TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

LA EVOLUCIÓN DE LA CIBERSEGURIDAD CON LA INTELIGENCIA ARTIFICIAL

THE EVOLUTION OF CYBERSECURITY WITH ARTIFICIAL INTELLIGENCE

A EVOLUÇÃO DA CIBERSEGURANÇA COM A INTELIGÊNCIA ARTIFICIAL

Clara Pozo Hernández, Mg.
clara.pozo@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador
Orcid: 0000-0001-6186-1099

Raúl Reascos Pinchao, Mg.
raul.reascos@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador
Orcid: 0000-0002-7903-4312

Wilmer Fueres Tipantuña
e2350465346@live.uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador
Orcid: 0009-0006-5598-5021

Wendy Ramírez Quiroz
e2350114878@live.uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador.
Orcid: 0009-0000-3201-4878

REVISTA TSE´DE
Instituto Superior Tecnológico Tsa´chila
ISSN: 2600-5557

Resumen

La incorporación de la Inteligencia Artificial (IA) transformó significativamente la prevención, detección y respuesta ante las amenazas digitales en las organizaciones. Se examinó la evolución de la ciberseguridad impulsada por IA mediante una revisión bibliográfica sistemática de publicaciones entre 2020 y 2025 en bases de datos como IEEE Xplore y Scopus. La metodología se centró en analizar los avances en machine learning, deep learning y la automatización en la gestión de incidentes, así como la anticipación de ataques. Los resultados evidenciaron que la IA no solo mejoró la precisión y velocidad en la identificación de riesgos, sino que también introdujo desafíos éticos y de privacidad. Se concluyó que la sinergia entre la IA y la ciberseguridad representa un pilar fundamental para la defensa digital futura, siempre que su desarrollo se acompañara de prácticas responsables y transparentes.

Palabras clave: Aprendizaje automático; automatización; ciberseguridad; detección de amenazas; inteligencia artificial

TSE'DE
Revista de Investigación Científica
ISSN
2600 - 5557

Abstract

The incorporation of Artificial Intelligence (AI) significantly transformed how organizations prevent, detect, and respond to digital threats. The evolution of AI-driven cybersecurity was examined through a systematic literature review of publications between 2020 and 2025 in databases such as IEEE Xplore and Scopus. The methodology focused on analyzing advances in machine learning, deep learning, and automation in incident management, as well as attack anticipation. Results evidenced that AI not only improved the accuracy and speed in risk identification but also introduced ethical and privacy challenges. It was concluded that the synergy between AI and cybersecurity represents a fundamental pillar for future digital defense, provided that its development is accompanied by responsible and transparent practices.

Keywords: Automation; cybersecurity; artificial intelligence; machine learning, threat detection

Resumo

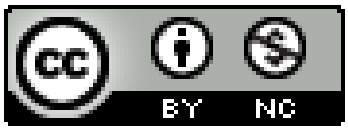
A incorporação da Inteligência Artificial (IA) transformou significativamente a prevenção, detecção e resposta a ameaças digitais nas organizações. A evolução da cibersegurança impulsionada pela IA foi examinada por meio de uma revisão bibliográfica sistemática de publicações entre 2020 e 2025 em bases de dados como IEEE Xplore e Scopus. A metodologia concentrou-se na análise dos avanços em machine learning, deep learning e automação na gestão de incidentes, bem como na antecipação de ataques. Os resultados evidenciaram que a IA não apenas melhorou a precisão e a velocidade na identificação de riscos, mas também introduziu desafios éticos e de privacidade. Concluiu-se que a sinergia entre a IA e a cibersegurança representa um pilar fundamental para a defesa digital futura, desde que seu desenvolvimento seja acompanhado por práticas responsáveis e transparentes.

