

CLAVES CEEYPP — PANORAMA PARA LA DECISIÓN · N° 4

Importancia de la IA en la construcción de una estrategia para el manejo del conflicto armado interno en Ecuador

Dr. Norberto Emmerich

Centro de Estudios en Estrategia y Políticas Públicas — Septiembre de 2026

Resumen

Ecuador enfrenta un conflicto armado interno no internacional contra organizaciones criminales que controlan corredores estratégicos de narcotráfico y ejercen violencia sistemática en diversas provincias. En este contexto, la inteligencia artificial emerge como un elemento clave para la estrategia de seguridad estatal, manifestándose principalmente a través del uso de drones con capacidades de vigilancia avanzada, análisis de datos e inteligencia predictiva. Este paper analiza cómo la IA está siendo incorporada en la estrategia ecuatoriana, sus resultados operativos documentados, los riesgos asociados a su implementación y los desafíos normativos pendientes, a partir de la evidencia disponible sobre operaciones militares, cooperación internacional y debate académico. Se argumenta que, aunque la IA ofrece ventajas tácticas significativas —como la mejora del 70% en precisión de intervenciones documentada en Ponce Enríquez—, su integración efectiva requiere un marco de gobernanza que aborde las limitaciones estructurales del Estado, los riesgos para derechos fundamentales y la necesidad de fortalecer la inteligencia humana más que reemplazarla.

Palabras clave: inteligencia artificial, conflicto armado interno, Ecuador, drones, seguridad, crimen organizado, gobernanza tecnológica.

1. Introducción

Ecuador declaró en enero de 2024 un conflicto armado interno, reconociendo que las organizaciones criminales —principalmente Los Choneros y Los Lobos— habían alcanzado un nivel de capacidad operativa que desafiaban el control soberano del Estado en amplias zonas del territorio, especialmente la frontera norte y el litoral pacífico ecuatorianos. El país, por donde transita aproximadamente el 70% de la cocaína que llega a los mercados internacionales de consumo, ha visto cómo los homicidios intencionales superan los 9 mil el pasado año 2025 con una tasa de 51,9 homicidios cada 100 mil habitantes, manteniéndose en un nivel superior a los 7 mil homicidios anuales en los últimos y recientes años. Más importante que eso, el control territorial se ha fragmentado en corredores que abarcan puertos, fronteras y economías locales fuertemente penetradas por el crimen organizado.

En este escenario de asimetría operativa, la tecnología ha pasado a ocupar un lugar central en la estrategia gubernamental. La inteligencia artificial, en particular, se presenta como una herramienta con potencial para optimizar la inteligencia, la vigilancia y la capacidad de respuesta estatal. Sin embargo, su incorporación no está exenta de tensiones: desde la dependencia tecnológica de proveedores externos hasta los riesgos para la privacidad y los derechos fundamentales, pasando por las limitaciones de una regulación que avanza más lento que la innovación, alimentada por la competencia mundial por el dominio de datos.

Este artículo examina el rol de la IA en la estrategia de manejo del conflicto armado interno ecuatoriano a partir de la evidencia disponible sobre su implementación, los resultados operativos documentados y los debates en torno a su gobernanza. La pregunta que guía el análisis es: ¿de qué manera la IA contribuye efectivamente a la estrategia estatal y cuáles son los límites y riesgos que deben abordarse para que su uso sea legítimo y sostenible?

2. Marco conceptual: la IA aplicada a la seguridad en contextos de conflicto

2.1 Definición operativa de la IA en seguridad

En el ámbito de la seguridad y defensa, la inteligencia artificial abarca un conjunto de tecnologías que permiten a los sistemas procesar grandes volúmenes de información, identificar patrones, apoyar la toma de decisiones y, en algunos casos, operar con cierto grado de autonomía. Sus aplicaciones incluyen el análisis de

inteligencia, la vigilancia automatizada, el reconocimiento facial, la ciberseguridad y el apoyo a operaciones tácticas.

