Criterios Éticos para la implementación de Tecnologías Emergentes en las Fuerzas Militares de Colombia

Mayor de I.M. Hauder Camilo Castillo Morales

Capítulo de libro para optar al título profesional:

Magister en Derechos Humanos y DICA

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor de I.M. Hauder Camilo Castillo Morales
Identificación	**:**	80207540
Programa académico	**:**	Maestría en Derechos Humanos y DICA
Tutor metodológico	**:**	Dr. Mauricio Antonio Torres Guarnizo
Tutor temático	**:**	CR. (R) Luis Eduardo Sánchez Aldana
Fecha de entrega	**:**	Agosto de 2024
Extensión	**:**	8.318 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este capítulo de libro fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este capítulo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este capítulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Criterios Éticos para la implementación de Tecnologías Emergentes en las Fuerzas Militares de Colombia

Ethical Criteria for the Implementation of Emerging Technology in the Colombian Armed Forces.

Hauder Camilo Castillo Morales[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza los desafíos éticos, jurídicos y operativos que plantea la incorporación de tecnologías emergentes en las Fuerzas Militares de Colombia. A través de una metodología cualitativa basada en análisis documental, el estudio se estructura en tres fases: identificación de dilemas éticos, evaluación de oportunidades y riesgos, y formulación de lineamientos normativos, abordando cinco áreas críticas: dignidad humana, rendición de cuentas, uso legítimo de la fuerza, compatibilidad con el Derecho Internacional Humanitario (DIH) y riesgos asociados al uso de tecnología dual. Además, el análisis revela oportunidades en eficiencia operativa, precisión y sostenibilidad, pero también desafíos en transparencia, regulación y control ético. Como resultado, se proponen diez lineamientos aplicables a doctrina, entrenamiento, adquisición y supervisión, orientados a fortalecer la legitimidad institucional y el cumplimiento del marco jurídico. Finalmente, se exponen unas conclusiones que destacan la necesidad de adoptar un enfoque ético y normativo solido que garantice una modernización responsable, legal y humanitaria de las capacidades militares, preservando los Derechos Humanos y el respeto al DIH frente a los escenarios futuros que enfrentan las Fuerzas Militares.

Palabras clave: Tecnologías Emergentes, Fuerzas Militares de Colombia, Inteligencia Artificial, Derecho Internacional Humanitario (DIH), Derechos Humanos (DD.HH.), Ética Militar, Control Humano Significativo.

Abstract: This chapter analyzes the ethical, legal, and operational challenges posed by the incorporation of emerging technologies into the Colombian Armed Forces. Through a qualitative methodology based on documentary analysis, the study is structured into three phases: identification of ethical dilemmas, evaluation of opportunities and risks, and formulation of normative guidelines.

[1]Mayor de Infantería de Marina de la Armada Nacional de Colombia. Candidato a Magíster en Derechos Humanos y Derecho Internacional para los Conflictos Armados, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Economista de la Universidad Militar Nueva Granada, Colombia. Magister en Gerencia de Proyectos de la Institución Universitaria Politécnico Grancolombiano, Colombia. Especialista en Política y Estrategia Marítima Escuela Naval de Cadetes "Almirante Padilla", Colombia. https://orcid.org/0009-0003-4794-5386 - Colombia. Contacto: hauder.castillo@esdeg.edu.co.

It addresses five critical areas: human dignity, accountability, legitimate use of force, compatibility with International Humanitarian Law (IHL), and risks associated with dual-use technologies. Additionally, the analysis reveals opportunities in operational efficiency, precision, and sustainability, while also identifying challenges related to transparency, regulation, and ethical oversight. As a result, ten guidelines are proposed, applicable to doctrine, training, procurement, and supervision, aimed at strengthening institutional legitimacy and compliance with the legal framework. Finally, the conclusions highlight the need to adopt a strong ethical and regulatory approach that ensures the responsible, lawful, and humanitarian modernization of military capabilities, preserving Human Rights and respect for IHL in the face of future scenarios confronting the Armed Forces.

Keywords: Emerging Technologies, Colombian Armed Forces, Artificial Intelligence, International Humanitarian Law (IHL), Human Rights (HR), Military Ethics, Meaningful Human Control.

Introducción

El precipitado avance de las tecnologías emergentes, han redefinido la posición del ser humano en un entorno global cambiante, transformando de forma relevante lo humanamente tradicional, en un acelerado proceso evolutivo que impacta significativamente los pilares fundamentales de la sociedad moderna (Tsamados et al., 2024). En este sentido, la humanidad se encuentra inmersa en una transformación digital sin precedentes, donde la interacción entre algoritmos autónomos, datos masivos y habilidades de adaptación y aprendizaje automática, plantea retos profundos para los sistemas normativos, éticos y jurídicos (Bayan & Fayyad, 2024).

En el contexto latinoamericano, la precaria integración tecnológica ha cobrado un interés creciente, especialmente en Colombia, cuyos procesos complejos de construcción de paz, reconciliación y redefinición del rol de la Fuerza Pública, han enmarcado escenarios híbridos que demandan capacidades adaptativas para mantener el orden público y fortalecer

la toma de decisiones en los distintos niveles de la guerra por parte de las Fuerzas Militares (FF.MM) (Segura et al., 2021).

Si bien es cierto, la tecnología en etapa inicial de desarrollo, nos permite viabilizar la importancia de satisfacer unas necesidades, con el fin de mejorar el estilo de vida y transformar los diferentes sectores de la sociedad. No obstante, la innovación es un proceso emergente en expansión, que hace que cada individuo pueda tomar la determinación de avanzar de acuerdo a sus propios intereses o motivaciones (Suleyman, 2025).

Así las cosas, el ámbito militar ha abierto un debate ético sobre el uso legítimo de la fuerza, la autonomía de los sistemas armados y la responsabilidad moral en contextos de guerra, problemática que debe ser abordada desde cuatro aproximaciones teóricas relevantes:

Primeramente, el escritor Isaac Asimov, formuló en el siglo XX, tres leyes de la robótica como una propuesta normativa para regir el comportamiento de las máquinas inteligentes: "un robot no debe dañar a un ser humano ni permitir que sufra daño; debe obedecer órdenes humanas, salvo que entren en conflicto con la primera ley; y debe proteger su existencia si no contradice las dos leyes anteriores". Dichas normas, a pesar de ser planteadas desde la ciencia ficción, anticiparon los dilemas éticos actuales de la Inteligencia Artificial (IA), donde los algoritmos deben ser diseñados para preservar la vida humana, actuar bajo supervisión y mantener mecanismos de autocontrol (Balkin, 2016).

En segundo lugar, la teoría de la "Guerra Justa", basada en los principios de Jus Ad Bellum y Jus In Bello, subraya que todo uso de la fuerza debe ser proporcional, distinguiendo los combatientes de no combatientes, ya que la integración de IA en operaciones militares plantea serios interrogantes sobre la capacidad de los sistemas autónomos en respetar estos

principios, durante la toma de decisiones sin intervención humana, factor clave para el cumplimiento de los Derechos Humanos (DD.HH) y el Derecho Internacional Humanitario (DIH). (Migliore J, 2005).

En tercer lugar, Hans Jonas, advierte sobre el principio de "responsabilidad" ante la implementación de tecnologías emergentes, enfatizando la necesidad de actuar con cautela, prudencia y obligación moral ante el poder transformador de la tecnología y sus posibles efectos colaterales sobre la humanidad y el entorno, implicando el anticipo de daños potenciales en su implementación mediante un marco ético, jurídico y operativo mitigando abusos o errores letales (De Siqueira, 2001).

Finalmente, la teoría de los Tiempos Posnormales de Ziauddin Sardar, ofrece una reflexión ética sobre la complejidad, la incertidumbre y la aceleración tecnológica del mundo actual, donde los modelos tradicionales de análisis se disuelven, proponiendo un desarrollo con enfoques flexibles y adaptativos, en escenarios múltiples, cambiantes y en constante tensión, anticipando riesgos, mediante criterios solidos en la toma responsable de decisiones (Sardar, 2010).

En efecto, es importante determinar que el uso ético de tecnologías emergentes exige a las Fuerzas Militares de Colombia, aplicar la doctrina con responsabilidad, afrontando la inestabilidad del conflicto interno mediante modernización, innovación y sinergia institucional, garantizando la protección de los DD.HH y el respeto al DIH. (MDN, 2021).

Por lo anterior, el propósito de esta investigación consiste en identificar los criterios éticos, riesgos y desafíos asociados con el uso de tecnologías emergentes en el ámbito militar, su impacto potencial antes de ser adoptada a mayor escala, y su viabilidad dentro del respeto

de los DDHH y DIH en Colombia, con el fin de proponer lineamientos que orienten a un ejercicio ético y responsable en el desarrollo de operaciones conjuntas por parte de las Fuerzas Militares.

Así las cosas, frente a las consideraciones éticas en la aplicación de nuevas tecnologías en la modernización de las Fuerzas Militares, se formula la siguiente pregunta: **¿Como puede la implementación de criterios éticos y responsables orientados a las buenas prácticas en el desarrollo de Tecnología Militar Emergente, garantizar el cumplimiento del DIH y minimizar la violación de DD.HH en desarrollo de operaciones militares dentro del Conflicto Armado Colombiano?**

Para comprender este interrogante, el análisis se estructura en tres aspectos clave; primero, la identificación de los desafíos éticos inherentes al desarrollo y uso de tecnologías emergentes en el ámbito militar; segundo, la evaluación de oportunidades operativas y riesgos éticos, jurídicos y estratégicos que ofrece el desarrollo de estas tecnologías en las operaciones militares y su implementación; y finalmente, el planteamiento de una propuesta de regulación ética adaptada al marco normativo colombiano y al entorno internacional, que armonice las políticas de innovación tecnológica con el cumplimiento del Derecho Internacional Humanitario y la protección efectiva de los Derechos Humanos.

Metodología

El enfoque de la investigación se fundamenta en una revisión sistemática de la literatura existente sobre tecnologías emergentes y su aplicación en el ámbito militar, aplicando un método exploratorio cualitativo no experimental, ya que permite la recolección de documentos con información relacionada, libros, artículos científicos, informes técnicos

y documentos oficiales como el Plan Estratégico Militar de Transformación PEMT 2042, el Plan Estratégico de Transformación Ejército del Futuro PETEF 2042, informes de organizaciones internacionales y propuestas políticas nacionales como el CONPES 4144, con el propósito de comprender y analizar los aspectos normativos y éticos, orientados a su implementación en los sistemas de modernización de las FF.MM, bajo los principios de control humano significativo, sustentados en el respeto a la dignidad humana, la soberanía nacional y los marcos jurídicos internacionales. Asimismo, Los repositorios utilizados para la búsqueda de información incluyen Google Scholar, Science Direct y Scopus. Por otro lado, se consultaron informes de organizaciones como Mind Foundry, RAND Corporation, Comité Internacional de la Cruz Roja, Unión Europea y el Foro Económico Mundial, que aportan perspectivas actualizadas sobre los riesgos emergentes en el uso militar.

