Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

La Inteligencia Artificial y su Impacto a la Seguridad del Estado Ecuatoriano

Artificial Intelligence and Its Impact on the Security of the Ecuadorian State

Jaime Ernesto Mayorga-Sandoval [1]
Oficial de Operaciones Psicológicas de la Primera División del Ejército "Shyris"
Ejército ecuatoriano
jaimemayorgas@gmail.com
Ana María Aldás-Benavides[2]
Docente
Universidad Técnica Particular de Loja UTPL
amaldas2@utpl.edu.ec
Quito, Ecuador

Resumen

En los últimos años, la Inteligencia Artificial [IA] multiplicó su potencial en varias áreas, inclusive la seguridad de los estados, mejorándola con el empleo de herramientas

1 Magíster en Seguridad y Defensa por la Universidad de las Fuerzas Armadas ESPE (2024); Magíster en Gestión de Sistemas de Información e Inteligencia de Negocios por la ESPE (2019). Teniente Coronel de Estado Mayor del Ejército ecuatoriano, Operador Psicológico, Observador Militar en la Misión Híbrida de Naciones Unidas UNAMID Darfur-Sudán (2015-2016). Actualmente se desempeña como Oficial de Operaciones Psicológicas de la Primera División del Ejército "Shyris", ha sido aceptado como alumno del Colegio Interamericano de Defensa en Washington – Estados Unidos, Clase 65 (2025-2026). Código ORCID: https://orcid.org/0009-0007-9862-8857

2 Magíster en Negocios por la Universidad de la Fuerzas Armadas ESPE (2003), Candidata a Doctora en Administración por la Universidad de Medellín UdeM (2018). Docente de la Escuela de Negocios de la Universidad Técnica Particular de Loja UTPL en áreas de Gestión, Estrategia, Innovación, Sostenibilidad y Transformación Digital. Se desempeñó como Directora de Negocios y Servicios Especializados de la Empresa Pública de la Universidad de la Fuerzas Armadas ESPE (2024), actualmente consultora para diferentes organizaciones del país. Código ORCID: https://orcid.org/0009-0005-7959-7405

que optimizan análisis de inteligencia, perfeccionan la ciberseguridad, la vigilancia y la lucha contra el crimen organizado. Sin embargo, existen riesgos como su posible uso malintencionado para desarrollar armas autónomas o perpetrar ciberataques que resultarían perjudiciales para la infraestructura crítica de una nación. El presente estudio tuvo por objetivo determinar la incidencia de la IA en la seguridad digital del Estado ecuatoriano y sus consecuencias físicas. Por esta razón, se efectuó una investigación al interior de las Fuerzas Armadas [FFAA] ecuatorianas para establecer el desarrollo que esta tecnología tiene en el sector de la defensa. Entre los hallazgos más relevantes se encontró que existe la necesidad de securitizar la IA por parte del Estado para prevenir el uso indebido; se debe incluir en la Agenda de Seguridad Nacional a la IA de modo que el impacto negativo del uso de la IA sea mínimo y represente más bien una oportunidad para reforzar la estrategia de defensa del Estado, convirtiéndola en herramienta clave para la seguridad, en un entorno cada vez más tecnológico y dinámico.

Palabras clave: inteligencia artificial, seguridad, Estado, defensa, Fuerzas Armadas

Abstract

Recently, Artificial Intelligence (AI) has multiplied its potential in various fields, including state security, by enhancing it through tools that optimize intelligence analysis, improve cybersecurity, surveillance, and the fight against organized crime. However, there are risks associated with its potential malicious use, such as the development of autonomous weapons or the execution of cyberattacks that could severely impact a nation's critical infrastructure. The objective of this

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

study was to determine the impact of AI on the digital security of the Ecuadorian state and its physical consequences. For this reason, research was conducted within the Ecuadorian Armed Forces (FFAA) to assess the development and application of this technology in the defense sector. Among the most relevant findings, it was observed that there is a need for the State to securitize AI to prevent its misuse; AI should be included in the National Security agenda so that the negative impact of its use is minimized and instead becomes an opportunity to strengthen the State's defense strategy, turning it into a key tool for security in an increasingly technological and dynamic environment.

Keywords: artificial intelligence, security, state, defense, armed forces

Introducción

Contar con tecnología de punta favorece la calidad de vida de quienes la utilizan. La IA está impactando significativamente en la vida del ser humano; este impacto se refleja en un entorno interconectado, tecnificado y globalizado, que ofrece grandes oportunidades de desarrollo, tanto por parte de las empresas como –de manera prioritaria– por los Estados (Ruiz-Baquero, 2018).

En los últimos años, existe un evidente despunte de los avances en IA, propiciado especialmente por empresas como Google, Amazon, IBM y Microsoft que se encuentran a la vanguardia en el desarrollo de sistemas de IA (Gartner Inc., 2023). Estos sistemas inteligentes permiten desde hacer consultas sobre diversos temas y tener respuestas con un elevado nivel de asertividad, hasta incluir ediciones multimedia

de personajes famosos con audio y video simulado, lo que ha generado un amplio debate que va desde lo legal hasta el tratamiento de los datos y la seguridad de la información que debe dar un Estado (Makridakis, 2017).

La seguridad y la defensa son ámbitos en los que el desarrollo de la IA es notable debido a la importancia que las potencias mundiales le han otorgado, puesto que constituye uno de los aspectos de la configuración de los escenarios bélicos que está estrechamente ligado a las capacidades tecnológicas de los Estados (Flores-Vivar et al., 2023). El conflicto entre Ucrania y Rusia es uno de los más recientes escenarios en el que se evidencia el empleo intensivo de tecnologías avanzadas en sistemas de mando y control, inteligencia, ciberdefensa y guerra cognitiva, que han complejizado el escenario bélico (García-Patos-Herreros, 2022). En este contexto, no se puede ignorar la situación que actualmente atraviesa Israel, que, a pesar de tener sistemas de defensa tecnificados y desarrollados, ha vivido uno de los peores escenarios bélicos de su historia debido al ataque terrorista de Hamas el 7 de octubre de 2023. Así mismo, en enero de 2024, Ecuador atravesó uno de los momentos más críticos de su historia reciente, cuando se perpetró un ataque terrorista en vivo, transmitido a través de las redes sociales en tiempo real y que activó la declaratoria de conflicto armado interno (Mayorga y Holguín, 2024).

Hasta hace poco tiempo, la configuración de un escenario plagado de instrumentos tecnológicos de última generación resultaba utópica, solo posible en el cine de ciencia. En estos días, con asombro se observa el uso sofisticado de instrumentos y aparatos tecnológicos en el campo de batalla. Soldados que cuentan con implementos que les facilitan estar

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

interconectados con visores, armamento, comunicaciones, mejorando su empleo y rendimiento, incluso con drones y robots (Stoppani, 2022).

