Journal of Multidisciplinary Novel Journeys & Explorations

ISSN: 3091-1990

Vol. 4 Núm. 1 (2026)

EDITORIAL JOGB

JMNJE V4. N1. 059

Protección de infraestructuras críticas de telecomunicaciones mediante inteligencia artificial frente a amenazas cibernéticas emergentes

Protecting critical telecom infrastructure with artificial intelligence from emerging cyber threats

Autores:
Kevin Alexis García Pérez
Instituto Superior Tecnológico "Centro Tecnológico Naval"
Salinas – Ecuador
kevin.garcia@cetnav.armada.mil.ec
https://orcid.org/0009-0006-1663-2258

Josseph Yaakob Catagua Cobos
Instituto Superior Tecnológico "Centro Tecnológico Naval"
Salinas – Ecuador
jcataguac@armada.mil.ec
https://orcid.org/0009-0004-0857-5762

Autor de correspondencia: *Kevin Alexis García Pérez*, kevin.garcia@cetnav.armada.mil.ec

Recepción: 26-abril-2026 **Aceptación:** 19-mayo-2026 **Publicación:** 17-junio-2026

Cómo citar este artículo:
García Pérez, K. A. ., & Catagua Cobos, J. Y. . (2026). Protección de infraestructuras críticas de telecomunicaciones mediante inteligencia artificial frente a amenazas cibernéticas emergentes. *Journal of Multidisciplinary Novel Journeys & Explorations*, *4*(1), 1-25. https://doi.org/10.63688/scvrpj92

© 2026; Los autores. Este es un artículo en acceso abierto, distribuido bajo los términos de una licencia Creative Commons (https://creativecommons.org/licenses/by/4.0) que permite el uso, distribución y reproducción en cualquier medio, siempre que la obra original sea correctamente citada.

ISSN: 3091-1990

Vol. 4 Núm. 1 (2026)

RESUMEN

En el contexto de la transformación digital y la creciente interconexión de los sistemas de comunicación, la protección de las infraestructuras críticas de telecomunicaciones se ha consolidado como un reto estratégico para asegurar la continuidad operativa, la seguridad de la información y la resiliencia de los servicios esenciales. El aumento de amenazas cibernéticas emergentes, caracterizadas por su alto nivel de sofisticación, automatización y capacidad de adaptación, demanda la adopción de enfoques innovadores que superen las limitaciones de los modelos tradicionales de defensa. En este sentido, el presente estudio analiza la aplicación de la Inteligencia Artificial como herramienta estratégica para la protección de dichas infraestructuras frente a amenazas cibernéticas emergentes, evaluando técnicas avanzadas de detección, prevención y respuesta automatizada ante incidentes de seguridad, con el fin de fortalecer la resiliencia operativa, optimizar la gestión de riesgos cibernéticos y garantizar la disponibilidad, integridad y confidencialidad de los sistemas de comunicación en entornos digitales complejos y dinámicos. La investigación se desarrolló mediante una revisión sistemática de la literatura, apoyada en el método PRISMA, lo que permitió recopilar, analizar y sintetizar evidencia científica relevante sobre la aplicación de la Inteligencia Artificial en la ciberseguridad de telecomunicaciones. Los hallazgos concluyen que estas infraestructuras son esenciales para la sociedad digital y que factores como la digitalización, las redes 5G y el Internet de las Cosas incrementan su exposición a riesgos, evidenciando la necesidad de fortalecer su protección mediante soluciones tecnológicas avanzadas.

Palabras clave: inteligencia artificial, ciberseguridad, infraestructuras críticas de telecomunicaciones, amenazas cibernéticas emergentes, resiliencia digital.

ABSTRACT

In the context of digital transformation and the increasing interconnection of communication systems, protecting critical telecommunications infrastructure has become a strategic challenge to ensure operational continuity, information security, and the resilience of essential services. The rise in emerging cyber threats, characterized by their high level of sophistication, automation, and adaptability, demands the adoption of innovative approaches that overcome the limitations of traditional defense models. In this regard, this study analyzes the application of Artificial Intelligence as a strategic tool for protecting such infrastructure against emerging cyber threats. It evaluates advanced techniques for detection, prevention, and automated response to security incidents, aiming to strengthen operational resilience, optimize cyber risk management, and guarantee the availability, integrity, and confidentiality of communication systems in complex and dynamic digital environments. The research was conducted through a systematic literature review, supported by the PRISMA methodology, which allowed for the collection, analysis, and synthesis of relevant scientific evidence on the application of Artificial Intelligence in telecommunications cybersecurity. The findings conclude that these infrastructures are essential for the digital society and that factors such as digitization, 5G networks, and the Internet of Things increase their exposure to risks, highlighting the need to strengthen their protection through advanced technological solutions.

Keywords: artificial intelligence, cybersecurity, critical telecommunications infrastructure, emerging cyber threats, digital resilience.

Doi: https://doi.org/10.63688/scvrpj92

ISSN: 3091-1990
Vol. 4 Núm. 1 (2026)

1. INTRODUCCIÓN

En el contexto de la transformación digital y la creciente interconexión de los sistemas de comunicación, la protección de las infraestructuras críticas de telecomunicaciones se ha convertido en un desafío estratégico para garantizar la continuidad operativa, la seguridad de la información y la resiliencia de los servicios esenciales. El incremento de amenazas cibernéticas emergentes, caracterizadas por su sofisticación, automatización y capacidad de adaptación, exige la implementación de enfoques innovadores que superen los modelos tradicionales de defensa. En este escenario, la Inteligencia Artificial (IA) adquiere una relevancia significativa al proporcionar mecanismos avanzados para la detección temprana de anomalías, el análisis predictivo de riesgos, la identificación de patrones de comportamiento malicioso y la respuesta automatizada ante incidentes de seguridad.

Los antecedentes de la protección de infraestructuras críticas de telecomunicaciones se remontan al desarrollo de mecanismos tradicionales de ciberseguridad basados en firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y protocolos de gestión de riesgos orientados a salvaguardar la continuidad de los servicios de comunicación. Sin embargo, la evolución de las tecnologías digitales, la expansión de redes de alta velocidad, la adopción de entornos de computación en la nube, el Internet de las Cosas (IoT) y las redes 5G han incrementado significativamente la superficie de exposición a ciberataques cada vez más complejos y dinámicos.

La presente investigación se justifica por la necesidad de fortalecer la seguridad y resiliencia de las infraestructuras críticas de telecomunicaciones frente al crecimiento exponencial de las amenazas cibernéticas emergentes, las cuales representan un riesgo significativo para la continuidad de los servicios esenciales, la protección de la información y la estabilidad de los entornos digitales. Desde una perspectiva académica, el estudio contribuye a la generación y actualización de conocimientos relacionados con la aplicación de la Inteligencia Artificial en el ámbito de la ciberseguridad, promoviendo el análisis de modelos innovadores para la detección, prevención y mitigación de ataques informáticos.