La estructura de esta investigación está segmentada en tres líneas analíticas progresivas e interdependientes que abordan el tema desde una perspectiva ética, operacional y normativa. Primeramente, se reconoce la complejidad ética que implica el desarrollo y la implementación de tecnologías emergentes en las Fuerzas Militares, explorando los desafíos morales vinculados con el principio de dignidad humana, la rendición de cuentas y el uso legítimo de la fuerza, analizando el impacto de los sistemas autónomos en los DD.HH y el DIH, y como su adopción debe ser precedida por una reflexión doctrinal sobre la ética institucional militar. Posteriormente, se identifican las oportunidades que estas tecnologías ofrecen para mejorar las operaciones militares y los principales riesgos éticos, jurídicos, estratégicos y operacionales, asociados a la implementación de tecnologías emergentes en operaciones militares, tales como la autonomía letal, los errores de identificación, los sesgos

algorítmicos y decisiones automatizadas sin Control Humano Significativo, por medio de un mapeo de escenarios críticos y posibles vulneraciones normativas que podrían surgir en el contexto del conflicto armado colombiano. Por último, se plantea una propuesta de regulación ética y jurídica orientada al diseño y uso responsable de tecnologías emergentes por parte de las Fuerzas Militares, con énfasis en escenarios de conflicto armado, estructurada con base en estándares internacionales, principios de control humano significativo, transparencia algorítmica, y mecanismos de rendición de cuentas y monitoreo, cuyo fin es garantizar el respeto a los DD.HH y el DIH, en desarrollo de operaciones conjuntas, edificando una normativa coherente, adaptativa e innovadora.

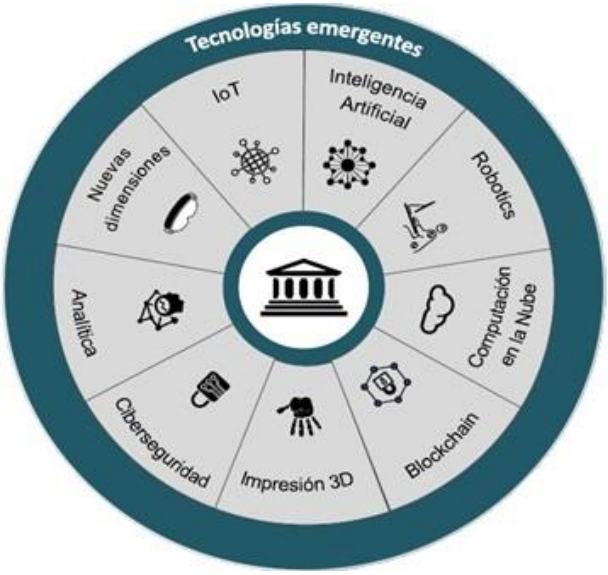
Desafíos Éticos en el Desarrollo de Tecnologías Emergentes y su Implementación en las Fuerzas Militares de Colombia

Para el desarrollo de este objetivo, es imperativo identificar previamente la definición de tecnología emergente (T.E en adelante). Según el College of Information Technology de la Universidad de Dubái (2013), la define como aquellas tecnologías que están en desarrollo o lo estarán en los próximos cinco a diez años, dependiendo del dominio, la región o el grado de adopción, sin depender de la novedad, sino de su impacto transformador y nivel de penetración en un contexto especifico (Halaweh, 2013).

Dentro de las T.E más relevantes en la actualidad, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC (2020), expone las siguientes:

Figura 1

Tecnologías Emergentes



Nota: Building the Digital State - Sep 2019 EY Global.

Por lo anterior, la veloz evolución de las T.E, desarrolla cada día nuevas soluciones que trascienden en diferentes industrias con diversas aplicaciones (Coman & Kifor, 2024). Así las cosas, para poder identificar los desafíos éticos de tan amplias categorías, se optó por un muestreo no probabilístico, el cual se centra en la selección intencionada de casos, personas, contextos o situaciones que ofrecen información significativa para el análisis cuyo objetivo, será la descripción de los desafíos éticos en el desarrollo de tecnologías emergentes. Bajo esta línea, se realizó un análisis de contenido temático cualitativo, siguiendo la metodología propuesta por Claudio Díaz Herrera (2015), adaptada a un enfoque inductivo basado en artículos académicos, informes internacionales, marcos regulatorios y políticas públicas, seleccionados por su pertinencia al tema de T.E, en contextos militares, incluyendo una lectura exploratoria, identificando fuentes que abordan dilemas éticos, vacíos jurídicos o

riesgos para los DDHH y DIH, lo que permitió la construcción de cinco categorías principales: dignidad humana, rendición de cuentas, uso legítimo de la fuerza, compatibilidad con el DIH y riesgos tecnológicos emergentes, como también variables que propiciaron una interpretación critica bajo un contexto del conflicto interno colombiano. En consecuencia, el análisis está enfocado en un análisis bibliográfico de acuerdo a la siguiente tabla:

Tabla 1

Análisis bibliográfico

Aspecto	Autor / Año	Propósito	Hallazgos	Aporte Ético
Dignidad Humana	Almache (2021)	Analizar el impacto de los sistemas autónomos sobre la dignidad en conflicto.	La automatización vulnera la dignidad al eliminar el juicio moral.	Refuerza el principio de humanidad frente a la automatización letal.
	Islam & Wasi (2024)	Denunciar sesgos en IA Militar.	La IA puede amplificar desigualdades si los datos son sesgados.	Visibiliza riesgos de exclusión por sistemas tecnológicos.
	Human Rights Watch (2012)	Cuestionar pérdida de empatía mediada por tecnología.	El Distanciamiento reduce la empatía y normaliza la violencia.	Alerta sobre la banalización del daño humano.
Rendición de Cuentas	Crootof (2020)	Explorar las zonas grises de imputabilidad.	No hay claridad sobre el responsable en decisiones automatizadas.	Revisa el marco jurídico asegurando rendición de cuentas.
	UNESCO (2021)	Evaluar trazabilidad algorítmica.	La opacidad impide reconstruir decisiones legales.	Exige transparencia en decisiones automatizadas.
	Pagallo (2013)	Analizar el conflicto entre responsabilidad estatal e individual.	La participación de privados diluye la responsabilidad legal.	Refuerza el rol del Estado como garante.
Uso Legítimo de la Fuerza	Cools (2020)	Evaluar toma decisiones proporcionales automatizadas.	Automatizar proporcionalidad aumenta riesgo de errores letales.	Reivindica el control humano significativo.
	Crootof (2020)	Cuestionar la pérdida de juicio humano en decisiones letales.	La autonomía total debilita la supervisión.	Toda decisión letal debe tener un componente humano.
	Almache (2021)	Evaluar limitaciones de IA en distinción.	Dificultades de IA en distinción de combatientes en entornos complejos.	Necesidad de adecuar la tecnología al contexto.
Compatibilidad con el DIH y Vacíos Normativos	Almache (2021)	Analizar regulación del DIH en LAWS.	Inexistencia de normas para armas letales autónomas.	Invoca la Cláusula Martens como principio orientador.
	Crootof (2020)	Evaluar los límites del DIH ante tecnologías.	El DIH diseñado para guerras humanas mas no automatizadas.	Adaptar marcos normativos sin renunciar a principios fundamentales.
	CONPES 4144 (2022)	Identificar riesgos éticos en tecnología militar.	Priorizar eficiencia afectaría cumplimiento del DIH.	Introduce visión crítica del Estado sobre tecnología y derecho.
Riesgos Eticos Emergentes por Tecnologías	Kuttner (2023)	Visibilizar uso Dual de tecnologías.	Tecnologias civiles utilizados con fines ofensivos.	Regulación uso bélico de infraestructura tecnológica comercial.

Nota: Elaboración propia

En virtud del anterior análisis bibliográfico, los principales desafíos éticos para las Fuerzas Militares, frente a la implementación de Tecnologías Emergentes, se agrupan en cinco áreas críticas: Primero, de acuerdo a De Siqueira, (2001), Hans Jonas expone, que la dignidad humana enfrenta el riesgo de deshumanización del conflicto, debido a que los sistemas autónomos pueden disgregar la responsabilidad moral individual en el uso de la fuerza representando un riesgo, por su impacto desproporcionado en ciertas poblaciones por consideraciones de género, raza, rasgos físicos o discapacidad, generando un sesgo algorítmico (De Siqueira, 2001; Muñoz W. et al, 2021).

Segundo, la rendición de cuentas exige marcos normativos claros para atribuir responsabilidades ante violaciones a los DD.HH y el DIH, como lo establece el Reglamento (UE) 2024/1689, frente al uso responsable de la Inteligencia Artificial y el procesamiento de datos, forjando la necesidad de regir su empleo, bajo límites éticos y jurídicos previos, asegurando el principio de la dignidad humana (Gantiva, 2022).

Tercero, como lo indica Perišić y Tomljenović (2024), el uso legítimo de la fuerza requiere preservar los principios de distinción, necesidad y proporcionalidad, especialmente en contextos donde la automatización puede generar decisiones autónomas letales, afianzando de que toda decisión letal debe tener un componente humano activo (Crootof, 2020).

Cuarto, es indispensable garantizar la compatibilidad con el DIH, tal como lo reconoce el CONPES 4144 de 2025 y finalmente, los riesgos éticos derivados de tecnologías que pueden tener uso tanto civil como militar (duales) y la militarización del entorno digital, requiriendo criterios de vigilancia, transparencia y control institucional, alineados con el

Decreto 1263 de 2022 (lineamientos y estándares para la transformación digital pública en el marco de la Política de Gobierno Digital) y la Resolución 0500 de 2021 del MINTIC (lineamientos y estándares para la estrategia de seguridad digital).

Con base en lo mencionado anteriormente, y teniendo en cuenta los cinco aspectos que interpretan los dilemas éticos, vacíos jurídicos o riesgos para los DDHH y DIH, en la figura 2, se enumeran los desafíos éticos más relevantes encontrados en el análisis bibliográfico, orientados a la implementación de las tecnologías emergentes, describiendo cada uno de ellos.

Figura 2

Desafíos éticos

Nota: Elaboración propia.

1. **Dignidad Humana y Despersonalización del Conflicto.**

- ***Despersonalización del conflicto y pérdida del juicio moral humano.*** El uso de sistemas autónomos de armas letales (LAWS) representa un riesgo al eliminar la intervención humana en decisiones críticas de combate, lo que amenaza la dignidad humana al suprimir el juicio moral, la empatía y la responsabilidad ética. Como advierte la UNESCO (2021), esta automatización puede transformar la guerra en una operación meramente técnica y deshumanizada (Almache, 2021).
- ***Sesgos algorítmicos y discriminación automatizada.*** Sobre este desafío hay que destacar que los sistemas de IA mal entrenados o sesgados pueden reproducir prejuicios estructurales de género, raza, condición física o nivel socioeconómico, lo que en un contexto militar podría derivar en decisiones letales basadas en patrones inmorales. Este desafío ético, como señalan Muñoz et al. (2021), requiere una gobernanza de datos responsable y un compromiso con la equidad algorítmica (Islam & Wasi, 2024).

2. **Rendición de cuentas.**

- ***Ambigüedad en la rendición de cuentas.*** El uso de Inteligencia Artificial en sistemas militares autónomos enfrenta el desafío de definir la responsabilidad ante violaciones al DIH, cuando una decisión letal proviene del propio sistema. Como señala Crootof (2020), la opacidad algorítmica y la tercerización tecnológica generan una "zona gris" que involucra a programadores, operadores y comandantes, creando un vacío ético y jurídico que vulnera el principio de justicia.

- ***Opacidad y falta de transparencia algorítmica.*** En el caso de los sistemas autónomos, plantean un desafío crítico para la legalidad y legitimidad del uso de tecnologías emergentes, al operar como "cajas negras" sin trazabilidad en sus decisiones. Según la UNESCO (2021), la transparencia entra en tensión con la confidencialidad operativa, lo que exige normativas éticas sólidas, auditorías técnicas y un control humano significativo permanente, tal como advierten Crootof (2016) y Scharre (2018), para salvaguardar los principios del DIH y los DD.HH.