La literatura especializada distingue entre sistemas de IA "asistiva" —que apoyan decisiones humanas— y sistemas "autónomos" —que pueden ejecutar acciones sin intervención humana directa—. Esta distinción es crucial para el análisis ético y jurídico de su uso en conflictos armados.

2.2 El contexto ecuatoriano: un conflicto híbrido

El conflicto que enfrenta Ecuador tiene características de guerra híbrida: combina tácticas militares con actividades criminales, control territorial, economías ilícitas y capacidades tecnológicas crecientes por parte de los actores no estatales. Las organizaciones criminales han demostrado capacidad para modificar drones comerciales para el transporte de armas y explosivos, los sistemas de comunicación encriptada y la vigilancia de los movimientos policiales. Esta tecnologización del crimen plantea un desafío de asimetría que el Estado busca compensar mediante la adopción de herramientas avanzadas, incluyendo la IA.

3. Implementación de la IA en la estrategia ecuatoriana

3.1 Uso de drones con capacidades de IA

La principal manifestación de la IA en la estrategia de seguridad ecuatoriana se da a través del uso de vehículos aéreos no tripulados (drones) equipados con sensores avanzados y capacidades de procesamiento de información. Las Fuerzas Armadas han incorporado equipos como el DJI Matrice 30T y el DJI DOCK 2, que cuentan con cámaras térmicas, telémetros láser y sistemas de vigilancia continua en condiciones climáticas adversas.

Según información documentada de operaciones militares en el cantón de Ponce Enríquez (el más peligroso de Ecuador, en la provincia de Azuay), el uso de estas tecnologías mejoró la precisión de las intervenciones en un 70%. Los drones permitieron realizar un buen reconocimiento aéreo en zonas de difícil acceso, identificar los movimientos de grupos armados (Los Lobos) y coordinar las operaciones tácticas con las unidades terrestres. Los equipos, diseñados para operar de forma permanente, brindaron percepción situacional a los equipos de combate y permitieron enfocar y dirigir los esfuerzos hacia objetivos claramente identificados como operativamente rentables.

3.2 Cooperación internacional y transferencia tecnológica

La incorporación de estas capacidades ha recibido un apoyo significativo de Estados Unidos, que en el marco de una visita del secretario de Estado Marco Rubio anunció una asistencia cercana a los 20 millones de dólares, de los cuales seis millones se destinaron específicamente a aportar drones para la Armada ecuatoriana. Además, Washington calificó y designó a grupos como Los Choneros y Los Lobos como organizaciones terroristas extranjeras, aproximando el combate al narcotráfico a la lógica propia de la guerra contra el terrorismo.

Este respaldo se enmarca en una transformación doctrinal más amplia: la creación del Southcom Autonomous Warfare Command (SAWC), que tiene la misión de integrar capacidades autónomas en operaciones en América Latina. Ecuador se ha convertido en uno de los primeros receptores visibles de esta estrategia, que incorpora parte de las lecciones aprendidas en el terreno de Ucrania, donde los drones comerciales modificados se han convertido en un insumo central de la guerra territorial contemporánea.

3.3 Inteligencia de datos y análisis predictivo

Más allá del uso táctico de drones, la nueva estrategia de seguridad gubernamental —identificada como "Ofensiva Total"— contempla la inteligencia de datos como uno de sus pilares críticos. La idea es cruzar

información proveniente de fuentes militares y civiles para identificar patrones de criminalidad y anticipar los movimientos de las organizaciones. En esta línea, algunos proyectos académicos como el RedLLM-Integrator, desarrollado por la Universidad San Francisco de Quito, proponen fortalecer los Centros de Operaciones de Seguridad mediante la integración de herramientas de IA explicativa para la identificación de vulnerabilidades y la generación de recomendaciones en formato textual, comprensibles en seguridad digital.