El objetivo de este estudio es analizar la aplicación de la Inteligencia Artificial como herramienta estratégica para la protección de infraestructuras críticas de telecomunicaciones frente a amenazas cibernéticas emergentes, mediante la evaluación de técnicas avanzadas de

Doi: https://doi.org/10.63688/scvrpj92

detección, prevención y respuesta automatizada ante incidentes de seguridad, con el propósito de fortalecer la resiliencia operativa, optimizar la gestión de riesgos cibernéticos y garantizar la disponibilidad, integridad y confidencialidad de los sistemas y servicios de comunicación en entornos digitales altamente dinámicos y complejos.

Tabla 1.

Identificación de las Variables de Investigación

Tipo de Variable	Variable	Definición Conceptual
Variable Independiente	**Inteligencia Artificial aplicada a la ciberseguridad**	Conjunto de tecnologías, algoritmos y técnicas computacionales basadas en Inteligencia Artificial que permiten analizar grandes volúmenes de datos, detectar patrones anómalos, predecir amenazas y automatizar procesos de protección en entornos de telecomunicaciones.
Variable Dependiente	**Protección de Infraestructuras Críticas de Telecomunicaciones frente a Amenazas Cibernéticas Emergentes**	Capacidad de los sistemas y redes de telecomunicaciones para prevenir, detectar, mitigar y responder eficazmente a amenazas cibernéticas emergentes, garantizando la disponibilidad, integridad, confidencialidad y resiliencia de los servicios críticos.

Fuente: Elaboración Propia

Basándonos en la investigación, formulamos las siguientes preguntas de investigación: ¿Cómo contribuye la aplicación de la Inteligencia Artificial a la protección de las infraestructuras críticas de telecomunicaciones frente a amenazas cibernéticas emergentes? ¿En qué medida la utilización de Inteligencia Artificial contribuye al incremento de la resiliencia operativa de las infraestructuras críticas frente a ciberataques avanzados?

Marco teórico

La protección de las infraestructuras críticas de telecomunicaciones fue reconocida como un elemento fundamental para garantizar la continuidad de los servicios esenciales y la seguridad de la información en entornos digitales cada vez más complejos. En este contexto, diversas investigaciones analizaron el impacto de las amenazas cibernéticas emergentes y

destacaron la necesidad de incorporar tecnologías avanzadas para fortalecer los mecanismos de defensa.

Infraestructuras Críticas de Telecomunicaciones

Las infraestructuras críticas de telecomunicaciones constituyen el conjunto de sistemas, redes, equipos y servicios tecnológicos que permiten la transmisión, el procesamiento y la distribución de información a través de diversos medios de comunicación. Según Henao (2021), estas infraestructuras desempeñan un papel esencial en el desarrollo de las actividades económicas, gubernamentales, educativas, sanitarias y sociales, debido a que garantizan la conectividad y el intercambio de datos en tiempo real.

Desde una perspectiva tecnológica y de ciberseguridad, las infraestructuras críticas de telecomunicaciones abarcan redes de comunicación fija y móvil, centros de datos, sistemas satelitales, plataformas de Internet, redes 5G y otros componentes que sustentan la conectividad global. En este sentido, Noll (2018) señala que la creciente digitalización y la interdependencia entre sistemas han incrementado la complejidad de su gestión, así como su nivel de exposición a riesgos operativos y amenazas cibernéticas cada vez más sofisticadas.

Importancia estratégica de las telecomunicaciones en la sociedad digital

Las telecomunicaciones constituyen un pilar estratégico de la sociedad digital contemporánea, ya que facilitan la conectividad, el intercambio de información y la comunicación en tiempo real entre personas, organizaciones e instituciones a nivel local y global. De acuerdo con Delgado (2026), su relevancia radica en que sustentan el funcionamiento de diversos sectores esenciales, entre ellos la educación, la salud, la administración pública, el comercio, la industria y los servicios financieros, permitiendo el acceso oportuno a recursos, conocimientos y plataformas digitales.

Desde una perspectiva económica y tecnológica, las telecomunicaciones desempeñan un papel determinante en los procesos de transformación digital y en la consolidación de ecosistemas inteligentes orientados a la innovación y a la gestión eficiente de la información. En este sentido Villa et al. (2025) sostienen que la evolución de tecnologías emergentes, como las redes 5G, la computación en la nube, el Internet de las Cosas (IoT) y la Inteligencia Artificial, ha incrementado significativamente la dependencia de infraestructuras de telecomunicaciones robustas, seguras y resilientes. Este escenario pone de manifiesto la

necesidad de fortalecer los mecanismos de protección de dichas infraestructuras frente a amenazas cibernéticas cada vez más complejas y sofisticadas.

Componentes principales de las infraestructuras de telecomunicaciones

Las infraestructuras críticas de telecomunicaciones fueron identificadas como elementos esenciales para garantizar la conectividad, el procesamiento de datos y la transmisión eficiente de la información en entornos digitales. En este contexto, Hernández (2025) destaca que las redes de comunicación, los centros de datos y los equipos de red constituyen la base tecnológica que posibilita el funcionamiento continuo y eficiente de los servicios de telecomunicaciones.

- **Redes de transmisión y comunicación:** Comprenden los medios físicos e inalámbricos que permiten el transporte de voz, datos y video entre diferentes puntos de una red. Incluyen tecnologías como fibra óptica, cables de cobre, enlaces de microondas, redes móviles (4G y 5G) y sistemas satelitales.
- **Equipos y dispositivos de red:** Incluyen los componentes tecnológicos encargados de dirigir, controlar y administrar el tráfico de información dentro de las redes de telecomunicaciones. Entre ellos se encuentran routers, switches, antenas, estaciones base, módems y sistemas de control de red.

Ciberseguridad en las Infraestructuras Críticas

La protección de infraestructuras críticas engloba el conjunto de estrategias, políticas, tecnologías y procedimientos orientados a garantizar la seguridad de los sistemas, redes y activos digitales que respaldan la prestación de servicios esenciales para la sociedad. Alves et al. (2025) destacan que estas infraestructuras comprenden sectores estratégicos como las telecomunicaciones, la energía, el transporte, la salud, las finanzas y la administración pública, cuya continuidad operativa resulta indispensable para preservar la estabilidad económica, el bienestar social y el normal funcionamiento de los Estados.

En el marco de la transformación digital, las infraestructuras críticas se encuentran expuestas a escenarios cada vez más complejos como consecuencia del aumento de la conectividad, la automatización de procesos y la creciente interdependencia tecnológica. Bajo esta perspectiva, Saldaña (2024) señala que dichas condiciones han favorecido una mayor exposición a amenazas cibernéticas avanzadas, entre las que sobresalen los ataques de

ransomware, las amenazas persistentes avanzadas (APT), los ataques distribuidos de denegación de servicio (DDoS) y las vulneraciones de información sensible.

