

GOBERNANZA ALGORÍTMICA EN SISTEMAS DE CONTROL Y DEFENSA MARÍTIMA: TRAZABILIDAD, SOBERANÍA DECISIONAL Y EL VACÍO NORMATIVO ARGENTINO



Secretaría de Asuntos Navales

Autor: ULISES LENTO

Analista en Precios de Transferencia en Grant Thornton Argentina y creador del marco TRIA (DNDA 2026), metodología de gobernanza algorítmica. Expone en universidades y colegios profesionales sobre IA institucional. Integra la Secretaría de Asuntos Navales y Marítimos de FOPREA.

RESUMEN

La incorporación de inteligencia artificial a los sistemas de control portuario, fiscalización aduanera y operaciones navales avanza en Argentina sin un marco normativo específico que regule su uso. Esta ausencia no es una cuestión técnica: es una cuestión de soberanía. Cuando un sistema algorítmico toma decisiones operativas en contextos de control fronterizo, seguridad marítima o apoyo a la decisión de mando sin que esas decisiones puedan ser auditadas, el Estado pierde la capacidad de verificar si sus propias instituciones actúan conforme a derecho.

El presente trabajo analiza el estado de la adopción de IA en sistemas navales y de control marítimo-portuario, identifica el vacío normativo específico al sector defensa frente a sectores más avanzados, y propone un marco mínimo de gobernanza algorítmica basado en trazabilidad, razonamiento auditable, participación humana suficiente y soberanía de decisión.

El marco conceptual de referencia es TRIA (Trazabilidad, Razonamiento, IA, Auditoría), articulado con el EU AI Act, los Principios OTAN, el Código IMO para buques autónomos e ISO/IEC 42001:2023. La tesis central es que la ausencia de un estándar de trazabilidad algorítmica no es solo un riesgo de eficiencia: es un riesgo de soberanía operativa, responsabilidad institucional y control civil.

Palabras clave: *inteligencia artificial, gobernanza algorítmica, trazabilidad, defensa marítima, soberanía de decisión, control aduanero*





ÍNDICE

1. Resumen y palabras clave.....	1
2. Metodología.....	2
3. Introducción.....	3
1. Estado del arte: IA en defensa y seguridad marítima.....	3
1.1. La integración global de IA en sistemas navales	
1.2. Vehículos autónomos marítimos	
1.3. IA en control portuario y aduanero	
1.4. El caso argentino	
2. Marco normativo internacional.....	3
2.1. EU AI Act	
2.2. Principios de IA de la OTAN	
2.3. Código IMO para buques autónomos (MASS)	
2.4. Debate sobre sistemas de armas autónomas letales	
2.5. ISO/IEC 42001:2023 y Principios OCDE	
3. El contexto institucional argentino.....	5
3.1. La Armada Argentina	
3.2. La Prefectura Naval Argentina	
3.3. ARCA y el control aduanero portuario	
3.4. El marco normativo argentino sobre IA	
4. El vacío algorítmico en el sector naval-marítimo.....	6
4.1. La dimensión del problema	
4.2. Comparación con sectores más avanzados	
4.3. El fenómeno de la Shadow IA en defensa	
5. Fundamentos conceptuales para una gobernanza algorítmica en defensa.....	7
5.1. Soberanía de decisión y cadena de mando	
5.2. Participación humana suficiente y ventana de control	
5.3. Supervisión escéptica sustantiva y responsabilidad de mando	
5.4. Deuda algorítmica	
6. Aplicación del marco TRIA al sector naval-marítimo.....	8
6.1. Estructura conceptual de TRIA	
6.2. Trazabilidad en vigilancia y detección naval	
6.3. Razonamiento auditable y scoring aduanero (MDMA)	
6.4. Auditoría en la cadena de mando	
7. Propuesta de estándar mínimo.....	9
7.1. Principios orientadores	
7.2. Niveles de riesgo y requisitos diferenciados	
7.3. Elementos estructurales	
7.4. Instrumento normativo propuesto	
7.5. El rol de FOPREA	
Conclusiones.....	10
Referencias.....	11

METODOLOGÍA

El presente trabajo emplea una metodología de análisis normativo-comparado. Se relevaron las principales fuentes primarias en materia de gobernanza de inteligencia artificial a nivel internacional —EU AI Act (2024), Principios OTAN (2021), Código IMO para MASS (2019), ISO/IEC 42001:2023, Principios OCDE (2019)— y se las contrastó con el marco normativo argentino vigente en defensa nacional, seguridad marítima y control aduanero.