3. **Uso legítimo de la Fuerza.**
   - ***Automatización del uso de la fuerza sin control humano significativo.*** En este desafío, Cools (2020), advierte que la autonomía de decisión algorítmica vulnera el juicio sobre proporcionalidad y distinción en el teatro de operaciones, comprometiendo los principios del DIH, siendo un riesgo inaceptable en escenarios militares. En este sentido, la OTAN (2024), enfatiza la necesidad de mantener supervisión humana significativa, y al igual que Suleyman (2023), advierte que las tecnologías autónomas sin supervisión, podría incrementar riesgos geopolíticos, éticos y estratégicos, deslegitimando el control estatal.
   - ***Vulneración de derechos fundamentales.*** El uso militar de tecnologías de vigilancia, reconocimiento facial o seguridad de datos, puede vulnerar derechos fundamentales como la privacidad, la libertad de expresión y la no discriminación. Según la UNESCO (2021), cualquier implementación

tecnológica debe asegurar el respeto irrestricto a los DD.HH., incluso en escenarios de seguridad nacional.

4. **Compatibilidad con el Derecho Internacional Humanitario.**

- ***Vacíos Normativos frente a Tecnologías Emergentes.*** Este desafío es crítico, pues no existen tratados internacionales específicos que las controlen, generando vacíos legales y operativos. Ante ello, se recurre a la Cláusula Martens como principio orientador del DIH y garante de la humanidad y la conciencia pública (Almache, 2021). En Colombia, instrumentos como el CONPES 4144 de 2025, el Decreto 1263 de 2022 y la Resolución 0500 de 2021 del MINTIC promueven una gobernanza ética y responsable de la IA en las FF.MM, apoyándose en referentes como la Recomendación de la UNESCO (2021) y el Reglamento (UE) 2024/1689.
- ***Desajuste entre eficiencia tecnológica y principios del DIH.*** La búsqueda de superioridad operacional y eficiencia puede llevar a decisiones que ignoren o subordinen los principios de distinción, proporcionalidad y precaución. El CONPES 4144 (2025) reconoce este desequilibrio como un riesgo estructural y propone fortalecer la gobernanza ética de la inteligencia artificial en Colombia.
- ***Impacto en la legitimidad del uso de la fuerza.*** Cuando el uso de tecnologías emergentes no está claramente regulado ni supervisado, existe el riesgo de deteriorar la legitimidad del accionar militar, afectando la confianza ciudadana, la percepción internacional y la capacidad de las FF.MM para operar con transparencia y legalidad jurídica y moral (PETEF 2042).

5. **Riesgos Éticos Emergentes por Tecnologías Duales y Militarización del Entorno Digital.**

   - ***Militarización de tecnologías civiles (uso dual).*** La adaptación de Tecnologías Emergentes en aplicaciones militares, tales como drones, redes satelitales o herramientas de vigilancia por parte de civiles y por grupos armados ilegales en el actual contexto del conflicto, son un desafío determinante para las FF.MM, ya que carecen de un marco regulatorio claro, representando riesgos éticos al uso indiscriminado, dificultando la aplicación efectiva del DIH y la supervisión estatal (Kuttner, 2023).

A nivel nacional, normativas como el CONPES 4144, el Decreto 1263/22 y la Resolución 0500/21, promueven trazabilidad, evaluación de riesgos y gobernanza ética. Sin embargo, Linda Eggert (2024), advierte que la ambigüedad normativa proporciona la explotación tecnológica sin control por adversarios, debilitando la seguridad nacional, resaltando así la teoría de H. Jonas, donde la ética tecnológica debe considerar los impactos a largo plazo de nuestras acciones, es decir, el enfoque de la doctrina militar debe ser preventivo y adaptativo respetando el marco jurídico y ético vigente, bajo interoperabilidad con estándares internacionales como el Reglamento (UE) 2024/1689 y la recomendación sobre la Ética de la IA de la UNESCO (2021).

Teniendo en cuenta los resultados del análisis temático, se evidencia que la carencia de un marco normativo firme y actualizado, orientado a la implementación de Tecnologías Emergentes en el contexto militar, representa un alto riesgo ético y jurídico. También, la toma de decisiones letales con sistemas autónomos obliga tener un control humano

significativo en las FF.MM, garantizando los principios de distinción, proporcionalidad, precaución, sin comprometer la dignidad humana, la rendición de cuentas y la legitimidad del uso de la fuerza en operaciones militares.

Respecto a los desafíos identificados, es imperativo que las FF.MM adopten estándares doctrinales y operacionales frente al uso de Tecnologías Emergentes, alineados con principios éticos reconocidos internacionalmente tales como el CONPES 4144/25, el Reglamento (UE) 2024/1689 y la Recomendación sobre la Ética de la IA de la UNESCO (2021), los cuales brindan bases importantes frente la innovación tecnológica responsable. Así, la incorporación de tecnologías garantizará priorice el respeto a los derechos humanos, la legalidad en el uso de la fuerza y la protección de la población civil.

Oportunidades Operativas en el uso de Tecnologías Militares Emergentes y los Riesgos Asociados con su Implementación

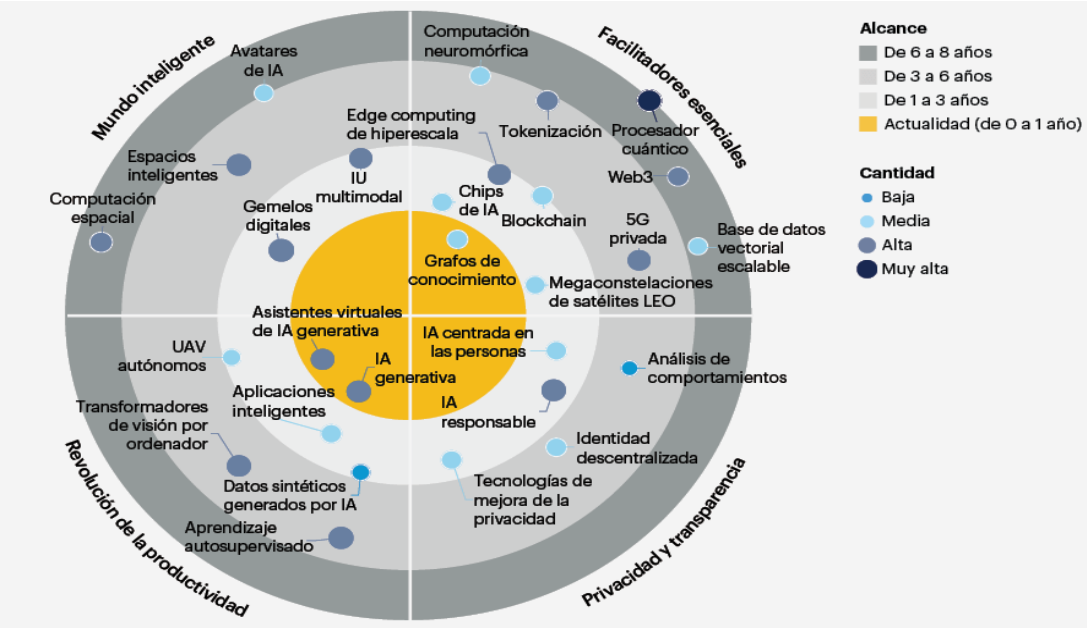
Para el desarrollo de la segunda fase de la investigación, inicialmente se evaluarán mediante método exploratorio cualitativo, las oportunidades estratégicas y posteriormente los riesgos éticos, legales y operacionales asociados a la implementación de tecnologías emergentes en las Fuerzas Militares.

Oportunidades Operativas.

Teniendo en cuenta las Tecnologías Emergentes identificadas, el contexto militar brinda una amplitud de oportunidades operacionales que transforman significativamente las capacidades de defensa nacional, fortaleciendo no solamente la eficiencia táctica y estratégica, sino permitiendo una mayor precisión en el uso de la fuerza, reduciendo los efectos colaterales en operaciones militares garantizado el respeto al DIH y los DD.HH.

Figura 3

Radar de Impacto Tecnologias Emergentes 2024 - 2032



Nota: Fuente Gartner Inc. 2024.

Con base en la figura 3, se observan las T.E en sus primeras etapas y su probable impacto a mediano y largo plazo, incentivando a las Fuerzas Militares a adaptarse a un entorno estratégico dinámico, complejo y tecnológicamente avanzado, planteando desafíos éticos y legales que deben ser abordados con responsabilidad cómo lo expone el Plan Estratégico Militar de Transformación (PEMT 2042) y el Plan Estratégico Ejército del Futuro (PETEF 2042). Dentro de las Tecnologías Emergentes que se perfilan como oportunidades se encuentran:

Inteligencia Artificial (IA). Su implementación fortalece la planificación logística, optimiza el reconocimiento de amenazas en tiempo real y el despliegue de vehículos autónomos, anticipándose ante amenazas mediante algoritmos predictivos en escenarios complejos, mitigando errores con respuestas más precisas (Simmons et al. 2024). También

de acuerdo a Wright N. (2022), integra sensores y algoritmos optimizando drones autónomos y sistemas de defensa inteligentes en el teatro de operaciones.

Internet de las Cosas (IoT). Facilita la interoperabilidad en dispositivos de comunicación, sensores y plataformas que recopilan, transmiten y procesan información en tiempo real mejorando la conciencia situacional y la capacidad de respuesta operacional (Groen, 2023).

Automatización de Procesos Robóticos (RPA). Permite automatizar tareas de sostenimiento, optimizando la cadena de suministro, la gestión documental y la planificación operacional, optimizando recursos (Maxwell, 2022).

Cloud Computing. Proporciona infraestructura esencial para la planificación y ejecución de operaciones conjuntas en múltiples teatros de operaciones, permitiendo acceso simultáneo a información crítica desde cualquier ubicación, fortaleciendo la interoperabilidad (UNESCO, 2022).

Blockchain. Fortalece la trazabilidad en la cadena de suministros, garantizando la ciberseguridad e integridad de datos en ambientes hostiles (Krelina, 2021).

Impresión 3D. Permite la fabricación de piezas de repuesto directamente en zonas de operaciones, reduciendo tiempos de respuesta, aumentando la autosuficiencia operacional, esencial en operaciones prolongadas o áreas de difícil acceso (Clement, 2024).

Ciberseguridad. Esencial para la protección de redes y sistemas de información, con capacidad de prevenir accesos no autorizados, gestionar identidades y detectar novedades en tiempo real (Cools, et al. 2024).

Analítica y Big Data. El análisis de datos masivos permite mejorar la predicción de acontecimientos, anticipándose a movimientos enemigos, prevención de amenazas y optimización de recursos estratégicos optimizando la toma de decisiones (Church et al. 2023).

Realidad Virtual (RV) y Realidad Aumentada (RA). Aplicadas en el entrenamiento militar, simulaciones tácticas y planificación estratégica, facilitando una inmersión realista optimizando la preparación de tropas en escenarios críticos de combate (UNESCO, 2022).

Biotecnología. Ofrece potencial en la medicina de combate, el rendimiento fisiológico de tropas y protección frente a amenazas biológicas. Sin embargo, el uso dual, genera un riesgo ético relevante (Ortiz et al. 2024).