Gestión de riesgos cibernéticos

La gestión de riesgos cibernéticos constituye un proceso sistemático orientado a la identificación, evaluación, control y monitoreo de las amenazas y vulnerabilidades que pueden comprometer los activos digitales, los sistemas de información y las infraestructuras tecnológicas de una organización. Mohamed et al. (2024) sostienen que su propósito principal es reducir la probabilidad de incidentes de seguridad y minimizar sus posibles impactos sobre la continuidad operativa, la integridad de los datos y la confidencialidad de la información.

En el contexto de las infraestructuras críticas de telecomunicaciones, la gestión de riesgos cibernéticos adquiere una importancia estratégica debido a la creciente sofisticación de las amenazas digitales y a la necesidad de garantizar la disponibilidad de servicios esenciales. En este escenario, Piña et al. (2025) señalan que la adopción de marcos de referencia internacionales, como ISO 27001, el NIST Cybersecurity Framework y otras buenas prácticas de seguridad, facilita la identificación de riesgos potenciales y respalda la toma de decisiones para su tratamiento efectivo.

Vulnerabilidades en redes y sistemas de telecomunicaciones

Las vulnerabilidades en redes y sistemas de telecomunicaciones corresponden a debilidades o fallas presentes en la infraestructura tecnológica, los protocolos de comunicación, las configuraciones de seguridad y los componentes de software y hardware que pueden ser aprovechadas por actores maliciosos para comprometer la disponibilidad, integridad y confidencialidad de los servicios. Solís et al. (2017) indican que estas vulnerabilidades pueden originarse por errores de diseño, configuraciones inadecuadas, software desactualizado, deficiencias en los mecanismos de autenticación o insuficientes controles de acceso.

Desde la perspectiva de la ciberseguridad, la identificación y gestión de vulnerabilidades constituyen procesos fundamentales para fortalecer la protección de las infraestructuras críticas de telecomunicaciones. Ruiz et al. (2021) destacan que el crecimiento de tecnologías emergentes, como las redes 5G, la computación en la nube, la virtualización de redes y el

Internet de las Cosas (IoT), ha ampliado significativamente la superficie de ataque, generando nuevos desafíos para los responsables de la seguridad digital.

Políticas y estándares internacionales de ciberseguridad

Las políticas y estándares internacionales de ciberseguridad constituyen marcos de referencia diseñados para establecer directrices, principios y buenas prácticas orientadas a la protección de los sistemas de información y a la gestión efectiva de los riesgos cibernéticos. En este sentido, Cardoso et al. (2021) señalan que estos instrumentos proporcionan lineamientos fundamentales para fortalecer la seguridad de los entornos digitales, promover una adecuada gobernanza de la información y mejorar la capacidad de respuesta frente a amenazas y vulnerabilidades emergentes.

- **ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI):** Su objetivo es establecer un marco de gestión que permita a las organizaciones proteger la confidencialidad, integridad y disponibilidad de la información mediante la identificación y tratamiento sistemático de riesgos.
- **NIST Cybersecurity Framework (CSF):** El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) constituye una referencia internacional para la gestión de riesgos cibernéticos.

Marcos normativos para la protección de infraestructuras críticas

Los marcos normativos para infraestructuras críticas comprenden el conjunto de leyes, regulaciones, políticas y estándares orientados a garantizar la seguridad, la continuidad operativa y la resiliencia de los sistemas considerados esenciales para el funcionamiento de un país. En este contexto, Morera et al. (2021) destacan que dichos marcos establecen lineamientos técnicos y organizacionales que guían a las instituciones públicas y privadas en la identificación de riesgos, la gestión de vulnerabilidades y la implementación de controles de seguridad.

En el ámbito de la ciberseguridad, los marcos normativos incorporan estándares y buenas prácticas reconocidos internacionalmente para mejorar la gestión de riesgos y la protección de infraestructuras críticas. Al respecto, Pasos et al. (2020) indican que estos marcos incluyen referencias a estándares como ISO/IEC 27001, ISO/IEC 27032, el NIST Cybersecurity Framework y diversas directivas adoptadas por organismos regionales e internacionales.

Amenazas Cibernéticas Emergentes

Las amenazas cibernéticas emergentes constituyen uno de los principales desafíos para la seguridad de las infraestructuras digitales en un entorno caracterizado por el crecimiento acelerado de la conectividad y la constante transformación tecnológica. Mattos et al. (2022) destacan que la evolución de los ecosistemas digitales ha propiciado la aparición de nuevas modalidades de ataque cada vez más sofisticadas, capaces de comprometer la disponibilidad, integridad y confidencialidad de la información.

- **Ransomware Avanzado:** Es una de las amenazas cibernéticas emergentes más peligrosas para las infraestructuras críticas de telecomunicaciones. Este tipo de malware cifra archivos, sistemas o bases de datos de una organización y exige el pago de un rescate para recuperar el acceso a la información.
- **Ataques Basados en Inteligencia Artificial:** representan una amenaza emergente debido a la capacidad de los ciberdelincuentes para utilizar algoritmos inteligentes que automatizan procesos de reconocimiento, explotación de vulnerabilidades y evasión de controles de seguridad.

Malware avanzado y ransomware

El malware avanzado comprende un conjunto de programas maliciosos diseñados para infiltrarse, comprometer o tomar el control de sistemas informáticos mediante técnicas sofisticadas que dificultan su detección y eliminación. En este sentido, Avilano (2023) explica que estas amenazas se diferencian del malware tradicional por incorporar mecanismos de evasión, cifrado, autoaprendizaje y propagación automatizada, lo que les permite adaptarse a distintos entornos tecnológicos y aumentar su capacidad de persistencia. Entre las manifestaciones más críticas del malware avanzado se encuentra el ransomware, una amenaza que ha experimentado una notable evolución en los últimos años. Yacout (2022) sostiene que esta modalidad se caracteriza por su capacidad para cifrar archivos, bases de datos e incluso sistemas completos, restringiendo el acceso legítimo a la información hasta que se efectúe el pago de un rescate.

Ataques distribuidos de denegación de servicio (DDoS)

Los ataques distribuidos de denegación de servicio (DDoS) constituyen una de las amenazas cibernéticas más significativas para las infraestructuras críticas de telecomunicaciones debido a su capacidad para afectar la disponibilidad y continuidad de los servicios tecnológicos. Rodríguez (2021) explica que estos ataques ocurren cuando un gran número de

dispositivos comprometidos, comúnmente denominados botnets, generan de forma simultánea un volumen masivo de solicitudes dirigidas a un servidor, red o plataforma digital con el propósito de saturar su capacidad de procesamiento y comunicación.

