



ESPAÑA

**RESOLUCIÓN DE LA ASAMBLEA GENERAL
DE NACIONES UNIDAS (AGNU) 79/239 DE 31 DE DICIEMBRE DE 2024**

***LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO MILITAR Y SUS
IMPLICACIONES PARA LA PAZ Y LA SEGURIDAD INTERNACIONAL.***

ABRIL 2025

INTRODUCCIÓN

La Inteligencia Artificial (IA) supone una revolución en todos los ámbitos, y también lo es para la Seguridad y la Defensa. Su desarrollo e integración conlleva consigo grandes avances, oportunidades, a la vez que plantea numerosos retos.

El impacto del uso de la IA en el ámbito militar es de gran magnitud y tiene implicaciones directas en la paz y la seguridad internacionales. La adopción de esta tecnología en las Fuerzas Armadas no solo redefine la forma en que se llevan a cabo las operaciones militares, sino que también transforma el equilibrio estratégico global.

El desarrollo e implantación de la IA en el Ministerio de Defensa se basa en un uso militar responsable, ético y legítimo acorde al Derecho Internacional Humanitario (DIH) y al respeto a los Derechos Humanos.

La IA está modificando la concepción tradicional del poder militar y la seguridad, proporcionando capacidades avanzadas para la recopilación y análisis de datos, la toma de decisiones y la ejecución de operaciones en entornos multidominio. Esto implica un cambio de paradigma en la forma en que los Estados abordan la Defensa y la Seguridad, facilitando respuestas más rápidas y precisas ante amenazas emergentes.

En el ámbito militar, la IA está impactando de manera disruptiva en el imprevisible campo de batalla en el que las Fuerzas Armadas habrán de actuar para defender y salvaguardar los intereses nacionales, lo que significa un cambio de paradigma en el planeamiento y conducción de las operaciones militares, afectando de modo transversal a las actividades militares desarrolladas por las Fuerzas Armadas que derivan del cumplimiento de sus misiones. También está impactando en otras cuestiones dentro del ámbito militar: logística, entrenamiento, gestión e interpretación de información, inteligencia, vigilancia, adquisición de objetivos y reconocimiento.

Coherentemente con el compromiso de España con el uso responsable de la IA, cabe destacar la organización de la Cumbre sobre “Inteligencia Artificial Responsable en el Dominio Militar (REAIM)” de 2025 como nación anfitriona, además de su adhesión a la “Llamada a la Acción” (La Haya, 2023) y el Plan de Acción presentado en la pasada Cumbre en 2024 y a otros compromisos internacionales para el uso responsable de la IA.

MARCO CONCEPTUAL Y NORMATIVO EN EL MINISTERIO DE DEFENSA

Con relación al marco conceptual, el desarrollo, despliegue y aplicación de la IA en el Ministerio de Defensa están guiados por un conjunto de principios fundamentales que garantizan su uso seguro, ético y conforme a las normativas nacionales e internacionales. Estos principios buscan maximizar las oportunidades que ofrece la IA para la Defensa, al mismo tiempo que buscan mitigar los riesgos asociados a su implementación en el ámbito militar.

Estos principios se encuentran compilados en la “*Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa*”, desarrollada mediante la Resolución 11197/2023 de la Secretaría de Estado de Defensa, y están alineados con la Estrategia de IA de la OTAN de 2021 (y revisada en el 2024), y son los siguientes:

- **Legalidad:** las aplicaciones de IA se desarrollarán y emplearán de acuerdo con el derecho nacional e internacional que sea de aplicación, incluida la Declaración Universal de Derechos Humanos y el Derecho Internacional Humanitario.
- **Responsabilidad Humana y Rendición de Cuentas:** cualquier desarrollo de IA, así como su utilización, deberá permitir una clara supervisión humana con el fin de garantizar la debida rendición de cuentas y la atribución de responsabilidades.