Computación Cuántica. Aumenta las capacidades de procesamiento y desciframiento de criptografía segura, optimizando operaciones, sistemas de mando y control y ciberseguridad, permitiendo construir redes de comunicación ultra seguras bajo el principio de entrelazamiento cuántico. Sin embargo, su uso podría desestabilizar equilibrios estratégicos si no se establecen normas multilaterales de uso responsable (Coman, et al. 2024).

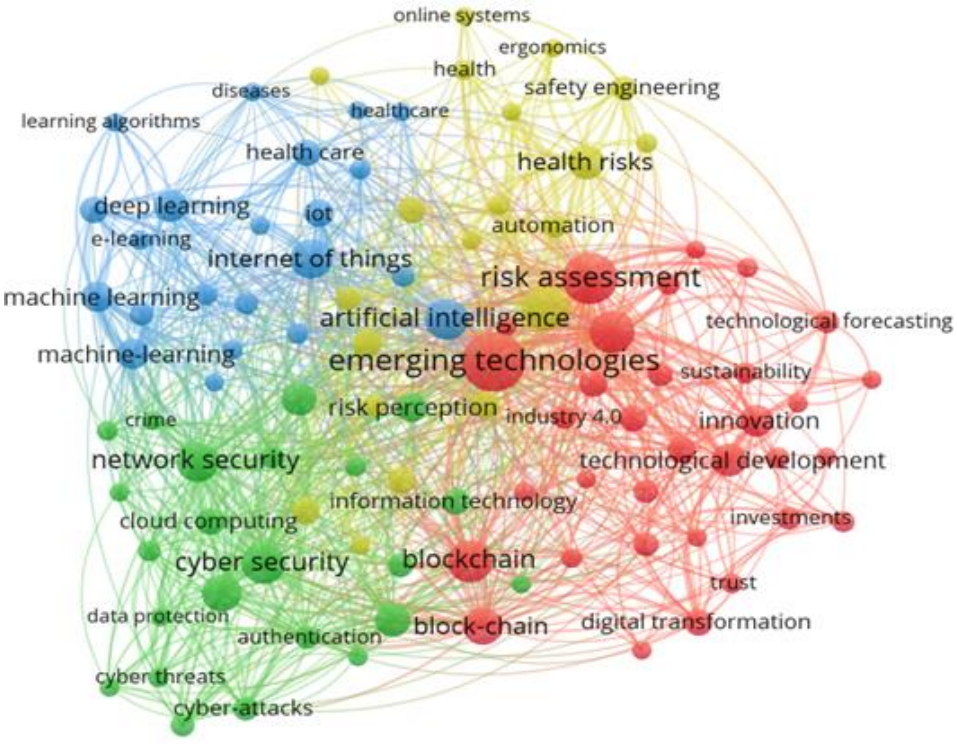
Por lo anterior, las oportunidades operativas de las Tecnologías Emergentes, mejoran la precisión, eficiencia y ejecución en operaciones militares, optimizando la toma de decisiones y reduciendo riesgos humanos y daños colaterales, actuando con mayor eficacia y respeto al DIH y los DD.HH.

Evaluación de Riesgos de las Tecnologías Emergentes.

Teniendo en cuenta las oportunidades que ofrecen las Tecnologías Emergentes aplicadas a las FF.MM bajo el contexto del conflicto armado, se evidencian riesgos éticos, jurídicos y estratégicos significativos que deben ser abordados previo a su implementación. En este sentido, se elaboró un análisis bibliométrico de publicaciones académicas entre los años 2022 y 2025, abarcando más de 143 artículos relacionados el tema de análisis, mediante el software VosViewer, cuyo mapeo científico presenta las redes de conexiones y coocurrencias de palabras claves, determinando los riesgos más relevantes identificadas con el clúster de color rojo.

Figura 4

Red de coocurrencia sobre las interacciones entre T.E y grupos de riesgo

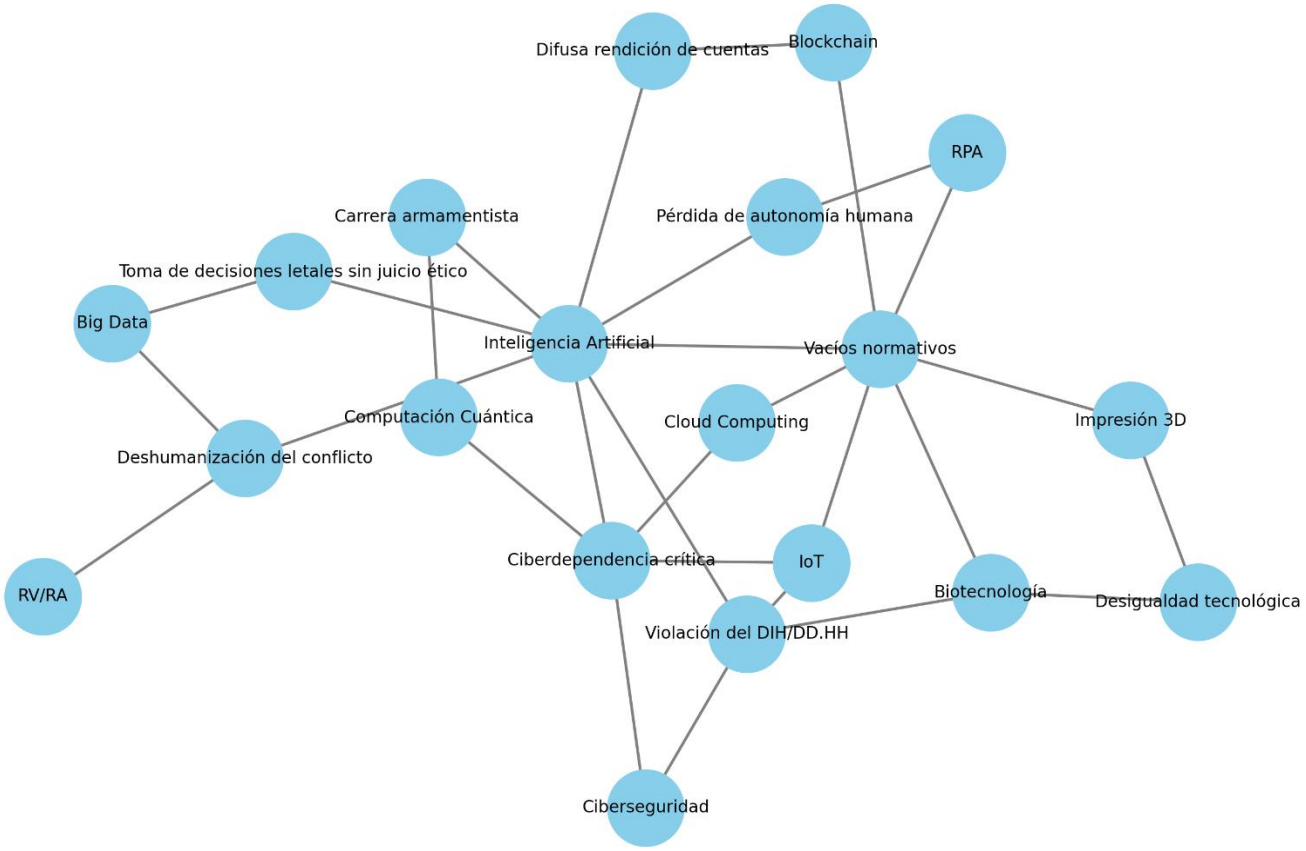


Nota: Elaboracion propia en uso del software VOSviewer.

La red de coocurrencia de la figura 4, indica la relación tecnológica con diversos riesgos clave, permitiendo identificar patrones y áreas críticas que deben ser abordadas con prelación en políticas de defensa y marcos éticos, identificando los más comunes como se muestra en la figura 5.

Figura 5

Red de Coocurrencia de Riesgos en las Tecnologias Emergentes.



Nota: Elaboración Propia.

El análisis interpretativo de la red de coocurrencia, expone los riesgos más comunes asociados con la implementación de T.E, agrupándolas en tres categorías principales: Riesgos éticos, Jurídicos y Estratégicos, cuyo análisis permite comprender las conexiones

críticas existentes entre el uso de la tecnología y los dilemas que enfrentan los actores involucrados en el teatro de operaciones así:

Riesgos Éticos.

Supresión del juicio humano en la toma de decisiones letales. Las tecnologías basadas en inteligencia artificial y sistemas de armas autónomas letales, al operar sin un control humano significativo, carecen de consideración ética y empatía, lo que las hace susceptibles de vulnerar los principios de humanidad, precaución y distinción, al tratar al ser humano como un "objetivo" y no como un sujeto con dignidad intrínseca (Docherty, 2020). En este marco, la Cláusula Martens y el principio de transparencia algorítmica se presentan como herramientas esenciales para regular tecnologías aún no contempladas en tratados internacionales específicos (Rasser et al., 2021).

Falta de Rendición de Cuentas. La delegación de decisiones militares a sistemas autónomos genera distorsiones en la atribución de responsabilidad jurídica y ética frente a posibles violaciones del DIH o de los DD.HH., creando vacíos legales que limitan la aplicación de medidas de imputabilidad penal o disciplinaria y afectan la eficacia de la justicia internacional (Ekelhof, 2019). Por ello, es indispensable mantener una supervisión humana significativa y evitar atribuir responsabilidades a los sistemas autónomos, estableciendo marcos normativos que garanticen la trazabilidad de decisiones críticas (González & Murillo, 2023).

Sesgos algorítmicos y discriminación. Los sesgos algorítmicos presentes en los sistemas de IA pueden generar prácticas discriminatorias en la selección de objetivos, vigilancia y clasificación de amenazas, reflejando estructuras sociales y relaciones de poder

preexistentes, y comprometiendo los principios de distinción, proporcionalidad y necesidad del DIH (Crawford, 2021). En consecuencia, el CICR (2023) destaca la necesidad de que los Estados implementen mecanismos efectivos para verificar y corregir sesgos, previniendo resultados imprevisibles o arbitrarios sobre la población civil.

Deshumanización del conflicto. Según Hans Jonas (1984) el Principio de Responsabilidad advierte que la implementación tecnológica no debe traducirse en una distancia moral. En este sentido, la implementación de drones, sistemas de armas autónomas, realidad virtual y aumentada, han transformado la guerra, automatizando el uso de la fuerza, diluyendo la empatía, responsabilidad y conciencia moral por parte del operador o decisor vulnerando el principio de humanidad del DIH (Sparrow, 2023).

Según la UNESCO (2022), esta desconexión emocional puede llevar a subestimar el uso de la fuerza, normalizando la violencia y los daños colaterales a las comunidades afectadas, contraviniendo los principios de proporcionalidad, humanidad y distinción, comprometiendo la responsabilidad individual y colectiva (Cools et al, 2024).

Riesgos jurídicos.

Responsabilidad difusa en el uso de Tecnologías Emergentes. La problemática jurídica frente la implementación de sistemas de IA y armas autónomas, dificultan la identificación de atribución de responsabilidad ante un resultado letal o desproporcionado en el teatro de operaciones. Según Human Rights Watch, (2023), Cuando un dron autónomo toma una decisión de ataque sin supervisión humana directa, surgen interrogantes jurídicos respecto la atribución de responsabilidad, respecto al operador, al programador, al fabricante o al Estado; comprometiendo el principio de rendición de cuentas del DIH, generándose una

zona gris al operar de forma algorítmica y no transparente, afectando la protección de civiles en el conflicto armado.