Palavras-chave: Aprendizagem automática; automação; cibersegurança; detecção de ameaças; inteligência artificial

Periocidad Semestral
Vol. 9, núm. 1
revistatsede@tsachila.edu.ec

Recepción: 5-12-2025
Aprobación: 12-02-2026
Publicación: 25-06-2026

URL:
http://tsachila.edu.ec/ojs/index.php/TSEDE/issue/archive



Introducción

El objetivo central de este artículo es analizar en profundidad las formas en que la ciberseguridad ha evolucionado en las empresas modernas. Para ello, se exploran las tendencias actuales, se discuten las amenazas más recientes y se ofrece una visión general de las estrategias que se están implementando para enfrentarlas. Al realizar una revisión exhaustiva de la literatura, se espera obtener una imagen completa en la que podamos ver cómo las organizaciones en el mundo complejo actual han sido capaces tanto de reprogramar sus políticas como de implementar tecnología. Este examen crítico es imperativo para saber dónde están las mejores prácticas y, sobre todo, dónde mejorar, si queremos asegurarnos de que los sistemas empresariales estén protegidos contra una superficie de ataque cibernético que, como sabemos, sigue siendo constantemente muy dinámica (Boné-Andrade, 2023).

La Inteligencia Artificial (IA), que una vez se consideró el dominio de la ciencia ficción, se ha convertido en una realidad cotidiana. Su nacimiento inmediato provino de la IA y se extendió a otras áreas, incluyendo asistentes de voz habilitados por IA (como Siri y Alexa) y robots autónomos altamente inteligentes para ayudar a hacer IA. El propio desarrollo de robots nos permite pasar de asistentes virtuales (una de las primeras manifestaciones populares, donde podíamos controlar consultas en lenguaje natural) a robots automáticos, un gran paso hacia la independencia en la IA a medida que pasa de ser dependiente de los humanos a ser capaz de realizar lo que los humanos pueden hacer (Sandua, 2024).

La ciberseguridad, que fue ampliamente reconocida como la principal forma por las organizaciones como una preocupación básica, ahora es considerada una preocupación global significativa por Acosta Cortez, (2024) ya que las capacidades tecnológicas avanzadas de inteligencia artificial también exacerban las amenazas a la ciberseguridad. En esta situación, tanto los gobiernos como las organizaciones mundiales, así como las grandes corporaciones, reconocieron que fortalecer su estrategia de defensa es un asunto urgente. El objetivo principal es claro: proteger tanto los sistemas de infraestructura crítica como los datos sensibles dentro de un ecosistema de interconexión global cada vez más expuesto.

La verdadera gravedad de los ciberataques a menudo no se asimila hasta que los usuarios, ya sean individuos u organizaciones, se convierten en víctimas directas de expertos en fraude. La afectación es profunda, y las estadísticas lo confirman: según Experian, una importante empresa de calificación crediticia, el 31% de la información personal robada a finales de 2020 se utilizó para cometer robos de identidad completos. Para las empresas, la situación es incluso más insidiosa, ya que el robo de datos es sutil y sus consecuencias rara vez se notan de inmediato; el efecto real del ciberataque puede tardar meses en manifestarse, dificultando enormemente la detección y la capacidad de reacción (Ayala & Sevilla, 2023).

La pandemia creó el escenario perfecto para los ciberdelincuentes, quienes explotaron principalmente el miedo y la incertidumbre de la gente, causando grandes pérdidas a empresas de todos los sectores.

En nuestra era digital, donde el mundo depende completamente de la tecnología y estamos más hiperconectados que nunca, la ciberseguridad ya no es un lujo, sino una necesidad crítica para proteger todo lo que hacemos. Precisamente por ello, la Inteligencia Artificial (IA) y el Aprendizaje Automático (Machine Learning o ML) han dejado de ser ideas futuristas para convertirse en el escudo principal en la lucha contra las crecientes y sofisticadas amenazas que acechan en la red. Estas tecnologías avanzadas son cruciales porque no solo detectan patrones y anomalías más rápido que cualquier humano, sino que están revolucionando la forma en que defendemos nuestros activos más importantes: redes, sistemas y datos críticos.