El análisis del contexto institucional argentino se realizó a partir de la legislación orgánica de las instituciones del sector (Leyes N.º 19.549, 23.554 y 18.398) y de la evolución reciente de los organismos relevantes (ARCA, Prefectura Naval Argentina, Armada Argentina). El marco conceptual de gobernanza algorítmica se construyó sobre los instrumentos TRIA (DNDA, Legajo N.º RL-2026-46255181) y MDMA (DNDA, N.º PV_2026-67047663-APN-DNDA#MJ), integrados con la literatura académica sobre Shadow IA, soberanía de decisión y control humano en sistemas autónomos.

La propuesta de estándar mínimo adopta un enfoque prescriptivo-institucional: no describe el estado del arte tecnológico sino las condiciones normativas e institucionales que deben cumplirse para que ese estado del arte sea compatible con el estado de derecho. La selección de casos comparados (EU AI Act, OTAN, IMO) responde al criterio de relevancia normativa: se priorizaron marcos que ya producen efectos directos o indirectos sobre actores institucionales argentinos del sector.



INTRODUCCIÓN

En los últimos cinco años, la inteligencia artificial ha ingresado a los sistemas de control estatal de manera silenciosa y acelerada. No por decisión política articulada, sino por la suma de decisiones técnicas individuales: una unidad que adopta un software de análisis de riesgo, un organismo que incorpora un sistema de scoring para priorizar fiscalizaciones, una fuerza de seguridad que integra reconocimiento de patrones en su proceso de detección. Cada adopción, vista de manera aislada, parece razonable. Vista en conjunto, representa un desplazamiento de facto del criterio humano hacia criterios algorítmicos que, en la mayoría de los casos, no pueden ser auditados.

El sector naval y marítimo —en sus dimensiones de defensa, seguridad y control aduanero-portuario— es uno de los espacios donde este proceso avanza de manera más pronunciada y con menor acompañamiento institucional. Los puertos son nodos críticos de la economía nacional. Las fuerzas navales son instrumentos de la soberanía territorial. El control aduanero-portuario es la primera línea de verificación de la legalidad del comercio exterior. La incorporación de IA a estos sistemas sin marcos de gobernanza adecuados no es un detalle técnico: es una decisión sobre quién decide, con qué criterio y con qué posibilidad de control posterior.

El análisis abarca tres dimensiones del sector naval-marítimo argentino: control aduanero y portuario (scoring de riesgo en cargas y operadores, análisis documental automatizado); seguridad marítima y control fronterizo (Prefectura Naval Argentina); y operaciones navales y apoyo a la decisión de mando (Armada Argentina). El foco no es la IA ofensiva ni los sistemas de armas autónomas letales —aunque se mencionan en el marco internacional—, sino la IA que ya está siendo utilizada o está en proceso de adopción y que carece de marcos de gobernanza específicos.



1. ESTADO DEL ARTE: IA EN DEFENSA Y SEGURIDAD MARÍTIMA

1.1. La integración global de IA en sistemas navales

La adopción de inteligencia artificial en operaciones navales y de seguridad marítima es un fenómeno global que avanza en múltiples dimensiones simultáneamente. En el plano de las grandes potencias navales, la integración de IA abarca desde la asistencia a la decisión humana hasta la autonomía operativa parcial o total en determinadas funciones. Estados Unidos ha desarrollado el Sea Hunter, vehículo de superficie no tripulado diseñado para operar semanas sin intervención humana directa, e integra IA en sistemas de análisis de inteligencia naval y detección de amenazas submarinas. China ha invertido masivamente en procesamiento en tiempo real de imágenes satelitales para detección de embarcaciones sospechosas y sistemas de enjambre para operaciones autónomas coordinadas. El Reino Unido, a través del programa NavyX, impulsa sistemas autónomos marítimos en operaciones de minería submarina y patrulla costera.

Estas experiencias comparten un denominador común: la velocidad de desarrollo tecnológico supera la velocidad de construcción de marcos normativos para su uso institucional. Incluso en países con sistemas de gobernanza de IA relativamente desarrollados, los marcos específicos para el sector defensa presentan lagunas significativas en trazabilidad, responsabilidad y control humano sobre las decisiones algorítmicas.