Sin embargo, la implementación efectiva de esta dimensión analítica enfrenta obstáculos estructurales. El más crítico es la opacidad de las fuentes primarias de información: el profundo desfase entre la criminalidad real y la registrada —lo que la literatura denomina 'cifra negra'— alcanza proporciones masivas en Ecuador. Según datos de victimización, nueve de cada diez ciudadanos no denuncian los delitos, lo que no solo priva al Estado de información fiable para el diseño de políticas, sino que distorsiona cualquier modelo predictivo al ocultar las dinámicas reales del conflicto y generar un vacío de inteligencia que ningún algoritmo puede suplir por sí solo.

En este sentido, la efectividad de la inteligencia artificial en el ámbito de la seguridad no depende exclusivamente de la sofisticación algorítmica, sino que sigue siendo fundamental la capacidad del Estado para capturar y sistematizar información veraz en el territorio. Sin una reducción sostenida de la cifra negra, los modelos predictivos operarán inevitablemente sobre un mapa incompleto de la criminalidad, lo que limita su utilidad táctica y estratégica.

Esta limitación revela una cuestión de fondo que trasciende lo técnico: el uso de inteligencia artificial en el manejo del conflicto armado no exime al Estado de sus obligaciones soberanas en materia de generación, custodia y administración de información. Por más avanzados que sean los algoritmos y las plataformas de vigilancia, estos operan sobre datos que deben ser producidos, validados y actualizados por instituciones estatales con presencia territorial efectiva. La soberanía de datos —entendida como la capacidad del Estado para capturar información veraz, procesarla con criterios propios y tomar decisiones fundamentadas en ella— no puede ser externalizada ni a proveedores tecnológicos extranjeros ni a sistemas automatizados. La IA puede asistir, acelerar y optimizar, pero no puede reemplazar la responsabilidad central del Estado de construir inteligencia a partir del territorio, de garantizar canales de denuncia confiables y de articular políticas públicas que trasciendan la lógica reactiva del combate inmediato.

4. Resultados operativos documentados

4.1 Caso Ponce Enríquez

La operación militar en Ponce Enríquez, en Azuay, que había experimentado altos niveles de violencia vinculada a la minería ilegal y el control territorial por grupos armados, constituye el caso más documentado de uso exitoso de tecnologías con IA. Durante las operaciones, se recabó información mediante drones que permitió identificar el ingreso de grupos armados a minas, sus tácticas de engaño para confundirse con trabajadores mineros y sus rutas de desplazamiento.

Los resultados incluyeron la reducción significativa de las muertes violentas y de homicidios en el cantón, así como el establecimiento de un régimen de trabajo permanente con la Agencia de Regulación y Control Minero y el Ministerio del Ambiente. La operación permitió determinar la existencia de una conflictividad social entre empresas mineras legales e ilegales, que derivaba en episodios de conflicto armado por las relaciones con grupos como Los Lobos y Lobos SAO BOX.

4.2 Capturas de cabecillas

Según la información oficial, los operativos que culminaron con las capturas de alias Sampayo, en Machala, y alias Churrón, en Guayaquil, contaron con el apoyo de los sistemas de vigilancia aérea que permitieron

monitorear objetivos en tiempo real y coordinar acciones terrestres con mayor precisión. Estos casos evidencian que los drones ya no son recursos complementarios, sino herramientas centrales para la obtención de información, el seguimiento de sospechosos y la vigilancia de zonas consideradas de alto riesgo.

5. Riesgos, limitaciones y desafíos

5.1 La ilusión de precisión y el problema de la inteligencia humana

Uno de los riesgos más significativos documentados en la literatura es lo que podría denominarse la "ilusión de precisión": la creencia de que la superioridad tecnológica resuelve los problemas fundamentales de identificación de objetivos y toma de decisiones. La experiencia estadounidense en Afganistán y Yemen mostró que los sistemas de vigilancia más sofisticados continúan dependiendo de información humana imperfecta, como hemos mencionado. Los errores de identificación, los daños colaterales y la opacidad en la cadena de decisiones no desaparecen por el hecho de incorporar nuevas plataformas. Como señala un análisis especializado, "el problema central sigue siendo político y jurídico, no tecnológico".

