

INFORME ESTRATÉGICO: II JORNADA DE INTELIGENCIA ARTIFICIAL RESPONSABLE EN EL ÁMBITO MILITAR

1. El Nuevo Paradigma de la Defensa: "Nubia" y la Gobernanza de la IA

El Ministerio de Defensa ha iniciado un salto cualitativo trascendental con la transición de la Infraestructura Integral de Información para la Defensa (I3D) hacia el modelo de **Nube Inteligente de la Defensa (Nubia)**. Este cambio de paradigma no constituye un mero trámite regulatorio, sino un **imperativo categórico** para garantizar la superioridad en el ciclo de decisión dentro de operaciones multidominio. En el actual teatro de operaciones, la gobernanza de la Inteligencia Artificial (IA) se erige como el centro de gravedad estratégico; no es una opción, sino una necesidad operativa donde la demora equivale a la irrelevancia. En defensa, alcanzar la "plata" no es un logro, sino una derrota estratégica: simplemente, no se puede quedar segundo. Nubia debe entenderse como un proceso de perfeccionamiento constante hacia un **modelo mínimo viable** que asegure la agilidad necesaria sin comprometer la integridad del sistema.

Basándose en el análisis forense del General de Brigada Luis Andrés Bárcenas sobre los estudios de **McKinsey** y los autores Pedreño y de Santes, se identifican los tres factores críticos que sentencian al fracaso al 90% de las implantaciones de IA:

- **Gobierno del dato deficiente:** La ausencia de una estructura que garantice la calidad, veracidad y disponibilidad del activo logístico más crítico.
- **Arquitecturas inexistentes o precarias:** La carencia de una base técnica robusta capaz de soportar el despliegue de modelos complejos y escalables.
- **Déficit de gobernanza integral:** La falta de marcos de responsabilidad, trazabilidad y control que permitan auditar el comportamiento de los sistemas bajo estándares militares.

Para mitigar estos riesgos, el ecosistema **Nubia** se cimenta sobre tres pilares de superioridad: el **Gobierno del dato**, la arquitectura de seguridad **Zero Trust** y una **IA bien gobernada**.

En cuanto a la implantación, el Ministerio distingue dos trayectorias estratégicas: la vía I3D/Nubia para servicios centralizados y los **Sistemas de Armas embebidos**. En estos últimos, se aplica una **evaluación de riesgos reversa**: mientras el CESTIC asume la responsabilidad técnica de evaluar la amenaza, es el usuario final —los Ejércitos o la Armada— quien ejerce su **autonomía operativa** para tomar la decisión soberana de despliegue en el campo de batalla.

Independientemente de la trayectoria, todo sistema debe integrarse bajo las siguientes funciones obligatorias:

Función de Gobernanza	Descripción Operativa
Registro	Inscripción preceptiva en el catálogo oficial del Departamento para control de ciclo de vida.
Inventario	Auditoría técnica de activos, dependencias de modelos y procedencia de algoritmos.

Evaluación de Riesgos	Análisis preceptivo en 5 dimensiones: Normativa, Ética, Tecnológica, Financiera y Operativa.
------------------------------	--

Esta estructura de gobernanza es la única vía para alcanzar una autonomía estratégica real frente a terceros países, blindando nuestra capacidad de decisión.

2. Soberanía Tecnológica: Modelos Propios y Autonomía Nacional

La soberanía tecnológica es la capacidad de ejercer un control integral sobre el *stack* tecnológico para evitar vulnerabilidades críticas. En un escenario de crisis, las directivas de exportación extranjeras podrían ejecutar un "**apagón tecnológico**" en apenas **90 minutos**, inhabilitando capacidades defensivas nacionales de forma remota. Por tanto, la soberanía no es aislamiento, sino la garantía de que el pulso operativo de la nación no dependa de interruptores ajenos.

- 1. Modelos Frontera vs. Commodities:** El Ministerio de Defensa postula la creación de un **modelo frontera militar diferencial** frente al uso de modelos comerciales generalistas. Un modelo soberano permite una **tokenización en castellano** optimizada para el dominio léxico y doctrinal militar puro, asegurando que los valores éticos y el código moral de las Fuerzas Armadas estén integrados desde la fase de diseño (*safety by design*).
- 2. IA Neurosimbólica y SLMs:** Para el combate en el **Edge** (borde táctico), los *Small Language Models* (SLMs) y la tecnología **neurosimbólica** son superiores a los grandes modelos genéricos. Al combinar el aprendizaje profundo con reglas lógicas tradicionales, la IA neurosimbólica actúa como el antídoto al problema de la "caja negra", permitiendo la **trazabilidad y auditabilidad** necesarias para la rendición de cuentas en combate, donde la precisión (**F1 Score**) es el único métrico aceptable.
- 3. El Ecosistema Industrial:** La cadena de valor de la IA de defensa se estructura mediante una colaboración simbiótica:
 - **Empresas Tractoras:** Responsables de la integración de sistemas complejos, la escala operativa y la sostenibilidad de infraestructuras críticas.
 - **PYMES:** Aportan una especialización técnica de alto nivel y agilidad en nichos tecnológicos críticos.
 - **Startups y Unicornios:** Motores de innovación disruptiva que asumen riesgos en el desarrollo de capacidades que el sector convencional no puede abordar inicialmente.

