Inteligencia Artificial y Blockchain para el fortalecimiento de los Derechos Humanos en la Armada Nacional de Colombia.

Mayor de I.M. Javier Andrés Patiño Velilla

Artículo para optar al título profesional:

Magister en Derechos Humanos y DICA.

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

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor de I.M. Javier Andrés Patiño Velilla
Identificación	**:**	80088329
Programa académico	**:**	Maestría en Derechos Humanos y DICA.
Tutor metodológico	**:**	Mauricio Torres
Tutor temático	**:**	Leonardo Miguel Hernández, PhD, No. teléfono. 3158346634
Fecha de entrega	**:**	26 de agosto de 2025
Extensión	**:**	7975 palabras

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

Inteligencia Artificial y Blockchain para el fortalecimiento de los Derechos Humanos en la Armada Nacional de Colombia.

Enhancing Human Rights in the Colombian Navy through Artificial Intelligence and Blockchain.

Javier Andrés Patiño Velilla [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente artículo analiza el impacto del uso de la Inteligencia Artificial (IA) y la tecnología Blockchain en las operaciones militares de la Armada Nacional de Colombia —¡una transformación que no puede abordarse únicamente desde la técnica!—, partiendo de una hipótesis central: si estas tecnologías no se implementan con mecanismos institucionales adecuados de control ético y legal, podrían generar vulneraciones al Derecho Internacional Humanitario (DIH) y a los Derechos Humanos. La investigación se desarrolla bajo una metodología cualitativa —de tipo exploratorio-descriptivo—, con enfoque hermenéutico-jurídico, utilizando análisis documental y estudio comparado. Se examinan precedentes internacionales (Estados Unidos, Estonia e Israel); se identifican los desafíos normativos actuales; y se propone un modelo práctico aplicable al contexto colombiano. Todo ello… con el fin de garantizar —y no solo prometer— transparencia, trazabilidad y responsabilidad en el uso militar de tecnologías emergentes.

Palabras clave: Blockchain; Derechos humanos; Estado; Inteligencia artificial; Planeamiento militar; Transparencia.

Abstract: This article analyzes the impact of Artificial Intelligence (AI) and Blockchain technology on military operations within the Colombian Navy. It is based on the central hypothesis that, if these technologies are not implemented alongside institutional mechanisms for ethical and legal oversight, they may lead to violations of International Humanitarian Law (IHL) and Human Rights. The research employs a qualitative methodology, exploratory-descriptive in nature, with a hermeneutic-legal approach that combines documentary analysis and comparative case studies. It examines international precedents (United States, Estonia, and Israel), identifies current normative challenges, and proposes

[1] Mayor de Infantería de Marina, Armada Nacional de Colombia. Candidato a magíster en Derechos Humanos y DICA., Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Política y Estrategia Marítima "Escuela Naval Almirante Padilla", Colombia. Profesional en Administración de Empresas, Universidad "Politécnico Grancolombiano", Colombia. https://orcid.org/0009-0006-7859-5384 Contacto: javier.patino@esdeg.edu.co.

a practical model tailored to the Colombian context. The objective is to ensure transparency, traceability, and accountability in the military use of emerging technologies through concrete institutional mechanisms rather than general declarations.

Keywords: Blockchain; Human rights; State; Artificial intelligence; Military planning; Transparency.

Introducción

En el contexto de transformación tecnológica que enfrentan las fuerzas armadas del siglo XXI, la incorporación de tecnologías emergentes como la Inteligencia Artificial (IA) y la tecnología Blockchain traza importantes retos y oportunidades en la mejora de la eficiencia, la seguridad, la toma de decisiones y trazabilidad en los procesos institucionales. Sin embargo, este desarrollo presuroso de estas tecnologías también plantea complejos desafíos jurídicos y éticos en la protección de los Derechos Humanos en el ámbito militar cuando estas tecnologías emergentes se integran en contextos tan sensibles como el uso de la fuerza y la conducción y el planeamiento de operaciones militares.

En la actualidad la Armada Nacional de Colombia, en su evolución hacia la modernización y el fortalecimiento doctrinal y operativo, ha comenzado a explorar la potencialidad de las tecnologías emergentes. En el caso de la IA, por ejemplo, ha denotado un potencial exponencial para el manejo y análisis de grandes volúmenes de datos, la capacidad de interrelacionar patrones en tiempo real, automatización de procesos operativos y asistir en la toma de decisiones estratégicas en escenarios con complejidad alta. Sin embargo, esta prometedora integración tecnológica no está exenta de riesgos y presenta serios desafíos éticos y jurídicos interrelacionados con la protección efectiva y real de los Derechos Humanos, especialmente bajo el marco del Derecho Internacional Humanitario (DIH) fundamentalmente con la distinción entre combatientes y no combatientes, uso de la fuerza, proporcionalidad y necesidad militar.

Estos riesgos ya han podido ser identificados por diferentes instituciones y organismos en el contexto internacional, como el Comité Internacional de la Cruz Roja (CICR) y el Consejo de Derechos Humanos de las Naciones Unidas, las cuales han advertido que la supervisión directa humana es esencial e imperiosa en la toma de decisiones críticas de sistemas semiautónomos o autónomos en el ámbito militar, con el fin de evitar condiciones que puedan surgir donde el juicio ético humano es indispensable. Actualmente, países como Estados Unidos y la Unión Europea están abordando este desafío con el desarrollo de principios éticos específicos al uso de la IA en las operaciones militares, empleando como principios la transparencia, la responsabilidad y la supervisión humana directa sobre las decisiones estratégicas, para garantizar la trazabilidad de sus decisiones, asegurándose que respondan bajo marcos normativos compatibles con estándares internacionales basados en Derechos Humanos *(CICR, 2021; ONU, 2019).*

Por el contrario, países como Rusia y China se encuentran en el ojo del huracán internacional debido a la escasa supervisión y transparencia en el uso y aplicación de sistemas de IA en sus operaciones militares, potencializando exponencialmente el riesgo de violaciones a los derechos humanos y al DIH. Estudios como los realizados se enfocan en priorizar la necesidad de mantener una transparencia efectiva en la implementación y en el diseño de algoritmos militares para detectar y prevenir vulneraciones éticas y jurídicas (Sharkey, 2020).

Por su parte, desde hace algunos años paralelamente se ha logrado apreciar como la tecnología Blockchain se ha convertido en una herramienta promisoria, disruptiva e

inmutable para abordar los desafíos actuales con la IA, está garantiza la transparencia institucional de los registros y facilita las auditoria en tiempo real en las decisiones críticas. La implementación de la tecnología Blockchain en los procesos de defensa, administrativos y logísticos en países como Canadá, Australia y Noruega, ha evidenciado su gran valor para reducir los índices de corrupción, rendición de cuentas y reducir los márgenes de discrecionalidad al interior de las fuerzas militares como frente a la sociedad civil. Estos casos de combinación con la IA se encuentran en estudios en instituciones tan prestigiosas como el MIT (Instituto Tecnológico de Masschusetts) Media Lab y la Universidad de Cambridge, las cuales han planteado que la integración de Blockchain e IA en contextos militares podrían ser importantes para garantizar decisiones auditables, trasparentes y resistentes a manipulaciones indebidas en escenarios operacionales complejos. Esto debido a que la tecnología Blockchain garantiza una inmutabilidad en el registro de datos. *(Pilkington, 2016; Tapscott & Tapscott, 2016).*

Por otro lado, en estudios recientes se ha observado que la implementación combinada de IA y Blockchain ha generado una mejora demostrativa en la gestión de información sensible disponible y la transparencia institucional, menguando conflictos internos y externos. Un claro ejemplo de esto es el uso de contratos inteligentes en operaciones militares, que responden al seguimiento y supervisión automatizada de acciones sensibles, minimizando riesgos jurídicos y éticos *(MIT Media Lab, 2020; Forster, 2020).*

Aunado a esto, desde la perspectiva operativa, la IA podría utilizarse para salvaguardar la ciberseguridad, la vigilancia marítima y tener un control en la prevención de delitos ambientales en operaciones navales. En la actualidad, Noruega posee un sistema de monitoreo marítimo basado en IA, el cual ha demostrado la reducción de incidentes relacionados con la pesca ilegal y el tráfico de sustancias ilícitas (Narcotráfico), lo que demuestra la importancia de la implementación y practicidad de sistemas basados en la IA. (Norwegian Ministry of Defence, 2020; MIT Media Lab, 2020).

Por otra parte, el uso de tecnología Blockchain en operaciones militares en Australia ha evidenciado la transparencia de los procesos críticos y operacionales, generando confianza institucional interna y mejora en la percepción pública. La aplicación de esta tecnología ha demostrado el aseguramiento de registros transparentes e inviolables que pueden auditarse en tiempo real por autoridades civiles si fuere el caso y militares, aumentando la confianza institucional y la legalidad ante la población civil.

