
# Empleo de la inteligencia artificial en el planeamiento de un despliegue de artillería de campaña

Mayor (EJC) Diego Hernando Rivas Camacho

Artículo para optar al título profesional:

Magister en Ciberdefensa y Ciberseguridad

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

| DATOS GENERALES | | |
|---|---|---|
| **Nombre del estudiante** | **:** | Mayor (EJC) Diego Hernando Rivas Camacho |
| **Identificación** | **:** | 1075216710 |
| **Programa académico** | **:** | Maestría en Ciberdefensa y Ciberseguridad |
| **Tutor metodológico** | **:** | Jairo Becerra |
| **Tutor temático** | **:** | Andrés Ernesto Salinas |
| **Fecha de entrega** | **:** | 7 de agosto de 2025 (100%) |
| **Extensión** | **:** | 8.860 |

# EMPLEO DE LA INTELIGENCIA ARTIFICIAL EN EL PLANEAMIENTO DE UN DESPLIEGUE DE ARTILLERÍA DE CAMPAÑA

**"Use of artificial intelligence in the planning of a field artillery deployment"**

**Diego Hernando Rivas Camacho**[1]
**Escuela Superior de Guerra "General Rafael Reyes Prieto"**

**Resumen:** La presente investigación adopta un enfoque aplicado y tecnológico, orientado a resolver un problema operativo concreto dentro del ámbito militar: la integración segura y doctrinalmente válida de la inteligencia artificial (IA) en el planeamiento de un despliegue de artillería de campaña. Para ello, se opta por una metodología mixta, que combina el análisis doctrinal y técnico con el diseño de soluciones algorítmicas y arquitectónicas, enmarcadas en principios de ciberdefensa y superioridad informativa. Este trabajo corresponde a un estudio de diseño aplicado con enfoque exploratorio-descriptivo. Explora la relación entre capacidades de IA y funciones tácticas en artillería, describe vulnerabilidades asociadas a su implementación en el dominio militar y propone una solución estructuralmente validada a partir de escenarios doctrinales.

**Palabras clave:** Inteligencia artificial; ciberseguridad militar; artillería de campaña; planeamiento operacional; sistemas expertos; toma de decisiones tácticas; validación doctrinal.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberdefensa y Ciberseguridad, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en defensa y derecho, economía, gestión y relaciones internacionales para la defensa y dinámicas industriales. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: diego.rivas@esdeg.edu.co

**Abstract:** This research adopts an applied and technological approach aimed at addressing a specific operational problem within the military context: the secure and doctrinally valid integration of artificial intelligence (AI) in the planning of a field artillery deployment. To achieve this, a mixed methodology is employed, combining doctrinal and technical analysis with the design of algorithmic and architectural solutions, framed within the principles of cyber defense and informational superiority. This work corresponds to an applied design study with an exploratory-descriptive focus. It explores the relationship between AI capabilities and tactical functions in artillery, describes vulnerabilities associated with its implementation in the military domain, and proposes a structurally validated solution based on doctrinal scenarios.

**Keywords:** Artificial intelligence; military cybersecurity; field artillery; operational planning; expert systems; tactical decision-making; doctrinal validation.

## Introducción

En los escenarios operacionales actuales, las Fuerzas Militares se enfrentan a realidades cada vez más complejas, donde confluyen amenazas hibridas, entornos informativos cambiantes y una transformación digital que redefina el arte de la guerra en "guerras asimétricas" (Payá & Luque, 2019, p.17). En este contexto, la inteligencia artificial (IA) emerge como un recurso estratégico capaz de asistir, optimizar y fortalecer la función de conducción de la guerra, particularmente en el ámbito del planeamiento y ejecución de los fuegos de artillería. La evolución doctrinal del arma de artillería, tradicionalmente apoyada en el cálculo balístico y la sincronización táctica, exige hoy una reconfiguración con base en la automatización de los procesos, la minería de datos operacionales y la toma de decisiones asistida por algoritmos. Sin embargo, el aprovechamiento de estas capacidades impone también desafíos y nuevos retos en materia de seguridad, gobernanza de datos y validación legal del empleo de la fuerza, especialmente en contextos donde la información puede ser manipulada, saboteada o explotada con fines adversarios

Este proyecto de investigación tiene como propósito principal proponer un modelo estructural de IA con medidas integradas de ciberseguridad, diseñado específicamente para apoyar el planeamiento de un despliegue de artillería en operaciones militares, bajo criterios de precisión, resiliencia algorítmica y conformidad normativa. La propuesta busca responder a las necesidades reales del comandante táctico, garantizando la confiabilidad de la información, la trazabilidad de las decisiones y la legitimidad del uso de los fuegos en entornos multidominios.

Para lograr tal propósito, se cumplirán objetivos específicos enmarcados en una estructura narrativa de la siguiente manera: en primer lugar, se realiza un repaso por la evolución del planeamiento de artillería en campaña. En segundo lugar, se analiza Analizar la tecnología de IA aplicada al ámbito militar, sus conceptos, tipologías operativas y aplicaciones, para evaluar

sus beneficios, riesgos y aportes al planeamiento y capacidad operativa de la artillería., en tercer lugar, se exponen las aplicaciones relevantes de IA en planeamiento militar y finalmente, se plantea la propuesta de modelo estructural de IA con medidas integradas de ciberseguridad.

## 1. Planeamiento de artillería de campaña

El planeamiento se puede rastrear desde el *Reglamento EJC-35 Empleo Táctico de la Batería del Ejército Nacional de Colombia* (Ejército Nacional de Colombia, 1961), hoy derogado, concebía la batería de artillería como la unidad fundamental de fuego del batallón. El planeamiento se orientaba a la selección y ocupación de posiciones considerando la misión, las condiciones del terreno, el encubrimiento, la dispersión y la cercanía a las vías de acceso. Para mediados del siglo XX, las marchas aún dependían de apoyo de mulares y los fuegos se ejecutaban mediante observación directa, mapas y brújulas, con base en el juicio del observador adelantado y el movimiento de las propias tropas. Este planeamiento exigía una elevada preparación técnica de los artilleros.

En el Manual 3-107 Apoyo de Fuegos y Táctica de Artillería de Campaña del Ejército Nacional de Colombia (2007), actualmente vigente, relaciona los componentes de un sistema de apoyo de fuegos integrado por medios de adquisición de blancos, sistemas de ataque y municiones, Sistemas e instalaciones de comando, control y coordinación (C3) y el sistema de apoyo técnico (p. 153). Si bien, este manual relaciona radares, sensores, observadores adelantados (OA) actuando como los "ojos" del sistema de apoyo, tropas en contacto y equipos de inteligencia de imágenes como medios de adquisición de blancos la realidad es que en esta época se realizaba mediante observación directa, dependiendo de la experiencia del comandante apoyado haciendo que el proceso de planeamiento y ejecución se desenvolvía con márgenes limitados de precisión y requería tiempos prolongados de preparación (EJC-OB, 2007, p. 2).

Este enfoque, aunque eficaz en su momento, resultaba vulnerable ante condiciones meteorológicas adversas, errores humanos y las limitaciones de los sistemas de comunicación de corto alcance. Como consecuencia, la doctrina ha avanzado priorizando la articulación entre los principios de la guerra y la modernización tecnológica, promoviendo el uso de sensores, radares y plataformas de inteligencia para el ciclo de selección de blancos, guiado por las fases de decidir, detectar, entregar y evaluar, como lo indica MCE 3-9 Artillería de Campaña y Apoyos de Fuegos (Ejercito Nacional de Colombia, 2018, p. 20).

Así, El planeamiento de artillería ha pasado de ser un procedimiento técnico a una función estratégica que integra doctrina, tecnología e inteligencia (C4ISR) para producir efectos decisivos incluso en guerras irregulares, exigiendo al comandante competencia técnica, comprensión del ambiente operacional y respeto por el DIH y los Derechos Humanos.

### 1.2 Transición hacia sistemas digitalizados y automatizados

A inicios del siglo XXI, la artillería de campaña experimentó un giro doctrinal y tecnológico con la incorporación de sistemas digitalizados que optimizan el ciclo de planeamiento, decisión y ejecución. Un ejemplo es el sistema VULCANO, desarrollado por la Dirección de Proyectos de Artillería, que integra inteligencia, priorización de blancos y coordinación en tiempo real mediante datos digitalizados y comunicaciones encriptadas (MTE 3-09.3, 2019, pp. 2-10).

La doctrina de mando tipo misión (MTM) y los sistemas C4ISR han sido incorporados para permitir un mando descentralizado pero coordinado, facilitando la interoperabilidad entre diferentes unidades del Ejército, la Fuerza Aérea y componentes aliados. Estos sistemas permiten el procesamiento inmediato de datos topográficos, meteorológicos y de inteligencia para ajustar las trayectorias de fuego y asignar recursos con base en análisis en tiempo real (MFRE 3-09, 2017, p. 4-2).

En este nuevo entorno operacional, el Centro Director de Tiro (CDT) ha evolucionado de ser un ente de cálculo manual a convertirse en un nodo digital que procesa múltiples variables de forma automatizada, incluyendo distancia, elevación, carga, ángulos verticales y horizontales, lo cual permite una ejecución mucho más precisa y eficiente del fuego indirecto (EJC 3-170, 2007, p. 4).

Adicionalmente, el empleo de sensores remotos, imágenes satelitales, radares de contrabatería y plataformas de vigilancia no tripuladas ha ampliado considerablemente el alcance, precisión y letalidad de los sistemas de artillería, transformando la naturaleza misma del combate terrestre. Este cambio ha implicado también una redefinición del entrenamiento del personal artillero, exigiendo competencias en sistemas digitales, redes de datos y análisis de información táctica (EJC 3-158, 2005, p. 11).

### 1.1. Proceso doctrinal del planeamiento artillero

La función esencial de la Artillería de Campaña es proporcionar apoyos de fuego oportuno y eficaz a las unidades comprometidas en la primera línea de las operaciones militares cuya misión es destruir, derrotar o desarticular una fuerza enemiga mediante el uso integrado de los fuegos integrados para permitir que los comandantes de la maniobra prevalezcan en las operaciones terrestres unificadas, como lo menciona el MCE 3-9 Artillería de Campaña y Apoyos de Fuegos (Ejercito Nacional, 2018, p. 18).