En la Unión Europea, por ejemplo, han existido sendos estudios y análisis con la finalidad de aplicar ciertas consideraciones de la IA en temas de defensa y, de la misma forma, presentar las restricciones correspondientes para salvaguardar la seguridad de los Estados (Palayer, 2020). En Latinoamérica, se han llevado a cabo estudios y en algunos casos se han desarrollado políticas, pero han sido muy limitadas, debido a cuestiones –esencialmente– de presupuesto. Países como Brasil, Argentina, Perú y Colombia buscan promover el desarrollo de tecnologías basadas en IA con un amplio apoyo gubernamental (Romero-Mier, 2019).

En el Ecuador, se han presentado estudios y análisis prospectivos respecto de las implicaciones del uso de la IA en varias áreas, principalmente las sociales. Una de las mayores preocupaciones resulta de la ausencia de regulaciones, supervisión y normativa, en especial por parte de las instituciones del Estado (Facultad Latinoamericana de Ciencias Sociales [FLACSO], 2023). La política de la defensa de Ecuador, desarrollada por el Ministerio de Defensa Nacional y plasmada tanto en el Libro Blanco de la Defensa de 2018 como en el Plan Específico del Sector Defensa 2021-2030 y en el Plan Sectorial de Defensa 2021-2025, no menciona siquiera el concepto de IA, mucho menos refiere a las repercusiones que podría tener el Estado por su implementación.

Varios países de Europa, Asia y Norteamérica han evidenciado la necesidad de incluir dentro de sus acciones de defensa esfuerzos dedicados exclusivamente a IA, puesto que

existen riesgos y amenazas para la seguridad de los Estados, con ataques que incluyen armamento, vehículos y robots autónomos, tecnología inteligente, ciberamenazas, manejo cognitivo de la información a través de redes sociales, entre otras (García-Patos-Herreros, 2022).

El problema radica en conocer si las FFAA del Ecuador están en condiciones de aprovechar las oportunidades y enfrentar las amenazas que se generan actualmente a la seguridad del Estado por medio de la IA; por ello, el presente estudio tiene por objeto determinar la incidencia de la IA en la seguridad digital del Estado ecuatoriano y sus consecuencias físicas. De esta forma se ha desarrollado una investigación al interior de las FFAA del Ecuador, a fin de establecer la comprensión y evolución de esta tecnología en el sector defensa. Entre los resultados más importantes se refleja la necesidad de securitizar la IA por parte del Estado, incluir en la agenda de Seguridad Nacional a la IA e implementar otras estrategias para minimizar el impacto de la IA y enfocar los esfuerzos para aprovechar las oportunidades que esta herramienta representa hoy en día.

Alcance de la IA

El origen de la IA está estrechamente relacionado con los fundamentos de la robótica, cuyos principios fueron introducidos por el escritor ruso Isaac Asimov en su obra *Runaround* (1942, en *The Complete Robot* de Asimov, 1982), donde destacó las leyes de la robótica, sentando las bases conceptuales para el desarrollo de esta disciplina (Jun et al., 2021). Posteriormente, Alan Turing (1950) propuso una prueba con la finalidad de demostrar la existencia de inteligencia en un dispositivo no biológico; se conoció como

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

el "Test de Turing", cuya hipótesis se resume en que, si una máquina se comporta en todos los aspectos como inteligente, entonces debe ser inteligente.

Existen varios modelos desarrollados sobre IA, entre ellos están: sistemas que piensan como humanos, sistemas que actúan como humanos, sistemas que piensan racionalmente y sistemas actuantes racionales. Cada uno de estos modelos emplea lógicas de información, datos y algoritmos propios (Jun et al., 2021). También, varias aplicaciones tienen como origen la IA y han sido apuntaladas por las ciencias informáticas y computacionales; entre ellas están los lenguajes de programación, las aplicaciones y sistemas expertos y los ambientes de desarrollo (Crespo et al., 2022).

Según Arend Hintze (2016), profesor de biología integrativa y ciencias de la computación e ingeniería en la Universidad Estatal de Michigan, la IA se puede categorizar en cuatro tipos: (a) máquinas reactivas, sistemas de IA no tienen memoria y manejan una tarea específica; se centran usualmente en el análisis de datos masivos para obtener predicciones o proyecciones (Gómez-Llinás, 2021); (b) de memoria limitada, sistemas de IA que tienen memoria y pueden utilizar experiencias pasadas para informar sobre futuras decisiones; automatizan tareas como los dispositivos de navegación de los automotores (Castro, 2022); (c) teoría de la mente, que se basa en un término psicológico y se refiere a la capacidad de las máquinas de comprender las creencias, deseos e intenciones de otros agentes basados en el aprendizaje continuo (Hintze, 2016); (d) autoconsciencia, que se refiere a la capacidad de la IA para percibir su entorno,

comprender su propia existencia y tomar decisiones basadas en ese conocimiento, llegando incluso a estar en condiciones de imitar a la consciencia humana (Gómez-Llinás, 2021).

Las áreas en las que más se ha aplicado la IA son: minería de datos, reconocimiento de imágenes, sistemas expertos, lógica difusa, vida artificial, sistemas tutores inteligentes, programación evolutiva, reconocimiento de patrones, interfaces inteligentes, algoritmos genéticos, programación lógica, optimización multiobjetivo, algoritmos bioinspirados, procesamiento del lenguaje natural, redes neuronales, aprendizaje de máquina, sistemas híbridos inteligentes, realidad aumentada, teoría de autómatas (Dwivedi et al., 2021).

Evolución de los Sistemas de Seguridad y Defensa

Las guerras de cuarta y quinta generación son términos acuñados para describir nuevas formas de conflicto y estrategias militares que han surgido en el contexto de la evolución de la tecnología y la geopolítica dinámica. Estos conceptos no están definidos de manera uniforme ni son ampliamente aceptados; sin embargo, se han utilizado en el análisis militar y estratégico para describir diferentes tipos de conflictos. Las Guerras de Cuarta Generación [4GW, por sus siglas en inglés] se basan mayoritariamente en amenazas asimétricas, con actores no estatales, un enfoque de guerra sicológica y el empleo de tecnología y comunicaciones (Haro-Ayerve, 2019). Por su parte, las Guerras de Quinta Generación [5GW, por sus siglas en inglés] tienen actualmente un concepto menos definido, pero sí enfocado en la guerra cibernética, IA y desafío a la estabilidad global (Gayozzo, 2021).