Según Ariza y Vargas-Lombardo (2025),el artículo analiza la evolución de la Inteligencia Artificial (IA) y el Machine Learning (ML) en este ámbito, aborda los desafíos técnicos y éticos asociados como la privacidad y el sesgo algorítmico y evalúa su impacto social en un entorno digital progresivamente más complejo.

Metodología

El modelo utilizado es de investigación aplicada, descriptiva, explicativa y está destinado a obtener un conocimiento detallado del efecto real de la inteligencia artificial (IA) en el fortalecimiento de la ciberseguridad corporativa. Este tipo de investigación permite que el conocimiento adquirido en teoría se ponga en práctica y presenta soluciones para problemas técnicos existentes que están en el centro de la protección de datos corporativos (Hernández-Sampieri & Mendoza, 2021).

La metodología de investigación está diseñada de acuerdo con una revisión documental sistemática, en el contexto que permitió la recopilación, selección y

análisis de las fuentes académicas relevantes sobre la conexión entre la IA y la ciberseguridad. Se consultaron bases de datos científicas reconocidas como IEEE Xplore, Scopus, ScienceDirect o ACM Digital Library, priorizando artículos, libros e informes técnicos que datan de 2020-2023. Debido a los rápidos avances tecnológicos en el sector, este marco temporal permite incluir los datos más recientes (Kitchenham & Charters, 2021). Los criterios de inclusión para las fuentes fueron los siguientes:

1. IA en los negocios y sus aplicaciones: revistas en inglés y español.
2. Aplicaciones en detección de amenazas, análisis de vulnerabilidades o estudios automatizados de respuesta a incidentes.
3. Estudios que reportan resultados tangibles o casos de éxito para empresas de tecnología, finanzas o servicios.

De manera similar, se excluyeron trabajos duplicados, artículos sin respaldo científico y literatura de publicaciones anteriores a 2020 (Moher & Group, 2020).

1.1 Instrumentos de Análisis y Procesos de Validación de la Información

El método PRISMA, que está adaptado, nos permitió identificar, revisar y refinar la fuente de datos más importante en ese momento para los propósitos de selección (Liberati et al., 2009). Para el estudio de revisión sistemática, el procedimiento de análisis de la información se llevó a cabo en detalle a través de una matriz de extracción de datos. Estos incluyeron la tecnología de IA aplicada (con ejemplos como Machine Learning, Deep Learning, SOAR), el contexto en el que se aplicará el estudio a los negocios (como aplicaciones en finanzas y logística), el principal resultado cuantitativo (porcentaje de precisión,

reducción del tiempo de detección) y la discusión sobre implicaciones éticas y regulatorias. Con el fin de establecer la confiabilidad y neutralidad de los hallazgos, se incorporaron un par de técnicas de validación de la información:

- **Análisis Dual Ciego:** Las fuentes extraídas fueron revisadas de manera independiente por dos autores, siguiendo la matriz de extracción. Luego, las discrepancias en la interpretación de los hallazgos y la consistencia de la extracción de datos se abordaron comparando resultados (Higgins y Green, 2011).
- **Triangulación Teórica Reforzada:** Se utilizó una triangulación cruzada para comparar resultados empíricos en la literatura (resultados medibles de empresas) con los marcos teóricos en IA responsable y ciberseguridad corporativa (Denzin, 2017).