Desde la perspectiva de la ciberseguridad, los ataques DDoS representan un desafío cada vez más complejo debido a la evolución de las técnicas empleadas por los atacantes y al incremento constante de dispositivos conectados a Internet, especialmente aquellos vinculados al Internet de las Cosas (IoT). En este contexto, Vazifehdust (2020) destaca que la creciente sofisticación de estas amenazas ha impulsado el desarrollo de mecanismos avanzados de mitigación basados en el monitoreo continuo, el análisis de tráfico en tiempo real y la aplicación de modelos de Inteligencia Artificial capaces de identificar comportamientos anómalos y ejecutar respuestas automatizadas.

Inteligencia Artificial aplicada a la Ciberseguridad

La Inteligencia Artificial constituye una disciplina tecnológica orientada al desarrollo e implementación de sistemas capaces de analizar grandes volúmenes de datos, identificar patrones de comportamiento, detectar anomalías y apoyar los procesos de toma de decisiones en materia de seguridad informática. Araújo et al. (2020) señalan que, mediante la aplicación de algoritmos avanzados de aprendizaje automático (Machine Learning), aprendizaje profundo (Deep Learning) y análisis predictivo, esta tecnología permite automatizar tareas de monitoreo y evaluación de riesgos que tradicionalmente requerían una intervención humana intensiva.

En el contexto de las infraestructuras críticas de telecomunicaciones, la Inteligencia Artificial desempeña un papel estratégico al fortalecer las capacidades de detección temprana de actividades maliciosas, vulnerabilidades e incidentes de seguridad. Desde esta perspectiva, Maslakov et al. (2020) sostienen que estas tecnologías facilitan el análisis en tiempo real del tráfico de red, la clasificación de amenazas y la generación de respuestas automatizadas ante eventos potencialmente peligrosos.

Aprendizaje automático (Machine Learning)

El aprendizaje automático (Machine Learning) constituye una rama de la Inteligencia Artificial centrada en el desarrollo de algoritmos y modelos computacionales capaces de aprender a partir de los datos, identificar patrones y generar predicciones o tomar decisiones sin necesidad de ser programados explícitamente para cada situación específica. Echeverría

et al. (2020) destacan que su funcionamiento se fundamenta en el análisis de grandes volúmenes de información mediante técnicas estadísticas y matemáticas que permiten a los sistemas mejorar progresivamente su desempeño a medida que incorporan nuevos datos.

En el campo de la ciberseguridad, el aprendizaje automático se ha convertido en una herramienta estratégica para la detección y prevención de amenazas digitales. Al respecto, Bustamante et al. (2025) indican que, mediante el análisis continuo del comportamiento de usuarios, dispositivos y redes, estos sistemas son capaces de identificar actividades anómalas, reconocer patrones asociados a ataques cibernéticos y anticipar posibles vulnerabilidades antes de que sean explotadas.

Aprendizaje profundo (Deep Learning)

El aprendizaje profundo (Deep Learning) constituye una subdisciplina avanzada del aprendizaje automático que emplea redes neuronales artificiales de múltiples capas para procesar grandes volúmenes de datos y extraer características complejas de manera automatizada. Orellana (2020) señala que este enfoque, inspirado en el funcionamiento del cerebro humano, permite a los sistemas identificar patrones, relaciones y estructuras ocultas dentro de conjuntos masivos de información, incrementando significativamente la precisión en tareas de clasificación, reconocimiento y predicción.

En el campo de la ciberseguridad, el aprendizaje profundo desempeña un papel fundamental en la detección de amenazas sofisticadas y en el fortalecimiento de los mecanismos de protección de infraestructuras críticas. Cornejo (2025) destaca que, gracias a su capacidad para analizar grandes cantidades de información en tiempo real, estos modelos pueden identificar comportamientos anómalos, detectar malware avanzado, reconocer patrones asociados a ataques cibernéticos y anticipar posibles incidentes de seguridad con elevados niveles de precisión.

Aplicación de la Inteligencia Artificial en la Protección de Infraestructuras de Telecomunicaciones

La Inteligencia Artificial ha transformado significativamente los enfoques tradicionales de la ciberseguridad al proporcionar herramientas avanzadas para la identificación, el análisis y la mitigación de amenazas digitales. Sahatcija et al. (2025) afirman que, mediante la aplicación de algoritmos de Machine Learning, Deep Learning y analítica predictiva, los sistemas basados en Inteligencia Artificial pueden procesar grandes volúmenes de datos generados

por redes y dispositivos de telecomunicaciones, detectando patrones anómalos y comportamientos sospechosos en tiempo real.

Asimismo, la Inteligencia Artificial desempeña un papel estratégico en el fortalecimiento de la capacidad de respuesta frente a ataques cibernéticos y en la mejora de la resiliencia de los sistemas de comunicación. En este marco, Puente et al. (2025) destacan que su aplicación facilita la detección temprana de intrusiones, la identificación de vulnerabilidades, el análisis continuo del tráfico de red y la implementación de respuestas automatizadas para contener incidentes de seguridad.

Optimización de la seguridad en redes 5G e Internet de las Cosas (IoT)

La seguridad en entornos 5G e Internet de las Cosas (IoT) constituye un aspecto fundamental en el contexto de la transformación digital, debido al crecimiento exponencial de los dispositivos conectados y a la expansión de los servicios basados en comunicaciones inteligentes. Bareño et al. (2025) sostienen que las redes 5G ofrecen mayores velocidades de transmisión, menor latencia y una capacidad superior para gestionar grandes volúmenes de datos, mientras que el Internet de las Cosas posibilita la interconexión de dispositivos, sensores y sistemas en diversos sectores estratégicos.

Desde una perspectiva tecnológica, la optimización de la seguridad en entornos 5G e IoT requiere la implementación de estrategias orientadas a fortalecer la protección de redes, dispositivos y servicios interconectados. Cortés et al. (2025) plantean que este proceso implica la adopción de enfoques basados en la gestión de riesgos, el monitoreo continuo, mecanismos robustos de autenticación y el uso de tecnologías de Inteligencia Artificial para la detección temprana de amenazas.

Desafíos éticos y de privacidad

- Los desafíos éticos y de privacidad constituyen aspectos fundamentales en el desarrollo e implementación de tecnologías digitales e Inteligencia Artificial. Molina (2025) advierte que el creciente uso de sistemas automatizados y el procesamiento masivo de datos han generado preocupaciones relacionadas con la protección de la información personal, la transparencia en los procesos de toma de decisiones y la posible presencia de sesgos algorítmicos.

- **Protección y confidencialidad de los datos personales:** Uno de los principales desafíos éticos y de privacidad consiste en garantizar la protección de los datos personales recopilados y procesados por sistemas digitales e Inteligencia Artificial.
- **Sesgos algorítmicos y uso responsable de la Inteligencia Artificial:** Los sistemas de Inteligencia Artificial pueden reproducir o amplificar sesgos presentes en los datos utilizados durante su entrenamiento, lo que podría generar decisiones injustas o discriminatorias.