El planeamiento para el desarrollo de un despliegue de artillería se fundamenta en la doctrina específicamente en el *Manual de Referencia del Ejercito Nacional MFRE 3-37 "Protección"* (2017) *; El Manual de Campaña del Ejército "MCE 3-09 Artillería de Campaña y Apoyos de Fuegos";* en el manual del *Ejercito Nacional Ejecutivo de la Batería del 3-52* "Ejecutivo de la Batería" en el cual simplifica el planeamiento del despliegue de una manera

rápida y organizada a las unidades de artillería en la sigla RSOP la cual se desglosa en Reconocimiento, Selección y Ocupación de una Posición y se divide en tres fases:

- Planeamiento y Preparación
- Reconocimiento y Selección
- Movimiento y Ocupación

En el MCE 3-9 (2018) doctrinalmente se relaciona el planeamiento de artillería varias fases críticas con el propósito de asegurar la efectividad en el despliegue de las unidades de apoyo en escenarios de operativos complejos (p.18). Inicialmente como en toda operación al recibir una misión se debe realizar con un análisis riguroso determinando los objetivos tácticos y operacionales. En este análisis se deben considerar diferentes factores esenciales como el tipo de blanco, las condiciones ambientales, las características del terreno y las capacidades del enemigo.

Posteriormente, se seleccionan las unidades y medios de artillería adecuados para cumplir la misión, evaluando disponibilidad de personal, armamento y municiones, estado operacional de vehículos y capacidad logística para el sostenimiento, como se observa en la tabla del Manual ECJ, 3-52 (1990): Tabla 1. Misiones Tácticas De Artillería

| MISION TACTICA DE | Responde Pedidos De Apoyo De Fuego En Prioridad | Establece Enlaces Con | Establece Comunicaciones Con | Tiene Como Zona De Fuego Asignada A | Suministra Observadores Adelantados | Ocupa Posiciones A Orden De | Fuegos Planeados Por |
|---|---|---|---|---|---|---|---|
| APOYO GENERAL | 1.Comando Superior De Artillería<br>2. Observadores Propios. | No le corresponde específicamente. | | La unidad apoyada | No suministra. | Comando superior de artillería Este las seleccionadas. | Comando superior de artillería. |
| APOYO DIRECTO | 1. Unidad de maniobra apoyada.<br>2. Observadores propios. | Unidad de maniobra apoyada | Unidad de maniobra apoyada. | Unidad de maniobra apoyada | A cada unidad fundamental de la unidad de maniobra apoyada. | Comandante de la unidad de artillería o Comandante superior de artillería | Su propio comando de artillería. |
| APOYO GENERAL DIRECTO | 1. Comando Superior de artillería.<br>2. Unidad de artillería reforzada.<br>3.Observadores propios | Unidad de artillería reforzada. | Unidad de artillería reforzada. | La unidad apoyada que normalmente es la zona de fuego de la artillería reforzada. | Pedido de la unidad de artillería reforzada previa aprobación del Comando superior de artillería. | Comando superior de artillería unidad de artillería reforzada previa aprobación del primero | Comando superior de artillería. |
| REFUERZO | 1. Unidad de artillería reforzada.<br>2. Observadores propios.<br>3. Comando superior de artillería. | Unidad de artillería reforzada | Unidad de artillería reforzada. | Unidad de maniobra reforzada | Pedido de Unidad de artillería reforzada ordenado por el Comando superior de artillería. | 1. La unidad de artillería reforzada.<br>2.Comando superior de artillería | La unidad de artillería reforzada. |

Fuente: Ejército Nacional de Colombia (1990). EJC, 3-52 Manual del Ejecutivo de la Batería. p. 67

Luego, el análisis de misión y objetivos —y una vez definidos quién, qué, cómo, dónde y para qué— el *EJC 3-52* recomienda el RSOP (Reconocimiento, Selección y Ocupación de la Posición) como herramienta central del planeamiento de la batería para garantizar un traslado rápido y seguro hacia la posición de fuego y su ocupación (Ejército Nacional, 1990, p. 20). El *MCE 3-01: Artillería de Defensa Antiaérea*, amplía este enfoque al incluir medidas específicas para neutralizar amenazas aéreas, asegurando así la protección integral del despliegue artillero en los niveles estratégico, operacional y táctico (Ejército Nacional, 2019, p. 152).

Esto demuestra que, el planeamiento doctrinal de artillería prioriza la eficacia del fuego, la movilidad y la seguridad táctica, pero frente a un entorno operacional VICA requiere un análisis crítico para identificar limitaciones y oportunidades de modernización e innovación.

### 1.2. Limitaciones operativas del modelo actual

Normalmente, la información necesaria no se encuentra actualizada ni sistematizada, teniendo que recurrir directamente a la revisión documental disponible. Además, se emplean medios abiertos como *Google Earth* para la graficar puntos estratégicos en el planeamiento o para realizar un análisis geográfico del terreno, o canales no institucionales para la recepción de documentos de planeamientos anteriores para tomarlos como base o parte de inicio al que se piense desarrollar para el cumplimiento de una nueva misión. Esto limita la respuesta temporal ante un despliegue de artillería y aumenta la exposición a vulnerabilidades cibernéticas que pueden mermar la efectividad del planeamiento en situaciones complejas.

Dadas las limitaciones y que actualmente la tecnología avanza a paso de gigantes, como lo demuestran las potencias armamentísticas, es de destacar la necesidad de incorporar herramientas como una inteligencia artificial propia como una solución poderosa para superar las actuales deficiencias operativas. En este sentido, la IA permite optimizar de manera significativa los procesos de planeamiento ofreciendo mayor precisión en los análisis (Adler, 2025, p. 2). Esto

fortalece de manera exponencial la capacidad de los apoyos de artillería de campaña y en especial el tiempo de respuesta ante una situación de emergencia.

En el desarrollo completo del planeamiento se consideran elementos adicionales que optimizan el despliegue artillero, tales como:

- Determinación del método y ruta de marcha.
- Azimut de tiro y ubicación precisa del punto de relevo.
- Análisis exhaustivo de obstáculos naturales y artificiales.
- Evaluación constante de puntos críticos y medidas específicas para la cobertura y el encubrimiento (camuflaje, protección y cubierta).

### 1.3. Necesidad de integrar herramientas tecnológicas avanzadas

Las herramientas tecnológicas como la inteligencia artificial empleadas en el planeamiento de un despliegue de artillería, no deben ser vistas como un lujo operacional sino como una necesidad imperativa. En un ambiente volátil, incierto, complejo y ambiguo (VICA), la asimetría de las amenazas y la celeridad de los ciclos de decisión militar exigen que las unidades tácticas y operacionales de artillería puedan contar con capacidades analíticas, predictivas y adaptativas en tiempo real que amplíen su efectividad. Tal como lo mencionan Galán et al., (2022) la inteligencia artificial es una herramienta en la que se puede emplear en la automatización de análisis de múltiples fuentes de información que faciliten las decisiones críticas con base a datos que podamos obtener de los objetivos (p.2). Esto en el ámbito militar, la generación masiva de datos críticos hace indispensable el uso de *machine learning* para su procesamiento y apoyo en la toma de decisiones, destacando la IA como herramienta clave donde la oportunidad y la precisión resultan decisivas. Así, la evaluación se complementa con recomendaciones de la IA sobre (baterías, tipo de armas, rutas).

En esta línea, el desarrollo de sistemas como COA-GPT representa una evolución significativa. Este modelo, presentado por Goecks & Waytowich (2024), utiliza modelos de

lenguaje reentrenados que incorporan doctrina militar y permiten a los comandantes ingresar información textual e incluso visual, obteniendo casi al instante recomendaciones de cursos de acción acordes con la intensión de la misión (p.3). La utilidad de este tipo de soluciones no se limita a la planeación inicial, sino que se extiende a la capacidad de reajuste durante la ejecución de la misión, permitiendo adaptaciones fundamentadas en nueva información o eventos que se puedan presentar en el desarrollo de una operación militar.

Los mismos autores, manifiestan que la IA también se ha implementado con éxito en el procesamiento de imágenes satelitales, el análisis de patrones de movimiento y la predicción de consumo logístico (Goecks & Waytowich 2024, p. 72). Estos elementos son especialmente útiles en la artillería, ya que permiten identificar y anticipar las mejores rutas que faciliten la cadena de suministros que puedan suplir con mayor efectividad la necesidad de reabastecimiento, estimar la capacidad de sostenimiento de una operación y prever contingencias que podrían afectar el cumplimiento de los objetivos.

En países como Corea del Sur, Israel y Estados Unidos ya han implementado herramientas de inteligencia artificial en procesos como inteligencia militar y planeamiento táctico, con resultados positivos en términos de reducción de errores, optimizando la efectividad en la ejecución y mejora en los tiempos de redacción (Galán et al., 2022, p.4). Estas experiencias refuerzan la viabilidad técnica y estratégica de adoptar sistemas inteligentes en el contexto Nacional.

De esta manera, la IA es una "herramienta relevante y útil que puede contribuir significativamente a la planificación de misiones, al reducir la carga cognitiva del personal militar y permitir enfoques más integrales para la toma de decisiones"(Bossio Ballesteros, 2023. p.5). Esta visión se alinea con la necesidad de transformar el planeamiento para un despliegue de

artillería en un proceso dinámico, flexible y adaptado a las exigencias de los conflictos actuales y futuros proyectando una vanguardia tecnológica regional. En especial, cuando las principales potencias militares del mundo actualmente presentan sus grandes avances en la carrera de las armas. Sin embargo, una de las cosas más importantes es que esta herramienta debe incluir en su diseño el respeto por los principios del Derecho Internacional Humanitario y los protocolos nacionales del empleo de la fuerza (Porcelli, 2021 p. 486).

En definitiva, la incorporación de la IA en el planeamiento artillero es una evolución doctrinal que fortalece la capacidad del Ejército para operar con ventaja en escenarios complejos y multidominio. La combinación entre la experiencia del comandante, la doctrina militar nacional y el poder de cómputo de la IA constituye una simbiosis estratégica orientada a potenciar la eficacia, eficiencia y legitimidad de las operaciones militares.