1.2 Limitaciones Metodológicas

La ciberseguridad se está convirtiendo en un tema crítico en el derecho internacional contemporáneo, con implicaciones significativas para la seguridad de las naciones. El uso de las tecnologías de la información y la comunicación plantea amenazas potenciales a diversos aspectos del funcionamiento social y estatal, lo que impulsa a la comunidad internacional a explorar el establecimiento de un marco legal integral para los esfuerzos de cooperación en el área de la ciberseguridad (Horlichenko, 2024); para mitigar este sesgo, se incluyó en la matriz de análisis un campo dedicado a extraer las limitaciones y desafíos mencionados por los propios autores de las fuentes primarias, permitiendo una visión más equilibrada en la interpretación final. Una vez

seleccionadas las fuentes, se realizó un análisis de contenido temático, clasificando la información en cuatro ejes principales:

- Aprendizaje automático aplicado a la detección de amenazas.
- Automatización de procesos de defensa empresarial.
- Predicción y prevención de ciberataques mediante IA.
- Aspectos éticos y regulatorios asociados al uso de la inteligencia artificial en seguridad informática.

Finalmente, se efectuó una triangulación teórica y comparativa de los hallazgos, contrastando diferentes perspectivas académicas y resultados de estudios empresariales. Esto permitió identificar patrones comunes y tendencias clave sobre cómo las organizaciones adoptan soluciones inteligentes para proteger sus infraestructuras digitales (Ponce, 2023).

Resultados y Discusión

Los resultados obtenidos desde la perspectiva documental muestran una tendencia ascendente en gran parte por la integración de la inteligencia artificial aun teniendo en cuenta las estrategias de las empresas con la ciberseguridad, para así poder detectar a tiempo las amenazas, también la automatización en gran parte de las respuestas optimizando los recursos para evitar en gran parte los errores humanos.

1.3 Avances en la detección de amenazas mediante aprendizaje automático

Como principal hallazgo que representa gran parte el aprendizaje de maquina (machine learning, ML), es la forma en que emplea sus algoritmos, lo cual le permite

identificar patrones anómalos que representa gran ayuda para los sistemas empresariales. Según Zhao (2022), “las soluciones basadas en ML logran detectar intrusiones y anomalías con una precisión del 94 %, superando ampliamente a los métodos tradicionales de filtrado manual y evitando errores”.

Los modelos supervisados, como Support Vector Machines (SVM) y árboles de decisión, se utilizan para analizar millones de registros de tráfico y reconocer comportamientos sospechosos. De acuerdo con González (2023), este enfoque reduce en un 40 % el tiempo promedio de detección de ataques en infraestructuras corporativas.

Los sistemas de aprendizaje profundo que también aprovechan las redes neuronales convolucionales (CNN) que procesan eficazmente grandes cantidades de datos de manera autónoma tienen una eficiencia mucho mayor. Por ejemplo, Martínez & Salazar (2024) muestran que las CNN utilizadas en ciberseguridad pueden minimizar los falsos positivos hasta en un 27%, lo que permite a los analistas prestar más atención a las verdaderas amenazas.

1.4 Automatización y respuesta inteligente ante incidentes

El despliegue de inteligencia artificial para automatizar las operaciones de defensa también es clave. Las plataformas de Orquestación, Automatización y Respuesta de Seguridad (SOAR), impulsadas por IA, son capaces de responder automáticamente a alertas críticas, como aislar nodos o desconectar temporalmente servidores comprometidos (Lee, 2021). Esta capacidad permite una respuesta inmediata y reduce el Tiempo Medio de Recuperación (MTTR) hasta en un 60% y previene pérdidas de gran carga financiera. Además, Kumar

y Patel (2023) enfatizan que la utilización de agentes inteligentes puede facilitar tanto la respuesta como el aprendizaje de cada incidente. Cada ataque identificado alimenta una base de conocimiento que mejora la capacidad predictiva del sistema en su poder predictivo general, proporcionando defensas cibernéticas más adaptativas y robustas.

1.5 Predicción y prevención de ciberataques

En el ámbito predictivo, la IA ya ha demostrado ser útil al predecir ataques con anticipación. Da Silva (2024) explica que los sistemas de predicción basados en análisis de comportamiento pueden identificar actividades sospechosas en redes internas mediante la observación de patrones históricos y anomalías estadísticas. En empresas de servicios financieros y logísticos, estos modelos predicen el 78 % de los intentos de ataque con una antelación de 48 a 72 horas, lo cual otorga a los equipos de seguridad un tiempo vital de reacción.