Estudios de casos

La investigación titulada Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: desafíos y perspectivas, desarrollada por Maldonado (2024), tuvo como objetivo analizar la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en un contexto caracterizado por el incremento del uso de tecnologías digitales y el crecimiento de los delitos informáticos. La investigación se desarrolló mediante una metodología basada en la revisión documental y la aplicación de encuestas a especialistas en ciberseguridad de la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador. Los resultados evidenciaron importantes vulnerabilidades en diversos sectores públicos y privados, identificándose como ciberdelitos más frecuentes el robo de información sensible, el phishing y la suplantación de identidad. Los hallazgos obtenidos destacan la importancia de fortalecer las estrategias de ciberseguridad mediante la incorporación de tecnologías basadas en Inteligencia Artificial para la prevención y mitigación de amenazas digitales.

Con el propósito de analizar el panorama de la ciberseguridad en el Perú, Torres et al. (2025) desarrollaron el estudio Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática. La investigación se sustentó en una revisión sistemática de literatura científica publicada entre 2020 y 2024, para lo cual se examinaron 24 estudios relacionados con los principales ciberataques, el nivel de madurez en ciberseguridad, la normativa vigente, la inversión empresarial, los avances tecnológicos y la disponibilidad de profesionales especializados. Los hallazgos revelaron que el país enfrentaba un elevado número de ataques informáticos, particularmente casos de phishing y fraude electrónico, los cuales ocasionaban importantes pérdidas económicas. Asimismo, se identificaron desafíos relacionados con el fortalecimiento de las capacidades de

ciberseguridad, la actualización de los marcos normativos y la formación de talento especializado para afrontar las amenazas digitales emergentes.

2. METODOLOGÍA

Para el desarrollo de la presente investigación se empleó la revisión sistemática de la literatura como método principal, con el propósito de recopilar, analizar y sintetizar rigurosamente la evidencia científica relacionada con la protección de infraestructuras críticas de telecomunicaciones mediante Inteligencia Artificial frente a amenazas cibernéticas emergentes. Este procedimiento permitió examinar estudios empíricos y aportes teóricos orientados a comprender los fundamentos tecnológicos, los mecanismos de ciberseguridad y las aplicaciones de la Inteligencia Artificial en la detección, prevención y mitigación de riesgos que afectan a las infraestructuras de telecomunicaciones.

En las etapas iniciales de la presente investigación se identificaron 110 registros en bases de datos académicas de alto impacto, como Scopus, Web of Science y SciELO, relacionados con la protección de infraestructuras críticas de telecomunicaciones mediante Inteligencia Artificial frente a amenazas cibernéticas emergentes. Tras el proceso de depuración, la aplicación de criterios de inclusión y exclusión, y la eliminación de documentos duplicados, se seleccionaron 80 artículos científicos y documentos especializados para su análisis detallado, lo que permitió construir un panorama actualizado sobre los avances tecnológicos, los enfoques de ciberseguridad y las aplicaciones de la Inteligencia Artificial en la protección de sistemas y redes de telecomunicaciones.

Se priorizaron estudios recientes con el propósito de garantizar que la evidencia analizada reflejara el estado actual del conocimiento sobre la protección de infraestructuras críticas de telecomunicaciones mediante Inteligencia Artificial. En este proceso, se evaluaron 31 artículos científicos y documentos especializados bajo criterios metodológicos rigurosos, considerando la coherencia entre los objetivos de investigación, el diseño metodológico, la fundamentación teórica y la pertinencia de los hallazgos en relación con aspectos como la ciberseguridad, la Inteligencia Artificial, el Machine Learning, el Deep Learning, la gestión de riesgos cibernéticos y la resiliencia digital. De este conjunto, 20 investigaciones fueron seleccionadas para la síntesis cualitativa, lo que permitió examinar en profundidad diversos enfoques tecnológicos, modelos de protección y estrategias de defensa orientadas al

ISSN: 3091-1990
Vol. 4 Núm. 1 (2026)

fortalecimiento de la seguridad de las infraestructuras de telecomunicaciones, mientras que 11 estudios fueron incorporados en la síntesis cuantitativa, aportando evidencia empírica sobre la efectividad de variables como la detección inteligente de intrusiones, la automatización de respuestas ante incidentes, la identificación de vulnerabilidades y la capacidad de los sistemas basados en Inteligencia Artificial para mejorar la disponibilidad, integridad y confidencialidad de los servicios críticos de telecomunicaciones.

Durante el proceso de revisión sistemática de la literatura, se excluyeron 49 artículos que no guardaban relación directa con la protección de infraestructuras críticas de telecomunicaciones mediante Inteligencia Artificial frente a amenazas cibernéticas emergentes, con el fin de garantizar la pertinencia y calidad de las fuentes analizadas. Como resultado, la investigación se centró en estudios especializados sobre ciberseguridad, Inteligencia Artificial, Machine Learning, Deep Learning, detección inteligente de amenazas, gestión de riesgos cibernéticos y resiliencia digital.

En la presente investigación se aplicó el método PRISMA como marco metodológico para la revisión sistemática de la literatura relacionada con la protección de infraestructuras críticas de telecomunicaciones mediante Inteligencia Artificial frente a amenazas cibernéticas emergentes. Este enfoque permitió identificar, seleccionar y depurar de manera rigurosa las investigaciones más relevantes, garantizando la inclusión de estudios que aportaran evidencia científica sobre la aplicación de la Inteligencia Artificial en la ciberseguridad de redes y sistemas de telecomunicaciones.