En este sentido, la presente investigación presenta un análisis crítico sobre el uso de la IA en las operaciones militares en la Armada Nacional de Colombia, visibilizando los desafíos éticos y jurídicos de su aplicación y proponiendo, además, la fusión con la tecnología Blockchain como garantía del amparo de los Derechos Humanos. Bajo un enfoque hermeneútico-jurídico, enfocándose en una metodología cualitativa tipo exploratorio-descriptivo, se analizarán los beneficios y los riesgos asociados a la fusión de estas tecnologías, enfatizando la necesidad a priori de establecer en la Armada Nacional de Colombia los mecanismos normativos y técnicos que aseguren un uso responsable, ético y trasparente de estas tecnologías. *(UNESCO, 2021; Comisión Europea, 2021).*

La propuesta que realizó Niklas Luhmann en su "Teoría de Sistemas" será esencial como marco conceptual para comprender, la Fuerzas Militares como un sistema social autopoiético, capaz de autorregularse y adaptarse rápidamente a cambios estructurales bajo la incorporación de subsistemas especializados. Bajo este acercamiento, podremos visualizar como la fusión de la IA y la tecnología Blockchain, puede generar no solo un salto operativo, sino también un fortalecimiento institucional en materia legal, en legitimidad y en protección en materia de los Derechos Humanos en operaciones militares.

En conclusión, el presente artículo busca realizar la formulación de una propuesta aplicable y práctica, que permita a la Armada Nacional de Colombia integrar tecnologías que permitan controlar y de una forma efectiva la combinación de IA y Blockchain, con el propósito de masificar la doctrina operacional con los más altos estándares del Derecho Internacional Humanitario y los Derechos Humanos, respondiendo así al imperativo ético y jurídico que exige la sociedad contemporánea en los escenarios de seguridad y defensa.

Metodología

Este artículo adopta un enfoque **cualitativo de tipo exploratorio-descriptivo**, fundamentado en el método **hermenéutico-jurídico**, con el fin de examinar de manera profunda los desafíos éticos y legales que plantea la implementación de tecnologías emergentes —en particular, la **Inteligencia Artificial (IA)** y la **tecnología Blockchain**— en

el planeamiento y ejecución de operaciones militares por parte de la Armada Nacional de Colombia.

Desde esta perspectiva, el análisis busca construir un **modelo normativo y técnico aplicable**, orientado a la **protección preventiva e integral** de los Derechos Humanos y del Derecho Internacional Humanitario (DIH), tanto en el contexto operacional como administrativo. La metodología está estructurada en tres ejes centrales: revisión normativa, análisis doctrinal y estudio comparado.

En primer lugar, se realizó un **análisis documental y normativo**, mediante el estudio de instrumentos internacionales vinculantes —como los Convenios de Ginebra y el Protocolo Adicional II—, así como normas nacionales como la **Ley 1862 de 2017**, el Código Penal Militar y sentencias relevantes de la **Corte Constitucional de Colombia** (por ejemplo, T-092/2019, T-401/2020, T-233/2022 y C-239/2012). Este análisis permite identificar los principios jurídicos que deben orientar el uso de tecnologías emergentes en escenarios de conflicto armado.

En segundo lugar, se incorporó una **revisión bibliográfica especializada**, que incluye trabajos sobre la aplicación de la IA en contextos militares (Asaro, 2008; Sharkey, 2010; Vigevano, 2021), estudios sobre integridad institucional mediante Blockchain (Palomo Zurdo, 2018; MIT Media Lab, 2020; Tapscott & Tapscott, 2016), y análisis doctrinal sobre la responsabilidad del mando (ONU, 2018; Pulido, 2023).

El tercer eje metodológico se estructura como un **estudio de caso comparado**, en el cual se analizan experiencias internacionales relevantes —como Estados Unidos, Estonia e Israel— donde ya se han implementado sistemas que integran IA y Blockchain en funciones de defensa y seguridad. La selección de estos casos se basa en criterios de:

1. Relevancia institucional.
2. Nivel de integración tecnológica.
3. Impacto en mecanismos de control ético y jurídico.

Finalmente, se toma como base conceptual la **Teoría de Sistemas** de Niklas Luhmann (1996), entendiendo a las Fuerzas Militares como un sistema social **autopoiético**, capaz de generar subsistemas especializados —por ejemplo, en ética digital y control institucional— para autorregular la implementación de tecnologías disruptivas sin perder legitimidad ni vulnerar derechos fundamentales (Carvajal, 2019).

Esta metodología permite articular de forma coherente el análisis jurídico, doctrinal, técnico y estratégico, con el propósito de generar una propuesta institucional **aplicable y verificable** para el uso ético de la IA y el blindaje legal mediante Blockchain, dentro del marco constitucional y del DIH colombiano.

Desafíos jurídicos y éticos derivados del uso de IA en operaciones militares de la Armada Nacional de Colombia

Inteligencia Artificial en el ámbito militar: eficiencia versus riesgo

El uso de la Inteligencia Artificial (IA) en la Fuerzas Militares del siglo XXI representa una sublevación tecnológica que acelera y mejora los procesos substancialmente en la toma de decisiones, análisis de inteligencia, vigilancia estratégica y conducción operacional. En el caso concreto de la Armada Nacional de Colombia, esta combinación ofrecería ventajas fundamentales en la conducción de operaciones navales, tales como las de vigilancia marítima, la ciberdefensa, el pronóstico de amenazas reales y la programación táctica automatizada (Pareja Pérez, 2023; CICR, 2021; Georgetown University, 2021).

Sin embargo, este potencial tecnológico podría conllevar riesgos jurídicos y éticos significativos, principalmente cuando las decisiones se transponen desde operadores humanos hacia algoritmos con autonomía parcial o total. El Comité Internacional de la Cruz Roja (CICR, 2021) ha manifestado claramente su advertencia sobre que "la supervisión humana significativa es una exigencia ética innegociable" en los sistemas autónomos y semi-autonomos en el contexto de conflicto armado.

En el contexto colombiano, la utilización de la IA en entornos operacionales se debe considerar dentro del bloque de la constitucionalidad (Artículo 93 CP), lo que significa que la aplicación del Derecho Internacional Humanitario (DIH) debe ser estricta, particularmente

los principios de distinción, proporcionalidad, necesidad militar y precaución. Cualquier tipo de violación de esos principios, aun mediada por tecnologías, puede constituir claras infracciones al DIH, lo que generaría responsabilidad jurídica del Estado o el mando directo *(ONU, 2018; Corte Constitucional, 2016).*

Principales riesgos jurídicos asociados al uso de la IA en la Armada Nacional de Colombia

1. Falta de regulación jurídica especifica en el ámbito nacional

Actualmente, nuestro país carece de un marco normativo específico el cual regule el uso de IA en operaciones militares, a diferencia de la Unión Europea, la cual ha logrado el desarrollo de la AI Act (2021) con base en mecanismos de evaluación ética obligatoria. Por causa de la ausencia de regulación nacional, se podrían abrir espacios de inseguridad jurídica que afecten el principio de legalidad, pilar esencial en un Estado social de derecho.

2. Responsabilidad penal y del mando frente a decisiones automatizadas

El más relevante dilema jurídico es la atribución de responsabilidad penal o disciplinaria cuando una decisión militar—por ejemplo, la activación de un arma, la selección de un objetivo o una omisión operacional—es tomada por un sistema basado en la IA. En este caso, el principio de responsabilidad del mando cobra especial importancia (ONU,2018; Ley

1862/2017), puesto que los comandantes deben prevenir, prever y ejercer control sobre los riesgos derivados del uso de estas tecnologías. Si descartan esta función podrían ser considerados responsables por omisión o negligencia (Corte Constitucional, Sentencia C-084/2016).

3. Riesgos de sesgos algorítmicos y discriminación

Los algoritmos de IA podrían replicar sesgos en las identificaciones con las que fueron entrenadas, lo que puede traducirse en la falta distinción operativa, o la selección incorrecta de blancos específicos o interpretaciones erróneas en la recolección y el análisis de inteligencia. Lo que deriva en una posible violación al principio de distinción como lo advierten estudios recientes sobre sesgos algorítmicos en entornos militares (UNESCO, 2021; Georgetown University, 2021). Esto sería una amenaza directa a la protección de civiles, poblaciones vulnerables y bienes protegidos por el derecho internacional.

4. Vulneración del principio de transparencia

En la actualidad muchos sistemas basados en IA poseen unas particularidades críticas en su "caja negra" u opacidad "confusión" algorítmica, lo que significa, que las IA en estos momentos no poseen capacidad para auditar o comprender el racionamiento que llevo a tomar una decisión específica. Lo que se define o se ve representado en la vulneración del principio de trazabilidad y la dificultad de rendir cuentas. De acuerdo con (MIT Media Lab, 2020; Forster, 2020) "ningún sistema autónomo debería operar en un contexto militar sin mecanismos robustos de supervisión humana y auditoria estricta estructural".

Desafíos éticos en el uso de la IA militar: tensiones morales y operacionales

1. ***Autonomía tecnológica vs juicio ético humano***

En el contexto mundial actual, la substitución del juicio humano por sistemas automatizados ha generado un claro dilema ético profundo. Los criterios jurídicos, culturales y contextuales del ser humano, permiten que la interpretación de situaciones graves sea de una forma ética bajo sus principios; por el contrario de los algoritmos, los cuales actúan bajo reglas binarias. Tal y como lo señala Vigevano (2021), "el juicio ético no es apta por la lógica computacional, sobre todo en las situaciones en donde la vida humana es susceptible".