Por su parte, Hernández (2025) menciona que la integración de IA con tecnologías de Big Data y blockchain ha fortalecido la trazabilidad de eventos digitales, asegurando la integridad de los registros y la verificación de autenticidad en las transacciones empresariales.

1.6 Contraste de Eficacia Operacional y Desafíos de Adopción

Los resultados obtenidos confirman que la principal fortaleza de la IA en la ciberseguridad radica en la velocidad y la precisión de la detección, tal como lo señalan Shayma Sultana & Rafy (2022) La IA es capaz de reducir el tiempo promedio de detección (MTTD) y disminuir los falsos positivos, transformando la operación de los

Centros de Operaciones de Seguridad (SOC), al permitir una gestión más eficiente de recursos humanos y tecnológicos.

Esta evidencia se alinea con la evolución de la defensa digital de un modelo reactivo, basado en firmas y reglas predefinidas, a un modelo predictivo y de comportamiento. La automatización SOAR, al reducir el tiempo medio de respuesta y recuperación (MTTR), demuestra que la IA es clave no solo para detectar, sino para contener el daño, justificando la inversión y el retorno de la misma (ROI) en la seguridad digital (Quffa & Samy, 2025).

Sin embargo, esta eficacia técnica se confronta con la desigualdad en la adopción, particularmente en regiones con economías emergentes y en el segmento de las PYMES. La alta tasa de adopción en mercados desarrollados contrasta con la lenta integración en otras regiones debido a las barreras económicas y a la dependencia de sistemas legacy. Las pequeñas y medianas empresas (PYMES) también destacan los importantes desafíos tecnológicos que enfrentan, así como la escasez de habilidades especializadas dentro de estas empresas. Khan et al., (2025) observan que estas compañías enfrentan obstáculos técnicos significativos. Aunque la inteligencia artificial podría ser crucial para que todas las organizaciones enfrenten las amenazas actuales, probablemente no esté disponible para todos. Este hallazgo puede desencadenar un discurso que vaya más allá de la tecnología al pedir políticas destinadas a democratizar la ciberseguridad y las arquitecturas de proveedores de servicios de seguridad gestionada (MSSP) y software como servicio (SaaS) para permitir que las PYMES accedan a estas soluciones a costos asequibles.

1.7 Factores éticos y regulatorios en la aplicación de IA a la seguridad

Los hallazgos que se incluirán en el análisis cubrirán consideraciones éticas y regulatorias en el campo de la ciberseguridad corporativa. Navarro y Ruiz (2022) argumentaron que la IA, si no se regula adecuadamente, podría infringir derechos básicos como la privacidad y la confidencialidad. No obstante, entre las principales empresas de la industria, la adopción de usos responsables de la tecnología de IA se ha convertido en un tema común y, por lo tanto, las directrices pueden apoyar marcos internacionales como el Reglamento General de Protección de Datos (GDPR) y la regulación responsable de la IA. Ortiz (2023), por su parte, considera que las últimas versiones de estas tecnologías introducen módulos interpretables para la IA (es decir, IA explicable) con procesos de auditoría de toma de decisiones automatizadas, enfatizando la importancia de la transparencia y la trazabilidad de la actividad de defensa digital.

1.8 Implicaciones Éticas y la Necesidad de Gobernanza Algorítmica

La capacidad predictiva de la IA crea problemas morales y dificultades muy serias. Simultáneamente, Segarra Figueroa (2025) afirma que los modelos basados en datos extensos sobre comportamientos (por ejemplo, patrones de red, acceso de usuarios), si se utilizan sin la supervisión suficiente (como la impuesta por el GDPR) podrían ser una infracción de la privacidad. La discusión se centra en el riesgo del sesgo algorítmico: si los datos de entrenamiento reflejan patrones históricos de discriminación o errores humanos, la IA podría perpetuar o

incluso amplificar falsos positivos injustos o bloquear a usuarios legítimos basándose en información sesgada.