## 2. La inteligencia artificial en entornos militares

La IA, como campo multidisciplinario en constante evolución, se estructura en una diversidad de técnicas que permiten su aplicación operativa en entornos complejos como el ámbito militar. En este contexto, su clasificación funcional puede organizarse a partir de capacidades específicas que contribuyen al planeamiento táctico, estratégico y operacional, particularmente en unidades de artillería de campaña. A continuación, se describen los principales conceptos y técnicas relevantes:

-*Machine Learning* (ML) para posicionamiento y la asignación de piezas: en la actualidad, el ambiente militar se ha distinguido por su alta fluctuación en la dinámica operacional, junto con amenazas asimétricas que cambiantes y constantes. A diferencia de los métodos convencionales de análisis balísticos o de estimación de blancos, el ML procesa grandes volúmenes de información provenientes de sensores, reportes SIGINT/IMINT y simulaciones operacionales, y produce predicciones como *Supprt Vector Machines* (SVM), *Random Forests* o redes neuronales

convolucionales han sido aplicados en dominios cibernéticos para detectar patrones de intrusión. Sin embargo, su extrapolación al dominio artillero posibilita anticipar trayectorias de ataque, evaluar la probabilidad de aparición de blancos móviles y proyectar zonas de mayor vulnerabilidad enemiga (Ramírez, et al., 2024, p.5).

Este tipo de modelos categoriza información en tiempo real, tales como coordenadas de drones, imágenes de satélite o mediciones térmicas que facilitan la agrupación de sucesos que señalen actividad hostil. Técnicas tales como el *Clustering K-Means* facilitan la segmentación de áreas geográficas en áreas con alta probabilidad de impacto, creando mapas de calor que guían el lugar ideal para las baterías de artillería (Singh & Jha, 2021, p. 3). El uso de estas metodologías mediante sistemas de control y gestión C4ICR podría reducir los ciclos de observación, toma de decisiones y acción.

Desde una perspectiva operacional, estos modelos no solo pueden prever sucesos bélicos, sino que también tienen la capacidad de modificar parámetros de fuego en tiempo real, tales como el ángulo de disparo, la carga explosiva o el instante ideal para iniciar fuego indirecto, disminuyendo la posibilidad de fallos humanos y reduciendo los efectos secundarios. La aplicación de estas herramientas requiere una integración cuidadosa con redes seguras, dada la vulnerabilidad de los modelos predictivos. Aun así, el aprendizaje automático proporciona ventajas tácticas y operativas en la predicción y ejecución de despliegues de artillería, superando las limitaciones humanas en velocidad y precisión. Además, la aplicación del *Machine Learning* al campo militar, de ser una herramienta complementaria para convertirse en un componente integral del planeamiento de fuegos (Montalvan-Velez et al, 2024 p. 175).

-Reconocimiento de imágenes satelitales y de drones: a través del uso de visión por computador (CV), la IA moderna habilita el análisis de imágenes satelitales y capturas aéreas desde drones

para identificar posiciones enemigas, fortificaciones, movimientos de tropas y equipos de artillería. Este reconocimiento automatizado se apoya en redes neuronales convolucionales (CNN), especializadas en clasificación y segmentación de imágenes (Aguilar et al., 2024, p. 121).

- Procesamiento del Lenguaje Natural (NLP) para análisis de informes de inteligencia: Este "hace referencia a todos aquellos aspectos de la inteligencia artificial relacionados con la capacidad de comunicación hombre-máquina mediante una lengua natural" (Muñoz, 2024, p. 17). En contextos militares, en los que los informes de inteligencia (HUMINT, SIGINT, IMINT) generalmente se expresan en lenguaje natural, esta tecnología permite el análisis automatizado de elementos esenciales como posiciones enemigas, duración de sucesos, clases de amenazas o rutas de movimiento, todo esto puede ser vital para la planificación y ejecución del fuego indirecto.

En los últimos años, PNL de tipo *transformer* como BERT o GPT, han demostrado capacidad de realizar tareas transferibles al ámbito de la inteligencia militar, en el cual resulta necesario sintetizar reportes extensos y determinar con precisión la veracidad, coherencia y relevancia operativa de los datos. Esta herramienta también puede beneficiar sistemas de control y mando (C2) logrando la automatización de análisis de información en centros de inteligencia de brigada o batallón, acortando el tiempo de duración entre la recopilación de la información y su utilización.

Por ejemplo, Mediante modelado de temas y clasificación supervisada se detectan rápidamente cambios en la operativa enemiga, permitiendo al jefe de artillería adaptar los fuegos. Doctrinalmente, esto refuerza la superioridad informativa al entregar a los líderes información priorizada y procesada; el PLN, por tanto, mejora la precisión del targeting, optimiza la selección de blancos y reduce el riesgo de daños colaterales.

Montalván-Vélez y colaboradores (2024) subrayan que el entendimiento semántico de documentos operacionales a través de IA no solo es útil para la predicción táctica, sino también para la retrospectiva del conflicto, ya que posibilita examinar sucesos anteriores y asesorar el sistema de decisión basándose en pruebas obtenidas de manera automática (p. 175).

- Planeamiento asistido por IA: el manejo efectivo de apoyos de artillería demanda un grado de análisis y sincronización que demanda un entrenamiento estricto y las habilidades humanas al lidiar con situaciones complejas, variables y llenas de información. El planeamiento asistido por IA consiste en la incorporación de algoritmos inteligentes en los sistemas de comando y control con el objetivo de automatizar o apoyar tareas como la priorización de objetivos, la elaboración de cursos de acción, la asignación de medios artilleros, y la evaluación de efectos. Esto es posible gracias al desarrollo de modelos predictivos, sistemas expertos, aprendizaje profundo y análisis de grandes volúmenes de datos históricos, geoespaciales y operacionales en tiempo real.

En entornos militares, las plataformas de IA permiten acelerar la transformación de datos en conocimiento táctico, favoreciendo así la superioridad en el ciclo OODA (Observar–Orientar–Decidir–Actuar). Como lo señalan Flores y Gómez (2023), el uso de algoritmos en operaciones militares posibilita la generación dinámica de hipótesis tácticas, la evaluación de riesgos operacionales y la proyección de los efectos del fuego sobre blancos previamente priorizados, todo esto desde una interfaz cognitiva que transforma los sistemas de mando en actores proactivos del campo de batalla (p.3).

Concretamente en artillería, la IA puede integrarse en cuatro fases del planeamiento:

- Análisis y estimación de la situación: mediante la combinación de minería de datos, aprendizaje automático y PLN, los sistemas inteligentes pueden analizar informes de inteligencia, identificar patrones operativos del enemigo y generar representaciones anticipadas de movimientos hostiles (Romero Mier, 2019, p. 54).

- Desarrollo del plan de fuegos: herramientas de IA como simuladores basados en redes neuronales permiten modelar escenarios futuros, calcular probabilidades de éxito de diferentes configuraciones de tiro y validar estrategias de empleo del fuego. Esto se logra mediante la evaluación continua de inputs topográficos, climáticos y operacionales, generando cursos de acción ajustados a la realidad del terreno (Gómez-de-Ágreda & Feijoo, 2021, p. 4).
- Asignación de medios y despliegue: los sistemas expertos, junto con algoritmos de optimización combinatoria, calculan las posiciones óptimas de las piezas de artillería teniendo en cuenta el alcance, los obstáculos, la cobertura y la amenaza de contrabatería, maximizando el impacto del fuego y minimizando la exposición (Ministerio de Defensa de España, 2024, p. 8).
- Evaluación y retroalimentación: mediante sensores de post-ataque y análisis automático de datos (videos de drones, imágenes térmicas, sensores sísmicos), la IA puede establecer si el objetivo fue neutralizado y ajustar en tiempo real los parámetros del siguiente tiro, logrando una efectividad acumulativa sin necesidad de intervención manual prolongada (Scott, 2023, p. 2).

Estas capacidades optimizan el rendimiento táctico de las unidades de artillería, permiten una adaptación más flexible y resiliente del mando frente a cambios imprevistos en el campo de batalla, reduciendo la dependencia de procesos lineales y favoreciendo esquemas de decisión iterativos, basados en datos y evidencia. Además, desde una perspectiva estratégica, este planeamiento asistido por IA habilita la convergencia entre dominios (cibernético, terrestre y aéreo), mediante la interoperabilidad de sensores, plataformas de fuego y centros de mando. Como indica Atkinson (2025), el uso de IA en ejércitos modernos

también facilita la integración de capacidades autónomas como enjambres de drones de observación y ataque, los cuales sincronizados con baterías artilleras actúan como multiplicadores de letalidad en misiones de tiempo crítico (p.5).

- Algoritmos de optimización para rutas de desplazamiento: La eficacia del despliegue artillero en operaciones depende en gran medida de la capacidad para ejecutar maniobras precisas, rápidas y seguras. La decisión sobre rutas de desplazamiento, especialmente en entornos de amenaza o movilidad reducida, constituye un elemento decisivo que incide en la supervivencia de las piezas de artillería, el cumplimiento de los tiempos de fuego y la sincronización con las fuerzas de maniobra. En este contexto, los algoritmos de optimización se establecen como herramientas clave para apoyar el planeamiento y ejecución de desplazamientos tácticos en tiempo real.

  Los algoritmos de optimización son procedimientos matemáticos o computacionales que buscan identificar la mejor solución posible dentro de un conjunto de restricciones y objetivos. En el ámbito militar, su aplicación permite resolver problemas del tipo *vehicle routing problem (VRP*) adaptados a condiciones operacionales, como evitar emboscadas, esquivar campos minados, minimizar exposición a observadores enemigos y reducir consumo logístico en función de la topografía, amenaza y tiempo disponible.
  En esta línea, Olivares Guzmán y Saavedra Moscoso (2025) presentan una revisión sistemática sobre el uso de algoritmos inteligentes para la planificación de rutas, señalando que técnicas como el recocido simulado (Simulated Annealing), los algoritmos genéticos, y los modelos de colonias de hormigas (Ant Colony Optimization) han demostrado ser eficaces para hallar trayectorias óptimas en sistemas complejos con múltiples restricciones (p. 17).