En el caso ecuatoriano, esta advertencia es particularmente relevante dado el contexto de debilidad institucional y la dificultad para distinguir entre actores criminales y población civil en zonas donde el control territorial es difuso.

5.2 Riesgos para los derechos fundamentales

La incorporación de IA y sistemas avanzados de vigilancia plantea riesgos para la privacidad y otros derechos fundamentales. Los expertos en ciberseguridad advierten que "la tecnología de vigilancia puede amenazar la privacidad de todos" y que el cruce de datos militares con información civil debe manejarse con extrema precaución para prevenir abusos como la discriminación y la vigilancia masiva.

Se ha propuesto la creación de una "gobernanza externa" híbrida (civil-política) que supervise que los datos se empleen exclusivamente para fines de seguridad y que garantice la legitimidad de los procesos. La confianza pública, se argumenta, será crucial para el éxito de estas iniciativas.

5.3 Limitaciones legales y regulatorias: la tensión entre libertad y seguridad

La implementación de la IA en seguridad enfrenta tensiones con el marco legal vigente. La Corte Constitucional suspendió algunos artículos de la Ley Orgánica de Inteligencia y su reglamento, lo que según analistas impacta significativamente en el desarrollo de las operaciones militares. Las restricciones incluyen limitaciones para el uso de herramientas tecnológicas en el espectro electromagnético sin autorización judicial, así como para actividades secretas de inteligencia.

Esta tensión refleja un desafío más amplio: mientras la tecnología avanza a gran velocidad, la legislación suele hacerlo a un ritmo mucho más lento. Para que el uso de IA sea legítimo y sostenible, se requiere una regulación adecuada que garantice su uso responsable y ético, previniendo abusos y estableciendo mecanismos claros de rendición de cuentas.

Esta disociación entre el despliegue tecnológico y el desarrollo normativo no es un fenómeno accesorio, sino una manifestación de una brecha estructural que caracteriza la gobernanza de la IA en Ecuador. Mientras el Estado incorpora sistemas de inteligencia artificial en áreas sensibles como la contratación pública, la videovigilancia y el control fiscal —a menudo mediante decretos ejecutivos y resoluciones sectoriales dispersas—, el marco legal integral que debería ordenar, fomentar y limitar estos usos permanece en un prolongado estancamiento legislativo. El proyecto de ley orgánica de IA, gestado desde 2024 a partir de la fusión de tres iniciativas, acumula más de dos años de trámite y enfrenta ahora un riesgo inminente de archivo: el 31 de agosto de 2026, la Comisión de Educación de la Asamblea Nacional recomendó su desestimación por considerarlo 'sobre-regulatorio' y con posibles obstáculos para la innovación, decisión que

deberá ser resuelta por el Pleno. Esta parálisis legislativa contrasta con la creciente actividad normativa de segundo nivel —como la resolución de la Superintendencia de Protección de Datos Personales sobre IA y la Estrategia Nacional EFIA-EC—, instrumentos que, si bien llenan vacíos puntuales, no sustituyen el debate democrático ni la definición soberana de estándares, responsabilidades y límites que solo una ley puede proporcionar. El resultado es un escenario paradójico: el Estado ecuatoriano avanza en la adopción de IA sin una regulación que le exija transparencia, rendición de cuentas o evaluación de impacto específica, mientras una ley que podría ordenar este proceso se debate entre la necesidad de fomento y el temor a la sobreregulación, dejando al país en un interregno jurídico que la propia tecnología no espera.