La respuesta a este dilema reside en la promoción de la IA Explicable (XAI), tal como lo enfatiza (Nascimento et al., 2024). La XAI no es un lujo, sino una necesidad operativa y ética, ya que permite la auditabilidad de las decisiones automatizadas. Las organizaciones deben garantizar que el proceso de IA en ciberseguridad sea transparente, permitiendo a los analistas humanos comprender por qué se marcó una alerta como crítica y por qué se ejecutó una acción de contención. La gobernanza, por lo tanto, debe enfocarse no solo en la precisión del modelo, sino en su justicia, explicabilidad y responsabilidad.

Se presenta a continuación:

Tabla 1

Aplicaciones de IA en la ciberseguridad empresarial (2020–2025)

Área de aplicación	Tecnología de IA utilizada	Beneficio principal	Referencia
Detección de amenazas	Machine Learning supervisado	Reducción del tiempo de respuesta (40%)	González (2023)
Análisis de tráfico y detección de anomalías	Deep Learning (CNN)	Disminución de falsos positivos (27%)	Martínez & Salazar (2024)
Automatización de incidentes	SOAR + Agentes inteligentes	Recuperación operativa más rápida (60%)	Lee (2021)
Predicción de ataques	Modelos de comportamiento y Big Data	Detección anticipada de amenazas (72 h antes)	Da Silva (2024)
Auditoría y ética digital	Explainable AI	Transparencia y cumplimiento regulatorio (GDPR)	Ortiz (2023)

Nota: Elaboración propia con base en la revisión bibliográfica (2020–2025).

1.9 La Ciberseguridad del Futuro: Hacia un Enfoque Híbrido y Adaptativo

La evolución de la ciberseguridad, impulsada por la IA, se dirige inevitablemente hacia un modelo híbrido y adaptativo. Los resultados indican que los sistemas modernos no

solo detectan, sino que también aprenden y se adaptan a las nuevas tácticas de los atacantes (Boné-Andrade et al., 2023). Sin embargo, esto plantea un desafío de la carrera armamentística entre el atacante y el defensor. Los ciberdelincuentes están utilizando, a su vez, técnicas de IA (como el Machine Learning Evasivo) para diseñar malware polimórfico que evade los sistemas de detección. Esta dinámica subraya que la IA defensiva debe ser tan ágil como la ofensiva.

En la última década, la IA ha dado paso a un paradigma de seguridad más predictivo y proactivo. Los sistemas de IA ahora tienen la capacidad de predecir vulnerabilidades potenciales y neutralizar ataques en tiempo real. La Inteligencia Artificial Explicable (XAI) ya no es un capricho; más bien, es una necesidad operativa y ética. Nos permite auditar aquellas decisiones tomadas automáticamente. En el campo de la ciberseguridad, las organizaciones exigen total transparencia en el funcionamiento de la IA. Esto es crucial para que los analistas humanos comprendan cómo una alerta de vulnerabilidad se considera "crítica" y qué provoca que se tomen acciones de contención. En los últimos años, la IA ha evolucionado hacia un modelo de seguridad más predictivo y proactivo. Esto se ha posibilitado en gran medida por el auge de los sistemas de detección automatizados que también están siendo desarrollados y aprovechados en su mayoría. Estos sistemas posibilitan que la Inteligencia Artificial opere de forma autónoma, anticipando amenazas antes de su materialización y fortaleciendo los mecanismos de protección, un ejemplo representativo es IBM Watson para ciberseguridad, una herramienta orientada a la detección y mitigación de amenazas en tiempo real mediante el procesamiento y análisis avanzado de

datos, lo que contribuye a una respuesta más eficiente y fundamentada. Con esta transformación, encontramos que, al usar computadoras para proteger sistemas digitales con tecnología de inteligencia artificial, la forma en que manejamos estas preocupaciones cambia notablemente. En nuevos entornos de este tipo, los expertos en IA y ciberseguridad han trabajado juntos y siguen trabajando juntos de la misma manera. Colectivamente, están creando sistemas que funcionan de manera más versátil, intelectual y éticamente responsable para un mundo cibernético más profundo y feroz (Martínez et al., 2024).