Estas técnicas, originadas en logística civil e industrial, se han transferido a entornos tácticos para planificar de forma segura rutas de medios móviles (drones, vehículos, piezas remolcadas); en particular, el recocido simulado se emplea en simulaciones militares para explorar soluciones subóptimas y luego converger en la mejor trayectoria en entornos urbanos complejos, útil en movimientos nocturnos o ante bloqueos imprevistos (Flores et al., 2023, p. 92).

Los algoritmos genéticos, basados en procesos evolutivos, han sido utilizados para ajustar planes de desplazamiento según criterios multiobjetivo: tiempo, seguridad, logística, visibilidad. Su capacidad de adaptación y recombinación de soluciones previas permite replantear rutas dinámicamente si cambia la posición enemiga, el terreno se vuelve intransitable o una unidad aliada requiere apoyo urgente (Olivares Guzmán & Saavedra Moscoso, 2025, p. 23). Estos modelos se integran fácilmente en plataformas C4ISR, al interactuar con sistemas de mando de artillería, proporcionan al comandante una visión predictiva de las rutas, junto con recomendaciones fundamentadas en escenarios simulados.

- Modelado y simulación de escenarios de combate: El despliegue eficiente de unidades de artillería exige una planeación rigurosa, como se ha mencionado. Para ello, la simulación de escenarios de combate se configura como herramientas esenciales para anticipar dinámicas operacionales y reducir la incertidumbre táctica. El uso de simuladores modernos ha sido ampliamente validado como recurso imprescindible para el entrenamiento de unidades y la validación de planes de fuego. Tal como lo señala Bueno (1992) la simulación constituye "uno de los instrumentos más ricos que las Fuerzas Armadas pueden usar para alcanzar un alto nivel de entrenamiento" (p. 25), permitiendo reducir costes y

aumentar la eficacia sin comprometer recursos reales. Estos sistemas optimizan el entrenamiento de artillería, la precisión de disparo y la evaluación de efectos.

El modelo de Lanchester ha demostrado ser una base sólida para estructurar simulaciones de combate. Es modelo, originalmente concebido para estimar las bajas en función del número de combatientes y su efectividad, puede ser adaptado a contextos específicos mediante técnicas de disgregación y regresión no lineal. Según Castro, Cerrada y Cerrada et al., (2019). "la simulación permite interpretar entornos complejos y evaluar escenarios probables, complementándose con técnicas de inteligencia artificial que mejoran la definición del comportamiento del adversario" (p.528).

El refinamiento de este enfoque se evidencia en la posibilidad de simular decisiones a nivel estratégico y operacional mediante bloques retroalimentados. Estos bloques permiten representar fases diferenciadas del combate, integrando variaciones en la concentración de fuerzas, efectos en el terreno y estado moral de las tropas. Este tipo de modelos habilita la selección dinámica de blancos, priorización de zonas de fuego y la proyección de efectos de segunda y tercera orden. Además, los simuladores avanzados implementados en sistemas de artillería contemporáneos integran IA para adaptar parámetros del escenario virtual a condiciones reales en evolución. Bueno (1992) menciona que el simulador debe responder a situaciones cambiantes durante el entrenamiento y comportarse casi como los sistemas que representan (p.2), esto requiere de una interacción constante entre el escenario global y los múltiples parámetros operativos.

- Predicción de daños colaterales y efectos de fuego amigo: esta capacidad constituye una prioridad operacional y ética. Las innovaciones en IA, especialmente las vinculadas al aprendizaje automático y a la integración de sensores avanzados, permiten la integración de sistemas que no solo apoyan la toma de decisiones tácticas, sino que también perfeccionan la

precisión y discriminación de objetivos. Según Brown (2020), la incorporación de IA en sistemas de combate plantea el reto de garantizar que las decisiones letales mantengan la supervisión humana, evitando así que el control total de la operación recaiga en algoritmos autónomos (p.30). Este principio doctrinal se fundamenta en la idea de que la confianza operativa en la Inteligencia Artificial debe construirse a partir de la competencia técnica del sistema, particularmente en tareas como la identificación precisa de amenazas o la discriminación entre combatientes y no combatientes.

Adicionalmente, desde una perspectiva geoestratégica, Sánchez Tapia (2024), destaca que la integración de la inteligencia artificial en los campos de batalla contemporáneos no solo incrementa la velocidad de respuesta ante amenazas, sino que permite disminuir el margen de error humano en la fase decisoria (p.12). Esto, teóricamente, se traduce en una menor probabilidad de fratricidio o daños colaterales, especialmente si los sistemas de IA cuentan con interfaces explicables y sensores de alta precisión.

- Sistemas expertos para la toma de decisiones tácticas: El despliegue de artillería en el teatro de operaciones, sobre todo en situaciones críticas exige decisiones tácticas de complejidad y de corto tiempo que determinan la selección de blancos, validación de amenazas, sincronización de fuegos y la evaluación de efectos. En este sentido, los sistemas expertos definidos como *software* que imitan el comportamiento humano usando la información que se le proporciona para poder dar una opinión sobre un tema especial (Quintanar, 2007, p. 5), se componen de una base de conocimiento, un motor de inferencia y una capacitad explicativa, haciendo de esto una herramienta digital de alto valor estratégico que emerge con capacidad de refinar el criterio de un oficial de artillería mediante conocimiento representado en reglas, heurísticas que le permiten evaluar múltiples variables como terreno, tipo de

munición, posiciones amigas o enemigas y las reglas de enfrentamiento que se les proporcione.

Por su parte, Badaró, Ibañez y Agüero (2013), señalan que los sistemas expertos aportan resultados equivalentes a los de un especialista, emulando la capacidad humana de tomar decisiones de acuerdo con las condiciones del ambiente operacional (p. 349). En el contexto de artillería esto puede reflejarse en una proposición de cursos de acción, generando alternativas con estimación de tiempos, recursos y riesgos; soporta cada recomendación con una justificación contextual explicando las razones detrás de cada una, lo cual facilita la supervisión humana; ello resulta fundamental para facilitar el análisis para determinar rutas optimizadas en el despliegue, validar posiciones seguras y evaluar automáticamente blancos según reglas de identificación, restricciones y prioridades de fuego.

La metodología de construcción de estos sistemas requiere del acompañamiento de expertos como oficiales y suboficiales de artillería que aporten su criterio y experiencia, como también la codificación de las reglas tácticas y el testeo iterativo. Existen etapas fundamentales como la adquisición del conocimiento, su representación simbólica y el diseño del motor de inferencia. Este enfoque asegura que la base de conocimiento contenga reglas validadas por doctrina y experiencia previas, y que las recomendaciones del sistema sean coherentes con protocolos operacionales. Un aspecto crítico del planeamiento de artillería es la verificación del razonamiento algorítmico como lo indica Brown (2020), contemplando la necesidad de que los sistemas expertos militares sean explicables, de modo que el operador comprenda por que ha sido descartada una trayectoria de fuego, o porque se recomienda determinada munición ante condiciones adversas (p. 30), esta trazabilidad fortalece la confianza del del artillero y previene el fenómeno de "Caja Negra" que puede deslegitimar el uso de la IA en misiones sensibles. En

conclusión, los sistemas expertos integrados en C4IST transforman datos en decisiones tácticas que fortalecen la eficacia y seguridad del despliegue de artillería.

### 2.1. Retos y riesgos del uso de la IA en contextos militares

La IA potencia la eficiencia y precisión militar, pero su adopción plantea retos éticos, técnicos y operativos que exigen una mirada crítica. La sofisticación de los sistemas inteligentes no garantiza, por si sola, una optimización en decisiones estratégicas o tácticas. Por el contrario, Brown (2020), advierte que si los operadores no comprenden el razonamiento de un sistema autónomo podría surgir un escenario en el que la maquina adquiera más poder relativo que no tuvo al principio, generando una disonancia entre la responsabilidad táctica del comandante y las recomendaciones del sistema (p.32).

A este riesgo se suma la posibilidad de errores en la identificación de blancos, alimentados por sesgos en los datos de entrenamiento o interpretaciones diferentes al contexto operacional. Montalvan Vélez et al., (2024), señala que los algoritmos dependen de la calidad y diversidad de los datos que los nutren, en el caso de que estos sean erróneos o incompletos la IA puede amplificar los errores críticos en la toma de decisiones (p. 179).

En el nivel estratégico, se puede identificar un riesgo importante el cual corresponde a la vulnerabilidad de los sistemas de IA a ciberataques, interferencias electrónicas o manipulación informativa, lo que puede comprometer el rendimiento y la seguridad general de las operaciones. Esta amenaza es especialmente relevante en escenarios de guerra hibrida, donde la manipulación de datos o la suplantación de sensores puede inducir decisiones erradas, incluso sin contacto directo con el adversario (Muñoz, 2024, p. 5). En el nivel Táctico, el uso de la IA en sistemas de armas plantea el dilema del control humano significativo, a medida que se desarrollan capacidades autónomas con poder letal como plataformas de artillería auto configurables, surge el interrogante sobre ¿Quién? o ¿Qué? Tomó la decisión final de atacar, en este sentido Sánchez Tapia (2024),

plantea que la supervisión humana debe mantenerse en todo momento priorizando la legitimidad y la responsabilidad sobre la velocidad de reacción, incluso si esto requiere limitar la eficiencia del sistema (p. 13).

Finalmente, la asimetría en el acceso a la IA militar genera un riesgo geopolítico en el cual los países o actores no estatales que logren desarrollar capacidades autónomas más rápidamente podrían adquirir ventajas desproporcionadas, alterando el equilibrio estratégico y dificultando la aplicación del Derecho Internacional Humanitario (De Diego, 2025). Esta brecha tecnológica ya se percibe en los desarrollos diferenciales entre potencias como Estados Unidos, China, Rusia e Israel, proyectada como un factor determinante en la competencia futura por la superioridad en el dominio cognitivo y cibernético del conflicto.

En consecuencia, si bien la IA ofrece una ventaja estratégica y táctica tangibles para la artillería de campaña enfocado en el planeamiento de un despliegue de los sistemas, su implementación debe realizarse dentro de los marcos normativos, doctrinales y éticos solidos que garanticen la supervisión humana, la transparencia de las decisiones y la integridad de los sistemas.