2. ***Reducción de la dignidad humana a datos***

En entornos donde la IA ha sido militarizada, los individuos "seres humanos" pueden ser convertidos en simples objetos de análisis, reducidos a patrones o amenazas estadísticas. Lo que podría convertirse en una clara violación a la dignidad humana, derecho principal del derecho internacional de los derechos humanos (Corte IDH, Opinión Consultiva OC-18/03). Desde el punto de vista operacional, implicaría que una decisión de ataque podría deshumanizar el blanco, viéndose incrementado el riesgo del uso excesivo o innecesario de la fuerza.

3. ***La ilusión de infalibilidad tecnológica***

La tendencia en la actualidad, es considerar que los sistemas de IA son infalibles por su carácter "científico" o computacional. Teniendo en cuenta esta "confianza", los operadores humanos pueden caer en el error de dejar de cuestionar ordenes generadas por algoritmos, inclusive si estas órdenes contradicen principios morales y legales. Tal y como nos advierte

Asaro (2008), esta transferencia de confianza sin mecanismos reales de control ¡podrían generar derivaciones funestas en contextos operacionales!

Riesgos de infracción al DIH y los Derechos Humanos

En las operaciones militares, el uso de la IA sin una normativa clara y efectiva podría derivar en infracciones graves al DIH y los Derechos Humanos. De los cuales identificamos los siguientes:

- Por errores en la selección de blancos se podrían producir ataques indiscriminados y desproporcionados.
- Por errores en el filtrado de información crítica, se podría producir omisiones asistenciales a la población y personal de combatientes fuera de combate.
- Sin la verificación humana, se podría realizar una escalada de violencia basada en sistemas predictivos.
- En labores de inteligencia y vigilancia, se podría producir afectación al derecho a la privacidad debido al uso indiscriminado de IA ¡sin controles legales!

Estos riesgos no son basados en casos hipotéticos, durante conflictos recientes se ha podido identificar varios de ellos, como es el caso "Siria y Yemen", donde el uso de tecnologías como la IA sin regulación ha provocado daños irreparables a bienes protegidos y población civil (CICR, 2021; Georgetown University, 2021).

Hacia un modelo normativo preventivo: observaciones iniciales

Para la implementación de estas tecnologías y poder mitigar estos desafíos en la Armada Nacional de Colombia, se propone que se adopten los siguientes lineamientos estratégicos así:

1. Instaurar un marco normativo interno sobre el uso de las IA en operaciones militares, basado en principios jurídicos y éticos del DIH y DD.HH.
2. En toda decisión critica se debe garantizar la supervisión humana significativa de las decisiones tomadas por las IA, especialmente en aquellas donde la violencia es usada, también en la clasificación de objetivos o acciones de ciberdefensa ofensiva.
3. Con la participación de asesores jurídicos militares y comités de ética operativa crear un sistema de auditorías algorítmicas internas.
4. Con el fin de garantizar la trazabilidad, inmutabilidad y transparencia de decisiones críticas, se debe aplicar tecnologías complementarias como el Blockchain, de acuerdo con estándares internacionales de rendición de cuentas (Pilkington, 2016; Tapscott & Tapscott, 2016).
5. Los contenidos normativos y éticos se deben fortalecer desde el contexto de la Doctrina y la Educación Militar, referente al uso responsable de las tecnologías emergentes y con el fin de prevenir la deshumanización operativa.

Jurisprudencia colombiana aplicable al uso de tecnologías emergentes

En el contexto de excepcionalidad del marco constitucional colombiano, se ha desarrollado bajo una jurisprudencia robusta del respeto estricto a los derechos fundamentales, como los operacionales militares y de seguridad nacional. Bajo esta premisa, la Sentencia **T-092** de **2019** de la Corte Constitucional establece que **"*el uso de herramientas tecnológicas por parte del Estado debe estar acompañado de medidas efectivas de control, rendición de cuentas y protección del mínimo vital".***

A pesar de que esta sentencia se utiliza en el ámbito civil-administrativo, su principio rector es completamente aplicable al uso de la IA en las FF.MM., especialmente cuando cita que la tecnología puede impactar directa o indirectamente derechos fundamentales (como la vida, la integridad, la intimidad o en el debido proceso del uso de la fuerza).

Cobrando una mayor relevancia en contextos donde la IA es utilizada para :

- Priorización de blancos enemigos y amenazas (targeting);
- En la planificación conjunta o interinstitucional de operaciones ofensivas y defensivas;
- En la recolección y análisis estricto de inteligencia humana o técnica;
- En entornos hostiles respecto de la activación de sistemas autónomos.

En los anteriores casos y en muchos más, la jurisprudencia constitucional colombiana exige que exista supervisión humana, transparencia en la toma de decisiones algorítmicas y capacidad de rendición de cuentas ante posibles errores y abusos. Es ahí, donde cobra especial relevancia el uso de la tecnología Blockchain, integrada a la arquitectura de la IA militar, que se podría dar cumplimiento real al mandato de la Corte Constitucional.

La incorporación de tecnologías emergentes por parte del Estado Colombiano —especialmente en entornos de Defensa y Seguridad Nacional— no está indultada de los límites constitucionales... ¡por el contrario! el principio de legalidad, la protección de los derechos fundamentales y el respeto al debido proceso se mantienen plenamente vigentes aun en contextos operacionales militares o situaciones excepcionales. La Corte Constitucional de Colombia ha diseñado una jurisprudencia sólida que orienta cómo debe emplearse la tecnología —y en especial, la Inteligencia Artificial— dentro de un marco de transparencia, control institucional y trazabilidad de decisiones.

En este sentido, la Sentencia **T-282 de 2022** constituye un hito relevante. En ella, la Corte analizó un caso en el que una persona fue afectada por una decisión automatizada adoptada por un sistema algorítmico sin mecanismos adecuados de revisión ni supervisión humana. La Corte fue enfática al señalar que:

"Las decisiones automatizadas adoptadas por el Estado deben ser comprensibles, verificables y sujetas a control, para no vulnerar el derecho al debido proceso de los ciudadanos."

Este criterio resulta plenamente aplicable al ámbito militar, donde la IA puede intervenir en procesos como la selección de blancos, la priorización de amenazas, o el análisis predictivo para operaciones conjuntas. En tales escenarios, es imperativo garantizar que cualquier decisión basada en algoritmos esté sujeta a revisión humana e institucional, con capacidad de auditoría... y con responsabilidad.

De forma complementaria, la Sentencia T-190 de 2023 reafirma que el uso de sistemas tecnológicos en decisiones estatales debe cumplir con los principios de legalidad, transparencia y rendición de cuentas. La Corte advirtió que:

"***El uso de algoritmos y sistemas automatizados por parte del Estado requiere mecanismos técnicos y jurídicos que permitan su supervisión efectiva; sin esto, se vulnera el derecho fundamental al debido proceso."***

En el marco del presente artículo, estos postulados refuerzan la propuesta de integrar tecnología Blockchain en los sistemas de IA militar como mecanismo para cumplir con la exigencia constitucional de trazabilidad y control. Blockchain —por su estructura descentralizada, segura e inmutable— ofrece justamente las condiciones que demanda la Corte: transparencia, control institucional, y posibilidad de reconstrucción de decisiones.

Ahora bien, el principio de precaución tecnológica, desarrollado en la **Sentencia C-239 de 2012**, establece que cuando se utilicen tecnologías cuyo impacto sobre los derechos fundamentales no sea del todo conocido... el Estado debe adoptar medidas preventivas, restrictivas y revisables. ¿Cómo se traduce esto en el uso militar de IA? Sencillo: cualquier sistema que tome decisiones sensibles debe ser sometido a revisión ética y legal antes, durante y después de su empleo táctico —¡nunca después de ocurrida la afectación! —, la tecnología Blockchain puede convertirse en ese canal de garantía, registrando en tiempo real cada decisión algorítmica, con su respectivo sello de tiempo (timestamp), creando así una línea de tiempo verificable.

En cuanto a la videovigilancia y tecnologías aplicadas a seguridad, la **Sentencia C-748 de 2011** señaló que, aún en el marco del orden público, es inconstitucional aplicar tecnología sin que existan límites claros de uso, autoridades responsables y mecanismos de supervisión.

Este pronunciamiento tiene especial importancia para el uso de IA en sistemas de vigilancia automatizada, patrullaje naval autónomo, o interdicción marítima... todos escenarios comunes para la Armada Nacional de Colombia.

Así las cosas, el marco jurisprudencial colombiano —¡sólido y progresista! — respalda que el uso de Inteligencia Artificial en operaciones militares debe estar acompañado de mecanismos claros de supervisión, responsabilidad institucional y trazabilidad técnica, lo cual puede garantizarse a través de la integración con tecnología emergente Blockchain. Esta arquitectura dual no solo evita la vulneración de los derechos humanos... también fortalece la legitimidad del accionar militar en escenarios complejos y dinámicos.