El eventual archivo de la ley de IA, sin embargo, no constituye el principal obstáculo jurídico para el despliegue operativo de las Fuerzas Armadas en el contexto del conflicto armado interno. La limitación más inmediata y gravosa proviene de otra fuente: la suspensión parcial de la Ley Orgánica de Inteligencia por parte de la Corte Constitucional, que ha anulado disposiciones clave para la obtención de información sensible. Esta decisión restringe el uso de herramientas tecnológicas en el espectro electromagnético sin autorización judicial, limita el acceso a datos de empresas de telecomunicaciones y anula la flexibilidad presupuestaria para operaciones encubiertas, todo ello en un escenario donde la velocidad y la precisión de la inteligencia son factores críticos. El resultado es un dilema que tensiona la eficacia operativa con el imperativo de control constitucional: mientras la suspensión busca prevenir abusos y garantizar derechos fundamentales, reduce la capacidad estatal para anticipar y neutralizar amenazas en un conflicto asimétrico. La paradoja es que, en la práctica, las FF.AA. enfrentan más restricciones legales para obtener información que para utilizar sistemas de IA en el procesamiento de la que ya poseen, lo que revela que el verdadero cuello de botella no es tecnológico ni normativo en materia de IA, sino la tensión no resuelta entre seguridad y libertad en el marco legal de la inteligencia.

El uso de IA en el conflicto armado interno no es, en última instancia, un problema tecnológico, sino una pregunta sobre el tipo de Estado que se quiere construir. Si la tecnología expande la capacidad de vigilancia estatal, también debiera expandir los mecanismos de control y rendición de cuentas. Esta tensión entre seguridad y libertad, clásica en la filosofía política, adquiere en el contexto ecuatoriano contornos inéditos que merecen un análisis aparte.

5.4 Dependencia tecnológica y soberanía

La transferencia tecnológica desde Estados Unidos, si bien aporta capacidades inmediatas, genera una dependencia estratégica. América Latina carece de una industria propia comparable a la estadounidense en el ámbito de sistemas autónomos y drones, lo que limita la autonomía de los países para desarrollar y mantener estas capacidades sin apoyo externo. Esta dependencia tiene implicaciones no solo operativas sino también políticas, al condicionar las alianzas internacionales y la capacidad de decidir soberanamente sobre el uso de estas herramientas.

5.5 La tecnologización del crimen: el dilema de seguridad

Un desafío adicional es que la incorporación de IA por parte del Estado puede generar una dinámica de escalada tecnológica con las organizaciones criminales. La evidencia disponible indica que el crimen organizado también está implementando herramientas tecnológicas para controlar territorios, incluyendo drones modificados, sistemas de comunicación encriptada y análisis de información geoespacial. Si bien no existe información pública concluyente sobre un uso sistemático de IA por parte de estas organizaciones, se identifican indicios de una adopción progresiva que podría acelerarse como respuesta a la presión estatal.

Esta dinámica plantea un dilema estratégico de primer orden: el Estado puede verse atrapado en una carrera tecnológica de rendimientos decrecientes, donde cada inversión en vigilancia y precisión operativa estimula una adaptación criminal equivalente o superior, sin que ello se traduzca necesariamente en una reducción

sostenida de la violencia. El resultado es una espiral en la que la tecnología, lejos de ser una solución, se convierte en un factor que eleva el costo del conflicto, profundiza la dependencia de proveedores externos y erosiona la legitimidad estatal si la ciudadanía no percibe mejoras tangibles en su seguridad. En este escenario, la IA no elimina la asimetría estructural entre el Estado y el crimen organizado; la traslada a un terreno donde las organizaciones criminales, por su naturaleza adaptativa y su menor sujeción a controles legales, pueden incluso tener ventaja.