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Laurent Murawiec (2017) ha posicionado el término de "guerra asimétrica", señalando que no es solamente la guerrilla ni la guerra del débil contra el fuerte, sino que introduce un elemento de ruptura tecnológico, estratégico o táctico, un elemento que cambia la idea preconcebida. Colin S. Gray (2002), por su parte, considera el conflicto asimétrico como un método de combate difícil de definir, pero que se basa en lo inusual, en lo inesperado y utiliza procedimientos ante los cuales no resulta fácil una respuesta mediante fuerzas y métodos convencionales. Sin embargo, pese a que se ha tratado de dar una definición sobre los conflictos asimétricos, no existe consenso al respecto. El conflicto asimétrico no se da solo por la desigualdad de potenciales, sino cuando los adversarios adoptan formas de combate no convencionales y con diferencias básicas en su modelo estratégico, empleando métodos alejados de las leyes y principios de la guerra y empleando armas de destrucción masiva (Haro-Ayerve, 2019).

Autores Richard Clarke y Robert Knake (2011) concuerdan con Thomas Rid (2020) en que las operaciones militares tienen cinco dominios: aire, tierra, mar, espacio, donde se desarrollan las actividades relacionadas con satélites, estaciones espaciales y otras tecnologías orbitales, y ciberespacio, dominio virtual constituido por redes informáticas, datos e infraestructura digital. Las Operaciones Multi-Dominio [Multi-Domain Operations o MDO] representan un nuevo enfoque táctico y operacional adoptado por los ejércitos de varios países del mundo, para abordar las cambiantes amenazas y desafíos en el escenario geopolítico contemporáneo. Esta estrategia se encuentra en fase de implementación y se centra en la capacidad de influir,

de manera coordinada, en todas las dimensiones del campo de batalla (Méndez-Vélez et al., 2019).

La teoría de los "Complejos de Seguridad" es relativamente nueva y ha sido desarrollada por Barry Buzan y la Escuela de Copenhague; consiste en un enfoque holístico que busca comprender la seguridad internacional, considerando las interconexiones entre Estados, la diversidad de amenazas y la importancia de la securitización en la formulación de políticas de seguridad. Algunos aspectos clave de esta teoría incluyen: (a) unidades de análisis: en lugar de centrarse en los Estados individuales, la teoría considera unidades más amplias, como los complejos de seguridad, que abarcan varios Estados interconectados por preocupaciones de seguridad compartidas; (b) interdependencia: los complejos de seguridad se caracterizan por la interdependencia entre los Estados miembros, lo que significa que las acciones de un Estado dentro del complejo pueden tener repercusiones en la seguridad de otros Estados en la región; (c) diversidad de amenazas: la teoría reconoce que las amenazas a la seguridad pueden ser diversas y no se limitan únicamente a las cuestiones militares tradicionales, incluyen aspectos económicos, sociales, ambientales y políticos que pueden afectar la estabilidad y la seguridad de un complejo de seguridad; (d) securitización: este concepto se refiere al proceso mediante el cual se convierten temas no tradicionales de seguridad en asuntos de seguridad legítimos que requieren una respuesta urgente. La securitización implica la construcción de narrativas que presentan ciertos problemas como amenazas a la seguridad, lo que justifica la adopción de medidas extraordinarias (Buzan, 2003).

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

La Seguridad del Estado Frente a la IA

La IA está siendo empleada por países como Rusia, Ucrania, Israel, Estados Unidos, en la toma de decisiones estratégicas para la seguridad nacional; su importancia radica en la capacidad para procesar grandes cantidades de datos de manera rápida y eficiente, identificar patrones, predecir posibles amenazas y proporcionar información valiosa para la toma de decisiones. La IA mejora la precisión y velocidad en la evaluación de situaciones de seguridad, permitiendo anticiparse a amenazas y tomar medidas preventivas. Además, puede utilizarse en sistemas de vigilancia autónomos como drones, para detectar amenazas de forma más eficaz. En el ámbito de la seguridad nacional, la IA aplicada en defensa nuclear permite respuestas más efectivas ante situaciones críticas, superando capacidades humanas. En resumen, la IA es una herramienta fundamental para fortalecer la seguridad nacional, ofreciendo capacidades avanzadas de análisis, vigilancia y toma de decisiones estratégicas en un entorno complejo y cambiante (Romero-Mier, 2019).

La IA aplicada en el ámbito de la defensa, como lo hiciera Israel en su conflicto con Hamas, mejora la eficiencia, precisión y rapidez en la toma de decisiones militares, optimiza las operaciones y estrategias, puesto que permite el análisis de grandes volúmenes de datos para decisiones informadas; permite operaciones independientes, con la utilización de sistemas autónomos para misiones eficientes y seguras; facilita la seguridad cibernética a través de la detección y prevención de ciberataques para proteger redes militares; ayuda al entrenamiento y simulación para mejorar habilidades operativas y tácticas. Ha generado innovación

tecnológica en FFAA para enfrentar desafíos futuros. La IA es crucial para modernizar y optimizar las operaciones militares, contribuyendo a la seguridad nacional en un entorno cada vez más líquido (Instituto Español de Estudios Estratégicos, 2019).

La implementación de tecnologías como la IA también se ha reflejado en usos militares. El empleo de los centros de manejo de información en las FFAA involucra análisis y procesos que podrían estar basados en IA (Mayorga, 2020). La automatización y la robótica en las FFAA ofrecen beneficios como el incremento de la seguridad de los soldados, mejora en la ayuda humanitaria, estudio del enemigo, capacidad de destrucción controlada y toma de decisiones. Sin embargo, también plantea desafíos morales, legales y de seguridad, tales como dilemas éticos en el uso de armamento autónomo, rechazo público a las bajas, dependencia tecnológica, necesidad de control y supervisión, y la adaptación y formación adecuada de los soldados y operadores. Es fundamental abordar estos desafíos de manera cuidadosa y responsable para aprovechar los beneficios de estas tecnologías en las FFAA (Centro Conjunto de Desarrollo de Conceptos, 2020).

La Percepción e Impacto en la Seguridad y Defensa del Ecuador

Es fundamental que el sector de defensa pueda contar con la información necesaria respecto de las oportunidades que tendrían las FFAA al implementar la IA para la defensa de la soberanía e integridad territorial en la protección de infraestructuras críticas, prevención del crimen y la seguridad de los ciudadanos; sobre todo, identificar las amenazas que podrían generarse a la seguridad y defensa del país a través del empleo de las diferentes herramientas que usan IA (Romero-Mier, 2019).

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Este estudio determinó que el Ecuador carece de instrumentos que permitan implementar, articular y emplear la IA en el sector de defensa. Existe poca investigación al respecto. De ahí el valor teórico de esta investigación, que ayudará a generar nuevas propuestas sobre cómo la IA podría emplearse para mejorar la seguridad del país.