Blockchain como blindaje ético y legal de la Inteligencia Artificial en contextos militares

La integración de Blockchain en sistemas de Inteligencia Artificial (IA) en el ámbito militar no solo representa un avance tecnológico; es, sobre todo, una necesidad estratégica, jurídica y ética en contextos donde la protección de los Derechos Humanos y el cumplimiento del Derecho Internacional Humanitario (DIH) deben ser prioridad ineludible. ¿Es posible garantizar que un algoritmo, entrenado con datos imperfectos y operando en entornos hostiles, respete los principios de distinción, proporcionalidad y precaución? ¡Sí!, siempre que se articule una arquitectura digital que permita la trazabilidad, transparencia y responsabilidad... es decir, una arquitectura basada en Blockchain.

Aplicabilidad funcional de la Blockchain en sistemas de IA: transparencia, inmutabilidad y trazabilidad

La tecnología Blockchain ---por su diseño descentralizado, criptográficamente seguro e inalterable--- permite registrar cada paso del ciclo de vida de una decisión algorítmica, desde la recolección de datos hasta la ejecución operacional. En operaciones militares donde la IA se emplea en procesos sensibles como la selección de blancos, la vigilancia autónoma o el análisis predictivo de amenazas, la aplicación de Blockchain permite:

- Registrar cada decisión en tiempo real con sello de tiempo (timestamp) verificable;
- Evitar la manipulación o eliminación posterior de datos;
- Facilitar auditorías internas y externas que garanticen el respeto al DIH y a los Derechos Humanos;
- Establecer líneas de responsabilidad institucional —y eventualmente individual—, cuando existan dudas sobre la legalidad de una operación automatizada.

Este diseño no solo minimiza el riesgo de impunidad... ¡lo desintegra de raíz!

Según Palomo Zurdo (2018), la tecnología Blockchain, aplicada en el sector defensa, tiene una alta viabilidad para la activación de sistemas de armas, gestión de la cadena de suministro y ciberseguridad, todos ellos nodos donde la IA ya tiene presencia activa. Por su parte, Pareja Pérez (2023) advierte que, si bien la IA mejora la eficiencia militar, debe acompañarse de mecanismos de rendición de cuentas sólidos; aquí es donde Blockchain actúa como un candado institucional para garantizar el respeto a los marcos legales internacionales.

Mecanismos de protección de derechos mediante Blockchain integrada en IA

A la luz del artículo 36 del Protocolo Adicional I a los Convenios de Ginebra, cualquier nuevo medio o método de guerra debe ser revisado para verificar su compatibilidad con el DIH. ¡Y esto aplica también a la IA y sus algoritmos autónomos! Implementar Blockchain en este tipo de sistemas permite cumplir dicho deber, mediante:

- Auditorías continuas por órganos de control internos (como las Inspectorías Generales) y externos (como los órganos de supervisión de DD.HH. y DIH);
- Sistemas de alertas automáticas ante comportamientos que se salgan de los parámetros programados de respeto a los derechos fundamentales;
- Registro automático e inmodificable de toda interacción con civiles, población vulnerable o infraestructura protegida;
- Creación de un repositorio histórico de decisiones tácticas y estratégicas basadas en IA para procesos judiciales, disciplinarios o de aprendizaje institucional.

Tal como indica el estudio de Vigevano (2021), la IA no puede reemplazar el juicio humano en escenarios complejos ni asumir responsabilidad legal. Por ello, los mecanismos de respaldo como Blockchain no son opcionales... ¡son mandatorios!

Desafíos de implementación en la Armada Nacional de Colombia y medidas de mitigación

¿Se puede aplicar esta arquitectura en Colombia y específicamente en la Armada Nacional de Colombia? ¡Por supuesto que sí! Sin embargo, existen varios desafíos:

Interoperabilidad de sistemas heredados

Muchos de los sistemas actuales de la Armada no están diseñados para integrar soluciones Blockchain. ¿Solución? Diseñar interfaces (APIs) intermedias que permitan migrar de forma progresiva.

Resistencia institucional al cambio

Como exponen autores como Tapscott & Tapscott (2016), la tecnología Blockchain desafía estructuras verticales tradicionales. Se requiere una transformación cultural en la Armada Nacional de Colombia, promoviendo la ética digital militar y la capacitación en tecnologías disruptivas con enfoque en DD.HH.

Marco normativo nacional e internacional

Actualmente, Colombia carece de regulación específica sobre IA y Blockchain en defensa. Por tanto, se debe trabajar en la formulación de protocolos internos de cumplimiento voluntario que se alineen con el derecho internacional, mientras se impulsa la generación de normativa nacional especializada.

Sinergias estratégicas para la garantía integral de derechos

El diseño de un ecosistema que combine IA y Blockchain debe enfocarse en una arquitectura de control multinivel:

- Nivel algorítmico: criterios programados de respeto al DIH.

- Nivel técnico-operacional: integración con Blockchain para garantizar inmutabilidad y trazabilidad.
- Nivel jurídico-institucional: protocolos claros de supervisión, auditoría y sanción.

Una propuesta concreta para la Armada Nacional de Colombia sería la creación de un "Centro de Supervisión Digital de Derechos Humanos", encargado de monitorear en tiempo real los algoritmos aplicados en operaciones, con capacidades forenses basadas en Blockchain.

Conclusión parcial del objetivo

La aplicabilidad de la tecnología Blockchain como mecanismo de blindaje jurídico y ético de los sistemas de Inteligencia Artificial en el contexto de la Armada Nacional no solo es viable, sino deseable y urgente. Su implementación, bien estructurada, permitirá a Colombia avanzar hacia una defensa moderna, humanitaria y transparente, donde la tecnología no sea un riesgo para los derechos, sino su mayor garantía.

Sinergias estratégicas para la garantía integral de derechos

La incorporación de Blockchain en la Inteligencia Artificial con fines militares debe superar el nivel meramente técnico o conceptual. Requiere un enfoque sistémico que articule la seguridad digital, la ética operacional y la juridicidad táctica dentro de una doctrina institucional de transparencia y protección de derechos. Este enfoque puede desarrollarse mediante una arquitectura en tres niveles interdependientes:

1. Nivel Algorítmico: Diseñado desde la ingeniería ética y jurídica, debe garantizar que los algoritmos estén programados con límites definidos conforme al DIH y los

Derechos Humanos (DD.HH.); por ejemplo, la exclusión automática de objetivos clasificados como civiles, patrimonio cultural o infraestructura protegida.

2. Nivel Técnico-Operacional: Blockchain se encarga aquí de registrar toda acción automatizada de la IA. Desde el momento en que un dron identifica una amenaza hasta que se activa una alerta o una orden de no-disparo, cada decisión queda registrada con sello de tiempo. ¡Así se asegura la trazabilidad!
3. Nivel Jurídico-Institucional: Este nivel exige la existencia de protocolos de auditoría digital, supervisión humana permanente, líneas claras de responsabilidad penal o disciplinaria y capacidad institucional de revisión y corrección inmediata.

Como bien sostiene Sharkey (2020), el problema no está en que los sistemas automáticos se equivoquen... ¡el verdadero riesgo es no poder saber cuándo lo hicieron ni por qué! Blockchain elimina esta opacidad. Es el equivalente digital de un "cuaderno de bitácora" inviolable, que permite a los operadores jurídicos reconstruir los hechos... y, por tanto, garantizar derechos.

Análisis comparado de modelos internacionales: integración de IA y Blockchain en defensa

El uso militar de tecnologías emergentes —como la Inteligencia Artificial (IA) y la Blockchain— ha adquirido una relevancia estratégica sin precedentes. No se trata únicamente de eficiencia operativa... sino de legitimidad, control y responsabilidad jurídica. A

continuación, se realiza un análisis comparado entre **Estados Unidos**, **Estonia** e **Israel**; tres modelos que —aunque diversos— coinciden en una verdad esencial: ¡la tecnología debe estar subordinada al Derecho... nunca al contrario!

Los criterios utilizados para esta comparación son claros y concretos:

1. **Nivel de integración tecnológica**,
2. **Marco jurídico de protección de los derechos humanos**, y
3. **Eficacia de los sistemas de auditoría y supervisión**.

Este ejercicio no busca idealizar modelos ajenos —ni replicarlos ciegamente— sino examinar cómo equilibran la innovación con la protección de principios éticos fundamentales (distinción, proporcionalidad, precaución, legalidad...).

Estados Unidos: Proyecto Maven y auditoría algorítmica.