1.2. Vehículos autónomos marítimos: el caso paradigmático

Los vehículos autónomos marítimos (VAM) — buques de superficie no tripulados (USV), vehículos submarinos no tripulados (UUV) y drones navales— representan el caso más visible de integración de IA en el ámbito naval. El interrogante central no es si estos sistemas funcionan: es sí, cuando toman una decisión operativa equivocada, es posible determinar quién es responsable, con qué dato fue alimentado el sistema, qué criterio produjo el error y cómo evitar su repetición.



En la mayoría de los sistemas actuales, la respuesta es parcial o directamente negativa.

1.3. IA en control portuario y aduanero

Los sistemas de targeting automatizado para identificación de cargas de riesgo existen en aduanas de países desarrollados desde principios de la década de 2000. El sistema ATS (Automated Targeting System) de la agencia CBP de Estados Unidos analiza millones de transacciones de comercio exterior para generar perfiles de riesgo. Sistemas similares operan en la Unión Europea, Australia, Japón y un número creciente de países latinoamericanos. La Organización Mundial de Aduanas (OMA/WCO) ha promovido activamente estas tecnologías en el Marco Normativo SAFE, sin acompañarlas de estándares equivalentes de trazabilidad.

La consecuencia práctica es que los sistemas de scoring de riesgo aduanero operan frecuentemente como cajas negras: generan outputs sin que el agente aduanero que debe actuar sobre esa información tenga acceso al razonamiento que la produjo. La firma del funcionario sobre la decisión resultante no constituye supervisión real: es validación formal de un criterio al que no tuvo acceso.

1.4. El caso argentino: adopción acelerada sin marco específico

La Agencia de Recaudación y Control Aduanero (ARCA, ex-AFIP) utiliza sistemas de análisis de riesgo para la priorización de fiscalizaciones en comercio exterior. El Puerto de Buenos Aires y los principales puertos del litoral han incorporado o están en proceso de incorporar sistemas de gestión de tráfico y control de acceso con componentes de automatización.

La Prefectura Naval Argentina ha explorado el uso de tecnologías de vigilancia con procesamiento automatizado de imágenes. Ninguno de estos desarrollos cuenta con un marco normativo específico que establezca estándares de trazabilidad, responsabilidad algorítmica o supervisión humana sobre los outputs de los sistemas.



2. MARCO NORMATIVO INTERNACIONAL

2.1. El Reglamento de Inteligencia Artificial de la Unión Europea

El Reglamento (UE) 2024/1689 —EU AI Act— clasifica los sistemas de IA en cuatro categorías de riesgo. Los sistemas de alto riesgo incluyen, de manera explícita: sistemas de gestión de infraestructura crítica, incluyendo transporte marítimo; sistemas de control fronterizo, evaluación de riesgo y detección de amenazas a la seguridad; e identificación biométrica en espacios públicos. Para todos los sistemas de alto riesgo, el Reglamento establece: documentación técnica completa, registro de logs que permita la trazabilidad de las decisiones, supervisión humana efectiva y ciberseguridad. Aunque no vinculante para Argentina, define el estándar internacional de referencia para el sector.

2.2. Los Principios de IA de la OTAN

En octubre de 2021, la OTAN adoptó los Principles of Responsible Use of Artificial Intelligence in Defence, con seis principios: legalidad, responsabilidad y rendición de cuentas, explicabilidad y trazabilidad, confiabilidad, gobernabilidad y mitigación de sesgos. El principio de trazabilidad establece que deben poder rastrearse las entradas de datos, el diseño del sistema y la cadena de decisión. Argentina mantiene el estatus de Major non-NATO Ally (MNNA) desde 1998, lo que establece una relación de cooperación que hace de estos principios una referencia normativa relevante.



2.3. El Código IMO para Buques de Superficie Marítimos Autónomos (MASS)

La Organización Marítima Internacional ha avanzado en el marco regulatorio para los MASS (Maritime Autonomous Surface Ships). Las directrices provisionales de 2019 (MSC-Circ.1604) constituyeron el primer paso formal. Los Convenios SOLAS, COLREG y MLC fueron diseñados para decisiones tomadas por seres humanos; la incorporación de sistemas autónomos plantea preguntas no resueltas sobre responsabilidad y trazabilidad de la cadena de decisión. Argentina, como estado de bandera, rector del puerto y ribereño, tiene intereses directos en la definición de estos estándares.