Es necesario, además, establecer un marco referencial que visualice de forma clara el potencial que tendrían las FFAA al implementar sistemas basados en IA y, por otra parte, evidenciar las amenazas que generaría al Estado el uso de la IA por elementos ajenos a las fuerzas de seguridad. La IA es una tecnología que ha experimentado un desarrollo exponencial en los últimos años y su aplicación a la seguridad y defensa está cobrando cada vez más realce. En el caso del Ecuador, el empleo de la IA en este ámbito podría tener un impacto significativo, contribuyendo a mejorar las capacidades de las FFAA en su afán de disuadir, detectar y responder a las nuevas amenazas que se generan (Hunter et al., 2023).

Metodología

El objetivo general de esta investigación fue determinar las oportunidades y amenazas actuales en la seguridad y defensa del Estado ecuatoriano generadas por la irrupción de la IA, para lo que se plantearon las siguientes preguntas de investigación: ¿Cómo impacta la IA en la seguridad y defensa de un Estado, considerando sus características, fortalezas y vulnerabilidades? ¿Qué nivel de implementación y regulación existe en el Ecuador respecto al uso de la IA en los sistemas de seguridad y defensa estatal? ¿Están las Fuerzas Armadas del Ecuador preparadas para aprovechar las oportunidades y enfrentar las amenazas que la IA representa para la seguridad del Estado?

Para el desarrollo de este análisis se emplearon varios tipos de investigación: una de tipo bibliográfica, descriptiva, a través del análisis de investigaciones relacionadas con el tema; otra de tipo descriptiva, cualitativa de fuentes primarias, por medio de entrevistas a cinco expertos en seguridad y defensa nacional; además, se realizó una investigación exploratoria, descriptiva, cuantitativa, no probabilística a través de encuestas digitales, para lo cual el tamaño de la muestra se definió a través de fórmula finita conforme a la población de oficiales superiores de las FFAA equivalente a 2.527 oficiales, un nivel de confianza del 90%, 5% de error de estimación y el 50% de probabilidad *p*, resultando una muestra de 176 personas.

Se realizaron entrevistas a expertos a fin de recopilar opiniones y perspectivas de profesionales con experiencia en el ámbito de la seguridad y defensa, para obtener un panorama sobre la percepción y el impacto de la IA en el contexto ecuatoriano. Las preguntas exploraron su visión sobre la IA y su relación con la seguridad del Estado. Las entrevistas permitieron identificar las concepciones sobre la IA, las vulnerabilidades del sistema de seguridad en relación con esta tecnología y las oportunidades que presentan para mejorar la defensa nacional. Los resultados revelaron una preocupación común entre los expertos sobre los riesgos potenciales que la IA puede representar y la necesidad de establecer un marco normativo que regule su uso en el ámbito de la seguridad. Se destacó la importancia de la capacitación y preparación de las FFAA para enfrentar los desafíos que la IA presenta, así como la necesidad de fomentar la investigación y el desarrollo tecnológico en este campo, proporcionando

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

información valiosa que complementa la investigación, subrayando la urgencia de abordar la implementación de la IA en la seguridad del Estado de manera ética y responsable.

Por otro lado, se diseñó un cuestionario estructurado para obtener información que permita determinar la percepción sobre el alcance que ha tenido la IA en el sector defensa. El cuestionario se aplicó a una muestra representativa, por medio de un formulario virtual difundido por canales electrónicos de forma aleatoria simple, dirigido al personal de oficiales en los diferentes niveles de mando y en cada una de las ramas de las FFAA. Si bien es cierto, estos resultados no son determinantes, constituyen una medición relativa de la incursión de la IA en el personal militar.

Resultados

De los datos demográficos más relevantes de la investigación resulta que la mayoría de los encuestados son hombres, lo que refleja una tendencia en la composición de las FFAA. Un alto porcentaje de los encuestados posee el grado de teniente coronel con el **59,66%, es decir,** que la mayoría de los participantes tienen un nivel significativo de experiencia y responsabilidad por estar al mando de las unidades militares. La mayoría de los encuestados pertenecen al Ejército **con un 48,30%** de la muestra. Finalmente, un **35,80%** de los encuestados se desenvuelve profesionalmente en unidades operacionales, lo que implica que tienen experiencia directa en la implementación de estrategias de seguridad y defensa.

En cuanto al conocimiento que el personal tiene respecto de la IA, casi el 50% la asocia principalmente con aplicaciones de texto generativas, como Chat GPT, lo que refleja una percepción limitada. Solo un 26,70% la relaciona

con sistemas informáticos en general, y un porcentaje menor la vincula con robótica o bases de datos. Aunque un 50% de los encuestados se siente al menos algo familiarizado con el uso de IA, un 49,68% se muestra poco o nada familiarizado. Esto sugiere que hay una falta de conocimiento y capacitación en su aplicación práctica dentro de las FFAA. Un 76,14% de los encuestados cree que la IA puede mejorar la seguridad y defensa del Estado, lo que indica una percepción positiva sobre el potencial de la IA en este ámbito.

En cuanto a la relación entre la IA y la seguridad de un Estado, un 76,14% de los encuestados considera que la IA puede representar una amenaza para la seguridad de los Estados, reflejando una preocupación significativa sobre los riesgos asociados con su uso; esto sugiere que, aunque se reconoce el potencial positivo de la IA, también hay un fuerte sentido de precaución respecto a sus implicaciones negativas. El 50% de los encuestados identifica los ciberataques como el mayor riesgo potencial, reflejando una preocupación por la vulnerabilidad de los sistemas ante amenazas digitales. La desinformación y el control de sistemas críticos también son considerados riesgos importantes, lo que apunta a que los encuestados son conscientes de las múltiples formas en que la IA puede ser utilizada de manera maliciosa. Un 76,13% de los encuestados está de acuerdo en que la IA puede ser utilizada como herramienta de vigilancia, reflejando una aceptación generalizada de su uso en este contexto; sin embargo, esto también plantea cuestiones éticas sobre la privacidad y el uso de la tecnología en la vigilancia estatal. Un 80,68% de los encuestados cree que la IA debería ser regulada en su uso en el ámbito de la seguridad, destacando una fuerte demanda de

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

marcos normativos que guíen su implementación. En lo que respecta al cruce de variables entre las áreas de aplicación y la percepción de lo que es la IA, el 24,43% considera que el Chat GPT se emplea en todas las áreas. Un dato que llama la atención es que el 0% cree que las bases de datos y el Chat GPT no se emplean como IA en el área de salud, como se puede evidenciar en la Tabla 1.