El Departamento de Defensa estadounidense lanzó el Proyecto Maven con el fin de automatizar el análisis de videos de vigilancia mediante IA. La iniciativa generó fuertes cuestionamientos éticos —¡y con razón!— debido a la falta de trazabilidad en las decisiones automatizadas. Esta iniciativa —más que un marco ético— es una jugada estratégica. El Proyecto Maven no nació del humanismo digital… sino del miedo a perder los conflictos. Para el Departamento de Defensa de los Estados Unidos, mantener la «superioridad decisional» es tan vital como el control del espacio aéreo o la supremacía marítima. En un

mundo donde pensar más rápido —y decidir antes— puede equivaler a vencer sin disparar, surge la guerra centrada en decisiones (decision-centric warfare). No se trata de reemplazar soldados por circuitos… sino de anticipar al adversario antes de que siquiera se mueva. Una IA sin supervisión es una bala perdida; una IA trazable, una ventaja táctica legítima. Como respuesta, en 2020 se adoptaron los Principios Éticos para la IA: supervisión humana significativa, transparencia, responsabilidad y mitigación de sesgos (Departament of Defense, 2020). A partir de entonces, se integró experimentalmente Blockchain para auditar decisiones operacionales —por ejemplo, la selección de blancos—. Según el MIT Media Lab (2020), el margen de error en misiones con IA sin supervisión se observó una reducción significativa tras incluir registros descentralizados verificables. ¿Conclusión? No basta con usar IA... se necesita un sistema que permita —si es necesario— reconstruir cada paso. Y Blockchain puede hacerlo.

Estonia: KSI Blockchain y ciber defensa nacional.

En un mundo donde las guerras ya no solo se libran con balas, sino con datos; donde el enemigo no siempre porta uniforme, sino líneas de código, Estonia decidió no esperar a ser víctima una segunda vez. Fue atacada —sí— pero no se rindió: digitalizó su defensa, descentralizó su Estado y blindó su verdad con tecnología.

Tras los ciberataques masivos de 2007, Estonia transformó el trauma en estrategia y fundó el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN (CCDCOE). Allí, algoritmos, inteligencia artificial y sistemas Blockchain dejaron de ser fantasía futurista para

convertirse en aliados de la seguridad nacional. Estonia entendió lo que muchos Estados aún temen admitir: que la trazabilidad y la transparencia no son una amenaza al poder, sino su legitimación.

Usando Blockchain en bases de datos sensibles —salud, defensa, propiedad, registros militares— Estonia blindó sus instituciones ante la manipulación y la opacidad. ¿Cuál fue El resultado?

Una arquitectura digital tan resistente como su voluntad democrática. Sus sistemas no sustituyen al mando militar, pero lo iluminan; no le quitan poder, pero le exigen rendición de cuentas. Esta apuesta por la supervisión tecnológica se ha hecho sin romper jerarquías, sin traicionar el secreto operacional y —lo más admirable— sin abandonar el principio de humanidad en tiempos de guerra. En el caso estonio, diversos estudios como el del Centre for Data Ethics and Innovation (2020) y el Ministerio de Defensa de Estonia (2020) sugieren que no se eligió entre seguridad y derechos, sino que se construyó una arquitectura capaz de proteger ambos principios simultáneamente.

Colombia, y en particular su Armada Nacional, ¡no está obligada a copiar ese modelo¡, pero sí a aprender de él. La doctrina de interoperabilidad, la acción integral y el respeto al Derecho Internacional Humanitario pueden —y deben— complementarse con tecnologías que, como la IA y Blockchain, ofrezcan trazabilidad, supervisión y ética digital.

Porque si un pequeño Estado báltico sin petróleo, sin maras ni guerrillas pudo hacerlo... ¿cómo no va a poder un país como Colombia, que ya ha demostrado ser resiliente, creativo y capaz de reinventarse?

Israel: Control jurídico en ciberoperaciones ofensivas.

Israel, a través de su **Comando Cibernético Militar**, ha desarrollado herramientas ofensivas con base en IA —por ejemplo, para desactivar infraestructuras enemigas sin intervención humana directa—. Sin embargo, en 2022 se implementó un protocolo ético que exige revisión jurídica previa antes de activar cualquier algoritmo con potencial destructivo (Sharkey, 2020).

Adicionalmente, el uso de Blockchain como "bitácora digital" ha permitido dejar trazabilidad de cada orden, cada modificación... ¡cada bit! De acuerdo con el **INSS** (2024), este sistema contribuyó a una mejora notable en la precisión de errores de atribución en ciberataques. Israel cumple con el **artículo 36 del Protocolo I** —evaluar la legalidad de todo nuevo medio de guerra— y demuestra que, incluso en contextos ofensivos, la supervisión humana es irrenunciable. En un entorno donde cada decisión bélica se transmite por satélite… y cada impacto es replicado en tiempo real por medios y cancillerías, Israel no puede improvisar: debe anticipar. Su doctrina de defensa activa le exige responder rápido, pero también con legitimidad jurídica. Por eso la trazabilidad tecnológica no es solo control interno, es escudo diplomático. La supervisión de cada algoritmo no desarma al comandante, lo protege: de sanciones, de narrativas adversas, de tribunales. Cada bit registrado en Blockchain puede ser mañana una defensa ante el Consejo de Derechos Humanos… o ante la historia misma.

Reflexión comparada y lecciones para Colombia

¿Qué nos enseñan estos tres modelos...? Que la tecnología no garantiza justicia —¡solo la hace posible cuando hay control, ética y norma!—. Estados Unidos prioriza principios éticos y comienza a auditar con Blockchain; Estonia blindó la defensa digital con trazabilidad criptográfica; Israel exige control jurídico ex ante... y registra cada acción automatizada con precisión forense.

Todos tienen algo en común: la confianza institucional ya no se basa en jerarquías... sino en trazabilidad.

Para Colombia —y especialmente para la Armada Nacional de Colombia— este análisis no debe ser solo ilustrativo; debe convertirse en hoja de ruta. Integrar IA sin Blockchain es arriesgado; usar Blockchain sin auditoría humana, inútil. Lo que está en juego no es solo la eficacia... ¡sino los derechos humanos, la vida, la legitimidad del uso de la fuerza!

Como advierte Brands (2024):

> *"La guerra del siglo XXI no se ganará con drones... sino con credibilidad jurídica ante el mundo"* (p. 198).

La incorporación ética de la IA y Blockchain en defensa no es opcional: es una condición sine qua non para operar en el siglo XXI con legitimidad, eficacia y respeto a los derechos fundamentales.

Aplicación metodológica y teórica en el contexto colombiano

La metodología hermenéutica-jurídica adoptada en este estudio no se limita a interpretar normas; busca desentrañar su funcionalidad práctica en escenarios reales de defensa y seguridad. Este enfoque permitió analizar de manera transversal los riesgos, vacíos y oportunidades jurídicas derivados del uso de tecnologías emergentes en la Armada Nacional —especialmente en relación con los Derechos Humanos y el Derecho Internacional Humanitario (DIH)—. A su vez, la estrategia exploratoria-descriptiva permitió caracterizar los modelos internacionales con base en evidencia empírica, doctrinal y normativa, sin perder de vista el contexto nacional.

El desarrollo del análisis comparado se apoyó en la interpretación normativa de marcos constitucionales —como el artículo 93 de la Constitución Política de Colombia—, tratados internacionales (como los Convenios de Ginebra y su Protocolo I), leyes nacionales (Ley 1862 de 2017, Código Penal Militar), y sentencias de la Corte Constitucional que establecen estándares exigibles a la acción estatal tecnológica (T-092/2019, T-401/2020, T-233/2022... entre otras).

Por otro lado, el marco teórico utilizado —la **Teoría de Sistemas de Niklas Luhmann**— aporta una visión estructural de las Fuerzas Militares como sistema social **autopoiético**, es decir, capaz de generar sus propias reglas, adaptarse al entorno y diferenciar subsistemas internos. Este concepto permite justificar la necesidad de **crear subsistemas autónomos y**

especializados, como el **Centro de Supervisión Digital de Derechos Humanos**, para garantizar control ético y trazabilidad institucional sobre las decisiones automatizadas.

Así como Luhmann sostiene que los sistemas evolucionan por diferenciación funcional (1996), este artículo plantea que la Armada Nacional de Colombia debe incorporar **nuevas unidades estructurales internas** capaces de:

- Vigilar el uso de IA y Blockchain;
- Activar mecanismos de respuesta jurídica inmediata;
- Y establecer una línea de trazabilidad objetiva frente a cualquier decisión tecnológica que pueda afectar derechos fundamentales.

De esta manera, la teoría y la metodología dejan de ser un marco conceptual y se convierten en **filtros de validación operativa y jurídica**. No se trata solo de "hablar" de ética militar y tecnología... sino de **diseñar estructuras concretas** que permitan actuar conforme a Derecho.

Diseño institucional sugerido para la Armada Nacional de Colombia

Como resultado del análisis metodológico, jurídico y doctrinal, se propone crear en la Armada Nacional de Colombia una estructura orgánica especializada, autónoma y permanente: el **Centro de Supervisión Digital de Derechos Humanos y Derecho Internacional Humanitario (CSD-DDHH/DIH)**. Esta unidad debe integrarse al Estado Mayor Conjunto, pero con dependencia funcional directa de la **Inspección General** y la

Dirección de Derechos Humanos del Ministerio de Defensa, garantizando su autonomía técnica y su neutralidad frente a las cadenas de mando operativas.

El objetivo fundamental de esta entidad será **monitorear en tiempo real** los sistemas algorítmicos aplicados a operaciones militares, velando por el cumplimiento de los principios de legalidad, trazabilidad, proporcionalidad, distinción y precaución. No se trata de crear una dependencia simbólica o decorativa… sino una verdadera **estructura institucional con dientes y función preventiva**.