La incorporación de la inteligencia artificial en el ámbito de las operaciones militares no constituye una mera actualización tecnológica, sino una mutación en la naturaleza misma del conflicto. No se trata de una guerra con elementos agregados —más precisión, más velocidad, más datos—, sino de una guerra diferente: una contienda donde el centro de gravedad se desplaza del territorio físico al dominio informacional, donde la temporalidad de la decisión se acelera hasta límites inhumanos y donde la agencia humana se ve progresivamente desplazada por sistemas autónomos. Esta transformación es tan profunda que cabe preguntarse si no estamos asistiendo, más que a una nueva forma de hacer la guerra, a una guerra sobre la guerra misma: una lucha por definir quién controla los algoritmos, quién posee los datos y quién tiene la capacidad de interpretarlos. En este nuevo escenario, el adversario ya no es solo el combatiente armado, sino también el sistema que lo detecta, el dato que lo anticipa y la red que lo conecta.

6. Hacia una estrategia integral: más allá de la tecnología

6.1 La necesidad de soluciones estructurales

Expertos en seguridad han señalado que la militarización y el despliegue de tropas son estrategias coyunturales que no ofrecen resultados sostenibles a largo plazo. La nueva estrategia gubernamental debe buscar soluciones estructurales que incluyan no solo el uso de tecnología, sino también la presencia estatal efectiva en el territorio, la inversión en servicios públicos en barrios estratégicos y el fortalecimiento del tejido social a través de educación y salud.

La diferencia fundamental entre las estrategias previas y la actual, según este análisis, radica en el alcance: mientras que el "Plan Fénix" planteó el choque para responder a una crisis inmediata, la nueva propuesta busca un establecimiento real en el territorio. La IA puede ser una herramienta valiosa en este proceso, pero no sustituye la necesidad de inteligencia humana, presencia institucional y políticas sociales.

6.2 Gobernanza colaborativa e interoperabilidad

La literatura especializada resalta que el Ecuador enfrenta debilidades estructurales en la interoperabilidad institucional y en las capacidades de ciberdefensa del Estado. Se requiere una transición de una gobernanza jerárquica a una "gobernanza colaborativa", en la que el Estado, la academia, la ciudadanía y el sector privado trabajen en conjunto. El sector privado, en particular, no debe ser visto únicamente como un financiador, sino como un aliado estratégico que posee información clave sobre lo que sucede en puertos, aeropuertos y comercios.

6.3 Securitización de la IA y agenda de seguridad nacional

Investigaciones al interior de las Fuerzas Armadas ecuatorianas han señalado la necesidad de incorporar la inteligencia artificial en la agenda de seguridad nacional, tanto para prevenir su uso indebido como para convertirla en un activo estratégico. Esta recomendación, sin embargo, contrasta con la ausencia del concepto en los documentos de direccionamiento del sector defensa —el Libro Blanco de la Defensa de 2018 y los planes sectoriales posteriores—, lo que evidencia un vacío de planificación institucional que la adopción tecnológica ya está desbordando. Incorporar la IA a la estrategia de seguridad implica, en la práctica, tres desafíos concurrentes: establecer un marco normativo que regule su uso en el ámbito de la defensa, garantizar la protección de datos y la rendición de cuentas, y formar al personal militar en el manejo

ético y efectivo de estas herramientas.

La incorporación de la IA en la agenda de seguridad nacional no puede limitarse al ámbito militar, pues su uso civil ya es una realidad extendida y en acelerada expansión dentro del Estado ecuatoriano. El Servicio de Rentas Internas la emplea para la detección de evasión fiscal, el Instituto Ecuatoriano de Seguridad Social para la gestión predictiva de servicios, el ECU 911 para la videovigilancia automatizada y el Servicio Nacional de Contratación Pública para la identificación de riesgos en compras estatales, mientras municipios como Cuenca operan sistemas de lectura de placas con IA. Este despliegue, sin embargo, ocurre sin un marco legal integral que lo regule, lo que genera un vacío que la agenda de seguridad no puede ignorar. Integrar el uso civil en esta agenda no implica militarizar su gestión, sino reconocer su impacto estratégico y establecer una gobernanza clara que defina protocolos de interoperabilidad entre entidades de defensa y seguridad ciudadana, garantice la protección de datos y los derechos fundamentales, y cree mecanismos de rendición de cuentas con supervisión híbrida —civil, política y técnica— que aseguren la legitimidad democrática de estas herramientas en un Estado que ya las está utilizando sin la discusión pública que su relevancia exige.