## 3. Aplicaciones relevantes de IA en planeamiento militar

Colombia en los últimos años ha consolidado progresivamente la normatividad institucional para afrontar los desafíos del ciberespacio, impulsando una estrategia nacional que integra la ciberseguridad y la ciberdefensa como componentes claves para la seguridad del Estado. La trayectoria normativa en el CONPES 3701, el cual es el primer documento de política pública el cual define las bases de la estrategia nacional en ciberseguridad, en respuesta en las amenazas cibernéticas como el ataque a las páginas oficiales durante el fenómeno "Anonymous" (Díaz & Cremades, 2023, p. 42).

Posteriormente, en el CONPES 3701 de 2016, consolida la creación del Comando Conjunto Cibernético (CCOC) y la articulación del grupo de respuesta a emergencias cibernéticas de

Colombia (ColCERT), fortaleciendo la respuesta estatal. Finalmente, el CONPES 3995 del 202, durante la pandemia, enfatiza la gobernanza del ciberespacio, la capacitación en resiliencia digital y la protección de infraestructura critica del estado (Díaz & Cremades, 2023, p. 42).

A nivel institucional, el Ministerio de Defensa Nacional, ha impulsado una estrategia de planeamiento por capacidades, donde la ciberseguridad paso a ser eje transversal para el sostenimiento de la fuerza y el aseguramiento de la logística (Barrios Torres, 2024, p. 98). El Ejercito, ha implementado el Sistema Integrado de Gestión Logística (SILOG), fundamentado en plataformas ERP, con módulos interconectados que manejan procesos logísticos, financieros, de mantenimiento y seguridad digital (Barrios Torres, 2024, p. 95). Esta digitalización, aunque es necesaria y eficiente puede generar vulnerabilidades críticas.

La respuesta institucional ante crisis cibernéticas ha sido reactiva en algunos casos, pero también ha buscado anticiparse mediante doctrinas de seguridad y ciberdefensa. Un ejemplo citado es el incidente SolarWinds, el cual ilustro las posibles consecuencias de ciberataques a sistemas de gestión logística militar y motivo el fortalecimiento de medidas preventivas en Colombia (Barrios Torres, 2024, p. 98).

### 3.1. Vulnerabilidades críticas en sistemas militares fundamentados en IA

Las nuevas capacidades en el sistema militar con la IA también han generado nuevas vulnerabilidades. Por eso es de vital importancia para el desarrollo o empleo de una IA en sistemas militares identificar las principales amenazas identificadas, con las estrategias defensivas que actualmente se estudian o aplican para mitigar sus efectos:

- Protección de algoritmos y redes neuronales

Los algoritmos de la IA utilizados en entornos militares basados en redes neuronales profundas, son susceptibles a ataques de adversarios que manipulan los datos de entrada para inducir errores significativos en los resultados. Este tipo de vulnerabilidades puede ser letal en

sistemas como radares inteligentes o plataformas de apoyo de fuego indirecto. Para contrarrestar estas amenazas, se han desarrollado técnicas de entrenamiento adversarial y mecanismos de prueba tipo *red-teaming,* los cuales consisten en simular ataques reales por parte de un equipo especializado con el objetivo de identificar debilidades explotables en los sistemas antes que el enemigo.

En el contexto militar, esta práctica se convierte en una herramienta preventiva de ciberdefensa, ya que permite poner a prueba los sistemas de IA bajo condiciones externas y escenarios de combate simulados, los que favorece la corrección temprana de vulnerabilidades algorítmicas y de arquitectura. Esta técnica, a sus vez puede integrar ciclos de mejora continua mediante pruebas automatizadas y ejercicios de validación en laboratorios de guerra cibernética, a su vez, el uso de entornos de ejecución seguros (*Trusted Execution Environments*) y sistemas de *watermarkink* algorítmico con el propósito de aislar los datos y codificar la información, lo cual brinda una capa adicional de protección estructural al núcleo de los modelos en escenarios hostiles, dificultando su ingeniería inversa o clonación por actos maliciosos (Ahmed et al., s.f., p. 3)

- Vulnerabilidades ante interferencias o ataques de manipulación de datos

La integridad de los sistemas de IA depende críticamente de la calidad de datos con los que son entrenados y operados, ataques como el data *poisoning* (envenenamientos de datos) o evasión durante la fase de inferencia pueden introducir sesgos o errores sistemáticos que conllevan a distorsionar la toma de decisiones tácticas. Esta amenaza es particularmente afecta sistemas que operan en tiempo real, como la asignación dinámica de blancos o evolución de daños colaterales.

Entre las contramedidas defensivas más relevantes se encuentran la validación cruzada de información con fuentes redundantes, el aislamiento a redes expuestas del pipeline de entrenamiento el cual en este caso debe ser orientado por el personal experto en planeamiento de

un despliegue de artillería y la auditoria automatizada del comportamiento algorítmico permiten detectar desviaciones anómalas que pudieran ser indicativas de manipulación hostil (Vassilev, 2025, p. 10).

- Compromiso de la integridad y confidencialidad del almacenamiento de datos operacionales

El almacenamiento de grandes volúmenes de datos propios, incluyendo bases de datos logísticas, registros de operaciones militares, patrones de inteligencia y perfiles de blancos representa un activo estratégico para las Fuerzas Militares. No obstante, estos repositorios se convierten en objetivos prioritarios para actores hostiles que buscan interrumpir operaciones, replicar capacidades o divulgar información clasificada. Las amenazas más comunes como lo indica Ahmed et al., p. (s.f, p. 4), incluyen exfiltración de datos mediante ataques persistentes avanzados (APT) el secuestro de información crítica (*ransomware)*, y sabotaje lógico de la integridad del sistema. Para contrarréstalas según (Pinelis & Vignard, 2025, p.18), se han consolidado prácticas como la segmentación de bases de datos por niveles de sensibilidad, el empleo de criptografía militar de alto nivel como el AES-256, la implementación de arquitecturas tipo *Zero Trust* que exija continuamente la identificación del funcionario y la replicación de datos en silos aislados geográficamente.

Así mismo, la capacitación del personal mediante ejercicios de *Cyber Range* y simulación de brechas de seguridad permiten evaluar la respuesta ante escenarios de compromiso, mejorando los protocolos de detección y contención temprana, permiten fortalecer la resiliencia de los modelos frente a perturbaciones maliciosas.

En última instancia, la seguridad de los sistemas de IA militar no depende exclusivamente de su precisión o eficiencia, sino de su capacidad para operar de forma robusta, confiable y

resiliente en entornos dinámicos, hostiles y disputados. Integrar una cultura de protección algorítmica y una gobernanza estratégica de los datos se configura en la actualidad como una condición indispensable para preservar la superioridad operativa y asegurar el cumplimiento de los objetivos militares en el ciberespacio. Como advierte (Pinelis & Vignard, 2025, p.17) la robustez de los sistemas de IA debe contemplarse como una prioridad fundamental de seguridad en entornos donde las decisiones automatizadas pueden tener consecuencias físicas, políticas o estratégicas irreversibles.

## 4. Propuesta de modelo estructural de IA con medidas integradas de ciberseguridad

### 4.1. Diseño conceptual del modelo estructural propuesto

El modelo estructural propuesto se fundamenta en una arquitectura modular y funcional, orientada a asistir el planeamiento y control operacional de fuego indirecto de artillería mediante IA. Sus componentes se enfocan en asistir en la recopilación, procesamiento, análisis, validación y decisión táctica, garantizando al mismo tiempo su operatividad en condiciones de disputa cibernética, estructurándose en cinco módulos funcionales interconectaos:

#### 4.1.1 Módulo de adquisición y depuración de datos:

Recibe información desde sensores ISR, redes logísticas, reportes meteorológicos y sistemas de mando y control. Incluye filtros de validación automática para eliminar redundancia, inconsistencias o patrones anómalos. Este módulo constituye el punto de entrada del sistema, encargado de capturar, consolidar y validar la información necesaria para el funcionamiento del modelo de IA. Su función es crítica, ya que la fiabilidad del análisis y la precisión de las decisiones tácticas depende la calidad de datos ingresados. En entornos operacionales complejos, caracterizados por condiciones cambiantes, guerra electrónica y amenaza cibernética persistente, este módulo actúa como un filtro inicial de integridad de la información.

La información se obtiene de diferentes fuentes que provienen de:


Fuente: Elaboración propia.

Este módulo a su vez debe cumplir con funciones técnicas como:

- Integración de datos heterogéneos que convierten formatos de imágenes, señales, texto o videos en estructuras procesables por la IA.
- Validación algorítmica que emplea rutinas de detección de inconsistencias, identificación de duplicados, limpieza de datos nulos y filtrados de relevancia operativa.
- Detección de anomalías estadísticas mediante análisis probabilístico y umbrales dinámicos, que permite identificar entradas atípicas que podrían corresponder a errores de sensores o intentos de manipulación (spoofing, data poisoning)

- Preclasificación semántica y temporal que organice los datos según su tipo (Táctico, logístico, meteorológico), tiempo de adquisición y nivel de criticidad.