- **Inteligibilidad y Trazabilidad:** las aplicaciones de IA serán comprensibles y transparentes para el personal relevante, incluyendo el uso de metodologías, fuentes y procedimientos auditables.
- **Fiabilidad y Transparencia:** las aplicaciones de IA estarán dirigidas a casos de uso explícitos, bien definidos y acotados y se proporcionará información para fomentar una comprensión general de estas aplicaciones por todas las partes interesadas. La seguridad, la protección y la solidez de estas capacidades estarán sujetas a pruebas y garantías dentro de estos casos de usos a lo largo de todo su ciclo de vida.
- **Gobernabilidad:** las aplicaciones de IA se desarrollarán y utilizarán de acuerdo con sus funciones previstas en el diseño, asegurando la capacidad de detectar y evitar consecuencias no deseadas. Se habilitarán mecanismos de desconexión o desactivación cuando se reconozcan comportamientos no previstos o indeseados.
- **Mitigación del Sesgo:** se tomarán todas las medidas necesarias para minimizar errores y orientaciones subjetivas en el desarrollo y aplicaciones de IA.
- **Privacidad:** el desarrollo, la implementación y el uso de aplicaciones basadas en IA deben respetar la privacidad de las personas, desde el diseño y durante todo el ciclo de vida.

Con respecto al marco normativo, para el desarrollo, implementación y uso de la IA en el ámbito militar dentro del Ministerio de Defensa se están elaborando un conjunto de normas y buenas prácticas que garantizan su aplicación responsable, eficiente y alineada con los marcos legales nacionales e internacionales, y en particular con el estricto cumplimiento con el DIH y los Derechos Humanos.

OPORTUNIDADES

El Ministerio de Defensa enfoca el desarrollo de sus capacidades en IA en múltiples áreas para mejorar la eficacia de las Fuerzas Armadas. Según la Estrategia, el uso de IA está enfocado a los ámbitos de operaciones, inteligencia, logística, ciberseguridad, así como al apoyo a la toma de decisiones.

La implantación de la IA en el ámbito militar ofrece un amplio abanico de oportunidades en diferentes ámbitos.

La IA permitirá incrementar la precisión, rapidez y efectividad en la toma de decisiones durante una operación militar siempre sujeta al DIH, en pos de una ejecución más eficiente de las misiones y reduciendo el riesgo para las tropas, así como contribuir a aumentar la protección de civiles y de los bienes de carácter civil en los conflictos armados.

Su capacidad para analizar grandes volúmenes de datos en tiempo real mejora la conciencia situacional y la capacidad de respuesta frente a amenazas, lo que refuerza la seguridad operativa. Toda esta mejora de capacidades siempre tiene presente el control humano, no delegando en las máquinas la responsabilidad.

En cuanto a formación y enseñanza militar, en el marco de la colaboración del grupo “C5 Commandants Group” de Escuelas de Estado Mayor Europeas (Gran Bretaña, Francia, Alemania, Italia y España), se está trabajando en la creación de un área de colaboración relativa a la IA en la enseñanza militar.

A su vez, se colabora con el grupo de trabajo DARB (*Data and AI Review Board*) de la OTAN para el uso responsable del dato y de la IA en el ámbito militar.

Por otra parte, el Ministerio de Defensa ha anunciado inversiones estratégicas en regiones específicas con el objetivo de impulsar proyectos relacionados con la IA y otras tecnologías avanzadas. Estas inversiones buscan no sólo fortalecer la industria, sino también promover la revitalización industrial de nuevas zonas regionales.

RETOS

El desarrollo y aplicación de la IA en el ámbito militar deben alinearse con marcos normativos nacionales e internacionales. Sin embargo, la rápida evolución de esta tecnología plantea desafíos regulatorios que deben ser atendidos. Actualmente el marco legal internacional se encuentra en desarrollo en relación con el uso de la IA en el ámbito militar.

Además, en relación con el imprescindible respeto al cumplimiento del DIH, se está trabajando para asegurar un control humano efectivo en decisiones críticas asociadas al empleo de la IA en operaciones militares.

Por otra parte, desde una perspectiva de Privacidad y Protección de Datos, la recopilación y procesamiento masivo de datos para entrenar modelos de IA plantea riesgos en materia de protección de datos personales y seguridad de la información.

Seguridad y fiabilidad

No obstante, el mayor reto se plantea en relación con el empleo seguro y fiable de la IA, siendo los principales riesgos asociados los siguientes:

- Los algoritmos de IA pueden presentar sesgos en los datos de entrenamiento, lo que puede llevar a decisiones erróneas o con consecuencias no deseadas.
- Un mal entrenamiento de los modelos de IA puede generar errores de interpretación, con consecuencias potencialmente catastróficas en operaciones militares.
- Los sistemas de IA pueden ser objetivo de ataques cibernéticos, que pueden manipular su comportamiento o inutilizarlos.
- Existe el riesgo de "envenenamiento de datos", donde actores malintencionados alteran los conjuntos de datos de entrenamiento para provocar fallos en los algoritmos.