Tabla 1

Áreas de aplicación vs Percepción de IA

OPCIONES	Base de datos		Chat GPT o similares		Robótica		Sistemas Informáticos		TOTAL
	Cant.	*%*	*Cant.*	*%*	*Cant.*	*%*	*Cant.*	*%*	
Computación	5	2,84%	15	8,52%	6	3,41%	5	2,84%	31
Diseño Gráf.	2	1,14%	10	5,68%	2	1,14%	8	4,55%	22
Educación	6	3,41%	14	7,95%	2	1,14%	7	3,98%	29
Salud	0	0,00%	0	0,00%	2	1,14%	3	1,70%	5
Seg. y Def.	4	2,27%	4	2,27%	2	1,14%	3	1,70%	13
Todas	8	4,55%	43	24,43%	4	2,27%	21	11,93%	76
TOTAL	**25**	**14,20%**	**86**	**48,86%**	**18**	**10,23%**	**47**	**26,70%**	**176**

Nota: Elaboración propia

Por otro lado, al considerar las capacidades y vulnerabilidades que podría generar la implementación de la IA en la seguridad del Estado, los datos más relevantes fueron los siguientes: un 76,14% de los encuestados considera que la IA puede mejorar la eficiencia en la gestión de la seguridad. Un 76,13% de los encuestados está de acuerdo en que la IA puede ser utilizada para la toma de decisiones estratégicas en seguridad. Un 80,68% de los encuestados considera que la implementación de la IA en seguridad podría generar dependencia tecnológica. Un 76,14% de los encuestados cree que la IA puede ser utilizada para mejorar la capacitación

del personal en seguridad. Un 76,13% de los encuestados considera que la IA puede contribuir a la prevención del delito. En lo que corresponde al cruce entre las áreas de aplicación de la IA en temas de seguridad y la posibilidad de ser consideradas como amenaza, el 42,05% cree que la ciberseguridad puede ser considerada como amenaza; la vigilancia tiene el segundo lugar con el 12,50%; sin embargo, el control fronterizo, la defensa, la inteligencia y los sistemas operativos del campo de batalla no son considerados como posibilidad de ser una amenaza a la seguridad de los Estados a través de la IA (resultados mostrados en la Tabla 2).

Tabla 2

Áreas de aplicación de IA en seguridad vs posibilidad de ser amenaza

OPCIONES	No		Si		Tal vez		TOTAL
	Cant.	*%*	*Cant.*	*%*	*Cant.*	*%*	
Ciberseguridad	2	1,14%	74	42,05%	12	6,82%	88
Control Fronterizo	0	0,00%	2	1,14%	1	0,57%	3
Defensa	0	0,00%	5	2,84%	1	0,57%	6
Gestión de Riesgos	1	0,57%	9	5,11%	3	1,70%	13
Inteligencia	0	0,00%	19	10,80%	6	3,41%	25
Otra	0	0,00%	3	1,70%	0	0,00%	3
SOCB´s	0	0,00%	8	4,55%	2	1,14%	10
Vigilancia	1	0,57%	22	12,50%	5	2,84%	28
TOTAL	**4**	**2,27%**	**142**	**80,68%**	**30**	**17,05%**	**176**

Nota: Elaboración propia

Finalmente, al indagar sobre la implementación de la IA en la seguridad del Estado, se pudo obtener los siguientes resultados: el 85,23% de los encuestados considera que la IA puede ser utilizada para mejorar la vigilancia en áreas críticas. Un 86,36% de los encuestados está de acuerdo en que la IA

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

puede ayudar en la identificación de amenazas en tiempo real; el 85,23% de los encuestados considera que la implementación de la IA en seguridad podría generar problemas éticos.

Propuesta

Como resultado del trabajo de investigación, se presenta una propuesta de implementación dentro de la política de la Defensa Nacional, a fin de establecer lineamientos en su tratamiento por parte del Estado ecuatoriano.

Figura 1

Inteligencia artificial en el sector de la defensa

Nota: Elaboración propia

Acciones Recomendadas para el Estado Ecuatoriano Frente a la IA

Es necesario que el Estado –entre otras acciones– impulse: a) El establecimiento de un marco legal y ético para el desarrollo y uso de la IA en el ámbito de la seguridad, a través de la definición de principios claros y transparentes para el desarrollo y uso responsable de la IA. Es necesario contar con

una regulación de la recopilación y uso de datos personales para garantizar la privacidad y protección de las libertades civiles, estableciendo mecanismos de rendición de cuentas y supervisión para garantizar su uso responsable. b) El fomento de la transparencia y la rendición de cuentas en el desarrollo y uso de la IA, con la publicación de información sobre los sistemas utilizados por las agencias de seguridad, a través de la creación de mecanismos para que la ciudadanía pueda solicitar información y presentar quejas sobre el uso de la IA, estableciendo mecanismos de revisión independiente para evaluar el impacto de la IA en la seguridad del Estado. c) La inversión en investigación y desarrollo de la IA para la seguridad, financiando proyectos de investigación para incorporar o desarrollar herramientas de IA más seguras y confiables. d) Promoción de la colaboración entre el sector público, privado y académico en el desarrollo de la IA para la seguridad, tanto en empresas nacionales como extranjeras. e) Capacitación del personal de seguridad en el uso responsable y ético de la IA, y f) Fortalecimiento de la cooperación internacional para abordar los desafíos globales de la IA en la seguridad, a través del desarrollo de normas y directrices internacionales para el uso responsable, generando el intercambio de información y mejores prácticas entre países, para prevenir y mitigar los riesgos de la IA, fomentando la colaboración en investigación y desarrollo de la IA en el sector defensa.

Direccionamiento Estratégico

El Estado debe incluir en sus documentos de direccionamiento estratégico a la IA, entre otras, por las siguientes razones:

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

a) La IA es una herramienta estratégica y de defensa, ya que permite la toma de decisiones más precisas basadas en el análisis de datos; su implementación se ha vuelto crucial en la protección de los intereses nacionales durante conflictos bélicos y en tiempos de paz, ante la complejidad de los nuevos escenarios de seguridad y defensa.
b) Vinculación de la IA con la defensa, ya que los programas basados en IA pueden responder de manera más eficiente que los humanos frente a amenazas críticas y la lucha contra el terrorismo.
c) Seguridad Nacional: la IA se ha integrado en las políticas de defensa y desarrollo de las principales potencias del mundo, siendo parte de sus planes estratégicos hacia el futuro, ya que su uso plantea desafíos tanto de origen tecnológico como humano.
d) Amenazas y beneficios: si bien la IA ofrece beneficios significativos en términos de seguridad y defensa, también plantea amenazas potenciales; su mal uso o falta de control podría representar un riesgo incalculable, como lo mencionó Stephen Hawking (Hawking, 2018) al referirse al futuro de las tecnologías de súper IA.