Para este módulo se deben emplear medidas de ciberseguridad aplicadas como:

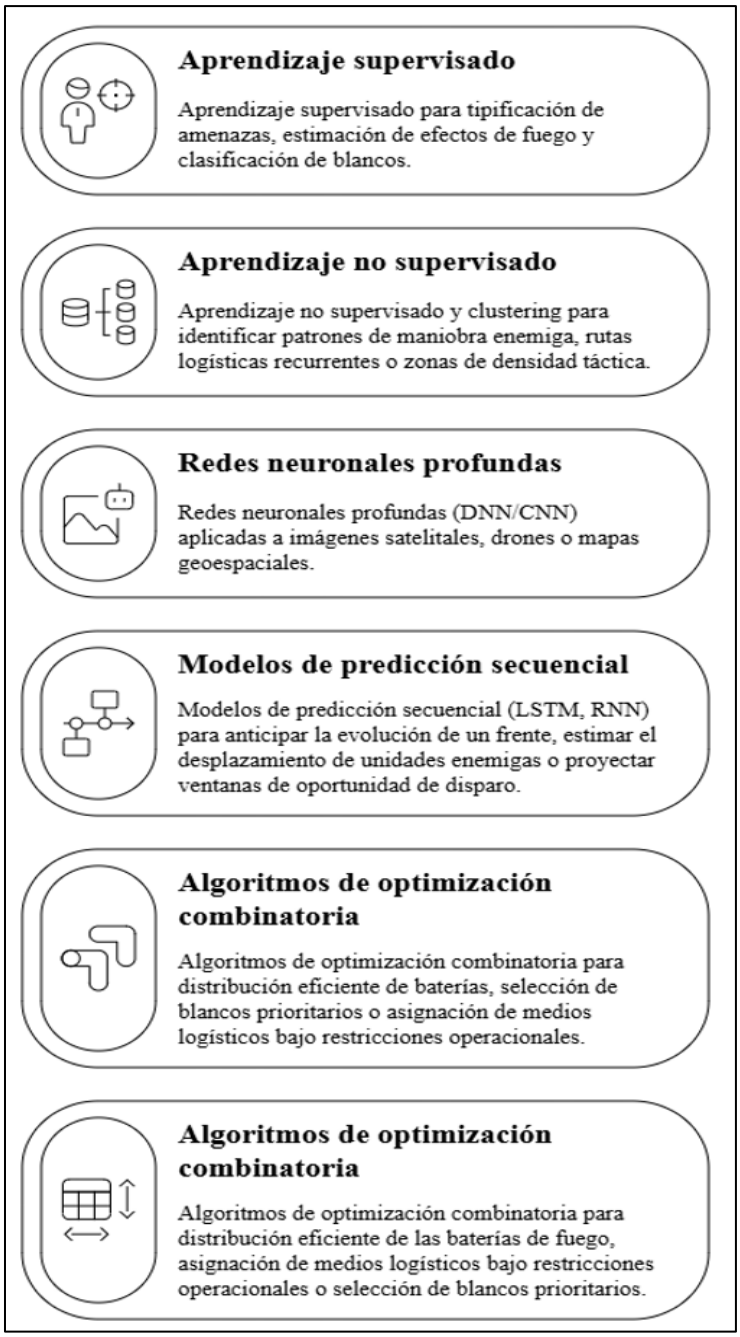
- Verificación de autenticidad en origen para que cada flujo de datos sea autenticado mediante certificados digitales y cifrado de extremo a extremo.
- Segmentación lógica por fuente y tipo que impida que un fallo o intrusión en una fuente contamine el resto del sistema.
- Control de integridad mediante hash criptográfico que garantice que los datos no han sido modificados desde su adquisición.
- Tolerancia a fallos y redundancia operativa con múltiples rutas de adquisición permitan mitigar el riesgo de pérdida total por sabotaje o interferencia electrónica.
- Monitoreo en tiempo real mediante SIEM (*Security Information and ecent management)* que detecte patrones anómalos o inconsistencias operativas asociadas a posibles ataques

Este módulo no solo cumple con una función de filtrado técnico, sino que representa un primer muro de defensa informacional clave para preservar la legitimidad y eficiencia de las decisiones que se deriven del sistema. La depuración efectiva de los datos alimenta al modelo con información confiables, oportuna y verificada, alineada con los principios de precisión, legalidad y oportunidad que rigen el empleo de la función de conducción de guerra Fuegos

### 4.1.2 Módulo de análisis y predicción táctica:

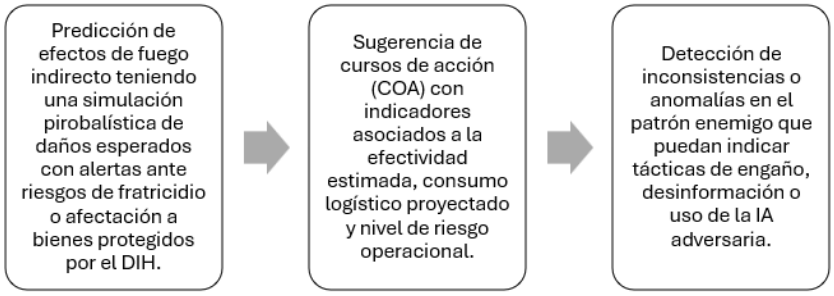
Este módulo constituye el núcleo algorítmico del modelo estructural donde convergen los datos previamente depurados para ser procesados por técnicas de inteligencia artificial con el fin de apoyar la toma de decisiones militares, su función se centra en la generación automatizada de propuestas de acción y predicciones operacionales, orientadas al planeamiento de artillería en escenarios de conflicto convencionales, híbridos o asimétricos.

El análisis y la predicción en este módulo se basan en el empleo de técnicas como:



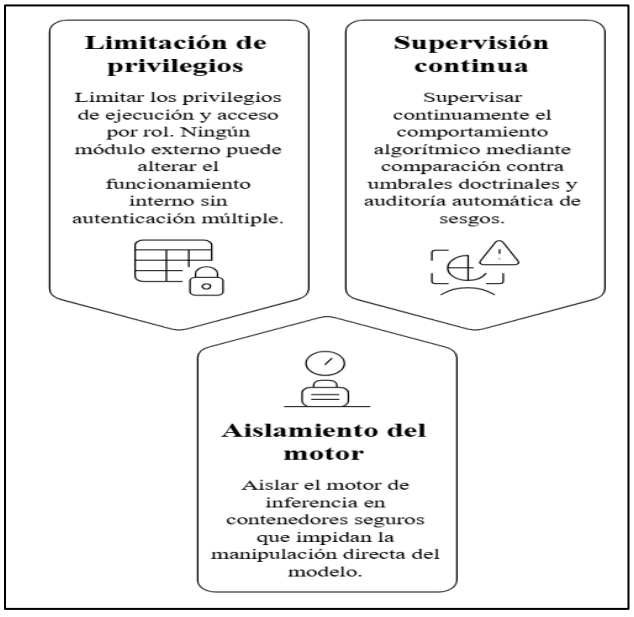

Fuente: Elaboración propia.

Se pueden incluir funciones tácticas y operacionales específicas como:




El módulo puede operar en ciclos iterativos cortos que se alimenten en tiempo real con los datos provenientes del módulo anterior. La IA evalúa permanentemente el entorno táctico y actualiza sus predicciones conforme evoluciona la situación en el área de operaciones. Cada salida del sistema como un posible curso de acción o una predicción de movimiento del enemigo, se entrega con su respectivo grado de confianza estadística y nivel de explicación, lo que permite su validación por parte del comandante.

Para este módulo se deben integrar medidas de seguridad como:




Fuente: Elaboración propia.

Este módulo representa la capacidad cognitiva del sistema y reduce el tiempo de decisión y mejora la proporcionalidad y legalidad del uso del fuego. En el contexto del arma de artillería,

proporcione una ventaja asimétrica al permitir planear con base en anticipación táctica, análisis multivariable.

### 4.1.3 Módulo de control y validación doctrinal:

Este módulo tiene como finalidad materializar la forma comprensible, confiable y operativamente útil los productos generados por los módulos anteriores basados en la adquisición datos y el análisis predictivo. Es la interfaz cognitiva entre el sistema de inteligencia artificial y el comandante táctico, permitiendo una lectura rápida, contextualizada y validable de las recomendaciones emitidas por la IA:

Funciones principales del módulo:

| Componente / Área | Descripción | Elementos gráficos / Ejemplos |
|---|---|---|
| **Indicadores de riesgo y confianza** | Mostrar el nivel de confianza estadística de cada propuesta y sus límites. | Gráficos de barras/intervalos de confianza; márgenes de error; umbrales críticos (semáforo); alertas doctrinales y legales (pop-ups). |
| **Representación de cursos de acción (COA)** | Visualizar opciones viables, rutas de despliegue y sectores de fuego con sus efectos proyectados. | Mapas con rutas; polígonos de sectores de fuego; conos de impacto; capas de dispersión balística, zona segura y efectos secundarios. |
| **Panel de control y priorización táctica** | Filtrado y comparación de propuestas según criterios doctrinales y logísticos; simulación rápida. | Panel con filtros (misión, tiempo, recursos, ROE); matriz de priorización; comparador de COAs; simulador acelerado (replay). |
| **Registro automático y auditoría** | Documentar interacciones, decisiones y cambios para trazabilidad y lecciones aprendidas. | Log cronológico exportable; marca de usuario/rol; hashes de integridad; reportes de efectividad. |
| **Aplicación: evaluación de apertura de fuego** | Criterios y visualizaciones para valorar conveniencia de disparar según proximidad a civiles y normativas. | Indicadores de proximidad a unidades amigas/infraestructura; checklist de DIH/proporcionalidad; semáforo de autorización. |
| **Aplicación: visualización en tiempo real del efecto de un tiro** | Simular impacto considerando meteorología, posición enemiga y efectos secundarios. | Animación del trayecto; overlay meteorológico; ventanas temporales críticas; estimación de daños colaterales. |
| **Aplicación: sugerencias de concentración/dispersión de fuegos** | Recomendaciones de IA según comportamiento proyectado del enemigo. | Recomendaciones con justificación (probabilidad); heatmaps de densidad de fuego; alternativas optimizadas. |
| **Aplicación: interfaz adaptable** | Interfaz usable tanto en puesto de mando de brigada como en batería avanzada con conectividad limitada. | Modo completo (web/GIS) y modo desconectado (mapas simplificados, datos cacheados). |
| **Medida de seguridad: autenticación reforzada** | Restringir acceso solo a personal autorizado con roles verificados. | MFA, SSO, listas de rol y permisos, control de sesiones. |
| **Medida de seguridad: cifrado de interfaz y datos** | Evitar exfiltración o manipulación de datos tácticos y COAs. | TLS, cifrado en reposo, encriptación de capas de mapa. |
| **Medida de seguridad: modo degradado** | Operación ante denegación de servicio o pérdida de red con visualizaciones simplificadas locales. | Vista simplificada local; datos sincronizados; operaciones esenciales offline. |
| **Medida de seguridad: integración C2 segura** | Sincronización con mandos y unidades mediante protocolos seguros. | Conectores C2/COMMS, autenticación mutua, registros de intercambio y reconciliación. |

Fuente: Elaboración propia

Desde una perspectiva doctrinal, este módulo se ajusta al principio de comando con conocimiento de la situación, al proporcionar al comandante una representación visual dinámica

del área de operaciones, con elementos clave priorizados, riesgos destacados y trayectorias proyectadas. Este módulo permite transformar la complejidad algorítmica en una herramienta de decisión humana clara, explicable y operativamente valiosa. Su correcto funcionamiento garantiza que la IA actúe como asistente de mando, no como sustituto, respetando el principio de mando con conocimiento y control, que es esencial en la conducción del fuego de artillería y la maniobra táctica.