Conclusiones

Una vez que se utiliza la IA en la ciberseguridad, se produce una ruptura con el antiguo marco defensivo. Ha sido un cambio de paradigma que comenzó con un modelo reactivo y también ha pasado a ser un modelo de predictibilidad. Como resultado, se ha observado que la resiliencia operativa se ha mejorado significativamente, con una notable disminución en el Tiempo Medio de Detección (MTTD) así como en el Tiempo Medio de Respuesta y Recuperación (MTTR). El progreso observado en estos desarrollos proporciona un claro Retorno de la Inversión (ROI).

Sin embargo, la utilidad de la IA se ve obstaculizada debido a desafíos, como el alto costo y la falta de conocimiento, especialmente en pequeñas y medianas empresas (PYMES) y países en desarrollo. Esto sugiere la necesidad de construir modelos de servicio para hacer disponibles tales herramientas de defensa sofisticadas, ya sea a través de Proveedores de Servicios de Seguridad Gestionada (MSSP) o enfoques de Seguridad como Servicio (SaaS).

En cuanto a la dimensión ética, es importante tratar la Inteligencia Artificial Explicable (XAI) como una necesidad operativa. De esta manera, fomenta la auditabilidad y la mitigación del sesgo en los algoritmos, y genera confianza en la toma de decisiones automatizada.

Finalmente, el futuro de la ciberseguridad se define por un enfoque híbrido, donde la inversión en tecnología ágil para la detección avanzada debe ir acompañada de la capacitación del personal para la gestión ética y estratégica de dichos sistemas, ya que el profesional de la ciberseguridad evoluciona de analista de alertas a estratega y auditor de los modelos de IA.

Referencias Bibliográficas

Ayala, F. M. & Sevilla, G. M. (2023). Mapeo del panorama actual de la ciberseguridad en la era moderna digital. *RECIMUNDO,* *7*(2), 441-452. https://doi.org/10.26820/recimundo/7.(2).jun.2023.441-452

Acosta Cortez, N. N. (2024). Impacto de la inteligencia artificial en la ciberseguridad empresarial: un análisis crítico de la evolución de amenazas y medidas preventivas. Babahoyo: UTB-FAFI. 2024. http://dspace.utb.edu.ec/handle/49000/15738

Ariza, A. & Vargas, M. (2025). Introducción a la Inteligencia Artificial y el Aprendizaje Automático en Ciberseguridad. Revista Colón Ciencias, Tecnología y Negocios, 12(1), 32–48. https://doi.org/10.48204/J.COLONCIENCIAS.V12N1.A6824

Boné-Andrade, M. F. (2023). Evaluación de la evolución de la ciberseguridad en sistemas empresariales modernos. Multidisciplinary Collaborative Journal, 1(2), 25–38. https://doi.org/10.70881/MCJ/V1/N2/14

Da Silva, M. (2024). *Predictive cybersecurity systems: AI and enterprise resilience. Springer.*

Denzin, N. K. (2017). The research act: a theoretical introduction to sociological methods.

Boné-Andrade, M., Pinargote-Bravo, V. y Bonilla-Fierro, L. (2023). Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto. Revista Científica Ciencia y Método, 1(4), 31–43. https://doi.org/10.55813/GAEA/RCYM/V1/N4/21

González, R. (2023). *Aprendizaje automático y detección temprana de amenazas informáticas.* Alfaomega.