Aunque la Ley de Inteligencia Artificial 2024/1689 de la Comisión Europea establece categorías de riesgo y obligaciones para sistemas autónomos, su alcance en el ámbito militar global resulta limitado, por lo que se requiere una doctrina ética institucional que promueva gobernanza tecnológica basada en transparencia, auditabilidad y responsabilidad distribuida, integrando la rendición de cuentas en el uso de estas tecnologías. En Colombia, MINTIC y el Ministerio de Defensa han avanzado en la regulación, control y sanción del uso de drones y sistemas anti dron, consolidando un marco jurídico que protege la infraestructura crítica, la privacidad y la convivencia ciudadana frente al uso dual de estas tecnologías.

Vacíos Normativos Internacionales. Al no existir una norma internacional que regule el uso tecnologías emergentes en el ámbito militar, se genera una incertidumbre jurídica, que incrementa el riesgo de decisiones automatizadas sin responsabilidad humana vulnerando los principios del DIH y DD.HH (HRW, 2023). Sin embargo, La OTAN (2023) y el documento CONPES 4144 (2025) reconocen que la rapidez del avance tecnológico ha superado la capacidad adaptativa de los marcos regulatorios, estableciendo la necesidad de aplicar un marco ético jurídico, que legitime el uso de la fuerza, evitando socavar la confianza pública de las FF.MM en el marco de operaciones conjuntas en los nuevos escenarios del conflicto armado.

Ciber jurisdicción Ambigua. Tecnologías como la IA, el Internet de las Cosas (IoT), Blockchain y el Cloud Computing, generan nuevos retos legales, gracias a empresas privadas multinacionales que prestan su servicio a otros países, como por ejemplo el software con

propósito militar, comprometiendo la seguridad nacional. En este sentido, si una operación militar utiliza un dron, que está controlado desde un servidor extranjero, programado por una segunda empresa extranjera y ejecutada en una tercera zona de conflicto, crea confusión por la dispersión geográfica de los actores y, ambigüedad sobre la atribución de responsabilidad legal en caso de vulnerar los principios del DIH, dificultando la investigación o juzgamiento de delitos, por la falta de claridad jurisdiccional, requiriendo así, avanzar en marcos legales internacionales que regulen este tipo de acciones tecnológicas transfronterizas (Rubiano, 2022).

Riesgos Estratégicos

Dependencia tecnológica externa. Según lo planteado por Miller (2023), la adopción de tecnologías emergentes como semiconductores o plataformas de IA, generan una alta dependencia de proveedores extranjeros, comprometiendo la soberanía operativa de las FF.MM, vulnerable ante presiones políticas, inestabilidad o variaciones comerciales y fallas de suministro, limitando su autonomía estratégica. En este sentido, el monopolio creado sobre la cadena de producción de chips y sistemas inteligentes por parte de estados minoritarios, crea una asimetría de poder utilizada como arma geopolítica en escenarios de conflicto o tensión internacional.

Aceleración de la Carrera Armamentista. Según lo indica la Human Rights Watch (2020), la implementación acelerada de tecnologías emergentes en el sector defensa puede desencadenar una nueva carrera armamentista a nivel global, debido al incentivo que tienen los Estados en desarrollar capacidades bélicas que superen las del adversario, tales como

sistemas autónomos, drones o armas biológicas como el CRISPR-Cas9[2], incrementando el riesgo en el conflicto (Ashima, 2023). En este caso, es imperativo la adopción de mecanismos efectivos de regulación internacional, que limiten las malas prácticas en conflictos no convencionales (HRW, 2020).

Ciberamenazas y Vulnerabilidades. las ventajas que ofrecen tecnologías como el Internet de las Cosas (IoT), el cloud computing o el blockchain, en conectividad y trazabilidad son significativas, pero vulnerables a ataques cibernéticos, ya que según Lindsay (2019), su implementación en sistemas críticos, exponen a las FF.MM a ciberataques que comprometen sus activos informáticos, infraestructuras criticas o de comunicaciones, afectando los sistemas de comando, control y comunicaciones (C3), en especial si dependen de redes abiertas o tecnologías desarrolladas por terceros sin evaluación ética ni control estatal previo.

Riesgo de Inestabilidad Operativa. La optimización de procesos militares mediante IA y sistemas autónomos, pueda que mejoren la reacción y exactitud en la toma de decisiones, pero generan un riesgo de inestabilidad operativa, cuando dichas decisiones se delegan a máquinas sin un control humano significativo, desencadenando acciones letales, que rompen las reglas de enfrentamiento o los principios del DIH. Según lo expone Wrigth (2022), la Organización para proyectos de defensa con investigación avanzada (DARPA), reconoce que dichos avances en automatización militar, no garantizan la capacidad de discernimiento ético y legal por parte de una máquina respecto al contexto del conflicto armado, desencadenando

[2] Es una técnica de edición genética que permite modificar secuencias de ADN de manera específica (Comunidad Biológica, 2024).

no solamente daños colaterales, sino credibilidad en la legitimidad institucional, desencadenando acciones diplomáticas en un contexto internacional.

Por lo anterior, se realiza una matriz de riesgos con el fin de evaluar los riesgos más relevantes derivados de la implementación de tecnologías emergentes en las FF.MM, asignando una ponderación del impacto y, su probabilidad de ocurrencia en escenarios complejos en el contexto del conflicto armado, así:

Tabla 2

Matriz de riesgos de las Tecnologías Emergentes.

RIESGO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
Deshumanización del conflicto	moderado	mayor	12
Delegación letal sin control humano	casi seguro	grave	25
Responsabilidad difusa	probable	mayor	16
Vulneración del DIH	casi seguro	grave	25
Discriminación algorítmica	moderado	significativo	9
Fallas operativas de sistemas autónomos	probable	mayor	16
Violación a la privacidad y protección de datos	moderado	significativo	9
Inestabilidad operativa y escalamiento del conflicto	probable	mayor	16
Dependencia tecnológica externa	improbable	mayor	8
Ambigüedad normativa internacional	moderado	significativo	9

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Significativo	Mayor	Grave
		1	2	3	4	5
casi seguro	5	5	10	15	20	25
probable	4	4	8	12	16	20
moderado	3	3	6	9	12	15
improbable	2	2	4	6	8	10
raro	1	1	2	3	4	5

NIVEL DE RIESGO	COLOR
Muy Bajo	
Bajo	
Medio	
Alto	
Muy Alto	
Extremo	

Nota: Elaboración propia.

El análisis cualitativo de los resultados indica que, primero, los riesgos de delegación letal sin control humano y la vulneración del DIH, se ubican en el cuadrante más crítico de la matriz con riesgo nivel 25, identificado como muy grave y altamente probable, requiriendo

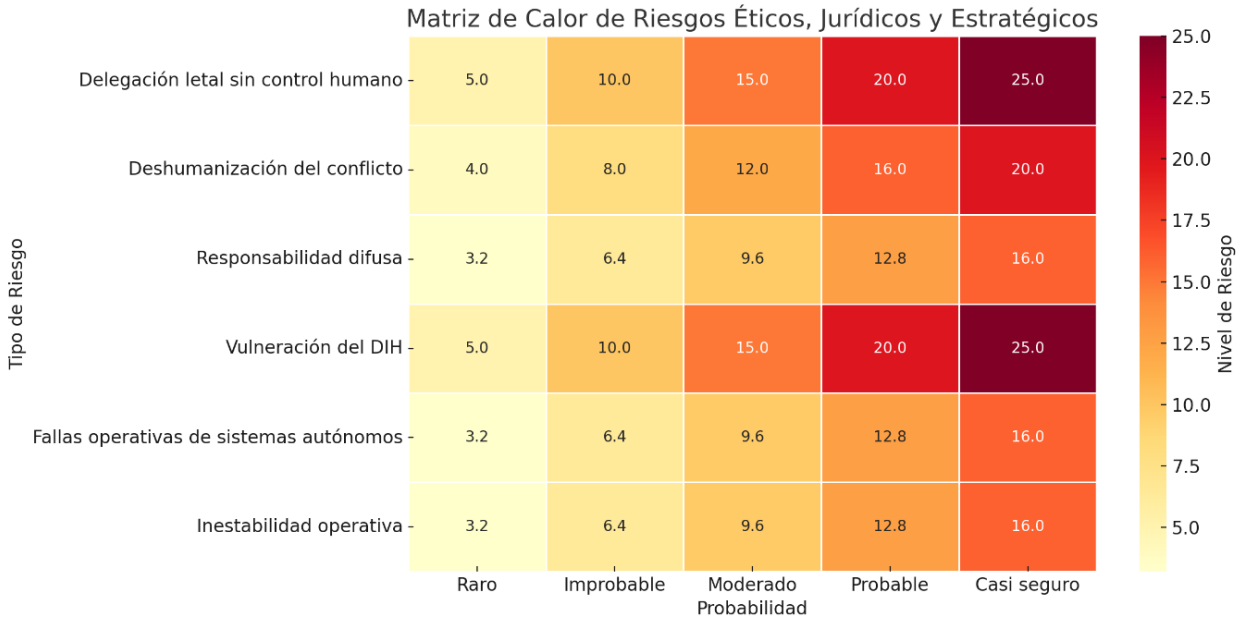
establecer limitaciones normativas y supervisión humana directa, conforme lo establece el CICR (2023) y la UNESCO (2022).

Segundo, la deshumanización del conflicto, aunque de menor gravedad relativa con riesgo nivel 20, sigue siendo un riesgo alto, debido a la pérdida del juicio moral en decisiones automatizadas, lo cual demanda la inclusión de principios como el de dignidad humana y responsabilidad ética en el desarrollo tecnológico (Asaro, 2012).

Por ultimo y siguiendo el mapa de calor (Tabla 3), se observa que la responsabilidad difusa, fallas e inestabilidad operativas, presentan niveles de riesgo medio-alto con 16 puntos, los cuales generan incertidumbre sobre la rendición de cuentas y el control efectivo de las operaciones, por lo que deben abordarse con marcos doctrinales y técnicos robustos (Lindsay, 2019).

Tabla 3

Mapa de calor de los riesgos de las T.E en el contexto militar.



Nota: Elaboración propia

Lineamientos Éticos y Normativos Para la Integración de Tecnologías Militares Emergentes en las Operaciones de las Fuerzas Militares de Colombia

Luego de haber identificado los riesgos que las tecnologías emergentes representan en su implementación, a continuación, se realiza una propuesta de 10 lineamientos éticos, divididos en cuatro bloques: primero, Ética y control humano en sistemas autónomos; Segundo, Supervisión, trazabilidad y gobernanza institucional; Tercero, Seguridad digital y soberanía tecnológica y cuarto, Uso legítimo y proporcional de la tecnología, ofreciendo así, una base coherente para la integración y el uso responsable ante la acelerada evolución de las tecnologías emergentes las cuales están transformando los escenarios militares tanto a nivel mundial como en el contexto del conflicto colombiano.

En este sentido, las Fuerzas Militares se enfrentan al reto inaplazable de adaptarse a nuevas realidades operacionales, técnicas y tácticas que incluyen inteligencia artificial, sistemas autónomos, robótica, biotecnología y herramientas de vigilancia avanzada. Sin embargo, esta transición o adaptación tecnológica no está exenta de dilemas éticos, riesgos operacionales y vacíos normativos que requieren una regulación clara, responsable y humana.

Ética y Control Humano En Sistemas Autónomos:

Lineamiento 1: Prohibición de Delegación Ética a Algoritmos Opacos.