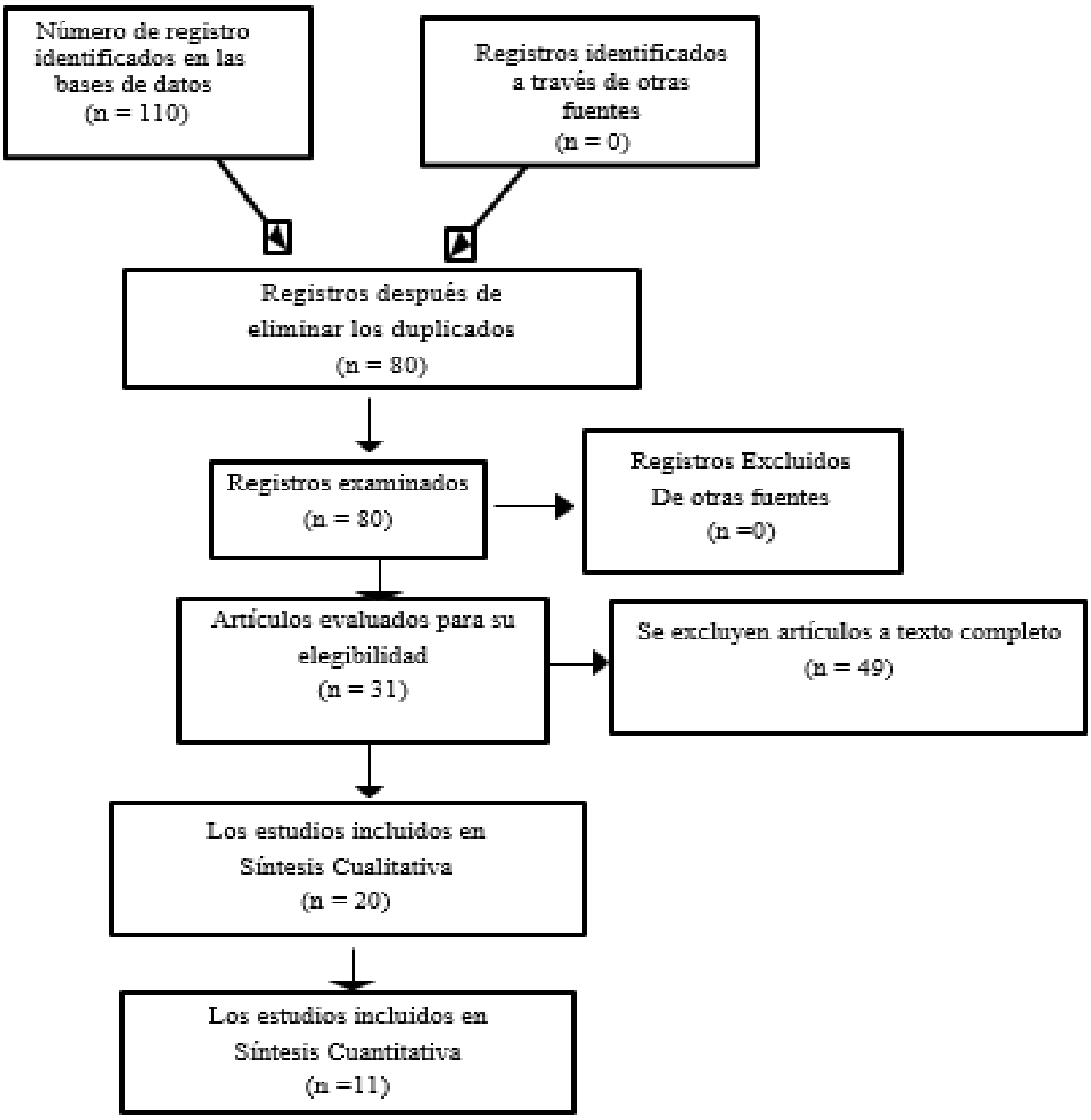
Figura 1

Método Prisma

Doi: https://doi.org/10.63688/scvrpj92

ISSN: 3091-1990

Vol. 4 Núm. 1 (2026)



Nota. Descripción del proceso de cribado a través del método PRISMA

3. RESULTADOS

Los resultados de la investigación evidenciaron que la Inteligencia Artificial desempeñó un papel fundamental en la protección de las infraestructuras críticas de telecomunicaciones frente a amenazas cibernéticas emergentes. A partir del análisis de la literatura científica, se identificó que tecnologías como el Machine Learning, el Deep Learning y los sistemas

Doi: https://doi.org/10.63688/scvrpj92

inteligentes de detección contribuyeron significativamente a la identificación temprana de amenazas, la automatización de respuestas ante incidentes y la optimización de la gestión de riesgos cibernéticos.

Tabla 2.

Resultados

Categoría analizada	Resultado principal encontrado	Impacto en las infraestructuras de telecomunicaciones
Infraestructuras críticas de telecomunicaciones	Fueron identificadas como activos estratégicos esenciales para la conectividad y continuidad de servicios digitales.	Garantizan la disponibilidad de servicios fundamentales para la sociedad digital.
Amenazas cibernéticas emergentes	Se evidenció un incremento de ataques sofisticados como ransomware, APT y DDoS.	Incrementan el riesgo de interrupciones operativas y pérdida de información crítica.
Gestión de riesgos cibernéticos	Se determinó que la evaluación continua de riesgos fortalece la seguridad organizacional.	Reduce vulnerabilidades y mejora la capacidad de respuesta ante incidentes.
Vulnerabilidades en redes y sistemas	Se identificó que las configuraciones inadecuadas y sistemas desactualizados representan las principales debilidades.	Aumentan la exposición a ataques y accesos no autorizados.
Políticas y estándares internacionales	Los marcos ISO/IEC 27001, ISO/IEC 27032 y NIST fueron reconocidos como referentes internacionales.	Favorecen la implementación de buenas prácticas y la resiliencia digital.
Inteligencia Artificial aplicada a la ciberseguridad	Demostró alta capacidad para analizar datos, detectar anomalías y automatizar respuestas.	Mejora significativamente la protección de infraestructuras críticas.
Machine Learning	Permitió identificar patrones de comportamiento asociados a amenazas digitales.	Fortalece la detección temprana y la prevención de ciberataques.

Categoría analizada	Resultado principal encontrado	Impacto en las infraestructuras de telecomunicaciones
Deep Learning	Mostró alta precisión para reconocer amenazas complejas y malware avanzado.	Incrementa la capacidad predictiva y la protección de redes críticas.
Redes 5G e Internet de las Cosas (IoT)	Incrementaron la conectividad, pero también ampliaron la superficie de ataque.	Requieren mecanismos avanzados de protección y monitoreo permanente.
Desafíos éticos y de privacidad	Se identificaron preocupaciones relacionadas con la transparencia algorítmica y la protección de datos.	Exigen marcos regulatorios y principios éticos para el uso de la IA.

Fuente: Elaboración propia

Los resultados presentados en la Tabla 1 evidenciaron que las infraestructuras críticas de telecomunicaciones enfrentaron una creciente exposición a amenazas cibernéticas emergentes, debido al incremento de la interconectividad digital y la evolución constante de los mecanismos de ataque. La literatura analizada destacó que amenazas como el ransomware, las amenazas persistentes avanzadas (APT) y los ataques DDoS representaron riesgos significativos para la continuidad operativa de los servicios esenciales, lo que hizo necesaria la implementación de estrategias avanzadas de ciberseguridad orientadas a fortalecer la resiliencia y la protección de los sistemas críticos.

Tabla 3.

Resultados

Tecnología basada en IA	Función principal	Resultado obtenido
Machine Learning	Detección de patrones y anomalías	Mejoró la identificación temprana de amenazas cibernéticas.
Deep Learning	Análisis avanzado de datos complejos	Incrementó la precisión en la detección de ataques sofisticados.
Sistemas Inteligentes	Monitoreo continuo y automatizado	Optimizó la vigilancia de redes críticas.
Analítica Predictiva	Anticipación de incidentes de seguridad	Facilitó la prevención de riesgos cibernéticos.

ISSN: 3091-1990
Vol. 4 Núm. 1 (2026)

Tecnología basada en IA	Función principal	Resultado obtenido
Respuesta Automatizada	Mitigación rápida de amenazas	Redujo los tiempos de reacción ante incidentes.
Detección Inteligente de Intrusiones	Identificación de accesos no autorizados	Fortaleció la seguridad y continuidad operativa de los servicios.