2.4. El debate internacional sobre sistemas de armas autónomas letales (LAWS)

En el marco de la Convención sobre Ciertas Armas Convencionales (CCW), el Grupo de Expertos Gubernamentales sobre LAWS debate desde 2014 el concepto de control humano significativo (meaningful human control): la exigencia de que un ser humano tome o apruebe la decisión de usar fuerza letal sin delegarla de manera irrevocable a un sistema algorítmico. Argentina ha sostenido posiciones favorables al establecimiento de estándares vinculantes de control humano, posición que no tiene aún correlato normativo doméstico en el sector defensa.

2.5. ISO/IEC 42001:2023 y los Principios OCDE

La norma ISO/IEC 42001:2023 establece los requisitos de un sistema de gestión para la inteligencia artificial, incluyendo la definición de políticas de IA, evaluación de impacto, gestión de riesgos, documentación del ciclo de vida y trazabilidad de las decisiones. Los Principios de IA de la OCDE (2019), adoptados por Argentina, incluyen transparencia y explicabilidad como principio rector: los actores de IA deben ser transparentes sobre los sistemas y proveer información comprensible sobre los factores que inciden en las predicciones o decisiones generadas.



3. EL CONTEXTO INSTITUCIONAL ARGENTINO

3.1. La Armada Argentina

La Armada Argentina es la rama naval de las Fuerzas Armadas, con competencia en la defensa del territorio marítimo y la soberanía en el Mar Argentino. Su marco normativo —Ley N.º 23.554 (1988) y Decreto N.º 727/2006— establece el sistema de defensa nacional y los mecanismos de conducción civil, sin contemplar en ninguna de sus disposiciones la incorporación de sistemas algorítmicos ni requisitos de trazabilidad o supervisión humana sobre ellos. El proceso de modernización tecnológica ha incorporado sistemas de análisis de inteligencia con procesamiento automatizado de datos sin actualización normativa equivalente.

3.2. La Prefectura Naval Argentina

La Prefectura Naval Argentina (PNA) ejerce competencia en ríos interiores, lagos y aguas territoriales hasta las 200 millas náuticas, con funciones de seguridad de la navegación, prevención de actividades ilícitas y control del tráfico marítimo y fluvial. Opera en la intersección de seguridad, defensa y control aduanero. Su ley orgánica (Ley N.º 18.398) no contempla el supuesto de decisiones algorítmicas ni establece requisitos de trazabilidad para los outputs de sistemas automatizados.



3.3. ARCA y el control aduanero portuario

La Agencia de Recaudación y Control Aduanero (ARCA, creada en 2024 en sustitución de la AFIP) es el organismo responsable del control aduanero de cargas que ingresan y egresan por vía marítima y portuaria. Sus sistemas de scoring procesan datos de comercio exterior y generan perfiles de riesgo que orientan decisiones operativas de agentes aduaneros. La calidad de estos sistemas — precisión, sesgos, coherencia con criterios normativos— no está documentada públicamente de manera accesible.

3.4. El marco normativo argentino sobre IA: estado actual

El marco normativo argentino sobre inteligencia artificial es fragmentario. El Plan Nacional de Inteligencia Artificial establece orientaciones de política general. La SIGEN ha emitido recomendaciones sobre uso de IA en el sector público sin carácter vinculante para organismos de defensa y seguridad. Argentina adhirió a la Declaración de Bletchley (noviembre 2023) y participa en los procesos de la OCDE y el G20. No existe marco normativo específico aplicable al uso de IA en defensa, seguridad marítima y control portuario-aduanero.



4. EL VACÍO ALGORÍTMICO EN EL SECTOR NAVAL-MARÍTIMO: DIAGNÓSTICO

4.1. La dimensión del problema

El vacío normativo identificado no es ausencia total de regulación: es un vacío específico. La normativa vigente en materia de defensa, seguridad marítima y control aduanero establece procedimientos, atribuciones y controles diseñados para decisiones tomadas por seres humanos. Lo que no prevé es el supuesto en que esas decisiones son generadas o pre-filtradas por sistemas algorítmicos cuyos criterios no son transparentes, cuyo funcionamiento no es documentado de manera auditable y cuya cadena de responsabilidad no está definida.