En España, el desarrollo de la IA en el ámbito militar se rige por los principios de responsabilidad y supervisión continua, implementando mecanismos de evaluación de riesgos, auditoría y trazabilidad en cada fase del ciclo de vida del sistema. Además, se aplicarán protocolos de gobernanza y mecanismos de desconexión para prevenir usos indebidos y garantizar que la autonomía de los sistemas esté sujeta a un control humano. Cualquier desarrollo de IA, así como su utilización, deberá permitir una clara supervisión humana con el fin de garantizar la debida rendición de cuentas y la atribución de responsabilidades, dejando clara trazabilidad de las actuaciones humanas relacionadas y tomadas en paralelo con la actuación de la IA, y no delegando la decisión final en máquinas.

Se subraya también que la IA debe ser fiable y previsible, manteniendo un nivel de autonomía controlado y supervisado por operadores capacitados.

Cualquier solución de IA se revisará en un entorno diferente al que fue entrenado, y será sometido a pruebas no funcionales: carga, stress y rendimiento bajo escenarios cambiantes definidos, para estudiar su comportamiento y desviación permitida.

Además, estas capacidades de IA estarán sujetas a pruebas rigurosas y auditorías constantes a lo largo de todo su ciclo de vida, permitiendo la detección temprana de posibles errores y

mejorando su fiabilidad operativa. Se implementarán protocolos de supervisión y control humano en todas las fases de despliegue, asegurando que las decisiones críticas no sean delegadas exclusivamente a la IA. En este sentido, se está trabajando para que los desarrollos de IA sean certificados por entidades reconocidas.

Con objeto de mejorar la robustez de los sistemas basados en IA y protegerlos frente a acciones externas, es clave integrar la seguridad desde el diseño, garantizando que estos sistemas sean resistentes a ciberataques y manipulaciones adversarias, para asegurar la integridad de los datos y modelos utilizados.

Como advertimos anteriormente, la IA puede ser objetivo de ataques como el “envenenamiento de datos” o la manipulación de modelos, por lo que se requiere una monitorización continua del desempeño de los sistemas y la implementación de pruebas de validación y auditorías regulares. Se fomentará el desarrollo de planes de respaldo y recuperación ante fallos, garantizando la operatividad de los sistemas en escenarios adversos.

En relación con lo anterior, se promueve la colaboración con organismos de ciberseguridad y expertos en IA, asegurando que las Fuerzas Armadas cuenten con las mejores herramientas y estrategias para proteger estos sistemas de amenazas externas y asegurar su fiabilidad operativa.

Por otra parte, el talento y la formación del personal en estas tecnologías es crítico por lo que es contemplado como uno de los cuatro pilares¹ en los que pone el foco el Ministerio de Defensa.

Se recalca la importancia de la formación específica del personal, asegurando que los operadores comprendan el alcance y las limitaciones de estos sistemas y puedan intervenir en caso de desviaciones en su comportamiento. Para ello, la formación y sensibilización del personal en el uso legal y ético de la IA es clave para mitigar los riesgos asociados a los sesgos, asegurando que su empleo en las Fuerzas Armadas sea objetivo, fiable, y conforme a las normativas nacionales e internacionales, especialmente con el DIH.

Actualmente se está trabajando en una guía de buenas prácticas que podría ser la base de un documento al que contribuyan todos los ámbitos del Ministerio de Defensa. Aprovechando la participación en el grupo de trabajo DARB por parte de personal del Ministerio de Defensa, se han divulgado aquellas buenas prácticas que desde la OTAN se proponen para el uso responsable de la IA en el ámbito militar. Un ejemplo es el *“NATO Responsible AI (RAI) Assessment and Toolkit”*, cuyo propósito es operacionalizar los Principios de Uso Responsable de la IA adoptados por la OTAN, que incluyen legalidad, responsabilidad, trazabilidad, fiabilidad, gobernabilidad y mitigación de sesgos. Igualmente España asume y hace suyos los principios recogidos en la “Llamada a la Acción” (La Haya, 2023) y el “Plan de Acción” presentado en la pasada Cumbre REAIM de Seúl en 2024.

¹ Pilares de la Estrategia sobre IA del Ministerio de Defensa de 2023: 1. Gestión del dato, 2. Infraestructuras para la IA, 3. Investigación, desarrollo e innovación, y 4. Formación, captación y retención del talento.