Fuente: Elaboración propia

Los resultados mostrados en la Tabla 2 evidenciaron que las tecnologías basadas en Inteligencia Artificial desempeñaron un papel estratégico en el fortalecimiento de la ciberseguridad de las infraestructuras críticas de telecomunicaciones. La revisión de la literatura permitió identificar que el Machine Learning y el Deep Learning mejoraron significativamente la capacidad de detección de amenazas mediante el análisis automatizado de grandes volúmenes de datos y la identificación de patrones asociados a actividades maliciosas.

4. DISCUSIÓN

Los hallazgos de la presente investigación evidenciaron que las infraestructuras críticas de telecomunicaciones desempeñan un papel fundamental en la continuidad de los servicios esenciales y en el funcionamiento de la sociedad digital. Estos resultados coinciden con lo planteado por Avilano (2023), quien reconoce la importancia estratégica de estas infraestructuras para garantizar la conectividad y el intercambio seguro de información en entornos altamente digitalizados.

Los resultados también demostraron que las amenazas cibernéticas emergentes, especialmente el ransomware avanzado, las amenazas persistentes avanzadas (APT) y los ataques distribuidos de denegación de servicio (DDoS), constituyen riesgos significativos para las infraestructuras de telecomunicaciones. Estos hallazgos guardan concordancia con lo expuesto por Cornejo (2025), quien destaca el impacto creciente de estas amenazas sobre la seguridad y continuidad operativa de los sistemas críticos.

Por otra parte, los resultados obtenidos evidenciaron que la Inteligencia Artificial se ha consolidado como una herramienta estratégica para el fortalecimiento de la ciberseguridad en entornos de telecomunicaciones. Estos hallazgos coinciden con lo planteado por Vazifehdust (2020), quien destaca el potencial de las tecnologías inteligentes para optimizar

Doi: https://doi.org/10.63688/scvrpj92

ISSN: 3091-1990
Vol. 4 Núm. 1 (2026)

los mecanismos de protección frente a amenazas cibernéticas cada vez más sofisticadas. Asimismo, los estudios revisados mostraron que herramientas basadas en Machine Learning y Deep Learning mejoran significativamente la capacidad de detección temprana de amenazas, el análisis de comportamientos anómalos y la automatización de respuestas ante incidentes de seguridad.

Finalmente, los resultados obtenidos evidenciaron que la implementación de soluciones basadas en Inteligencia Artificial se encuentra acompañada de importantes desafíos éticos, normativos y de privacidad. Estos hallazgos son consistentes con lo señalado por Torres et al. (2025), quienes destacan que la incorporación de tecnologías inteligentes en entornos digitales requiere considerar aspectos relacionados con la protección de datos, la transparencia en la toma de decisiones y la mitigación de posibles sesgos algorítmicos.

5. CONCLUSIÓN

La presente investigación permitió concluir que las infraestructuras críticas de telecomunicaciones constituyen componentes esenciales para el funcionamiento de la sociedad digital, debido a su papel estratégico en la transmisión de información y la prestación de servicios fundamentales. Asimismo, se evidenció que la creciente digitalización, la expansión de las redes 5G y el desarrollo del Internet de las Cosas (IoT) incrementaron significativamente la exposición a amenazas cibernéticas emergentes, generando nuevos desafíos para la seguridad y continuidad operativa de estos sistemas.

Los resultados obtenidos demostraron que la Inteligencia Artificial se consolidó como una herramienta estratégica para la protección de las infraestructuras críticas de telecomunicaciones frente a amenazas cibernéticas avanzadas. La evidencia científica analizada reveló que tecnologías como el Machine Learning, el Deep Learning y los sistemas inteligentes de detección contribuyeron significativamente a la identificación temprana de vulnerabilidades, la detección de intrusiones, la prevención de ataques y la automatización de respuestas ante incidentes de seguridad.

La aplicación de la Inteligencia Artificial contribuye de manera significativa a la protección de las infraestructuras críticas de telecomunicaciones frente a amenazas cibernéticas emergentes, al permitir la detección temprana de patrones anómalos, la identificación automatizada de vulnerabilidades y la clasificación precisa de eventos de seguridad en

Doi: https://doi.org/10.63688/scvrpj92

grandes volúmenes de datos. Tecnologías como el Machine Learning y el Deep Learning fortalecen la capacidad de análisis en tiempo real, lo que facilita la prevención de ataques como ransomware, APT y DDoS antes de que generen impactos operativos relevantes.

Finalmente, se concluyó que la implementación efectiva de la Inteligencia Artificial en la ciberseguridad de las infraestructuras de telecomunicaciones requiere no solo avances tecnológicos, sino también el fortalecimiento de marcos normativos, estándares internacionales y principios éticos que garanticen un uso responsable de estas herramientas. La investigación evidenció que aspectos relacionados con la privacidad de los datos, la transparencia algorítmica y la gobernanza tecnológica constituyeron factores determinantes para maximizar los beneficios de la Inteligencia Artificial y minimizar los riesgos asociados a su aplicación.

REFERENCIAS BIBLIOGRÁFICAS

Alves, P. A., & Cunha, B. D. (2025). Evaluación psicológica como herramienta de diagnóstico organizacional: Evaluación de la salud mental en una empresa de telecomunicaciones en Angola. *Revista Psicologia e Saúde*. https://doi.org/10.20435/pssa.v1i1.3023

Araújo, S. B., & Levy, I. S. (2020). Arkangel: Sobre la devastación en la relación madre-hija en la era digital. *Estudios en Psicoanálisis*. https://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S0100-34372020000100014&lang=pt

Avilano, F. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*. https://www.scielo.sa.cr/scielo.php?pid=S2215-24582023000100092&script=sci_abstract&tlng=es

Bareño, G. R., & Báez, R. H. (2025). Recomendaciones de ciberseguridad bajo la implementación de políticas de defensa en profundidad en las organizaciones: revisión sistemática de la literatura. *Información Tecnológica*. http://dx.doi.org/10.4067/s0718-07642025000300001

Bustamante, S., & Castañeda, P. (2025). Desafíos de la gestión de la seguridad de la información en el sector industrial: una revisión sistemática. *Enfoque UTE*. https://doi.org/10.29019/encuesta.1152

Cardoso, P. B., & Correia, C. A. (2021). Estrategias de comunicación adoptadas por la gestión del Sistema Brasileño de Salud durante la pandemia de Covid-19 – Brasil. *Interface - Comunicação, Saúde, Educação*. https://doi.org/10.1590/interface.200785

Cornejo, H. (2025). Madurez en ciberseguridad y resiliencia digital en PYMEs iberoamericanas: diagnóstico y desafíos estratégicos. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*. https://doi.org/10.17013/risti.60.127-141