Generación de un Marco Normativo Legal para la IA

Una de las vulnerabilidades que tiene nuestro país respecto de la IA y las nuevas tecnologías es la carencia de un marco legal que permita, limite, restrinja y sancione prácticas básicas en este campo. Es necesario generar un marco legal normativo efectivo para la IA, con las siguientes consideraciones:

· transparencia y responsabilidad para evitar decisiones incorrectas o dañinas, especialmente en temas relacionados con la seguridad del Estado;

· protección de datos, con regulaciones que garanticen la privacidad de los individuos en el contexto de la IA, con la prevención de posibles vulneraciones a la seguridad de las personas;

· evaluación de impacto, tanto ético como social, para identificar posibles riesgos, sesgos algorítmicos y efectos no deseados en diferentes sectores; participación multisectorial, fomentando la colaboración entre profesionales, responsables de políticas, funcionarios de las carteras de seguridad y defensa, expertos en tecnología y representantes de la sociedad civil;

· formación y capacitación, incluyendo en el marco normativo la promoción de programas enfocados en ética y regulación de la IA para garantizar que los profesionales involucrados en su desarrollo y aplicación estén preparados para enfrentar los desafíos;

· actualización continua con mecanismos que permitan la modernización constante del marco legal en función de los avances tecnológicos y los nuevos desafíos que surjan, asegurando su adaptabilidad a un entorno en constante evolución.

La IA como Amenaza

La IA podría utilizarse de manera maliciosa para llevar a cabo ciberataques sofisticados, desinformación automatizada, manipulación de datos o incluso para desarrollar armas autónomas. Estos escenarios representan desafíos significativos para la seguridad nacional, ya que podría ser aprovechada por actores hostiles para socavar la estabilidad y la integridad de un país. En el actual conflicto entre Israel y Hamas, existe un sistema de procesamiento de datos

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

denominado "Lavanda", empleado por las Fuerzas de Defensa de Israel [FDI], encargado de procesar recomendaciones sobre posibles blancos a atacar. Si bien es cierto que consiste en una ayuda potencial, también se genera un riesgo sobre la configuración de blancos y la no discriminación entre tropas enemigas y civiles, lo que podría ocasionar daños colaterales de incalculables consecuencias (García, 2024).

Por otro lado, la IA también puede ser una herramienta estratégica para fortalecer la seguridad y defensa nacional, empleándose en la detección temprana de amenazas, análisis de grandes volúmenes de datos para identificar patrones y tendencias, mejorar la ciberseguridad y optimizar la toma de decisiones en tiempo real; un claro ejemplo constituye el "domo de hierro", con el cual las FDI neutralizan los ataques efectuados a sus centros poblados e infraestructura crítica, a través de sistemas de misiles de múltiples clases (Zarzoso, 2024).

Acciones para Securitizar a la IA en el Ecuador

Bajo la teoría de Buzan (2003), la inclusión de la IA en el ámbito de la seguridad podría abordarse desde una perspectiva ampliada que considera no solo las amenazas tradicionales, como las militares y políticas, sino también los desafíos emergentes relacionados con la IA. Algunas formas incluyen:

- Las amenazas cibernéticas, ya que la IA puede ser utilizada tanto por actores estatales como no estatales para llevar a cabo ciberataques sofisticados que pongan en peligro la seguridad de

los sistemas informáticos, la infraestructura crítica y la privacidad de las personas; bajo la perspectiva de Buzan, estas amenazas podrían considerarse como parte de un complejo de seguridad que abarca tanto aspectos tradicionales como nuevos desafíos tecnológicos.

- El impacto en la toma de decisiones, ya que la IA también puede influir en este sentido en materia de seguridad, ya sea a través de la automatización de procesos de análisis de inteligencia o de la identificación de posibles amenazas. Siendo así, la integración de la IA en los procesos de seguridad podría cambiar la forma en que se perciben y gestionan los riesgos.
- Los desafíos éticos y legales como la privacidad, la transparencia y la responsabilidad en el uso de algoritmos: bajo la teoría de Buzan (2003), estos aspectos podrían considerarse como parte de un complejo de seguridad más amplio que abarca no solo las amenazas convencionales, sino también las implicaciones éticas y legales de la IA.

Para ejecutar el proceso de securitización, se deberá identificar las amenazas potenciales, construir narrativas de riesgo, movilizar recursos y brindar atención para involucrar a los actores clave.

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Figura 2

IA y la seguridad en el Ecuador

Nota: Elaboración propia

Perspectiva de la IA en la Seguridad Integral

Desde esta perspectiva, la IA puede ser aproximada como un tema necesario de seguridad nacional al considerar los siguientes puntos: (a) la sensibilización y educación, puesto que es fundamental sensibilizar a la opinión pública sobre los riesgos y beneficios asociados con la IA en el contexto de la seguridad nacional. La educación pública puede ayudar a crear conciencia sobre las implicaciones en la toma de decisiones, la ciberseguridad, la privacidad y otros aspectos relevantes para la seguridad y que podrían estar en riesgo debido a la ausencia de acción por parte del Estado; (b) el debate público informado sobre el papel de la IA en la seguridad nacional es esencial para involucrar a los ciudadanos en la discusión y en la formulación de

políticas relacionadas, lo que puede generar expectativas y opiniones para enriquecer el proceso de toma de decisiones y aumentar la legitimidad de las medidas de seguridad relacionadas con la seguridad del Estado; (c) la transparencia y rendición de cuentas es crucial para generar confianza en las instituciones y actores involucrados, contribuyendo a una mayor legitimidad y aceptación de las políticas de seguridad en este ámbito; (d) la protección de derechos y valores, ya que es importante que la opinión pública participe en la discusión sobre cómo garantizar el respeto por los derechos fundamentales, los valores democráticos y la ética en el uso de la IA. La participación de la sociedad civil puede ayudar a identificar posibles riesgos y a establecer salvaguardias para proteger los intereses públicos en este contexto.