### 4.1.4 Módulo de seguridad y residencia algorítmica:

Este módulo constituye el mecanismo de garantía normativa, ética y operacional del modelo estructural propuesto, cuya función principal es actuar en forma de capa de validación cruzada que asegure que las recomendaciones y predicciones generadas por la IA se encuentre en conformidad con las reglas de enfrentamiento, la doctrina militar vigente, los principios del DIH y las condiciones tácticas reales del teatro de operaciones. Asimismo, se integra una barrera de seguridad decisional, con capacidad para bloquear, modificar o condicionar las recomendaciones del sistema si estas se desvían de los parámetros definidos, esto con el fin de asegurar que el juicio militar del comandante sea reemplazado por el sistema automatizado.

Funciones claves del módulo:

- Verificación del cumplimiento de las reglas de enfrentamiento, en la que se compara cada curso de acción sugerido por la IA con las reglas específicas de empleo de la fuerza aprobadas para la operación en curso (áreas de no fuego, calibre de munición a emplear)
- Evaluación de proporcionalidad y necesidad del uso de artillería mediante parámetros doctrinales como el valor militar del blanco, su grado de amenaza y la disponibilidad de medios alternativos para determinar si el empleo de la artillería es justificado en cada caso.
- Análisis de afectación colateral y riesgo a la población civil en la que la IA proyecta un impacto significativo en zonas sensibles, por medio de alertas que emite los sistemas ya sean doctrinales o legales la cuales tengan validación del comandante explicita.

- Supervisión de sesgos algorítmicos que se verifiquen patrones repetitivos que podrían indicar sesgos discriminatorios, escaladas no justificadas o pérdida de diversidad en los cursos de acción propuestos.
- Generación de trazabilidad jurídica y operacional en la que todo curso de acción validado o rechazado queda registrado con su justificación normativa, la evidencia táctica considerada y la participación humana en la decisión.

Marcos normativos y doctrinales considerados:

- DIH – Convenios de Ginebra y Protocolos adicionales
- Reglas ROE
- Doctrina artillera (MCE 3-09, MFRE 3-107)
- Lineamientos de los Comités Jurídicos Operacionales (CJO)
- Manual de Derecho Operacional Terrestre (MFRE 6-27)
- Principios de necesidad militar, distinción, proporcionalidad y humanidad

Medidas de ciberseguridad asociadas:

- Bloque de modificaciones externas al módulo en la que solo el personal con credenciales de alto nivel puede ajustar los criterios doctrinales o las reglas de enfrentamiento establecidas en el sistema.
- Encriptación y segmentación del entorno de decisión que garantice que la validación doctrinal sea inmune a manipulaciones externas.
- Monitoreo y reporte automatizado de excepciones, en la que cualquier decisión tomada en contravía de las advertencias doctrinales se registra y se notifica a instancias superiores.

Este módulo asegura que el empleo de sistemas basados en IA en el ámbito militar no se aparte de los límites legales, éticos y doctrinales establecidos por las fuerzas militares de Colombia y el marco internacional. Su existencia refuerza la legitimidad del empleo de los fuegos de artillería en un entorno de velocidad de decisión y la precisión operacional no pueden sacrificar el cumplimiento del derecho de los conflictos armados.

### 4.2. Medidas Específicas de ciberseguridad integradas en el modelo

La integración de la IA en procesos militares requiere una arquitectura de ciberseguridad sólida, escalable y adaptativa. En el modelo propuesto para apoyar el planeamiento y ejecución del fuego de artillería mediante sistemas inteligentes, la ciberseguridad se incorpora como principio transversal desde la concepción y trazabilidad operativa del sistema, especialmente en entornos con amenazas cibernéticas. Debido a las constantes amenazas, a continuación, se presentan en la tabla las medidas de ciberseguridad aplicables a cada módulo

| Módulo del modelo | Medidas de ciberseguridad | Objetivo estratégico |
|---|---|---|
| Módulo de adquisición y depuración de datos | • Verificación de autenticidad en origen<br>• Segmentación lógica por fuente y tipo<br>• Control de integridad mediante hash criptográfico<br>• Tolerancia a fallos y redundancia operativa<br>• Monitoreo en tiempo real con SIEM | Preservar la integridad informacional y filtrar amenazas desde el origen |
| Módulo de análisis y predicción táctica | • Limitación de privilegios de ejecución y acceso por rol<br>• Aislamiento del motor de inferencia en contenedores seguros<br>• Supervisión continua del comportamiento algorítmico<br>• Auditoría automática de sesgos en las predicciones | Asegurar la confiabilidad de la inferencia algorítmica y prevenir manipulaciones |
| Módulo de visualización y apoyo a la decisión | • Autenticación reforzada de usuarios<br>• Cifrado de la interfaz gráfica<br>• Modo de operación degradado<br>• Integración segura con sistemas de mando y control | Proteger la interfaz de decisión y mantener operatividad bajo ataque |
| Módulo de control y validación doctrinal | • Bloqueo de modificaciones externas al módulo<br>• Encriptación y segmentación del entorno de decisión<br>• Monitoreo y reporte automatizado de excepciones | Garantizar el cumplimiento doctrinal, normativo y ético del uso del fuego |

Estas medidas lejos de ralentizar el despliegue de la IA constituyen su condición habilitante para operar en entorno de combates modernos, donde el ciberespacio es tan disputado como el territorio físico. La integración de la ciberseguridad desde la arquitectura garantiza que el sistema

no solo sea eficaz, sino también seguro, resiliente y doctrinalmente legítimo, preservando la confianza del comandante y la coherencia con los principios del poder militar colombiano.

## 5. **Conclusiones**

El planeamiento de la artillería de campaña ha experimentado una evolución notable desde métodos tradicionales basados en observación directa, cálculos manuales y dependientes de la habilidad humana individual hacia sistemas altamente automatizados y digitalizados. Inicialmente, el planeamiento dependía en gran medida de factores humanos, incluyendo la interpretación directa del terreno mediante mapas topográficos, brújulas ópticas y (OA), lo que resultaba en una alta vulnerabilidad a errores humanos, condiciones ambientales adversas y limitadas capacidades de comunicación. La introducción de tecnologías avanzadas como sensores ISR, radares de contrabatería, y plataformas digitales, ha revolucionado el proceso operativo, incrementando sustancialmente la precisión, rapidez y seguridad del fuego indirecto. Sin embargo, este salto tecnológico también implica nuevas vulnerabilidades críticas frente a amenazas cibernéticas, subrayando la necesidad urgente de integrar mecanismos robustos de protección digital y seguridad de datos, aspectos vitales para garantizar la integridad operacional y la confidencialidad estratégica.

La integración efectiva de la IA en entornos militares representa una transformación sustancial en la capacidad táctica y estratégica, optimizando significativamente la recopilación, procesamiento y análisis de información para la toma de decisiones críticas en tiempo real. Técnicas avanzadas como el aprendizaje automático (*Machine Learning*), el reconocimiento automatizado de imágenes provenientes de satélites y drones, y el procesamiento del lenguaje natural (PLN), han probado su eficacia en acelerar la identificación de amenazas, mejorar la precisión en la asignación de blancos y optimizar el uso de recursos operacionales. Estas herramientas tecnológicas no solo facilitan decisiones más rápidas y precisas, sino que también

proporcionan una superioridad táctica crucial, especialmente en contextos operacionales caracterizados por alta volatilidad e incertidumbre. No obstante, esta transformación tecnológica exige un entrenamiento actualizado y constante del personal militar, fortaleciendo habilidades digitales y analíticas necesarias para la correcta interpretación y aprovechamiento pleno de estos recursos.

A pesar de los evidentes beneficios operativos de la IA en contextos militares, su implementación masiva plantea importantes desafíos éticos, técnicos y operacionales que deben abordarse cuidadosamente. La dependencia excesiva en sistemas automatizados puede generar riesgos éticos considerables, especialmente relacionados con la responsabilidad humana en decisiones críticas, incluyendo aquellas relacionadas con fuego letal. Además, la falta de transparencia y explicabilidad en los modelos más complejos de inteligencia artificial, especialmente aquellos basados en redes neuronales profundas, puede conducir a situaciones de pérdida de control humano efectivo sobre las decisiones tácticas, aumentando el riesgo de daños colaterales inadvertidos o incidentes de fuego amigo. Estas preocupaciones resaltan la importancia crítica de desarrollar protocolos robustos de explicabilidad algorítmica y transparencia operativa, combinados con medidas de ciberseguridad avanzadas que garanticen una operación segura y confiable en entornos digitales adversos.

El contexto colombiano en materia de ciberseguridad militar entre 2011 y 2021 evidencia una evolución significativa desde una postura eminentemente reactiva hacia un enfoque más estratégico y proactivo. La creación del Comando Conjunto Cibernético (CCOC) y del ColCERT representa un avance considerable hacia la gobernanza integrada del ciberespacio, especialmente en la protección de infraestructuras críticas y sistemas logísticos esenciales para la operación efectiva del Ejército Nacional. Sin embargo, la creciente digitalización de procesos y la adopción

de tecnologías avanzadas como la IA han incrementado las superficies potenciales de ataque, requiriendo una vigilancia constante y una mejora continua de las capacidades defensivas. Incidentes internacionales relevantes como el ataque SolarWinds han demostrado claramente la necesidad de mantener actualizadas y robustas las medidas preventivas y reactivas frente a vulnerabilidades cibernéticas emergentes, destacando la importancia estratégica de anticiparse efectivamente a estos riesgos.