Uno de los dilemas éticos más relevantes en el uso de tecnologías militares emergentes es la dependencia de sistemas de inteligencia artificial (IA) opacos, conocidos

como "cajas negras". Estos algoritmos, al operar sin transparencia, pueden tomar decisiones críticas sin que sus procesos internos sean comprensibles para operadores o diseñadores, lo que representa un riesgo significativo en contextos militares.

En este sentido, Frank Pasquale (2015) advierte que los algoritmos opacos pueden gobernar áreas sensibles sin control democrático ni rendición de cuentas. A su vez, Burrell (2016), identifica tres tipos de opacidad: intencional, técnica e intrínseca, lo que refuerza la necesidad de evitar delegar decisiones militares en sistemas no explicables.

Por ello, Floridi y Cowls (2019), proponen la explicabilidad como principio rector de la IA responsable, mientras que el principio de Hans Jonas, exige prever los efectos de la tecnología sobre la vida humana. En consecuencia, este lineamiento propone prohibir el uso de IA no explicable en operaciones militares críticas y establecer protocolos de certificación algorítmica, garantizando supervisión humana, trazabilidad y cumplimiento del Derecho Internacional Humanitario (DIH).

Lineamiento 2: Control Humano Significativo y Supervisión Operacional en Sistemas Autónomos y Semiautónomos.

La creciente incorporación de sistemas autónomos y semiautónomos en operaciones militares plantea un desafío ético y estratégico fundamental, consistente en asegurar que las decisiones críticas, especialmente aquellas relacionadas con el uso de la fuerza letal, permanezcan bajo supervisión humana directa y significativa. Por ello, este lineamiento establece que las Fuerzas Militares, deben adoptar el principio de Control Humano significativo, en su doctrina operacional, garantizando que ningún sistema tecnológico pueda ejecutar ataques sin la validación de un operador humano cualificado.

En apoyo a esta postura, el CICR, advierte que delegar funciones letales a máquinas compromete los principios de distinción y proporcionalidad del DIH. Asimismo, la ONU (2024), a través del Grupo de Expertos sobre Sistemas de Armas Autónomas Letales (LAWS), considera el Control Humano Significativo como un estándar mínimo para preservar la legitimidad operacional.

Desde una perspectiva filosófica, este lineamiento se fundamenta en la teoría de la guerra justa de Walzer (Migliore, 2005) y en el principio de responsabilidad de Hans Jonas (De Siqueira, 2001), ambos coinciden en que el juicio moral y la previsión ética no pueden ser reemplazados por algoritmos. En consecuencia, su implementación requiere mecanismos de supervisión en tiempo real, trazabilidad de decisiones humanas y protocolos para suspender operaciones automatizadas que representen riesgos ilegítimos para la vida humana.

Lineamiento 3: Transparencia Algorítmica en Entornos Operativos Militares.

La creciente incorporación de IA, en operaciones militares exige garantizar su gobernanza y transparencia para preservar la legitimidad y el control ético. Este lineamiento establece que todo sistema algorítmico, incluyendo plataformas de defensa, análisis de amenazas o reconocimiento autónomo, debe cumplir con criterios de explicabilidad, auditabilidad y trazabilidad. La opacidad algorítmica, como advierten Pasquale (2015) y Burrell (2016), puede ser intencional, técnica o intrínseca, dificultando el control democrático y la atribución de responsabilidades.

Normativamente, organismos como la UNESCO (2022) y la ONU (2024) recomiendan que los Estados adopten regulaciones que obliguen a la trazabilidad de sistemas

autónomos, especialmente en contextos donde puedan surgir violaciones al DIH o a los DD.HH. Así las cosas, éticamente, este lineamiento se fundamenta en el principio de responsabilidad de Hans Jonas, que exige anticipar y mitigar los riesgos tecnológicos, cuya implementación en Colombia implicaría protocolos de gobernanza algorítmica, auditorías internas y externas, con el fin de asegurar la trazabilidad de decisiones críticas.

Supervisión, Trazabilidad y Gobernanza Institucional:

Lineamiento 4: Transparencia, Auditoría y Trazabilidad en el Uso de TE.

La integración de Tecnologías Militares Emergentes (TME) exige evitar la confusión en su desarrollo, adquisición y uso operacional. Por ello, este lineamiento establece que todo sistema adoptado por las Fuerzas Militares, debe contar con mecanismos de transparencia, auditoría independiente y trazabilidad verificable en cada etapa del diseño, prueba, implementación y operación.

Particularmente en tecnologías como Blockchain, Big Data, IA autónoma y reconocimiento facial, la trazabilidad permite identificar fallos, responsabilidades y usos indebidos. Según la UNESCO (2022), la transparencia algorítmica fortalece la confianza institucional y protege derechos fundamentales. Asimismo, la ONU (2024) advierte que, sin rendición de cuentas, las armas autónomas podrían violar el DIH sin responsables claros.

Así las cosas, este lineamiento se fundamenta en la ética de responsabilidad de Hans Jonas, que obliga a anticipar los daños potenciales de la tecnología. Su implementación implica auditorías periódicas, bitácoras digitales auditables y registros automáticos en sistemas operativos desplegados (De Siqueira, 2001).

Lineamiento 5: Gobernanza Ética y Supervisión Civil-Militar en la Integración de TE.

La integración de Tecnologías Militares Emergentes, requiere no solo marcos técnicos y legales, sino también una gobernanza ética que garantice transparencia y control democrático. Por ello, este lineamiento propone crear un Consejo Nacional de Supervisión Tecnológica Militar, conformado por representantes de las Fuerzas Militares, el Ministerio de Defensa, entes de control civil, la academia y representación internacional, encargados de auditar todas las fases de implementación tecnológica.

Esta propuesta responde a la necesidad de evitar opacidad institucional y asegurar el uso legítimo de las TE. La UNESCO (2022), recomienda órganos interdisciplinarios para vigilar la ética de la IA, mientras que la ONU (2024), destaca la importancia del control civil-militar para la credibilidad internacional.

Filosóficamente, este enfoque se sustenta en la teoría de la guerra justa de Walzer, que exige criterios morales en el uso de la fuerza, y en el principio de responsabilidad de Hans Jonas, el cual demanda control ético sobre el poder tecnológico. Su implementación en las FF.MM, fortalecería la legitimidad institucional, la confianza ciudadana y la reputación internacional en defensa ética y transparente.

Lineamiento 6: Supervisión y Evaluación Continua de Tecnologías Militares Emergentes.

La adopción de tecnologías militares emergentes, requiere más que marcos normativos iniciales; demanda una supervisión y evaluación continua que permita auditar su desempeño, garantizar la rendición de cuentas y anticipar impactos éticos, jurídicos y estratégicos. Por ello, este lineamiento propone la creación de un comité interdisciplinario permanente, conformado por expertos militares, juristas en DD.HH. y DIH, ingenieros en

IA, representantes civiles y observadores internacionales, encargado de revisar todas las fases del ciclo tecnológico: diseño, pruebas, despliegue y evaluación postoperacional.

En este sentido, como lo indica el principio de responsabilidad de Hans Jonas, que exige vigilancia constante sobre tecnologías de alto impacto, la UNESCO (2022), el CICR (2023) y la ONU (2024), recomiendan sistemas de verificación que acompañen el despliegue de TE para evitar violaciones al DIH y a los DD.HH, ya que su implementación fortalecería la legitimidad institucional y la cooperación internacional, mediante auditorías, monitoreo en tiempo real y revisiones post operacionales que permitan corregir fallas y prevenir riesgos futuros.

Seguridad Digital y Soberanía Tecnológica:

Lineamiento 7: Protección de Datos, Ciberseguridad y Soberanía Digital en las Fuerzas Militares.

En el contexto de la integración de Tecnologías Militares Emergentes, la protección de datos y la ciberseguridad se convierten en pilares fundamentales, dado que la información representa uno de los activos estratégicos más vulnerables. Por ello, este lineamiento establece que las Fuerzas Militares, deben consolidar un ecosistema de ciberseguridad integral, que proteja tanto los datos personales como los operacionales, estratégicos y logísticos.

En este sentido, es indispensable que la infraestructura digital crítica permanezca bajo soberanía nacional, reduciendo la dependencia de proveedores extranjeros que puedan comprometer la autonomía estratégica. Esto implica que plataformas como la nube, sistemas

de mando y control (C2) y algoritmos de IA estén alojados en entornos controlados nacionalmente o en alianzas seguras (NATO, 2023).

Como advierte Lindsay (2019), los ataques a sistemas de vigilancia, mando y control nuclear, evidencian que la vulnerabilidad digital puede tener consecuencias devastadoras. Desde una perspectiva ética, Hans Jonas, plantea que la falta de precaución tecnológica puede derivar en daños irreversibles. Entre tanto, pare este lineamiento, la UNESCO (2022) y el CICR (2023), propone establecer centros de ciberdefensa, auditorías digitales continuas y normativas de seguridad a partir del diseño.

Lineamiento 8: Ciberseguridad Integral y Resiliencia Tecnológica en Operaciones Militares.

Bajo el contexto de guerra híbrida y digitalización creciente, la ciberseguridad y la resiliencia tecnológica son esenciales para garantizar la continuidad y legitimidad de las operaciones militares. Por ello, este lineamiento establece que las Fuerzas Militares, deben implementar estructuras de ciberdefensa que integren prevención, detección, respuesta y recuperación ante ciberataques, especialmente en infraestructuras críticas como redes de mando y control, satélites, sistemas autónomos y bases de datos.

Como advierte Lindsay (2019), los ataques a sistemas de Comando Nuclear, Control y Comunicaciones (NC3), pueden comprometer la estabilidad estratégica. De igual forma, la OTAN (2023), señala que la resiliencia digital es clave para la disuasión frente a amenazas híbridas. En el caso colombiano, esta capacidad debe extenderse a escenarios de ciberterrorismo y crimen transnacional.

En este sentido, desde una perspectiva ética, Hans Jonas, plantea que se deben anticipar los daños irreversibles derivados de tecnologías de alto riesgo. Además, la UNESCO (2022) y el CICR (2023), recomiendan normativas que prioricen la seguridad digital como garantía de los DD.HH. Su implementación requiere equipos de respuesta rápida, redundancia tecnológica y simulaciones periódicas de ciberataques.

Uso Legítimo y Proporcional de la Tecnología:

Lineamiento 9. Regulación del Uso Dual de las Tecnologías Emergentes

Las tecnologías emergentes, como la inteligencia artificial, el Blockchain o el IoT, presentan una naturaleza de uso dual, es decir, pueden ser aplicadas tanto en contextos civiles como militares. Esta dualidad, aunque útil, plantea importantes desafíos éticos y jurídicos, especialmente cuando facilita la militarización de infraestructuras civiles.

En consecuencia, este lineamiento propone establecer un marco regulatorio claro que distinga los ámbitos de aplicación y garantice que bienes civiles no sean convertidos en objetivos militares. Esta propuesta se fundamenta en el principio de distinción del DIH, recogido en el Protocolo Adicional I a los Convenios de Ginebra (CICR, 2023), el cual exige diferenciar entre objetivos militares y bienes civiles en todo conflicto armado.

Además, desde una perspectiva filosófica, Ziauddin Sardar (2010), advierte que vivimos en tiempos posnormales, donde las fronteras tecnológicas son difusas. Por ello, se requiere un control más estricto y preventivo sobre sus usos.

Finalmente, implementar este lineamiento en las Fuerzas Militares, implica diseñar protocolos de validación dual que aseguren la legitimidad del uso tecnológico, respeten el DIH y protejan a la población civil.