Este vacío tiene cinco consecuencias operativas: motivación administrativa sin fundamento real (Ley N.º 19.549 exige motivación que el sistema no provee); control externo imposible (SIGEN, AGN y Poder Judicial no pueden reconstruir razonamientos no documentados); atribución de responsabilidad indefinida (ningún actor puede ser responsabilizado con certeza); vulnerabilidad a la impugnación judicial (el organismo no puede proveer la información que el proceso judicial requiere); y erosión de la soberanía decisional (el funcionario que valida un resultado que no comprende delega en el sistema sin saberlo).

4.2. Comparación con sectores más avanzados

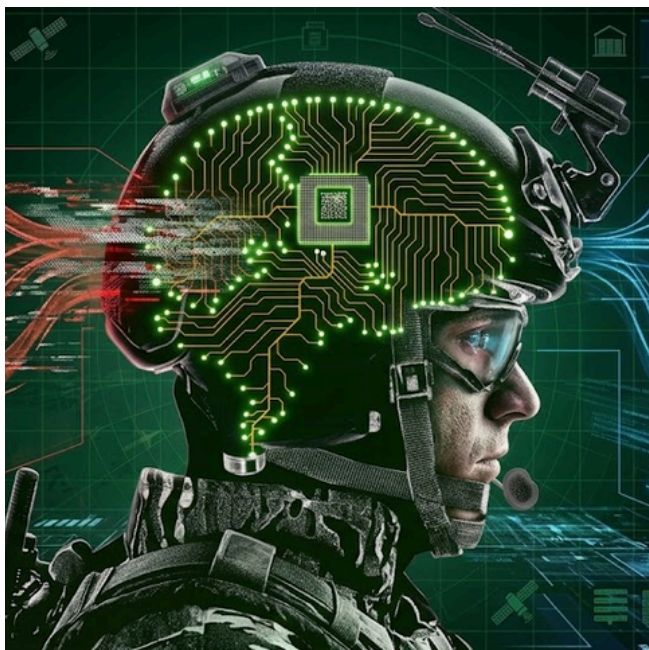
El sector judicial —donde el Comité de Estandarización en IA del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires ha avanzado en criterios de explicabilidad y supervisión humana— presenta mayor desarrollo normativo que el sector naval-marítimo.

Lo mismo ocurre en el sector fiscal y sanitario. Este rezago comparativo no está justificado por un menor nivel de riesgo institucional: las decisiones del sector naval-marítimo involucran soberanía territorial, seguridad física de personas y bienes, y ejercicio de potestades coercitivas del Estado.



4.3. El fenómeno de la Shadow IA en defensa

El concepto de Shadow IA —el uso de inteligencia artificial en entornos institucionales sin marcos de supervisión, sin documentación del razonamiento y sin ventana de control que preserve la decisión humana (Gavilán, Balbi y Lento, 2026)— adquiere gravedad adicional en defensa. Implica riesgos de errores operativos con consecuencias irreversibles, vulneración de la cadena de mando y pérdida de control civil sobre las decisiones de fuerza. La Shadow IA en defensa no requiere sistemas secretos: resulta simplemente de no haberse planteado la pregunta de qué sucede cuando el sistema falla o cuando su resultado es cuestionado.



5. FUNDAMENTOS CONCEPTUALES PARA UNA GOBERNANZA ALGORÍTMICA EN DEFENSA

5.1. Soberanía de decisión y cadena de mando

La soberanía de decisión (Lento, 2026) refiere a la capacidad real de un agente institucional de ejercer criterio propio sobre un resultado algorítmico, con información suficiente para validarlo o rechazarlo.

En las fuerzas de defensa y seguridad, su erosión afecta la estructura de mando: si las decisiones operativas son generadas por sistemas cuyos criterios no son transparentes para los mandos intermedios, la cadena de mando pierde su función sustantiva y se convierte en validación formal. El control civil efectivo presupone que las decisiones operativas puedan ser revisadas, cuestionadas y modificadas por la autoridad política. Si esas decisiones tienen una componente algorítmica no trazable, esa revisión se vuelve imposible.

5.2. Comparación con sectores más avanzados

La participación humana suficiente refiere al nivel de involucramiento del agente humano necesario para que su firma constituya supervisión real —no mera validación formal— del resultado algorítmico (Lento, 2026). No exige que el ser humano tome cada decisión sin asistencia algorítmica: exige que comprenda el razonamiento que generó la recomendación y pueda ejercer criterio propio.