Finalmente, el modelo estructural propuesto en este estudio responde directamente a la pregunta de investigación planteada, integrando inteligencia artificial y medidas avanzadas de ciberseguridad para reforzar el planeamiento y ejecución operacional en despliegues de artillería de campaña. Este modelo, de carácter modular y funcional, incorpora desde la adquisición inicial y validación de datos hasta la emisión final de recomendaciones tácticas auditables y verificables, garantizando eficiencia operativa y protección robusta frente a amenazas cibernéticas persistentes. La propuesta presentada establece además bases sólidas para futuras investigaciones, particularmente en términos de implementación práctica en entornos reales, evaluación continua de la efectividad operativa bajo escenarios variados, exploración de tecnologías emergentes como *blockchain* e inteligencia artificial distribuida, y un análisis más profundo sobre las implicaciones éticas, jurídicas y normativas asociadas al uso extensivo de estas tecnologías avanzadas en el ámbito militar.

## Referencias

Adler, J. N. (2025, agosto). *Modernizing military decision-making: Integrating AI into Army planning* [Artículo]. *Military Review Online Exclusive*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2025/Modernizing-Military-Decision-Making/Modernizing-mdmp-UA1.pdf

Aguilar, I., Alepuz, V., Alfaro, J., Bañón, J. J., Botti, V., Despujol, I., Giménez, J., Linares, J., Linares, J. M., Majadas, V., Martínez, J., Monsoriu, M., Montesa, E., Morillas, C., Muñoz, J. M., Ortega, J., Ortuño, A., Peñarrubia, J. P., Plasencia, A., Rieta, J., Sales, M., y Segarra, R. (2024). *Guía básica de la IA* (1.ª ed.). Smar3t Digital. https://multimedia2.coev.com/pdfs/Guia-Basica-IA.pdf

Ahmed, S., Vokkaliga, B., Sathyanarayana, G., Kumar, S., Mishra, P., Anand, R., & Akurathi, B. (n.d.). A Comprehensive Review of Adversarial Attacks on Machine Learning.

Atkinson, R. (2025). *Innovación estratégica y riesgos emergentes: La inteligencia artificial en la guerra moderna*. *Military Review*, 2(2025). https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/OLE/2025/Atkinson-SPA-2025/Atkinson-SPA-Q2-2025-UA.pdf

Badaró, S., Ibañez, L. J., & Agüero, M. J. (2013). Sistemas expertos: Fundamentos, metodologías y aplicaciones. *Ciencia y tecnología, 13*, 349–364.

Barrios Torres, S. (2024). La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia. In Tecnologías disruptivas, logística, seguridad y defensa en el ciberespacio (pp. 77–110). *Escuela Superior de Guerra*. https://doi.org/10.25062/9786287602700.03

Bossio Ballesteros, V. E. (2023). La Inteligencia Artificial en el Ámbito Militar: Una Herramienta Relevante y Útil. *Revista Seguridad y Poder Terrestre*, 2(3), 53–61. https://doi.org/10.56221/spt.v2i3.33

Brown, M. W. (2020). Preparándonos para confiar en los sistemas de inteligencia artificial de los equipos de combate. Military Review – Edición Hispanoamericana, 2(2), 26–35. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/Brown-preparandonos-para-confiar-en-los-sistemas-de-inteligencia-artificial-de-los-equipos-de-combate-SPA-Q2-2020.pdf

Bueno Sevilla, F. (1992). Simulador de combate terrestre. *Cuadernos de estrategia*, (57), 25–34. https://dialnet.unirioja.es/servlet/articulo?codigo=2776464

Castro, G. M., Cerrada, C., & Cerrada, J. A. (2019). Estudio del modelo de combate de Lanchester como soporte para la construcción de un decisor estratégico operacional militar mediante bloques retroalimentados. En *XL Jornadas de Automática: Libro de actas* (pp. 528–534). Ferrol: Servizo de Publicacións. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=AkoG94MAAAAJ&citation_for_view=AkoG94MAAAAJ:u5HHmVD_uO8C

De Diego, M., & Fernández Sáez, P. (2025, 26 de febrero). *Auge de la IA en el ámbito militar y sus riesgos*. Global Affairs, Universidad de Navarra. https://www.unav.edu/web/global-affairs/auge-de-la-ia-en-el-ambito-militar-y-sus-riesgos

Díaz Acevedo M., & Cremades Guisado A. (2023). La evolución de la estrategia de ciberseguridad de. *Universidad Nebrija*, 1 (La evolución de la estrategia de ciberseguridad de Colombia), 30–55. https://doi.org/10.13140/RG.2.2.22241.58723

Ejército Nacional de Colombia. (1961). Reglamento EJC-35 "Empleo Táctico de la Batería". Público.

Ejército Nacional de Colombia. (1990). Manual 3-52, Ejecutivo de la Batería.

Ejército Nacional de Colombia. (2005) EJC 3-158, Manual de Planeamiento para la Conducción de Pequeñas Unidades. Reservado.

Ejército Nacional de Colombia. (2007) EJC 3-170, Manual de Centro de Tiro. Restringido.

Ejército Nacional de Colombia. (2007). Manual 3-107 Apoyo de fuegos y táctica de Artillería de Campaña. público.

Ejército Nacional de Colombia. (2017) MFRE 3-37, Manual de Referencia del Ejercito Nacional "Protección". Público.

Ejército Nacional de Colombia. (2017). MFRE 3-09, Manual de Referencia, Público.

Ejército Nacional de Colombia. (2018). MCE 3-09 Artillería de Campaña y Apoyo de Fuegos.

Ejército Nacional de Colombia. (2019). MCE 3-01 Artillería de Defensa Antiaérea.

Ejército Nacional de Colombia. (2019). MTE 3-09.3 Artillería de Campaña y Apoyo de Fuegos.

Flores Vivar, J. M., Gómez de Ágreda, A., & Gómez López, J. (2023). Taxonomía de la inteligencia artificial en el entorno cognitivo de los conflictos. *Anuario Electrónico De Estudios En Comunicación Social "Disertaciones"*, *16*(2). https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804

Galán, J. J., Carrasco, R. A., & Latorre, A. (2022). Military Applications of Machine Learning: A *Bibliometric Perspective*. Mathematics, 2022, 10.

Goecks, V. G., & Waytowich, N. (2024). COA-GPT: Generative Pre-trained Transformers for Accelerated Course of Action Development in Military Operations. http://arxiv.org/abs/2402.01786

Gómez-de-Ágreda, Ángel; Feijóo, Claudio; Salazar-García, Idoia-Ana (2021). "Una nueva taxonomía del uso de la imagen en la conformación interesada del relato digital. Deep fakes e inteligencia artificial". Profesional de la información, v. 30, n. 2, e300216 https://doi.org/10.3145/epi.2021.mar.16

Ministerio de Asuntos Económicos y Transformación Digital. (2024). *Estrategia nacional de inteligencia artificial 2024*. https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf

Montalván-Vélez, C. L., Mogrovejo-Zambrano, J. N., Romero-Vitte, I. J., & Pinargote-Carrera, M. L. D. C. (2024). Introducción a la inteligencia artificial: Conceptos básicos y aplicaciones cotidianas. *Journal of Economic and Social Science Research, 4*(1), 173–183. https://doi.org/10.55813/gaea/jessr/v4/n1/93

Muñoz Guillena, R. (2024). *Procesamiento del lenguaje natural como eje central de la inteligencia artificial generativa*. Universidad de La Rioja. https://dialnet.unirioja.es/descarga/libro/985766.pdf

Muñoz Meoño, R. E. (2024). *Desafíos y soluciones en la defensa nacional: Un marco integral para contrarrestar amenazas híbridas* [Artículo para optar al título profesional, Maestría en Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto"]. Repositorio ESDEG. https://www.esdegrepositorio.edu.co/bitstream/handle/20.500.14205/11266/TG-MY%20MU%C3%91OZ%20RONALD-MAESD%20AULA%20I.pdf?sequence=1&isAllowed=y

Olivares Guzmán, C. S., & Saavedra Moscoso, C. W. (2025). *Optimización de rutas mediante aprendizaje por refuerzo en logística sostenible* [Tesis de grado, Universidad Señor de Sipán]. Repositorio USS-Institucional. https://hdl.handle.net/20.500.12802/14679

Payá Santos, C. A., & Luque Juárez, J. M. (2019). Aproximaciones al concepto de amenazas híbridas. En *Convergencia de conceptos: Propuestas de solución a las amenazas actuales para la seguridad y defensa de Colombia* (cap. 1). Editorial ESDEGUE.

Pinelis, J., & Vignard, K. (2025). *Artificial intelligence in the military domain and its implications for international peace and security*.

Porcelli Adriana Margarita. (2021). La inteligencia artificial aplicada a la robótica en los conflictos armados. Debates sobre los sistemas de armas letales autónomas y la (in) suficiencia de los estándares del derecho internacional humanitario. *Estudios Socio-Jurídicos,* 23(1). https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.9269

Quintanar, T. L. (2007). *Sistemas expertos y sus aplicaciones* (Tesis de licenciatura). Universidad Autónoma del Estado de Hidalgo, Pachuca de Soto, Hidalgo, México. https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Sistemas%20expertos%20y%20sus%20aplicaciones.pdf

Ramírez-Fonegra, C. C., Reina-Galíndez, J. A., Parra-Uribe, B. S., & Peña-Guzmán, C. A. (2024). Aplicación del machine learning como herramienta para la detección de liderazgo militar. *Brújula Semilleros De Investigación*, *12*(23), 4–15. https://doi.org/10.21830/23460628.155

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://portal.amelica.org/ameli/journal/262/2621457007/2621457007.pdf

Sánchez Tapia, G. B. (2024). *La tecnología como catalizador del cambio en la guerra*. Center for Global Affairs & Strategic Studies, Facultad de Derecho-Relaciones Internacionales, Universidad de Navarra. https://www.unav.edu/documents/16800098/85691452/gaj-6-enero-2024.pdf

Scott, B., & Michell, A. (2023). *El futuro de la comprensión situacional: la inteligencia artificial*. *Military Review*, enero 2023. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/OLE/2023/Scott/Scott-SPA-Jan-2023.pdf

Singh, K., & Jha, S. (2021). Cyber threat analysis and prediction using machine learning. *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 1981–1985. https://doi.org/10.1109/ICAC3N53548.2021.9725445

Vassilev, A. (2025). Adversarial Machine Learning: https://doi.org/10.6028/NIST.AI.100-2e2025