Inclusión de la IA en la Agenda de Defensa

La IA puede desempeñar un papel fundamental en la política de seguridad nacional al proporcionar capacidades avanzadas para la recopilación, análisis y utilización de información en tiempo real; también podría constituirse en una amenaza para el Estado, debido a la connotación y diversidad de usos y aplicaciones que día a día van generándose con este tipo de tecnología. Algunas de las razones por las que se debe incluir la IA en la política de seguridad nacional son: (a) análisis de big data ya que, al procesar grandes volúmenes de datos de diversas fuentes, se puede identificar patrones, tendencias y amenazas potenciales de manera más eficiente que los métodos tradicionales; (b) detección de amenazas: a través de algoritmos de IA se puede monitorear y detectar actividades sospechosas –virtuales y físicas–, como propaganda o desinformación, patrones de actividades

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

y rostros, permitiendo una respuesta predictiva más rápida y efectiva; (c) predicción de conflictos, ya que, con un análisis, se puede anticipar posibles conflictos o amenazas emergentes, permitiendo una planificación proactiva; (d) seguridad cibernética, ya que puede identificar y neutralizar amenazas en tiempo real, así como mejorar la detección de vulnerabilidades en sistemas críticos; (e) automatización de tareas, liberando recursos humanos para actividades de mayor valor estratégico en materia de seguridad nacional; (f) análisis de imágenes y vídeos, para identificar objetos, personas o comportamientos relevantes para la seguridad, facilitando la vigilancia y el reconocimiento; (g) toma de decisiones: los sistemas de IA pueden proporcionar análisis y recomendaciones basadas en datos para apoyar la toma de decisiones estratégicas en crisis o conflicto.

Conclusiones

La investigación muestra que es importante incluir dentro de la agenda de la Defensa Nacional a la IA, debido a su potencial tecnológico y a la connotación actual que puede tener para la seguridad de los Estados. Se identifica que existen oportunidades y amenazas en la implementación de la IA en la seguridad nacional. La revisión bibliográfica muestra que la IA puede mejorar la detección de amenazas, la eficiencia operativa y la toma de decisiones estratégicas en defensa, pero también plantea desafíos como la vulnerabilidad a ciberataques y el riesgo de mal uso por actores malintencionados. Es fundamental que el Estado ecuatoriano esté preparado para aprovechar al máximo las ventajas que ofrece la IA en seguridad nacional, al tiempo

que se protege de posibles amenazas y se garantiza un uso ético y responsable de esta tecnología en beneficio de la defensa del país.

Es recomendable la implementación de propuestas que permitan gestionar de manera efectiva los riesgos y potencialidades de la IA y que incluyan la creación de marcos regulatorios claros, la capacitación del personal en tecnologías emergentes, la colaboración con expertos en IA y la adopción de prácticas éticas en el uso de esta tecnología. Como evidencia la encuesta, existe una concepción errónea respecto de lo que verdaderamente constituye la IA, situación que puede ser riesgosa al patentizar la falta de interés o capacitación de los miembros de las FFAA en este tema, y que podría aumentar las vulnerabilidades del sistema de seguridad del Estado en el ámbito de la IA.

De la misma forma, las particularidades de la IA no son adecuadamente comprendidas, según se desprende de los resultados, lo que podría configurar a la IA como una potencial amenaza a la seguridad del Estado. La implementación de la IA en la seguridad nacional tendría un impacto positivo, al permitir el desarrollo de sistemas y procesos para la vigilancia y el monitoreo, facilitando la detección de patrones de comportamiento inseguros y contribuyendo a una vigilancia más eficiente y precisa para la prevención de delitos. Esto significa que la IA puede mejorar la capacidad de las autoridades para identificar posibles amenazas y prevenir delitos al analizar grandes cantidades de datos de manera eficiente y precisa, generando un entorno y percepción de seguridad favorable para el Estado ecuatoriano.

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Existe preocupación por la posibilidad de manipulaciones a sistemas gubernamentales a través de ciberataques utilizando algoritmos de IA, lo que representa un impacto negativo en la seguridad nacional. Esta preocupación se centra en el potencial de la IA para ser utilizada de manera maliciosa por actores externos para comprometer la seguridad de un país, lo que destaca la importancia de establecer medidas de ciberseguridad robustas que incluirían a la IA. Existe una marcada inquietud por los sistemas inteligentes autónomos en el ámbito de la seguridad y defensa, lo que plantea dilemas morales y legales en la discriminación de acciones sin necesidad de decisión humana. Esta tendencia refleja la discusión ética en torno a la autonomía de los sistemas de IA en la toma de decisiones que pueden tener implicaciones significativas en términos de responsabilidad y control, lo que sugiere establecer un debate oportuno que permita generar un marco legal normativo eficaz y eficiente.

La investigación cualitativa y cuantitativa realizada permitió conocer las teorías de IA aplicadas a la defensa, así como la realidad de las Fuerzas Armadas ecuatorianas frente a la IA. Esto establece una base para enfocar estrategias de implementación de IA en áreas de seguridad y defensa. Este enfoque en la investigación proporciona una comprensión de cómo la IA puede integrarse de manera efectiva en las operaciones de seguridad y defensa, viendo necesaria la securitización de la IA en forma inmediata para evitar riesgos derivados del uso de esta tecnología en el futuro.

Resulta imprescindible que el Estado ecuatoriano considere la IA en sus documentos estratégicos, dada su importancia en la seguridad nacional. Esta conclusión

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

destaca la importancia de incorporar la IA en la planificación estratégica del Estado para garantizar una respuesta efectiva a los desafíos de seguridad actuales y futuros.

Se evidencia la necesidad de contar con nuevos instrumentos de investigación que ayuden a identificar nuevas oportunidades para el empleo de la IA en temas de seguridad, basados en la investigación, el desarrollo y la innovación, teniendo un impacto significativo en la seguridad del país, fortaleciendo a las FFAA en su afán de tener capacidades innovadoras para responder de mejor manera a las amenazas generadas en los nuevos escenarios, que podrían dar paso a nuevas teorías y conocimientos sobre la aplicación de la IA en la seguridad y defensa. Se espera que esta investigación sirva para desarrollar futuros estudios sobre la IA en la defensa del Estado en áreas específicas como el desarrollo de armas y sistemas autónomos, o la prevención de los efectos de amenazas y riesgos de distinta índole.

Referencias

Asimov, I. (1982). The Complete Robot. Editorial, Doubleday.