Lineamiento 10: Principio de Proporcionalidad y Precaución Tecnológica en el Empleo de Tecnologías Militares Emergentes.

El principio de proporcionalidad, consagrado en el Derecho Internacional Humanitario (DIH), establece que el daño incidental a civiles no debe ser excesivo en relación con la ventaja militar concreta y directa prevista (Protocolo Adicional I, 1977). En consecuencia, este lineamiento exige que toda tecnología militar emergente (TME), sea sometida a una evaluación ética y operacional rigurosa antes de su despliegue.

Asimismo, tecnologías como la inteligencia artificial autónoma, la biotecnología aplicada al combate o la ciberseguridad ofensiva deben ser analizadas previamente en cuanto a sus riesgos y beneficios, con el fin de evitar consecuencias desproporcionadas o irreversibles. En este contexto, Hans Jonas (1984) propone el principio de precaución como guía ética, advirtiendo que las innovaciones con alto poder destructivo deben ser anticipadas y controladas antes de su uso.

Además, organismos como la UNESCO (2022) y el CICR (2023), coinciden en que la precaución tecnológica no limita el desarrollo, sino que garantiza su aplicación ética y legal. Por tanto, aplicar este lineamiento en Colombia, implica incorporar evaluaciones de proporcionalidad tecnológica en la doctrina operacional y en los procesos de adquisición, fortaleciendo la legitimidad institucional ante la comunidad nacional e internacional.

En la siguiente tabla se reflejan lineamientos éticos propuestos para las FF.MM:

Tabla 4.

Propuesta de lineamientos éticos y normativos para la integración de tecnologías militares emergentes

N°	Lineamiento	Descripción	Base Doctrinal
1	**Prohibición de delegación ética a algoritmos opacos**	Prohíbe el uso de IA opaca en decisiones críticas militares.	Opacidad algorítmica (Pasquale, Burrell); Principio de explicabilidad (Floridi & Cowls).
2	**Control humano significativo y supervisión operacional**	Exige supervisión humana directa en sistemas autónomos y semiautónomos.	Meaningful Human Control (ONU, CICR); Teoría de la guerra justa (Walzer).
3	**Gobernanza y transparencia algorítmica**	Establece trazabilidad y explicabilidad en sistemas algorítmicos militares.	Opacidad algorítmica (Pasquale, Burrell); Principio de explicabilidad (Floridi & Cowls).
4	**Transparencia, auditoría y trazabilidad**	Requiere registros verificables y auditorías en todo el ciclo tecnológico.	Imperativo categórico (Kant); Principio de responsabilidad (Hans Jonas).
5	**Gobernanza ética y supervisión civil-militar**	Propone un consejo nacional para supervisar la adopción de TME.	Teoría de la guerra justa (Walzer); Ética de la responsabilidad (Hans Jonas).
6	**Supervisión y evaluación continua**	Establece un comité interdisciplinario para monitorear el uso de TME.	Ética de la responsabilidad (Hans Jonas); Gobernanza tecnológica internacional (UNESCO/ONU).
7	**Protección de datos y soberanía digital**	Exige infraestructura digital bajo control nacional y protección de datos.	Soberanía digital; Principio de precaución tecnológica.
8	**Ciberseguridad integral y resiliencia tecnológica**	Propone estructuras de defensa digital y respuesta ante ciberataques.	Ética de la precaución (Hans Jonas); Doctrina de ciberdefensa (OTAN).
9	**Regulación del uso dual de tecnologías**	Establece límites entre Duales de TME.	Principio de responsabilidad (Hans Jonas); DIH (Convenios de Ginebra).
10	**Proporcionalidad y precaución tecnológica**	Exige evaluación previa de riesgos antes del uso de TME.	Principio de proporcionalidad (DIH); Ética de la precaución (Hans Jonas).

Nota: Elaboración propia

La tabla anterior muestra las principales rutas para una integración ética de las tecnologías emergentes, asociando un marco teórico con medidas prácticas y normativas. En suma, de lo descrito anteriormente, el enfoque de la teoría de la guerra justa actúa como garante de la compatibilidad legal y moral de las tecnologías en contextos bélicos, mientras que el principio de responsabilidad de Jonas nos obliga a considerar la sostenibilidad moral de estas tecnologías a largo plazo. Por último, Sardar nos recuerda que vivimos en tiempos de incertidumbre, lo que hace indispensable una gobernanza tecnológica flexible y participativa.

Conclusiones

La implementación de tecnologías emergentes en las Fuerzas Militares de Colombia, tiene el potencial de transformar significativamente la eficiencia y seguridad operativa, aportando mejoras en diversos ámbitos estratégicos y tácticos. Sin embargo, esta innovación plantea desafíos significativos, que requieren lineamientos éticos previos a su aplicación, con el fin de proteger los DD.HH y respetar el DIH, legitimando el uso de la fuerza en el cumplimiento a la misión establecida en el artículo 216 de la Constitución Política de Colombia.

La investigación demuestra que la implementación tecnológica debe estar subordinada al juicio ético y al control humano significativo, ya que este principio como lo indica CICR (2023), debe ser un eje doctrinal ineludible en la adopción de sistemas autónomos, garantizando que la tecnología complemente mas no sustituya el juicio moral en desarrollo de operaciones militares

La incorporación de tecnologías emergentes en las FF.MM, deben estar subordinadas al respeto irrestricto por la dignidad humana. Tal como lo plantea Hans Jonas (De Siqueira, 2001), la tecnificación del conflicto no puede despersonalizar al ser humano ni reducirlo a una variable algorítmica. En este sentido, las Fuerzas Militares están llamadas a integrar soluciones tecnológicas que preserven la vida, mitiguen el sufrimiento y fortalezcan su legitimidad jurídica y ética ante los marcos normativos nacionales e internacionales, consolidando así su rol institucional en defensa de los derechos fundamentales.

La implementación de I.A en operaciones militares debe estar sujeta a estrictos estándares de transparencia algorítmica y trazabilidad, elementos esenciales para garantizar la rendición de cuentas. La opacidad tecnológica vulnera el principio de legalidad y dificulta la atribución de responsabilidades ante posibles violaciones a los derechos humanos. Por ello, resulta imperativo establecer mecanismos robustos de registro, auditoría y verificación en toda la cadena operativa, fortaleciendo así la legitimidad institucional y el control jurídico.

La armonización entre innovación tecnológica y marcos normativos es imperativa para garantizar una gobernanza militar responsable en el uso de I.A. El CONPES 4144 de 2025, establece directrices éticas y de gobernanza para Colombia, promoviendo el desarrollo de capacidades institucionales y mecanismos de verificación, El Reglamento (UE) 2024/1689 refuerza la necesidad de una IA confiable, centrada en el ser humano y alineada con los derechos fundamentales, y complementariamente, la recomendación de la UNESCO (2021), subraya la importancia de principios éticos universales para evitar sesgos, exclusión y vulneraciones a la dignidad humana.

Las tecnologías de uso dual plantean desafíos críticos para el DIH, especialmente cuando sistemas civiles como drones o redes satelitales son empleados con fines bélicos. Según el CICR, esta práctica puede comprometer la distinción entre objetivos militares y bienes civiles, generando riesgos humanitarios significativos. Por tal motivo, las Fuerzas Militares deben implementar protocolos éticos y jurídicos que regulen su aplicación diferenciada, conforme a principios de distinción, proporcionalidad y precaución, minimizando impactos colaterales y fortaleciendo la legitimidad operacional.

La investigación permite identificar que la interoperabilidad tecnológica debe estar respaldada por una sólida soberanía digital y una arquitectura robusta de ciberseguridad. experiencias como el conflicto de Ucrania, ha evidenciado que la superioridad digital es clave para preservar la autonomía estratégica y proteger infraestructuras críticas frente a actores externos. En consecuencia, la OTAN ha adoptado principios de uso responsable de Tecnologías Emergentes, promoviendo la protección de datos y la resiliencia operativa como pilares de su estrategia digital. Asimismo, expertos en ciberseguridad advierten que la I.A, sin regulación ética, puede comprometer la privacidad y amplificar amenazas digitales, lo que exige una gobernanza rigurosa y preventiva

El análisis demuestra que la ética institucional debe integrarse desde la planificación, diseño, compra y evaluación de sistemas militares. En este sentido, se propone conformar comités éticos interinstitucionales con participación civil, jurídica, técnica y operativa, que garanticen el uso responsable de tecnologías emergentes, fortaleciendo la legitimidad y la rendición de cuentas en contextos de defensa.

Finalmente, esta investigación reafirma que la legitimidad del uso de tecnologías emergentes en las Fuerzas Militares, depende de su alineación con principios éticos como: el respeto a la dignidad humana, control humano significativo, transparencia algorítmica y rendición de cuentas. Estos criterios no solo garantizan el cumplimiento del DIH y la protección de los DD.HH, sino que posicionan a las FF.MM. como una fuerza moderna, responsable y jurídicamente coherente en escenarios complejos, reafirmando así, que la ética, no limita la tecnología, sino constituye la condición esencial para su aplicación justa y legal en el conflicto armado.

Referencias

Almache Barreiro, J. C., y Albert Márquez, J. (2023). Implicaciones éticas de la IA y su potencial impacto en el derecho internacional. Revista San Gregorio, 1(54), 209–231. https://doi.org/10.36097/rsan.v1i54.2458

Almache Barreiro, J. C., y Albert Márquez, J. J. (2024). Imprevisibilidad normativa en el Derecho Internacional respecto a los sistemas de armas autónomas letales. Revista Logos Ciencia & Tecnología. http://www.scielo.org.co/pdf/logos/v16n1/2422-4200-logos-16-01-16.pdf

Anderson, S. L. (2008). Asimov's "Three Laws of Robotics" and machine metaethics. AI & Soc, 22, 477–493. https://doi.org/10.1007/s00146-007-0094-5. https://cdn.aaai.org/Symposia/Fall/2005/FS-05-06/FS05-06-002.pdf.

Ashima J, (2023). Technological Advances and Evolution of Biowarfare: A Threat to Public Health and Security. In International Conference Health, Social Science & Engineering, KnE Life Sciences, pages 401–416. DOI: https://doi.org/10.18502/kss.v8i14.13853. https://knepublishing.com/index.php/KnE-Social/article/download/13853/22373.

Asaro, P. (2012). On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. International Review of the Red Cross, https://doi.org/10.1017/S1816383112000768. https://international-review.icrc.org/sites/default/files/irrc-886-asaro.pdf.

Bayan, H., y Fayyad, M. (2024). The Ethics of AI: Navigating the Moral Dilemmas of Artificial Intelligence. https://doi.org/10.36571/ajsp661.

Bojor, L., Petrache, T., y Cristescu, C. (2024). Emerging Technologies in Conflict: The Impact of Starlink in the Russia – Ukraine War. Land Forces Academy Review, 29(2), 185–194. https://doi.org/10.2478/raft-2024-0020. https://www.armyacademy.ro/reviste/rev2_2024/Bojor_Petrache_Cristescu_RAFT_2_2024.pdf.

Braun, V., y Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. DOI:10.1191/1478088706qp063oa. https://share.google/8xjs8YliHZv6dw2Qs.

Burrell, J. (2016). How the machine 'thinks': Understanding Opacity In Machine Learning Algorithms. Big data & society. https://doi.org/10.1177/2053951715622512. https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512.

Clement, S. (2024). NATO and Artificial Intelligence: Navigating the challenges and opportunities. Preliminary Draft Special Report. https://zero5g.com/wp-content/uploads/2025/07/download-file.pdf.