La soberanía tecnológica es la única garantía para una IA éticamente segura y operativamente infalible, protegiendo la libertad de acción nacional.

3. La "Guerra del Dato": Infraestructura, Calidad e Interoperabilidad

En el ámbito militar, el axioma "*Garbage In, Garbage Out*" adquiere una dimensión existencial. Si el dato es defectuoso, la decisión será errónea y las consecuencias, letales. El dato debe gestionarse con el mismo rigor logístico que el suministro de munición; es el combustible que alimenta la superioridad táctica y estratégica.

El Ministerio distingue rigurosamente entre el **Gobierno del Dato** (la decisión estratégica y política) y la **Gestión del Dato** (la ejecución técnica). Para asegurar la excelencia, se han adoptado las normas **UNE 77 a 85**, que no solo estandarizan la calidad, sino que proporcionan el marco de **auditabilidad** exigido por la nueva Ley de IA de la Unión Europea.

La interoperabilidad en entornos multinacionales, bajo el marco de las **Redes de Misión Federadas (FMN/OTAN)**, exige una **seguridad centrada en el dato**. Esto permite que la protección y el etiquetado de clasificación "viajen" con la información, asegurando que la soberanía nacional se mantenga incluso cuando el dato cruza el perímetro hacia aliados internacionales.

Para blindar esta soberanía, se impulsan zonas de control y espacios de datos específicos. El proyecto **Numantia**, en Soria, se consolida como la infraestructura crítica de referencia para el almacenamiento y tratamiento de datos clasificados en una nube privada, permitiendo la certificación de sistemas en entornos aislados (*air-gapped*) antes de su despliegue operativo. Esta arquitectura es el puente necesario para que la academia valide científicamente la robustez de nuestros procesos de datos.

4. El Triángulo de Innovación: Defensa, Universidad y Empresa

Es imperativo superar la brecha entre la investigación teórica y la necesidad operativa. La universidad debe evolucionar de un centro de formación a un **evaluador científico independiente** que certifique la robustez y neutralidad de los algoritmos de defensa.

- **Investigación Orientada a la Misión:** Frente a la elucubración académica, se promueve el modelo de **Doctorados Industriales** y convenios que transformen el conocimiento fronterizo en capacidades reales. La urgencia militar exige que el talento científico trabaje sobre el terreno, acortando los ciclos de innovación.
- **Certificación Continua:** Dado que la IA evoluciona en ciclos semestrales, el modelo de certificación estática es obsoleto. La evaluación debe ser un proceso dinámico y constante que verifique la ausencia de sesgos y la explicabilidad durante toda la vida operativa del sistema.
- **Nodos Estratégicos del "Triángulo Virtuoso":** España ha estructurado su liderazgo mediante tres centros de excelencia:
 - **A Coruña (AESIA):** Referente en regulación y supervisión normativa.
 - **Jaén (CETEDEX):** Especializado en experimentación y certificación de sistemas autónomos.
 - **Soria (Proyecto Numantia):** El nodo estratégico para la soberanía del dato y la computación avanzada.

En este contexto, España lidera el ámbito hispanohablante con la plataforma **Nexus Reim**, un foro internacional para la IA responsable que proyecta nuestros valores éticos a nivel global. Esta infraestructura de innovación solo es efectiva si se conecta con la responsabilidad ineludible de las personas que operarán estos sistemas.

5. El Factor Humano y la Ética del Control Significativo

La IA debe ser un multiplicador de la inteligencia humana, no un sustituto que genere "**deuda cognitiva**". El mando militar no puede delegar su juicio moral ni confiar ciegamente en una sugerencia algorítmica. El concepto de **Control Humano Significativo** asegura que el juicio ético permanezca siempre como una competencia militar no delegable, alineada con el código moral castrense.

La formación se articula para crear "**IA Champions**" en las unidades, actuando como guardianes contra el **sesgo de automatización**. Los niveles de formación son:

1. **Básico:** Cultura general de IA para toda la fuerza.
2. **Analista:** Explotación de datos en Estados Mayores.
3. **Desarrollador:** Personal técnico para el ajuste fino de modelos soberanos.
4. **Decisor:** Mandos con capacidad crítica para evaluar riesgos operativos y éticos.

Un pilar fundamental de la preparación es la capacidad de operar en "**Modo Degradado**". El militar debe estar capacitado para cumplir la misión incluso ante el fallo o la neutralización de los sistemas de IA por el adversario. Esta competencia no es un plan de contingencia, sino una capacidad nuclear del combatiente moderno. El pensamiento crítico es la última línea de defensa contra la dependencia tecnológica.

La visión de futuro de las Fuerzas Armadas reafirma un compromiso inquebrantable con una IA que salvaguarda los valores democráticos, la ética operativa y la eficacia en la defensa de la Nación.