Funciones esenciales del CSD-DDHH/DIH:

1. **Autorizar el uso de algoritmos militares** con implicaciones éticas, jurídicas o tácticas antes de su activación operacional.
2. **Administrar el repositorio Blockchain** donde se registren todas las decisiones automatizadas (por ejemplo: análisis predictivo, selección de blancos, activación de sistemas autónomos, etc.).
3. **Emitir alertas ético-jurídicas** ante riesgos detectados en sistemas de IA —¡antes de que ocurran posibles violaciones!—.
4. **Realizar auditorías forenses digitales**, con facultad de reportar a la Procuraduría General de la Nación y al Congreso de la República, cuando se detecten riesgos de infracción a derechos fundamentales.
5. **Capacitar a los mandos operacionales** en ética digital militar, transparencia institucional, trazabilidad y responsabilidad del mando bajo sistemas inteligentes.

Estructura y legitimidad

El CSD-DDHH/DIH debe contar con personal interdisciplinario:

- Oficiales en servicio activo con formación jurídica, especialización o maestrías en DDHH, DIH y DICA y experiencia operacional,
- Asesores civiles en derechos humanos y DIH,
- Ingenieros en IA y Blockchain,
- Y observadores institucionales permanentes del **CICR** y la **Oficina del Alto Comisionado de Naciones Unidas para los DD.HH.** (con acceso parcial y protocolos de seguridad).

Este modelo no es solo viable, sino **urgente**. La experiencia internacional muestra que los errores algorítmicos sin trazabilidad conducen a **impunidad técnica** —y esa impunidad deslegitima toda acción militar—. Al incorporar una arquitectura de control técnico-jurídico basada en Blockchain, Colombia puede garantizar que ninguna decisión automatizada escape al control ético, institucional ni legal.

Justificación normativa y teórica

Esta propuesta encuentra su respaldo directo en:

- El **principio de legalidad y transparencia** (artículos 6 y 15 de la Constitución Política),
- La jurisprudencia constitucional que exige mecanismos de revisión sobre decisiones automatizadas (T-233 de 2022; T-401 de 2020),

- Y la Teoría de Sistemas de Luhmann (1996), que permite diseñar subsistemas funcionales diferenciados para responder con eficiencia y adaptabilidad al entorno institucional y tecnológico.

De esta manera, el CSD-DDHH/DIH no sería un obstáculo para las operaciones… sino un **facilitador de la legitimidad táctica**, protegiendo tanto al mando como a la tropa en escenarios complejos e híbridos.

Evaluación de riesgos y consideraciones futuras

La implementación de tecnologías como la Inteligencia Artificial (IA) y Blockchain en la Armada Nacional de Colombia —aunque prometedora— conlleva **riesgos reales, complejos y multidimensionales** que deben ser previstos con responsabilidad. La historia reciente y los modelos comparados demuestran que los errores tecnológicos, cuando no existen controles adecuados, no solo pueden causar afectaciones operacionales… sino también violaciones graves a los derechos humanos —¡e incluso crímenes de guerra!—

A continuación, se identifican los principales riesgos, seguidos de recomendaciones jurídicas y estratégicas orientadas a prevenirlos:

1. Riesgo de manipulación o vulneración de datos sensibles

Aunque Blockchain ofrece altos niveles de seguridad, su implementación en contextos militares exige redes cerradas, cifrado avanzado y control estricto de accesos. De lo contrario —si se adopta sin ciberdefensa robusta— podría convertirse en un punto de vulnerabilidad institucional.

Medida preventiva: Implementar Blockchain exclusivamente sobre redes privadas militares (no públicas) y bajo entornos de encriptación cuántica, con actualizaciones periódicas de los nodos de validación.

2. Brechas de formación en el personal militar

La IA y Blockchain requieren una cultura organizacional digital. La falta de formación específica puede llevar a errores operacionales, omisiones de supervisión o uso indebido de sistemas automatizados sin comprender su alcance. **Medida preventiva:** Incluir módulos obligatorios en la Escuela Naval, en el Curso de Estado Mayor y en la capacitación continua de mandos sobre ética digital, auditoría algorítmica y uso jurídico de tecnologías disruptivas.

3. Ausencia de reconocimiento legal probatorio de registros Blockchain

En Colombia —aún hoy— no existe una ley que establezca expresamente el valor jurídico y probatorio de un registro Blockchain en el contexto penal militar. Esta omisión puede afectar procesos disciplinarios, operacionales o judiciales en caso de controversias. **Medida preventiva:** Impulsar una reforma al **Código Penal Militar (Ley 1407 de 2010)** para incluir la **admisibilidad de registros digitales inmutables**, con certificación técnica, como prueba en investigaciones internas o externas.

4. Delegación ciega de decisiones a sistemas autónomos

La confianza excesiva en los algoritmos puede generar deshumanización operativa. Este fenómeno —conocido como "ilusión de infalibilidad tecnológica"— ha sido identificado por Sharkey (2020) como uno de los principales riesgos en entornos militares automatizados.

Medida preventiva: Prohibir normativamente cualquier operación automatizada que no incluya verificación humana significativa. Además, establecer un principio rector: **toda decisión que pueda afectar la vida, integridad o derechos de una persona debe pasar por revisión humana documentada**.

5. Falta de auditoría externa y control institucional transversal

Si el uso de IA y Blockchain queda en manos exclusivamente militares, sin veeduría institucional ni observación internacional —como lo ha demostrado el caso de China y Rusia— se incrementan los riesgos de opacidad, abuso o irresponsabilidad táctica. **Medida preventiva:** Incluir en la arquitectura del **Centro de Supervisión Digital de Derechos Humanos** observadores con acceso limitado a registros Blockchain, pertenecientes al Ministerio de Justicia, la Procuraduría, y eventualmente al CICR o ACNUDH.

Consideración estratégica final

El principio de **precaución tecnológica**, establecido en la **Sentencia C-239 de 2012**, impone al Estado la obligación de anticipar, restringir y supervisar cualquier innovación que pueda afectar derechos fundamentales. En este contexto, no se trata de detener el avance… sino de encauzarlo jurídicamente. Como advierte la Corte Constitucional:

"Las decisiones automatizadas deben ser comprensibles, verificables y sujetas a control; de lo contrario, se vulnera el debido proceso" (T-233/2022).

Colombia —a diferencia de países autoritarios— tiene el marco constitucional necesario para liderar una implementación **ética, jurídica y operacionalmente sólida** de estas tecnologías.

La Armada Nacional de Colombia, como institución garante del orden, tiene la oportunidad histórica de construir un modelo de referencia para América Latina… o, por el contrario, de repetir errores evitables.

¡La diferencia entre ambos caminos está en las decisiones que se tomen ahora… y en los sistemas que garanticen su trazabilidad!

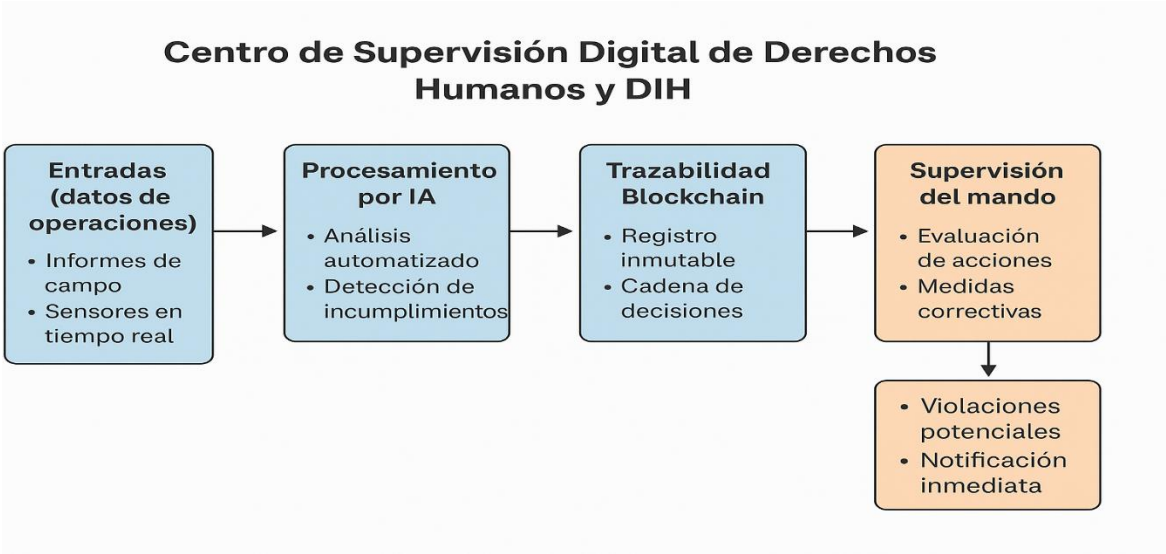
Conclusión extendida del objetivo específico

En conclusión, determinar la aplicabilidad de la tecnología Blockchain en los sistemas de Inteligencia Artificial de la Armada Nacional de Colombia no es un ejercicio meramente académico o especulativo. Es una obligación jurídica, operativa y ética, enmarcada en la necesidad de garantizar que las nuevas formas de conducción del conflicto no vulneren los principios fundamentales del Derecho Internacional Humanitario ni los Derechos Humanos. La adopción de Blockchain como tecnología de blindaje, asegura que las decisiones automatizadas no se conviertan en espacios de impunidad sino en herramientas de legalidad. Es una oportunidad histórica para que la Armada Nacional de Colombia lidere, desde el Sur Global, una transformación profunda hacia una defensa ética, humanitaria y técnicamente avanzada.