La ventana de control es su correlato operativo: el punto donde el agente puede intervenir, validar o rechazar el output antes de que produzca efectos. En contextos operativos navales donde la rapidez es crítica, esta ventana puede ser breve pero no puede ser eliminada. La velocidad operativa no es incompatible con la trazabilidad.

5.3. Supervisión escéptica sustantiva y responsabilidad de mando

La supervisión escéptica sustantiva refiere a la actitud profesional ante el output algorítmico: no validación automática, sino evaluación activa de su razonabilidad a la luz del criterio propio, el contexto y los estándares normativos (Gavilán, Balbi y Lento, 2026). En defensa, esta supervisión es un componente de la responsabilidad de mando: un oficial que valida una decisión sin comprender su fundamento no ejerce mando responsable.

Los regímenes de responsabilidad de las fuerzas armadas atribuyen responsabilidad a los mandos por las decisiones bajo su autoridad, independientemente de si fueron asistidas por sistemas tecnológicos.



5.4. Deuda algorítmica: el pasivo institucional de la opacidad

La deuda algorítmica (Lento, 2026) es el pasivo institucional que se acumula cuando se toman decisiones con sistemas algorítmicos no trazables. En el sector naval-marítimo se acumula en cuatro dimensiones: legal (decisiones aduaneras no trazables que enfrentarán impugnaciones), operativa (errores que no podrán ser diagnosticados ni corregidos), institucional (pérdida de confianza en los sistemas de control estatal) y de soberanía (dependencia de proveedores externos que no pueden ser auditados). Como toda deuda, resulta más costosa cuando se paga tarde que cuando se previene desde el diseño.



6. APLICACIÓN DEL MARCO TRIA AL SECTOR NAVAL-MARÍTIMO

6.1. El marco TRIA: estructura conceptual

El marco TRIA (Trazabilidad, Razonamiento, IA, Auditoría) —registrado ante la Dirección Nacional del Derecho de Autor, Legajo N.º RL-2026-46255181— propone una metodología de implementación de gobernanza algorítmica en entornos institucionales articulada en cuatro pilares. Trazabilidad: capacidad de reconstruir la cadena de

datos, criterios y procesos que llevaron al resultado. Razonamiento: inteligibilidad del proceso; el agente humano puede comprender por qué el sistema produjo ese resultado y no otro. IA: caracterización adecuada del sistema, sus capacidades, limitaciones conocidas y áreas de incertidumbre. Auditoría: posibilidad de revisión externa del funcionamiento y resultados del sistema.

6.2. Trazabilidad en sistemas de vigilancia y detección naval

La aplicación del pilar de trazabilidad a los sistemas de vigilancia de la Armada Argentina y la Prefectura Naval implica procedimientos de registro que documenten: el dato de entrada que generó cada alerta o clasificación de riesgo; la versión del modelo utilizada y la fecha de su última actualización; el umbral de confianza del sistema en la clasificación producida; y la identidad del agente humano que revisó el output y la decisión adoptada. Estos registros no requieren sistemas técnicos sofisticados: pueden implementarse mediante procedimientos operativos estándar.

6.3. Razonamiento auditable en scoring aduanero y diagnóstico MDMA

La aplicación del pilar de razonamiento a los sistemas de scoring de ARCA implica mecanismos de explicación accesibles para los agentes aduaneros: no la explicación matemática interna del modelo, sino una descripción comprensible del criterio determinante. Este nivel de explicación es técnicamente alcanzable con modelos interpretables y técnicas de explicabilidad post-hoc. La brecha entre lo que es posible y lo que se implementa no es de capacidad: es de exigencia institucional.

Para diagnosticar con precisión en qué punto se encuentra un sistema de scoring respecto de los cuatro pilares, la Matriz Diagnóstica de Madurez Algorítmica (MDMA) —registrada ante la Dirección Nacional del Derecho de Autor, N.º PV_2026-67047663-APN-DNDA#MJ— provee un instrumento estructurado que evalúa el nivel de madurez actual en cada dimensión: qué documenta el sistema, qué explica al agente que lo utiliza, cómo fue caracterizado institucionalmente y con qué posibilidad real de auditoría opera.



La aplicación de la MDMA a los sistemas de scoring de ARCA permitiría identificar, antes de cualquier intervención normativa, qué brechas específicas deben cerrarse y en qué orden priorizarlas.