Una regulación integral no solo ordenaría estos usos, sino que potenciaría su capacidad para prevenir la corrupción, un beneficio que ya comienza a vislumbrarse en la práctica: el Servicio Nacional de Contratación Pública (Sercop) ha incorporado IA para identificar patrones de riesgo en compras estatales, el Servicio de Rentas Internas la emplea para detectar la evasión fiscal, la Contraloría la utiliza para seleccionar declaraciones juramentadas con posibles irregularidades patrimoniales y el Servicio Nacional de Aduana ha logrado un incremento del 15% en la recaudación mediante sistemas automatizados de análisis de riesgo. Sin embargo, estas experiencias —calificadas oficialmente como "aisladas y sin una estrategia coordinada" — operan sin un marco común que garantice transparencia algorítmica, evaluación de impacto o mecanismos de impugnación. Una ley abarcativa convertiría estas iniciativas dispersas en un sistema articulado de control, donde la IA no solo detecte irregularidades, sino que rinda cuentas sobre cómo lo hace.

7. Conclusiones

La inteligencia artificial está adquiriendo una importancia creciente en la estrategia de manejo del conflicto armado interno en Ecuador, principalmente a través del uso de drones con capacidades de vigilancia y apoyo táctico. La evidencia disponible muestra que estas herramientas han contribuido a mejorar la precisión de las intervenciones militares y la capacidad de monitoreo estatal, como se documentó en las operaciones en Ponce Enríquez y en las capturas de cabecillas criminales.

Sin embargo, su incorporación no está exenta de riesgos y limitaciones. La ilusión de precisión que generan los sistemas tecnológicos no resuelve los problemas fundamentales de inteligencia humana e identificación de objetivos. El uso de IA plantea riesgos para los derechos fundamentales que requieren una regulación adecuada y mecanismos de control híbridos. La dependencia tecnológica de proveedores externos limita la soberanía estatal, mientras que la tecnologización del crimen puede generar una dinámica de escalada.

El desafío central para Ecuador no es tecnológico sino político y jurídico. La IA puede ser una herramienta valiosa para fortalecer la inteligencia y la capacidad de respuesta estatal, pero su efectividad depende de la existencia de un Estado con presencia territorial efectiva, instituciones interoperables, una regulación que equilibre seguridad y derechos, y estrategias sociales que aborden las causas estructurales del conflicto. La tecnología, por sí misma, no puede reemplazar la necesidad de gobernanza colaborativa, inteligencia humana y soluciones sostenibles en el territorio.

Referencias

Academia de Guerra del Ejército Ecuatoriano. (2026a). Integración de aprendizaje automático en sistemas de vigilancia y reconocimiento militar: un desafío para la garantía de la seguridad en Ecuador. Revista de la Academia de Guerra del Ejército