Buzan, B. (2003). Regions and powers: the structure of international security. Cambridge University Press. https://ir101.co.uk/wp-content/uploads/2018/11/Buzan-Waever-2003-Regions-and-Powers-The-Structure-of-International-Security.pdf

Castro, R. J. (2022). La inteligencia artificial y sus diferencias con los sistemas expertos. *Journal TechInnovation, 1(2),* 88-96. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.88-96

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Centro Conjunto de Desarrollo de Conceptos. (2020). Usos militares de la Inteligencia Artificial, la automatización y la robótica (IAA&R). Ministerio de Defensa de España. https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx.-_VV.AA.pdf

Clarke, R. A. y Knake, R. K. (2011) Guerra en la red: Los nuevos campos de batalla. Barcelona: Ariel. https://www.planetadelibros.com/libro-guerra-en-la-red/48833

Crespo, F., Alves, T., y Soto, M. (2022). Ciencia de Datos, Inteligencia Artificial, y sus impactos sobre la sociedad. *Observatorio Económico, (169),* 9-11. https://doi.org/10.11565/oe.vi169.474

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirugi, A., Galanosj, V., Ilavarasank, P. V., Janssen, M., Jonesm, P., Kark, A., Kizginb, H., Kronemannm,B., Lalf, B., Lucini, B., … y Williamsz, M. D.. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information *Management, 57.* https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Facultad Latinoamericana de Ciencias Sociales [FLACSO] - Ecuador. (2023). -. Inteligencia artificial y big data: debates, usos y retos en América Latina. FLACSO. https://www.flacso.edu.ec/es/inteligencia_artificial_bigdata

Flores-Vivar, J. M., Gómez-de-Ágreda, Á., y Gómez-López, J. (2023). Taxonomía de la inteligencia artificial en el entorno cognitivo de los conflictos. *Disertaciones:*

Anuario Electrónico de Estudios en Comunicación Social Disertaciones, 16(2). https://produccioncientifica.ucm.es/documentos/64e645fdd253553455706408

García, A. (2024). Inteligencia artificial y desinformación: Papel en los conflictos del siglo XXI. Revista *Seguridad y Poder Terrestre, 3(3),* 87-113. https://www.researchgate.net/profile/Adolfo-Arreola/publication/390237343_N3_julio_-septiembre/links/67e57d449f23086421910bb8/N3-julio-septiembre.pdf

García-Patos-Herreros, P. J. (2022). La inteligencia artificial en los nuevos escenarios de conflicto: Ucrania. *Ejército: de tierra español, (981),* 20-28. https://dialnet.unirioja.es/servlet/articulo?codigo=8784343

Gartner Inc. (2023). Magic Quadrant for Cloud AI Developer Services. Gartner Inc.
https://www.gartner.com/en/documents/4372099

Gayozzo, P. (2021). Guerra de quinta generación en la Cuarta Revolución Industrial. *Futuro Hoy, 2(1).* https://doi.org/10.52749/fh.v2i1.9

Gómez-Llinás, D. A. (2021). El impacto de la inteligencia artificial sobre el ser humano y sobre su seguridad. *Instituto de Estudios Geoestratégicos y Asuntos Políticos,* 1-11. https://www.umng.edu.co/documents/20127/0/EL+IMPACTO+DE+LA+INTELIGENCIA+ARTIFICIAL.pdf/8007b6ca-5b02-b7f1-4a64-4a27ac3a9060?t=1639080191820

Gray, C. S. (2002). Thinking asymmetrically in times of terror. The US Army War College Quarterly: *Parameters,* 5-14. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2079&context=parameters

Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M.
pp. 226 - 260
Recibido: 05-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Haro-Ayerve, P. (2019). La guerra de cuarta generación y las amenazas asimétricas. *Revista Política y Estrategia, (134),* 93-113. https://www.politicayestrategia.cl/index.php/rpye/article/view/788

Hawking, S. (. (2018). Breves respuestas a las grandes preguntas. Barcelona: Crítica. https://www.academia.edu/43163430/Breves_respuestas_a_las_grandes_preguntas

Hintze, A. (2016). Understanding the four types of AI, from reactive robots to self-aware beings. *The Conversation, 14.* https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

Hunter, L. Y., Albert, C. D., Henningan, C., y Rutland, J. (2023). The military application of artificial intelligence technology in the United States, China, and Russia and the implications for global security. *Defense & Security Analysis, 39(2),* 207-232. https://ideas.repec.org/a/taf/cdanxx/v39y2023i2p207-232.html

Instituto Español de Estudios Estratégicos. (2019). Documentos de Seguridad y Defensa No. 79: La IA aplicada a la Defensa. Madrid: Ministerio de Defensa de España.

Jun, Y., Craig, A., Shafik, W., y Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyberdefense. *Wireless communications and mobile computing, (2021),* 3329581. https://doi.org/10.1155/2021/3329581

Makridakis, S. (2017). The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. *Futures, 90,* 46-60. https://helios.ntua.gr/2021-22/pluginfile.php/146209/mod_resource/content/1/AI%20Revol.pdf

Mayorga, J., Vargas-Borbúa, R., Reyes, R. P., y Gualotuña, T. (2020). Jayor2: A Proposal of Information management system for command and control centers (C3I2) in the Armed Forces. *Develoments and Advances in Defense and Security,* 271-282. https://bit.ly/3GqCpGL

Mayorga, J. y. Holguín, R. (2024). Las redes sociales como instrumento del terrorismo en el Ecuador. *Revista de la Academia del Guerra del Ejército Ecuatoriano, 17(01),* 91-102. https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/3401

Méndez-Vélez, L. A., Gaitán-Vanegas, S., Fuquen-Flautero, V. P. (2019). Los dominios de la guerra: una aproximación al nuevo escenario de la COVID-19. *Estudios en Seguridad y Defensa, 14(28),* 237-257. https://doi.org/10.25062/1900-8325.282

Murawiec, L. y Gaddy, C. (2017). The Higher Police. In Russia in the National Interest. Londres: Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315128870-19/higher-police-laurent-murawiec-clifford-gaddy

Palayer, J. (2020). Naturaleza de los conflictos e inteligencia artificial: ¿ruptura de una continuidad. *Revista de Estudios en Seguridad Internacional, 6(2),* 63-79. http://dx.doi.org/10.18847/1.12.4

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Profile Books. https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939

Romero-Mier, S. G. (2019). Inteligencia artificial como herramienta de estrategia y seguridad para defensa

de los Estados. *Revista de la Escuela Superior de Guerra Naval, 16(1),* 51 – 70. https://doi.org/10.35628/resup.v16i1.67

Ruiz-Baquero, P. E. (2018). Avances en inteligencia artificial y su impacto en la sociedad. In Simposio Iberoamericano de Filosofía Política. Universidad Pontificia Bolivariana. 396-412. https://repository.upb.edu.co/bitstream/handle/20.500.11912/4942/Inteligencia%20artificial%20impacto%20social.pdf?sequence=1&isAllowed=y

Stoppani, G. (2022). Impacto del uso de la inteligencia artificial y la robótica inteligente en la defensa.

Turing, A. (1950). Computing Machinery and Intelligence. *Mind, 49,* 433-460. https://courses.cs.umbc.edu/471/papers/turing.pdf

Zarzoso, J. (2024). Evolución en la lucha antiterrorista de Israel: antecedentes, políticas y respuestas. *GEOCONFLICTS & INTELLIGENCE: Revista sobre Seguridad Global y Terrorismo, 2(2),* 123-158. https://dialnet.unirioja.es/servlet/articulo?codigo=9879232