6.4. Auditoría en la cadena de mando

El marco TRIA (Trazabilidad, Razonamiento, IA, Auditoría) —registrado ante la Dirección Nacional del Derecho de Autor, Legajo N.º RL-2026-46255181— propone una metodología de implementación de gobernanza algorítmica en entornos institucionales articulada en cuatro pilares. Trazabilidad: capacidad de reconstruir la cadena de



7. PROPUESTA DE ESTÁNDAR MÍNIMO DE GOBERNANZA ALGORÍTMICA

7.1. Principios orientadores

La propuesta se basa en cuatro principios: proporcionalidad al riesgo (los requisitos se calibran según el nivel de riesgo institucional del sistema); adaptabilidad a la cadena de mando (la gobernanza algorítmica se integra en los procedimientos operativos estándar, no se superpone); viabilidad de implementación gradual (avance por etapas,

comenzando por trazabilidad mínima); y coherencia con el marco normativo vigente (implementable mediante instrumentos disponibles sin necesidad de ley específica en el corto plazo).

7.2. Niveles de riesgo y requisitos diferenciados

Se proponen tres niveles. Nivel I — Alto riesgo: sistemas cuyo output produce efectos jurídicos directos o incide en decisiones con consecuencias físicas irreversibles (scoring aduanero con efectos de retención; clasificación de amenazas que incide en interceptación; identificación de embarcaciones por la Prefectura Naval). Requisitos: documentación técnica completa, registro de trazabilidad por output, explicación comprensible del razonamiento, ventana de control humana definida en el procedimiento operativo, responsable nominado y auditoría interna periódica.

Nivel II — Riesgo significativo: sistemas que informan decisiones con consecuencias institucionales relevantes pero con instancia humana intermedia antes del efecto final (análisis de inteligencia que genera insumos para mando; gestión de tráfico marítimo). Nivel III — Riesgo bajo: asistencia a funciones administrativas o de soporte sin incidencia directa en decisiones con efectos jurídicos u operativos.

7.3. Elementos estructurales del estándar

Cuatro elementos aplican a todos los sistemas, independientemente del nivel de riesgo. Registro de adopción: toda institución mantiene un registro de los sistemas algorítmicos en uso, con indicación del proveedor, función, tipo de decisiones y nivel de riesgo asignado. Procedimiento de habilitación institucional: ningún sistema de Nivel I o II puede operar sin proceso formal de habilitación.

Para sistemas ya en operación sin haber atravesado este proceso, la habilitación retroactiva puede instrumentarse mediante la Matriz Diagnóstica de Madurez Algorítmica (MDMA), N.º PV_2026-67047663-APN-DNDA#MJ, que identifica el nivel de madurez actual y define un plan de adecuación con plazos concretos. Protocolo de incidentes algorítmicos: procedimiento específico para cuando un sistema produce un output identificado como



erróneo o cuestionable. Revisión periódica: los sistemas de Nivel I son objeto de revisión anual.

7.4. Auditoría en la cadena de mando

La implementación puede avanzar mediante instrumentos disponibles sin necesidad de ley específica en el corto plazo: una Resolución del Ministerio de Defensa estableciendo los principios de gobernanza algorítmica para las Fuerzas Armadas; una Instrucción de Servicio de la Prefectura Naval Argentina para los procedimientos de seguridad marítima y control portuario; y una Resolución de ARCA estableciendo estándares de trazabilidad y supervisión humana para los sistemas de gestión de riesgo aduanero. En el mediano plazo, estos instrumentos sectoriales deberán articularse en un marco normativo de rango legal.

7.5. Auditoría en la cadena de mando

La posición institucional de FOPREA —con su red de vinculación entre fuerzas navales, academia y perfiles de política pública— la ubica en posición privilegiada para contribuir al marco propuesto en tres dimensiones: producción de conocimiento aplicado sobre gobernanza algorítmica en el sector naval-marítimo; articulación institucional entre los actores del sector y los desarrollos normativos disponibles; y formación de profesionales del sector en principios y herramientas de gobernanza algorítmica.

CONCLUSIÓN

El sector naval-marítimo argentino presenta un vacío normativo específico en materia de gobernanza algorítmica que no está justificado por un menor nivel de riesgo institucional. Los sistemas de IA están siendo incorporados de manera progresiva y acelerada —en los sistemas de scoring de ARCA, en la vigilancia marítima de la Prefectura Naval, en los sistemas de análisis de la Armada— sin que ninguno de estos desarrollos cuente con un marco normativo específico de trazabilidad, responsabilidad algorítmica o supervisión humana real.