A continuación, se presenta una visualización esquemática del modelo propuesto: el Centro de Supervisión Digital de Derechos Humanos y DIH. Este diagrama —estructurado como un flujo lógico— muestra la secuencia desde la recolección de datos operacionales en tiempo real, pasando por el análisis automatizado mediante Inteligencia Artificial; la trazabilidad e integridad garantizadas por tecnología Blockchain; hasta la activación de alertas jurídicas y

la supervisión por parte del mando. ¡Todo el sistema está diseñado para prevenir vulneraciones a los Derechos Humanos y reforzar los mecanismos de control ético en contextos militares complejos!

Figura 1. Diagrama del modelo institucional propuesto: Centro de Supervisión Digital de DD.HH. y DIH



Conclusión

Este artículo ha abordado —de manera crítica, jurídica y aplicada— el impacto del uso de tecnologías emergentes, particularmente la Inteligencia Artificial (IA) y la tecnología Blockchain, en el contexto operacional de la Armada Nacional de Colombia. A través de un enfoque hermenéutico-jurídico, con respaldo en doctrina comparada y en la teoría de sistemas de Niklas Luhmann, se logró cumplir cada uno de los tres objetivos específicos planteados al inicio.

En primer lugar, se establecieron los **desafíos jurídicos y éticos** derivados del uso de la IA en entornos militares, identificando riesgos estructurales como: la delegación de decisiones críticas a algoritmos opacos (caja negra); la deshumanización operativa; los sesgos algorítmicos que podrían vulnerar el principio de distinción del Derecho Internacional Humanitario (DIH); y la ausencia de normativas específicas que obliguen a la trazabilidad... Todos ellos representan una amenaza directa a los Derechos Humanos, y exigen —de forma urgente— mecanismos de control real.

En segundo lugar, se demostró la **aplicabilidad de la tecnología Blockchain** como blindaje ético y legal para los procesos de IA. Su inmutabilidad, trazabilidad y descentralización permiten auditar decisiones algorítmicas en tiempo real, asegurar responsabilidad institucional y evitar la impunidad técnica. Así lo demuestran —con claridad— modelos como el estonio, el estadounidense y el israelí. ¡La tecnología no solo es útil… es necesaria cuando se trata de proteger la dignidad humana!

En tercer lugar, se formuló un **modelo práctico y aplicable al contexto colombiano**, mediante la creación del **Centro de Supervisión Digital de Derechos Humanos y DIH (CSD-DDHH/DIH)** como subsistema funcional dentro de la Armada Nacional. Esta estructura —teóricamente fundamentada en Luhmann y normativamente viable según el bloque de constitucionalidad— permitiría integrar IA y Blockchain para certificar, en cada operación, la transparencia de los procesos, la trazabilidad de las órdenes y la supervisión ética sobre el uso de la fuerza. Con ello se da cumplimiento expreso al tercer objetivo específico... y se propone una ruta institucional concreta para no solo usar tecnología, sino encauzarla conforme al Derecho.

Así las cosas, no basta con modernizar capacidades tácticas —ni con adquirir sistemas inteligentes de última generación— si no se acompaña ese avance de estructuras jurídicas sólidas, auditorías efectivas, principios éticos vinculantes… y decisiones humanas bien fundamentadas.

Porque, al final, **la superioridad tecnológica sin control normativo no es poder… es vulnerabilidad**.

Referencias

Asaro, Peter M. (2008). *How Just Could a Robot War Be?* In *Current Issues in Computing and Philosophy*. Amsterdam: IOS Press.

Brands, Hal. (2024). *The New Makers of Modern Strategy.* Princeton: Princeton University Press.

Brundage, M. et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute, University of Oxford. https://arxiv.org/pdf/1802.07228.pdf

Carvajal, J. (2019). *Aplicación de la teoría de sistemas en el ámbito militar. Revista Colombiana de Ciencias Militares, 7(2), 57-72.*

Centre for Data Ethics and Innovation. (2020). IA Barometer Report 2020. Londres: UK Government.

CICR. (2021). *Directrices Éticas para Sistemas Autónomos y Semiautónomos. Comité Internacional de la Cruz Roja.* Recuperado de https://www.icrc.org

Corte Constitucional de Colombia. (1992-2024). *Sentencias sobre Derechos Humanos y Tecnología.* Bogotá: Sala Plena.

Corte Interamericana de Derechos Humanos (2003). Opinión Consultiva OC-18/03. Condición Jurídica y Derechos de los Migrantes Indocumentados. San José, Costa Rica.

Comisión Europea. (2021). *Propuesta de Reglamento para la Regulación de la Inteligencia Artificial.* Bruselas: Comisión Europea.

Departamento de Defensa de Estados Unidos (DoD). (2020). *Ethical Principles for Artificial Intelligence.* Washington, D.C.: DoD.

Estonian Ministry of Defence. si Digital Defence Strategy 2020–2030. Tallin: Republic of Estonia.

European Commission. (2019). Ethics Guidelines for Trustworthy IA. Brussels. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-IA

Flick, U. (2022). *An Introduction to Qualitative Research* (7th ed.). Sage.

Forster, T. (2020). *Transparency in Military Operations through Blockchain Technology*. *Defense & Technology Journal*, 13(2), 102-118.

Forster, A. (2020). IA, Ethics and Accountability in Military Decision-Making. Defence & Security Journal, 8(3), 45-62.

Georgetown University. (2021). *Artificial Intelligence and Accountability in Military Contexts.* Washington, D.C.: Georgetown Law.

Georgetown University. (2021). Human Rights and Technology Policy Report. Institute for Tech & Society.

Luhmann, Niklas. (1984*).* ***Soziale Systeme: Grundriß einer allgemeinen Theorie. Frankfurt: Suhrkamp.*

Luhmann, Niklas. (1996). *Teoría de Sistemas y Sociedad. Barcelona: Anthropos Editorial.*

MIT Media Lab. (2020). *Blockchain and Military Applications: Ensuring Transparency and Accountability.* Cambridge, MA: MIT.

Norwegian Ministry of Defence. (2020). IA and Maritime Surveillance: Enhancing Security and SustIAnability in the North Sea. Oslo: Ministry of Defence.

Organización de las Naciones Unidas – Consejo de Derechos Humanos. (2019). *Informe sobre el Impacto de la Inteligencia Artificial en los Derechos Humanos.* Ginebra: Naciones Unidas.

Organización de las Naciones Unidas (2018). *Directrices sobre la responsabilidad del mando y su implementación en contextos operativos*. Naciones Unidas.

Organización de las Naciones Unidas. (2018). *Directrices sobre la responsabilidad del mando y su implementación en contextos operativos. Naciones Unidas.* Recuperado de https://www.un.org.

Palomo Zurdo, R. J. (2018*).* ***«Blockchain»: La descentralización del poder y su aplicación en la defensa***. Madrid: Ministerio de Defensa de España.

Pareja Pérez, M. M. (2023). *Usos, retos y oportunidades de la inteligencia artificial en el Ejército. De Lege Ferenda.* https://doi.org/10.30827/dlf.1.2023.28553

Pilkington, M. (2016). *Blockchain technology: Principles and applications. Research Handbook on Digital Transformations*, 225-253. https://doi.org/10.4337/9781788970067.00017

Pulido, Guillermo. (2023). *Guerra Multidominio y Mosaico. Bogotá: Villegas Editores.*

República de Colombia. (2017). *Ley 1862 de 2017. Código Disciplinario Militar*.

Sharkey, Noel. (2010). *Saying "No!" to Lethal Autonomous Targeting. Journal of Military Ethics, 9*(4), 369-383.

Sharkey, Noel. (2020). The impact of autonomous weapons systems on human rights. Oxford University Press.

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Portfolio.

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

United Nations Institute for Disarmament Research (UNIDIR). (2017). Artificial Intelligence and the Future of Warfare. Geneva: UNIDIR. https://unidir.org/publication/artificial-intelligence-and-future-warfare

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. https://unesdoc.unesco.org

**Vigevano, M. R. (2021*).* Inteligencia artificial aplicable a los conflictos armados: Límites jurídicos y éticos. *Arbor,* 197(800). https://doi.org/10.3989/arbor.2021.800002

Zwitter, A., & Boisse-Despiaux, M. (2020). Blockchain for Humanitarian Action and Development IA. Journal of International Humanitarian Action, 5(1), 1–12. https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-3

Corte Constitucional de Colombia. (2023). *Sentencia T-190 de 2023*. M.P. Juan Carlos Cortés González.

C**orte Constitucional de Colombia. (2022).** *Sentencia T-282 de 2022*. M.P. Antonio José Lizarazo Ocampo.

