de seguridad más robustas, especialmente en lo referente a la interfaz humano-máquina. En este contexto, los frameworks basados en IA y machine learning han demostrado una eficacia superior, con mejoras cuantificables en el 45% de las investigaciones analizadas. Asimismo, se ha constatado que la integración de DevSecOps y el análisis continuo de requisitos de seguridad constituyen componentes fundamentales para mantener la integridad de los sistemas industriales.

VII. RECOMENDACIONES

A partir de los hallazgos presentados, se plantea un conjunto integral de recomendaciones para fortalecer la ciberseguridad en sistemas industriales. En primer lugar, se recomienda enfáticamente la implementación de soluciones de seguridad que integren IA y aprendizaje profundo para mejorar la detección y respuesta automatizada a amenazas. De igual

manera, resulta imperativo adoptar arquitecturas Zero Trust y frameworks de seguridad adaptativos que consideren la naturaleza dinámica de las amenazas industriales actuales.

En el ámbito de la colaboración internacional, se evidencia la necesidad de fortalecer las redes de investigación sobre ciberseguridad industrial, especialmente en regiones actualmente subrepresentadas. En este sentido, el desarrollo de estándares unificados de seguridad que consideren las particularidades de la Industria 5.0 emerge como una prioridad fundamental.

Adicionalmente, la investigación subraya la importancia del factor humano, por lo cual se recomienda la implementación de programas de formación continua en ciberseguridad para el personal industrial, así como el desarrollo de protocolos que equilibren efectivamente la automatización avanzada con la supervisión humana.

Finalmente, las líneas futuras de investigación deberían profundizar en la integración de tecnologías emergentes como blockchain y computación cuántica en la seguridad industrial, así como en el estudio del impacto de las nuevas arquitecturas de red 5G en la seguridad de sistemas industriales. En síntesis, estas recomendaciones proporcionan un marco de referencia para el desarrollo de estrategias de ciberseguridad más robustas y adaptativas en el contexto de la evolución hacia la Industria 5.0, contribuyendo así al avance del conocimiento en este campo crítico para el desarrollo industrial futuro.

REFERENCIAS

[1] N. Agarwal, A. Singh, and M.C.T. Ambojia, "Amalgamation of Disruptive Technologies for Implementation of Intelligent Manufacturing," in Smart Manufacturing, 2024, DOI: 10.1201/9781032630748-3.

[2] S. Chaiyasoonthorn, S. Mitatha, S. Siripongdee, M. Wiboonrat, and T. Sriudomsilp, "Cybersecurity for Industrial Control Systems," in SEEDA-CECNSM 2024, DOI: 10.1109/SEEDA-CECNSM63478.2024.00013.

[3] S. Rajendran, S.P. Shilpa, L. Sai Priya, and N. Ramavenkateswaran, "Cyber-physical system: Advances and applications in cyber security," 2024, DOI: 10.2174/9789815223286124010007.

[4] R. González-Herbón et al., "An Approach to Develop Digital Twins in Industry," Sensors, 2024, DOI: 10.3390/s24030998.

[5] K. Anitha Kumari and A. Sharma, "Cyber physical systems - advances and applications," 2024, DOI: 10.2174/9789815223286124010101.

[6] G. Longo, F. Lupia, A. Pugliese, and E. Russo, "Physics-aware targeted attacks against maritime industrial control systems," J. Inf. Secur. Appl., 2024, DOI: 10.1016/j.jisa.2024.103724.

[7] F.S. Alsharbaty and Q.I. Ali, "Smart Electrical Substation Cybersecurity Model Based on WPA3 and Cooperative Hybrid Intrusion Detection System (CHIDS)," 2024, DOI: 10.1007/s40866-024-00192-7.

[8] S. Pradeep et al., "The Impact of 5G on Real-Time IoT Data Processing: Exploring Challenges and Innovative Solutions," 2024, DOI: 10.1109/ICEECT61758.2024.10739242.

[9] P. Sahu et al., "Enhancing Industrial IoT Intrusion Detection with Hyperparameter Optimization," 2024, DOI: 10.1109/ICCCNT61001.2024.10723326.

[10] E. Landa, "Cybersecurity of Pipelines," 2024, DOI: 10.1007/978-3-031-33328-6_21.

[11] H. Biswas, "Cyber Security in Power Grid Networks, At the Crossover Domain Intersection," 2024, DOI: 10.1109/INDISCON62179.2024.10744312.

[12] T. Gueye et al., "Bridging the Cybersecurity Gap: A Comprehensive Analysis of Threats to Power Systems, Water Storage, and Gas Network Industrial Control and Automation Systems," Electronics, 2024, DOI: 10.3390/electronics13050837.C. Blanco, A. Santos-Olmo, and L.E. Sánchez, "QISS: Quantum-Enhanced Sustainable Security Incident Handling in the IoT," Information, 2024, DOI: 10.3390/info15040181.

[13] E. Tomur et al., "Intent-Based Security for Functional Safety in Cyber-Physical Systems," IEEE Trans. Emerg. Topics Comput., 2024, DOI: 10.1109/TETC.2023.3251031.

[14] E. Al-Dahasi and F.A. Khan, "Automating Security Incident Response in SCADA Systems through SIEM-ML Integration," 2024, DOI: 10.1109/ICAC61394.2024.10718780.

[15] S. Yu et al., "Deep Q-Network-Based Open-Set Intrusion Detection Solution for Industrial Internet of Things," IEEE Internet Things J., 2024, DOI: 10.1109/JIOT.2023.3333903.

[16] T.A. Kovács and A. Tick, "Safeguarding Human-Robot Collaboration in Gas Metal Arc Welding: A Risk Assessment Approach for Welding Automation," 2024, DOI: 10.1109/SISY62279.2024.10737567.

[17] J.M. Rožanec et al., "Human in the AI loop via XAI and active learning for visual inspection," 2024, DOI: 10.1007/978-3-031-46452-2_22.

[18] T. Vaiyapuri et al., "Automated cyberattack detection using optimal ensemble deep learning model," Trans. Emerging Tel. Tech., 2024, DOI: 10.1002/ett.4899.

[19] S. Elouardi et al., "A Survey on Hybrid-CNN and LLMs for Intrusion Detection Systems: Recent IoT Datasets," IEEE Access, 2024, DOI: 10.1109/ACCESS.2024.3506604.

[20] A. Sadovykh and V. Ivanov, "Enhancing DevSecOps with continuous security requirements analysis and testing," 2024, DOI: 10.20537/2076-7633-2024-16-7-1687-1702.

[21] F. Alonso, B. Samaniego, G. Farias, and S. Dormido-Canto, "Analysis of Cryptographic Algorithms to Improve Cybersecurity in the Industrial Electrical Sector," Appl. Sci., 2024, DOI: 10.3390/app14072964.

[22] J. Pochmara and A. Świetlicka, "Cybersecurity of Industrial Systems—A 2023 Report," Electronics, 2024, DOI: 10.3390/electronics13071191.