Church, K. W., & Chandrasekar, R. (2023). Emerging trends: Risks 3.0 and proliferation of spyware to 50,000 cell phones. Natural Language Engineering, 29(3), 824–841. doi:10.1017/S1351324923000141. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/E493E2949551DB0D1CCB3C873E30C143/S1351324923000141a.pdf/emerging-trends-risks-30-and-proliferation-of-spyware-to-50000-cell-phones.pdf.

Crootof, R. (2016). A meaningful floor for meaningful human control. Temple International & Comparative Law Journal, 30(1), 53–65. https://sites.temple.edu/ticlj/files/2017/02/30.1.Crootof-TICLJ.pdf

Cools, K y Maathuis, C. (2024). Trust or Bust: Ensuring Trustworthiness in Autonomous Weapon Systems. 182-189. https://doi.org/10.48550/arXiv.2410.10284

Coman, M & Kifor, C. (2024). Las Tecnologías Emergentes y Disruptivas: Un Enfoque Basado en el Riesgo. https://doi.org/10.2478/kbo-2024-0084

De Siqueira, J. (2001). El Principio de Responsabilidad de Hans Jonas. Acta Bioethica, 7(2), 277–285. https://dx.doi.org/10.4067/S1726-569X2001000200009

Departamento Nacional de Planeación. (2025). CONPES 4144: Política Nacional para la Inteligencia Artificial y Tecnologías Emergentes. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

Docherty, B. (2020). The Need for and Elements of a New Treaty on Fully Autonomous Weapons. Human Rights Watch and the Harvard Law School International Human Rights Clinic.https://www.hrw.org/sites/default/files/media_2020/06/202006arms_rio_autonomous_weapons_systems_2.pdf

Riley S.E, Ryan P. B, Shayne L y Kanaka R, (2024). Position: AI-powered autonomous weapons risk geopolitical instability and threaten AI research. Article 1851, 45508–45524. https://doi.org/10.48550/arXiv.2405.01859

Favaro, M., y Williams, H. (2023). False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation. Journal for Peace and Nuclear Disarmament, 6(1), 28–46. https://doi.org/10.1080/25751654.2023.2219437

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1

Franke, U. (2021). Artificial Intelligence diplomacy: Artificial Intelligence governance as a new European Union external policy tool. European Parliament's Special Committee on Artificial Intelligence in a Digital Age. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf

Gantiva, C. (2024). Ética militar e inteligencia artificial: reflexiones para Colombia desde el contexto global actual. [Artículo de Maestría, Escuela Superior de Guerra "Rafael Reyes Prieto"]. Volumen II. Ética militar y nuevas formas de guerra. Repositorio institucional ESDEG. https://doi.org/10.21830/9789585377134.05

Gómez Torre, R. A. (2025). Reglamento (UE) 2024/1689, del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos: (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) [DOUE-L-2024-81079]. *AIS: Ars Iuris Salmanticensis*, *12*(2), 112–114. Recuperado a partir de https://revistas.usal.es/cuatro/index.php/ais/article/view/32243/30154

Groen, A. (2013). Introduction to the Field of Emerging Technologies. Creativity and Innovation Management, 22(2), 91–96. https://doi.org/10.1111/caim.12019

Horowitz, M. (2018). Artificial intelligence, international competition, and the balance of power. Texas National Security Review, 1(3), 37–57. https://repositories.lib.utexas.edu/server/api/core/bitstreams/74307125-fc5e-4706-86fc-1b035e4bbfbc/content

Huelss, H. (2025). Transcending the fog of war? US military 'AI', vision, and the emergent post-scopic regime. European Journal of International Security (2024), 1–21. https://doi.org/10.1017/eis.2024.21. En línea: https://www.scilit.com/publications/f7d03b0c198b0d775f95438e200fae0f

International Human Rights Clinic IHRC, (2020). Cuidado con el vacío: La falta de responsabilidad con respecto a los robots asesinos. ISBN: 978-1-6231-38059.

https://www.hrw.org/es/report/2015/04/09/cuidado-con-el-vacio/la-falta-de-responsabilidad-con-respecto-los-robots-asesinos.

Human Rights Watch y Harvard Law School International Human Rights Clinic. (2012). Losing humanity: The case against killer robots. Human Rights Watch. ISBN: 1-56432-964-X. https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots.

Human Rights Watch & Human Rights Clinic. (2020). Construyendo el caso. Los peligros de los robots asesinos y la necesidad de una prohibición Preventiva. ISBN: 978-1-6231-38042. https://www.hrw.org/sites/default/files/report_pdf/arms1216sp_web.pdf.

Islam, M. y Wasi, A. (2022). Balancing power and ethics: A Framework for Addressing Human Rights Concerns in Military AI.. https://openreview.net/pdf?id=KjBQumXLqw

Krelina, M. Quantum technology for military applications. EPJ Quantum Technol. 8, 24 (2021). https://doi.org/10.1140/epjqt/s40507-021-00113-y

Martínez, J. (2024). Military technology companies and human rights Accountability. https://doi.org/10.31219/osf.io/5dxau

Halaweh, Mohanad. (2013). Emerging Technology: What is it. Journal of technology management & innovation. 8. 108-115. DOI: 10.4067/S0718-27242013000400010

Maxwell M. (2013). Enhanced Warfighters: Risk, Ethics, and Policy. Case Research Paper Series in Legal Studies Working Paper 2013-2. https://case.edu/law/sites/default/files/2021-01/mehlman%20CLE%202-2021.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2020). Guía con lineamientos generales para el uso de tecnologías emergentes https://gobiernodigital.mintic.gov.co/692/articles-160829_Guia_Tecnologias_Emergentes.pdf

Migliore, J. (2005). Michael Walzer y el problema de la guerra justa. ISSN-e 1850-003X, Nº. 16, 13–46. https://repositorio.uca.edu.ar/bitstream/123456789/9820/1/michael-walzer-problema-guerra.pdf

Ministerio de Defensa Nacional. (2021). Plan Estratégico Militar de Transformación PEMT 2042. República de Colombia. Planeación Estratégica y Transformación. https://drive.google.com/file/d/1veJV4c8q4bpSKSrHi9ljV6fFuIk9eAk2/view

Muñoz, W., y Díaz, M. (2021). Los riesgos de las Armas Autónomas: Una Perspectiva Interseccional Latinoamericana. Red Seguridad Humana en América Latina y el Caribe SEHLAC. https://www.stopkillerrobots.org/wp-content/uploads/2020/09/Los-riesgos-de-las-armas-autonomas-una-perspec-min.pdf

Nuno S. (2024). The Artificial Intelligence Act: critical overview. https://www.nsousaesilva.pt/images/_Data/Publicacoes-outrosmateriais/EN_NSS_AI_Act.pdf

Ortiz Arellano, E., & Bustamante García, V. H. (2024). La tecnología y su uso en la guerra: desafío para la seguridad internacional. Ciberespacio, Tecnología e Innovación, 3(5), 89-104.

https://doi.org/10.25062/2955-0270.4853

Pagallo, U. (2017). The laws of robots: Crimes, contracts, and torts. Springer Dordrecht. ISBN 978-94-007-6563-4. eBook ISBN: 978-94-007-6564-1. DOI: https://doi.org/10.1007/978-94-007-6564-1

Pasquale, F. (2015). The Black Box Society, the Secret Algorithms That Control Money and Information. Cambridge, MA. Harvard University Press. https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf. DOI: https://doi.org/10.4159/harvard.9780674736061

Perišić, P., y Tomljenović, M. (2024). Legal permissibility of autonomous weapon systems, with specific reference to the principles of international humanitarian law. 61(4), 531–555. https://doi.org/10.31141/zrpfs.2024.61.154.531. En línea: https://hrcak.srce.hr/file/469075

Pérez-Ugena, M. (2024). La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales. Estudios de Deusto, 72(1), 307–337. https://doi.org/10.18543/ed.3108

Reichberg, G. M., y Syse, H. (2021). Applying AI on the Battlefield: The Ethical Debates. In Robotics, AI, and Humanity: Science, Ethics, and Policy (pp. 147–159). Springer. https://www.researchgate.net/publication/349268308_Applying_AI_on_the_Battlefield_The_Ethical_Debates

Rubiano E. (2022). Propuesta de un modelo de inteligencia de amenazas cibernéticas para el fortalecimiento de las capacidades de ciberinteligencia de la Fuerza Aérea Colombiana. Escuela Superior de Guerra "General Rafael Reyes Prieto". https://hdl.handle.net/20.500.14205/11154

Sampieri, Fernández y Baptista. (2014). Metodología de la investigación sexta edición. https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Sardar, Z. (2010). Emerging Epistemologies: The Changing Fabric Of Knowledge In Postnormal Times. International Institute of Islamic Thought. https://iiit.org/wp-content/uploads/Emerging-Epistemologies.pdf

Scharre, P. (2018). Army of none: Autonomous Weapons and the future of war. W. W. Norton & Company. LCCN 2017053908. ISBN 9780393608984. Ebook: ISBN 978-0-393-60899-1

Segura, Cabarcas, y Hernández. (2021). Aplicación de tecnologías de realidad aumentada en procesos logísticos militares. Brújula Semilleros de Investigación, 9(18), 44–55. https://doi.org/10.21830/23460628.95

State Council of China. (2024). Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars). CSET. https://cset.georgetown.edu/wp-content/uploads/t0592_china_ai_law_draft_EN.pdf

Suleyman, M. (2025). La Ola Que Viene: Tecnología, Poder y el gran dilema del siglo XXI. Penguin Random House Grupo Editorial. ISBN: 978-628-7669-77-2

Simmons et al. (2024). AI-Powered Autonomous Weapons Risk Geopolitical Instability and Threaten AI Research. Harvard University. arXiv:2405.01859v2. En: https://openreview.net/pdf?id=XHL0tZ9ena

Sparrow, Robert. (2023). Technology ethics assessment: Politicising the 'Socratic approach'. Business Ethics, the Environment & Responsibility. 32. 454-466. DOI: 10.1111/beer.12518. En linea: https://onlinelibrary.wiley.com/doi/epdf/10.1111/beer.12518

Tsamados, A., Floridi, L., y Taddeo, M. (2024). Human control of AI systems: from supervision to teaming. AI and Ethics. https://doi.org/10.1007/s43681-024-00489-4

Turing, A. M. (1950). Computing Machinery and Intelligence. Mind, 49, 433–460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

UNESCO. (2022). Recomendación sobre la ética de la inteligencia artificial. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa.

Vigevano, M. R. (2021). Inteligencia artificial aplicable a los conflictos armados: límites jurídicos y éticos. Arbor, 197(800). https://arbor.revistas.csic.es/index.php/arbor/article/view/2417/3639.

Viveros Álvarez, J. S. (2021). Sistemas de armas autónomas: El dilema de la rendición de cuentas. Instituto de Investigaciones Jurídicas, UNAM. https://scm.oas.org/pdfs/2023/Armasautonomas.pdf

Watling, J. (2023). Emerging Technologies: From Concept to Capability. En M Weissmann & N. Nilsson (Eds.), Advanced Land Warfare. Oxford University Press. https://academic.oup.com/book/45784/chapter/400599751

Wright N. (2022). DARPA's Magic Ingredient Speed Can Help Build a Fleet of Allied "DARPAs". Commentary, Center for Strategic and International Studies. 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/220127_Wright_DARPAs_Magic_Ingredient.pdf