Corte Constitucional de Colombia. (2012). *Sentencia C-239 de 2012*. M.P. Jorge Iván Palacio Palacio.

Corte Constitucional de Colombia. (2011). *Sentencia C-748 de 2011*. M.P. María Victoria Calle Correa.

Corte Constitucional de Colombia. (2021). *Sentencia SU-146 de 2021*. M.P. Antonio José Lizarazo Ocampo.

Corte Constitucional de Colombia. (2016). Sentencia C-084 de 2016. M.P. Bogotá: Sala Plena.

ANEXO TÉCNICO — PLAN ESTRATÉGICO Y PLAN DE NEGOCIO PARA EL CENTRO DE SUPERVISIÓN DIGITAL DE DERECHOS HUMANOS Y DIH (CSD-DDHH/DIH)

Porque una propuesta sin presupuesto es como una brújula sin norte: tal vez señale algo... pero jamás llegará a puerto seguro.

I. Diagnóstico Estratégico Integrado (DOFA extendido)

Fortalezas	**Oportunidades**
- Legitimidad jurídica sustentada en jurisprudencia (T-092/2019, T-401/2020). - Experiencia operacional de la Armada en entornos complejos. - Existencia de doctrina ética y tecnológica emergente.	- Cooperación internacional con OTAN, CICR, ONU. - Recursos FONSET y cooperación técnica bilateral (Israel, Estonia). - Interés institucional en trazabilidad y control algorítmico.
Debilidades	**Amenazas**
- Brechas formativas en IA y Blockchain dentro del personal militar. - Infraestructura digital aún centralizada y fragmentada. - Poca interoperabilidad entre sistemas heredados.	- Riesgos de ciberseguridad si no se implementan redes cerradas. - Resistencia cultural a la trazabilidad interna. - Riesgo reputacional si no se ejecuta con transparencia.

II. Objetivo General del Plan Estratégico

Diseñar e implementar un subsistema institucional funcional, autónomo y auditable —el Centro de Supervisión Digital de Derechos Humanos y DIH— que articule las tecnologías de Inteligencia Artificial y Blockchain para garantizar en la Armada Nacional la legalidad, trazabilidad y responsabilidad operativa, alineadas con el Derecho Internacional Humanitario.

III. Ejes Estratégicos del Plan

1. **Eje Normativo y Ético:** Marco jurídico interno conforme al bloque de constitucionalidad (art. 93 CP) y Protocolo I de Ginebra.

2. **Eje Tecnológico:** Desarrollo de una arquitectura híbrida IA + Blockchain de tipo permissionada (Hyperledger Fabric).

3. **Eje Organizacional:** Creación del Centro como subsistema autónomo, adscrito funcionalmente a la Inspección General.

4. **Eje Financiero y Operativo:** Estructuración de un plan de negocio viable, escalable y auditable.

Gráfico de flujo del modelo de ejecución.

IV. Cotizaciones y Costeo Real Estimado (Año Fiscal 2025)

Concepto	Detalle técnico y funcional	Costo estimado (COP)
1. Infraestructura tecnológica inicial	4 servidores dedicados en red militar cerrada (Dell PowerEdge XR7620, RAID 10, 256GB RAM, 2 CPUs Intel Xeon Gold)	$520.000.000
2. Desarrollo de software IA + Blockchain	Arquitectura basada en Hyperledger Fabric con módulo forense y trazabilidad algorítmica.	$680.000.000
3. Personal especializado (año 1)	3 ingenieros IA/Blockchain, 1 auditor jurídico-algoritmo, 2 oficiales capacitados + soporte externo.	$450.000.000
4. Capacitación interna (mandos + operadores)	Curso certificado de 120 horas. Convenio con Universidad Nacional y ESDEGUE.	$120.000.000
5. Consultoría legal y certificación internacional	Protocolo ONU + asesoría MIT Media Lab / CCDCOE-OTAN (virtual/híbrido).	$180.000.000
6. Gastos generales (hosting, licencias, soporte)	Licencias, mantenimiento, upgrades, backup militar.	$100.000.000
TOTAL INICIAL AÑO 1		**$2.050.000.000 COP** (≈ **US$ 523.000** aprox.)

Porque la transparencia no se improvisa: se diseña, se financia y se blinda... ¡con Blockchain y con voluntad!

V. Modelo de Negocio (Canvas adaptado a sector defensa)

Elemento	Detalle
Segmentos clave	Armada Nacional; Comando General; Ministerio de Defensa; organismos internacionales de control.
Propuesta de valor	Supervisión institucional digital, trazabilidad ética y reducción del riesgo jurídico-operacional.
Canales	Plataforma digital de monitoreo; informes forenses; acceso restringido por claves militares.
Relación con usuarios	Formal, auditable, de alta seguridad y con enfoque de control cruzado.
Actividades clave	Supervisión en tiempo real; auditoría forense algorítmica; generación de alertas jurídicas.
Recursos clave	Plataforma IA + Blockchain; personal interdisciplinario; red privada cifrada.
Socios estratégicos	CICR, MIT, CCDCOE, Universidad Nacional, Ministerio de Justicia, ACNUDH.
Estructura de costos	Infraestructura, personal, licencias, formación continua, mantenimiento.
Fuentes de financiación	FONSET, PISCC, cooperación internacional, presupuesto defensa 2025-2027.

VI. Cronograma de Ejecución (Fases Trimestrales)

Fase	Actividad	Duración	Responsable
Fase 1	Diseño técnico-jurídico y socialización	T1 - 2026	JEMCO + Dirección DD.HH.
Fase 2	Desarrollo e integración IA-Blockchain	T2 - 2026	Jefatura de Tecnología
Fase 3	Capacitación e implementación piloto	T3 - 2026	Dirección de Talento Humano
Fase 4	Evaluación, ajustes y despliegue nacional	T4 - 2026	Inspección General

VII. Indicadores de Impacto (KPIs)

- % de decisiones operativas con trazabilidad validada: **Meta año 1: 70%**
- **de auditorías jurídicas digitales realizadas por semestre: Meta: 6**
- **de alertas emitidas y resueltas éticamente: Meta: ≥12 anuales**
- Nivel de aceptación institucional: **Meta: 85% satisfacción**

VIII. Mejoras Estratégicas Adicionales

Aunque el presente plan cumple con los estándares requeridos para su viabilidad e implementación, se han identificado cuatro áreas clave en las que puede fortalecerse aún más su contenido estratégico y técnico:

1. **Proyección Financiera Trienal (2025–2027)**

   Se recomienda incluir una proyección financiera de tres años que contemple:

- Inversión inicial
- Costos de operación y mantenimiento
- Escalabilidad tecnológica
- Retorno en términos de eficiencia operativa y reducción del riesgo jurídico

   Una proyección de este tipo no solo fortalece el análisis de viabilidad institucional, sino que permite anticipar necesidades presupuestales y justificar la sostenibilidad del proyecto ante entes financiadores nacionales e internacionales.

2. Matriz de Riesgos con Plan de Mitigación

La inclusión de una matriz de riesgos detallada —clasificada por categorías (jurídicos, tecnológicos, operacionales y de percepción)— con medidas de mitigación asignadas a cada uno, fortalece la resiliencia institucional. Esta matriz debe incluir:

- Probabilidad de ocurrencia
- Impacto estratégico
- Responsables del control
- Plan de contingencia

> *¡Porque incluso la mejor arquitectura institucional puede naufragar si no anticipa la tormenta de los imprevistos!*

3. Estimación de Retorno Social/Institucional

Un análisis cualitativo del retorno institucional de esta inversión permitiría estimar:

- Impacto en la legitimidad operativa
- Aumento de la transparencia
- Fortalecimiento del principio de responsabilidad del mando

Esta evaluación puede alinearse con indicadores del Objetivo de Desarrollo Sostenible 16 (Paz, Justicia e Instituciones Sólidas), facilitando sinergias con agencias de cooperación internacional.

4. Estrategia de Comunicación Institucional

Se requiere un plan estratégico de comunicaciones que visibilice:

- El funcionamiento del centro ante actores clave
- Su compatibilidad con principios democráticos y de control civil
- Los mecanismos de auditoría y responsabilidad

La comunicación no es un accesorio político, sino un blindaje institucional frente a interpretaciones erróneas. Informar antes que justificar... siempre será mejor.

IX. Referencias

- Corte Constitucional de Colombia. (2019). *Sentencia T-092/2019*. https://www.corteconstitucional.gov.co/relatoria/2019/T-092-19.htm

- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

- Palomo Zurdo, R. (2018). *Blockchain y trazabilidad institucional: retos en el entorno público*. Revista Española de Transparencia, 8(2), 45-62.

- MIT Media Lab. (2020). *Blockchain and Public Accountability in Military Decision-Making*. Cambridge, MA.

- Sharkey, N. (2020). *The Impact of Autonomous Military Systems on Human Rights*. Oxford Review of Ethics, 12(1), 1-22.

- UNESCO. (2021). *Ethics of Artificial Intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000381137

- Centre for Data Ethics and Innovation. (2020). *AI Barometer Report*. UK Government. https://www.gov.uk/government/publications/cdei-ai-barometer

-