Ecuatoriano, 19(01), 11. <https://doi.org/10.24133/AGE.VOL19.N01.2026.13>

- Academia de Guerra del Ejército Ecuatoriano. (2026b). Análisis de las interacciones entre la inteligencia artificial y las redes criminales en la frontera norte del Ecuador. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, 19(01), 13. <https://doi.org/10.24133/AGE.VOL19.N01.2026.06>
- Benalcázar, M. (2026, 4 de septiembre). Archivar la ley y no el desarrollo de IA en Ecuador. *El Comercio*. <https://www.elcomercio.com/opinion/desarrollo-inteligencia-artificial-ecuador-marco-benalcazar-columnista/>
- Diario Extra. (2026, 12 de agosto). Guerra de drones en Ecuador: cómo el crimen y el Estado pelean el control aéreo. *Diario Extra*. <https://www.extra.ec/noticia/ecuador/guerra-drones-ecuador-crimen-pelean-control-aereo-160401.html>
- Diario Los Andes. (2026, 25 de junio). Mujeres militares reforzarán controles contra organizaciones delictivas. *Diario Los Andes*. <https://diariolosandes.com.ec/mujeres-militares-reforzaran-controles-contra-organizaciones-delictivas/>
- Diario Red. (2026). Ecuador: primer ensayo de la guerra autónoma.
- El Universo. (2025). La CC y las FF. AA.
- El Universo. (2026, 31 de marzo). Ecuador y Estados Unidos refuerzan estrategias de seguridad con intercambio de inteligencia y nuevas tecnologías. *El Universo*. <https://www.eluniverso.com/noticias/seguridad/ecuador-y-estados-unidos-refuerzan-estrategias-de-seguridad-con-intercambio-de-inteligencia-y-nuevas-tecnologias-nota/>
- Expreso. (2026, 9 de agosto). Mafias más tecnológicas: ¿cómo se prepara el Ejército de Ecuador para enfrentarlas? *Diario Expreso*. <https://www.expreso.ec/justicia/mafias-tecnologicas-prepara-ejercito-ecuador-enfrentarlas-291967.html>
- Lexis Ecuador. (2026, 16 de abril). Asamblea Nacional aprueba proyecto de Ley Orgánica de Educación Financiera. *Lexis Ecuador*. <https://www.lexis.com.ec/noticias/asamblea-nacional-aprueba-proyecto-de-ley-organica-de-educacion-financiera>
- Mayorga-Sandoval, J. E. y Aldás-Benavides, A. M. (2025). La inteligencia artificial y su impacto en la seguridad del Estado ecuatoriano. *Revista Enfoques de la Comunicación*, (13), 226-260.
- Plan V. (2026). Seccionales del 2026, elecciones marcadas por la desconfianza.
- Programa FRIDA. (2025). RedLLM-Integrator: Fortalecimiento de SOCs a través de Integración Responsable de Agentes de IA y Transferencia de Capacidades. <https://programafrida.net/archivos/project/redllm-integrator-fortalecimiento-de-socs-a-traves-de-integracion-responsable-de-agentes-de-ia-y-transferencia-de-capacidades>
- Radio Pichincha. (2026). Nueva estrategia de seguridad del Gobierno debe buscar soluciones estructurales en territorio.
- Radio Pichincha. (2026). Daniel Noboa: "Vamos a iniciar una etapa de guerra total". *Radio Pichincha*. <https://www.radiopichincha.com/daniela-noboa-guerra-total/>
- Rauh, C., & Mueller, H. (2026). Impact: AI and conflict. University of Cambridge, Faculty of Economics. <https://www.econ.cam.ac.uk/impact/impact-ai-and-conflict>
- ReliefWeb. (2024, 28 de octubre). Utilising Artificial Intelligence and Open Source Intelligence for Conflict Prevention: Lessons Learned from Latin America and the Caribbean. <https://reliefweb.int/report/world/utilising-artificial-intelligence-ai-and-open-source-intelligence-osint-conflict-prevention-lessons-learned-latin-america-and-caribbean>
- Revista de la Academia de Guerra del Ejército Ecuatoriano. (2026). Análisis de las interacciones entre la inteligencia artificial y las redes criminales en la frontera norte del Ecuador.
- Revista de Seguridad y Defensa, ESPE. (2025). Operaciones militares en Ponce Enríquez: uso de tecnología e inteligencia artificial.
- Wiley Online Library. (2026). Artificial intelligence in conflict resolution and peacebuilding mechanisms. En *Implementing SDG 16 Goals with Artificial Intelligence*. <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394398355.ch14>