Hernández, J. (2025). *Blockchain e inteligencia artificial en la protección de datos corporativos.* Pearson Educación.

Hernández-Sampieri, R. & Mendoza, C. (2021). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill.

Higgins y Green, (2011) Manual Cochrane para Revisiones Sistemáticas de Intervenciones. Versión 5.1.0. La Colaboración Cochrane. - Referencias - Publicaciones de Investigación Científica. (n.d.). Retrieved January 4, 2026, from https://www.scirp.org/reference/referencespapers?referenceid=2225527

Horlichenko, S. (2024). Specific aspects of the legal and regulatory framework for cybersecurity in different countries of the world in the context of the international security system. Grail of Science, 36, 90–97. https://doi.org/10.36074/GRAIL-OF-SCIENCE.16.02.2024.013

Khan, N., Furnell, S., Bada, M., Nurse, J. & Rand, M. (2025). The hidden barriers to cyber security adoption amongst Small and Medium-Sized Enterprises. Information and Computer Security. https://doi.org/10.1108/ICS-04-2025-0135

Kitchenham, B. & Charters, S. (2021). *Guidelines for performing systematic literature reviews in software engineering. Elsevier.*

Kumar, A. & Patel, D. (2023). *AI-driven automation for enterprise security management.* Elsevier.

Lee, C. (2021). *SOAR architectures and automated response in cybersecurity operations.* CRC Press.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J., Clarke, M., Devereaux, P. J., Kleijnen, J. & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. Journal of Clinical Epidemiology, 62(10), e1–e34. https://doi.org/10.1016/j.jclinepi.2009.06.006

Martínez, L. B., Semenets, V. H., Carmona, M. Á. & Ordiano, J. G. (2024). *La inteligencia artificial en la ciberseguridad.* ReinvenTec.

Martínez, L. & Salazar, P. (2024). *Redes neuronales aplicadas a la seguridad informática empresarial.* McGraw-Hill.

Moher, D. & Group, P. (2020). *Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement.* PLOS Medicine.

Nascimento, S. M., Paiva, T.M. de, Kasuga, M. P., Silva, T. de A. F., Crozara, C. M., Byk, J. & Furtado, S. da C. (2024). La inteligencia artificial y sus implicaciones éticas y legales: revisión integradora. Revista Bioética, 32, e3729PT. https://doi.org/10.1590/1983-803420243729PT

Navarro, F., & Ruiz, S. (2022). *Ética y regulación en la inteligencia artificial empresarial.* Editorial UOC.

Ortiz, V. (2023). *Explainable AI y transparencia en la ciberseguridad corporativa.* Reverté.

Ponce, J. (2023). *Inteligencia artificial aplicada a la ciberseguridad corporativa.* Alfaomega.

Quffa, A. & Samy. (2025). A Rule-Based Expert System for Cybersecurity ThreatDetection: Evolution, Applications, and the Hybrid AI Paradigm. *Information Technology Department Faculty of Engineering and Information Technology, 9*(8), 44-62. https://doi.org/ISSN: 2643-9085

Sandua, D. (2024). Evolución De La Inteligencia Artificial: de asistentes virtuales a robots autónomos.

Segarra Figueroa, O. N. (2025). Gobernanza algorítmica y democracia: desafíos éticos de la inteligencia artificial en el estado. *Sage Sphere en Inteligencia Artificial, 3*(1), 1-11. https://doi.org/https://sagespherejournal.com/index.php/SSAI/article/view/91

Shayma Sultana, M. M., & Rafy, A. (2022). AI-Powered Threat Detection: Enhancing Real-Time Response in Enterprise Environments. *World Journal of Advanced Engineering Technology and Sciences, 6*(2), 136-146. https://doi.org/ https://doi.org/10.30574/wjaets.2022.6.2.0079

Zhao, L. (2022). *Machine learning for real-time intrusion detection in corporate networks.* Academic Press.