Cortés, C. B., & Scheechler, C. C. (2025). Ciberseguridad en el derecho chileno: Estado, desafíos y proyecciones. *Revista Internacional CONSINTER de Direito*. https://doi.org/10.19135/revista.consinter.00020.13

Delgado, E. H. (2026). Seguridad de los datos en las empresas de telecomunicaciones peruanas: una iniciativa de sensibilización a través de una aplicación móvil. *Aula Virtual*. https://doi.org/10.5281/zenodo.18958666

Echeverría, M., & Garaycoa, M. (2020). ¿Están preparados los millennials ecuatorianos contra un ataque informático? *Revista Chakiñan de Ciencias Sociales y Humanidades*. https://doi.org/10.37135/chk.002.10.05

Henao, C. L. (2021). Calidad de servicio y valor percibido como antecedentes de la satisfacción de los clientes de las empresas de telecomunicaciones en Colombia. *Contaduría y Administración*. https://doi.org/10.22201/fca.24488410e.2020.2318

Hernández, L. F. (2025). La prensa estadounidense y el inicio de la televisión mexicana (1950-1955). *Comunicación y Sociedad*. https://doi.org/10.32870/cys.v2025.8860

Maldonado, C. (2024). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: desafíos y perspectivas. *Revista Criminalidad*. https://doi.org/10.47741/17943108.660

Maslakov, S. I., & Shitova, N. V. (2020). Investigando los aspectos psicológicos de la socialización cibernética entre estudiantes modernos. *Propósitos y Representaciones*. https://doi.org/10.20511/pyr2020.v8n2.512

Mattos, M. G., & Couto, T. V. (2022). Sueñan los autómatas con amantes cibernéticos. *Ágora: Estudos em Teoria Psicanalítica*. https://doi.org/10.1590/1809-44142022001011

Mohamed, K. A., & AbuBakr, N. (2024). La evolución de la teledetección después del COVID-19: el paso de la respuesta a la crisis a las soluciones a largo plazo. *Odovtos International Journal of Dental Sciences*. http://dx.doi.org/10.15517/ijds.2024.59571

Molina, D. P. (2025). El ciudadano europeo ante el reto actual de la implantación de la administración electrónica. *Revista Internacional CONSINTER de Direito*. https://doi.org/10.19135/revista.consinter.00020.33

Morera, H. T., & Bruzos, C. C. (2021). Trabajando la relación Universidad-sociedad. Abordaje multidisciplinar y difusión social. *FEM: Revista de la Fundación Educación Médica*. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S2014-98322021000100008&lang=pt

Noll, R. G. (2018). Evaluación de las políticas de telecomunicaciones en México. *El Trimestre Económico*. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-718X2013000300603&lang=pt

Orellana, C. (2020). Aprendizaje profundo en la formación docente: experiencia con estudiantes de Enseñanza de la Educación de la Universidad de Costa Rica. *Revista Innovaciones Educativas*. [Falta enlace o DOI exacto del artículo].

Pasos, S. E., & Archibold, S. R. (2020). Barreras y comportamientos negativos que prevalecen en la prevención y el control del dengue en Cartagena, Colombia. *Revista de Salud Pública*. https://doi.org/10.15446/rsap.V22n1.77989

Piña, M. M., & Villegas, I. J. (2025). Metaanálisis del desarrollo de la inteligencia artificial y el internet de los objetos: la transformación del trabajo y la vida. *Revista de Ciencias Tecnológicas*. https://doi.org/10.37636/recit.v7n3e350

Puente, Z. J., & Atarama, V. D. (2025). Educación segura en la era digital, aprendizajes desde la ISO 27002:2022: una revisión sistemática. *Revista Simón Rodríguez*. https://doi.org/10.62319/simonrodriguez.v.5i10.55

Rodríguez, P. I. (2021). Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*. https://doi.org/10.23913/ride.v12i23.980

Ruiz, M. I., & Ruiz, M. M. (2021). Las pautas de comunicación digital de los principales movimientos ciudadanos en Málaga (España) en el periodo 2018-2019. *Convergencia*. https://doi.org/10.29101/crcs.v28i0.14303

Sahatcija, R., & Memaj, F. (2025). Fortalecimiento de la educación en ciberseguridad para estudiantes universitarios: cerrando brechas de vulnerabilidad y fomentando prácticas. *Millenium - Journal of Education, Technologies, and Health*. https://doi.org/10.29352/mill0227e.41111

Saldaña, P. J. (2024). Resoluciones sobre prácticas monopólicas y concentraciones: marco legal y práctica. *Revista Eurolatinoamericana de Derecho Administrativo*. https://doi.org/10.14409/redoeda.v11i2.13088

Solís, F., Pinto, D., & Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. *Enfoque UTE*. https://doi.org/10.29019/enfoqueute.v8n1.123

Torres, N., & Zúñiga, M. (2025). Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática. *Revista InveCom*. https://doi.org/10.5281/zenodo.15605545

Vazifehdust, H. (2020). Técnicas proyectivas para comprender el dominio del cibermercado en las redes sociales. *Revista Brasileira de Gestão de Negócios*. https://doi.org/10.7819/rbgn.v22i3.4074

Villa, Á. F., & Córdova, A. E. (2025). Aplicación de los métodos REBA y NIOSH para la reducción de riesgos ergonómicos en una empresa de telecomunicaciones. *SciELO Preprints*. https://doi.org/10.1590/SciELOPreprints.14031

Yacout, S. (2022). Un sistema de control de procesos cibernéticos basado en el reconocimiento de patrones y la computación en la nube. *Gestão & Produção*. https://doi.org/10.1590/1806-9649-2022v29e5221

Conflicto de Intereses: Los autores afirman que no existen conflictos de intereses en este estudio y que se han seguido éticamente los procesos establecidos por esta revista. Además, aseguran que este trabajo no ha sido publicado parcial ni totalmente en ninguna otra revista.

FINANCIAMIENTO

Los autores no recibieron financiamiento para el desarrollo de esta investigación.

ISSN: 3091-1990

Vol. 4 Núm. 1 (2026)

CONTRIBUCIÓN DE AUTORÍA:

Nombres de autores e iniciales: Kevin Alexis García Pérez (KAGP), Josseph Yaakob Catagua Cobos (JYCC).

1. Conceptualización: (KAGP)
2. Curación de datos: (KAGP)
3. Análisis formal: (KAGP)
4. Adquisición de fondos: (KAGP)
5. Investigación: (KAGP)
6. Metodología: (KAGP)
7. Administración del proyecto:(KAGP)
8. Recursos: (JYCC)
9. Software: (JYCC)
10. Supervisión: (JYCC)
11. Validación: (JYCC)
12. Visualización: (JYCC)
13. Redacción – Borrador original: (JYCC)
14. Redacción – Revisión y edición: (JYCC)

Doi: https://doi.org/10.63688/scvrpj92