El marco normativo internacional —EU AI Act, Principios OTAN, Código IMO, Principios OCDE, ISO/IEC 42001:2023— converge en cuatro exigencias mínimas: trazabilidad del output,

explicabilidad del razonamiento, supervisión humana real y posibilidad de auditoría externa. Argentina ha adherido a los marcos internacionales relevantes y sostenido posiciones constructivas en debates multilaterales sobre sistemas autónomos en defensa. La brecha entre esa posición y la ausencia de regulación doméstica específica es un problema de coherencia que el país tiene la capacidad y el interés estratégico de cerrar.

El estándar mínimo propuesto —articulado sobre los cuatro pilares del marco TRIA y calibrado para la realidad institucional del sector— no es una propuesta de parálisis tecnológica. Es una propuesta de modernización con soberanía: que las instituciones del sector adopten IA de manera que puedan rendir cuentas por las decisiones que esa IA informa o genera, que los mandos puedan ejercer supervisión real y que el Estado pueda controlar sus propias herramientas.

Un Estado que no puede auditar los sistemas algorítmicos que informan sus decisiones de control fronterizo, seguridad marítima y defensa naval no ejerce soberanía plena sobre esos procesos. Argentina tiene la oportunidad de posicionarse como actor propositivo en la definición de estándares de gobernanza algorítmica naval en el ámbito latinoamericano. Esa oportunidad requiere, como condición previa, desarrollar el marco normativo interno que dé sustancia a esa posición.

La automatización sin trazabilidad no es modernización. Es riesgo diferido.



REFERENCIAS

Gavilán A., Balbi D. y Lento U. (2026, junio 16). *Inteligencia artificial en el ejercicio profesional: ¿qué tener en cuenta?, ¿cómo afecta al contador? y ¿por qué la trazabilidad es el nuevo estándar?* Errepar+. <<https://documento.errepar.com/doctrina/inteligencia-artificial-en-el-ejercicio-profesional-que-tener-en-cuenta-como-afecta-al-20260616134649333>>

Gobierno del Reino Unido. (2023, noviembre 1). *Bletchley Declaration on AI Safety*. AI Safety Summit. <<https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration>>
International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Artificial intelligence — Management system*. ISO.

International Maritime Organization. (2019). *MSC-Circ.1604: Interim guidelines for trials of Maritime Autonomous Surface Ships (MASS)*. IMO.

Lento U. (2026). *Marco TRIA: Trazabilidad, Razonamiento, IA, Auditoría*. Dirección Nacional del Derecho de Autor, Legajo N.º RL-2026-46255181.

Lento U. (2026). *Matriz Diagnóstica de Madurez Algorítmica (MDMA)*. Dirección Nacional del Derecho de Autor, N.º PV_2026-67047663-APN-DNDA#MJ. Expediente EX-2026-677047649-APN-DNDA#MJ.
Naciones Unidas, Secretario General. (2018, abril 3). *Informe sobre los sistemas de armas autónomas letales (A/73/94)*. ONU. <<https://undocs.org/A/73/94>>

North Atlantic Treaty Organization. (2021, octubre). *Principles of Responsible Use of Artificial Intelligence in Defence*. NATO. <https://www.nato.int/cps/en/natohq/official_texts_187617.htm>

Organización de Cooperación y Desarrollo Económicos. (2019, mayo 22). *Recomendación del Consejo sobre Inteligencia Artificial (OCDE/LEGAL/0449)*. OCDE. <<https://oecd.ai/en/ai-principles>>

Organización Mundial de Aduanas. (2023). *Marco Normativo SAFE para asegurar y facilitar el comercio mundial*. OMA.

Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 — Reglamento de Inteligencia Artificial (EU AI Act)*. Diario Oficial de la Unión Europea.

República Argentina. (1969). *Ley N.º 18.398: Ley Orgánica de la Prefectura Naval Argentina*. Boletín Oficial.
República Argentina. (1972). *Ley N.º 19.549: Ley de Procedimientos Administrativos*. Boletín Oficial.

República Argentina. (1988). *Ley N.º 23.554: Ley de Defensa Nacional*. Boletín Oficial.

República Argentina. (2006). *Decreto N.º 727/2006: Reglamentación de la Ley de Defensa Nacional*. Boletín Oficial.