El artículo analiza la necesidad de transformar el poder fluvial peruano en la Amazonía mediante el concepto de Flotilla Inteligente Amazónica y Segura (FIAS), integrando vigilancia persistente, sistemas no tripulados, inteligencia artificial, ciberdefensa e interoperabilidad interagencial. A partir de un enfoque cualitativo y documental, propone un modelo orientado a fortalecer la presencia del Estado, optimizar recursos y mejorar la conciencia situacional frente a amenazas híbridas y transnacionales en el siglo XXI.

Flotillas inteligentes en la Amazonía, innovación operacional, vigilancia persistente y transformación del poder fluvial peruano en el siglo XXI

Smart Flotillas in the Amazon: Operational Innovation, Persistent Surveillance, and the Transformation of Peruvian Riverine Power in the Twenty-First Century

The article examines the need to transform Peruvian riverine power in the Amazon through the concept of the Smart and Secure Amazon Flotilla (FIAS), integrating persistent surveillance, unmanned systems, artificial intelligence, cyber defense, and interagency interoperability. Based on a qualitative and documentary approach, it proposes a model aimed at strengthening state presence, optimizing resources, and enhancing situational awareness against hybrid and transnational threats in the twenty-first century.

Montoya Ruibal, J. (2026). Flotillas inteligentes en la Amazonía,innovación operacional, vigilancia persistente y transformación del poder fluvial peruano en el siglo XXI. Revista *Pensamiento Conjunto,* Año 14, N° 1. pp. 44-54. ISSN° 2707-367X

Fecha de recepción: 14 de mayo de 2026.
Fecha de aceptación: 17 de junio de 2026.
Fecha de publicación: 30 de junio de 2026.

Capitán de Fragata
José Carlo Montoya Ruibal
orcid.org/0009000659678141

Licenciado en Ciencias Marítimas Navales por la Escuela Naval del Perú. Primer puesto en la III Maestría en Ciberseguridad y Ciberdefensa con Mención en Transformación Digital por la Escuela Nacional de Marina Mercante y, primer puesto del XIX Programa de Comando y Estado Mayor Conjunto (XIX PCEMC) de la Escuela Superior Conjunta de las Fuerzas Armadas. Ha sido distinguido con la Condecoración de las Naciones Unidas por su desempeño en la Misión de Paz en la República Centroafricana (MINUSCA); Medalla y Diploma de Honor al Mérito del Comando Conjunto de las Fuerzas Armadas del Perú por el primer puesto del XIX PCEMC; y Navy and Marine Corps Commendation Medal, otorgada por el Department of the Navy de los Estados Unidos, por su desempeño excepcional como Oficial de Enlace. Actualmente se desempeña como Comandante de la Flotilla de Unidades Fluviales de la Amazonía y cursa la III Maestría en Ciberdefensa y Ciberseguridad con mención en transformación digital en el CAEN.

INTRODUCCIÓN

La Amazonía peruana es, simultáneamente, frontera, reserva estratégica, corredor fluvial, espacio ambiental crítico y zona de encuentro entre seguridad y desarrollo. Desde una perspectiva de defensa nacional, no puede ser interpretada únicamente como un territorio alejado del centro político-administrativo, sino como un sistema vivo de comunicaciones, economías, comunidades y riesgos transnacionales. En ese sistema, los ríos constituyen las principales vías de movilidad, logística, presencia estatal y articulación social..

La jurisdicción amazónica presenta una complejidad singular: extensas distancias, cambios hidrológicos estacionales, dispersión de comunidades, limitada infraestructura terrestre, presencia de fronteras vivas y coexistencia de actividades lícitas e ilícitas. En consecuencia, el dominio fluvial se convierte en el espacio donde la soberanía se ejerce, se comunica y se sostiene. La unidad fluvial no solo patrulla; representa al Estado, transporta servicios, protege poblaciones, disuade amenazas y conecta territorios que de otro modo permanecerían aislados.

En este escenario, el cargo de Comandante de la Flotilla de Unidades Fluviales de la Amazonía adquiere una dimensión que excede la conducción administrativa de medios navales. Supone la responsabilidad de articular

PALABRAS CLAVE: AMAZONÍA, PODER FLUVIAL, VIGILANCIA PERSISTENTE, SISTEMAS AUTÓNOMOS, INTELIGENCIA ARTIFICIAL, CIBERDEFENSA, OPERACIONES MULTIDOMINIO, SEGURIDAD Y DESARROLLO.
KEYWORDS: AMAZON, RIVERINE POWER, PERSISTENT SURVEILLANCE, AUTONOMOUS SYSTEMS, ARTIFICIAL INTELLIGENCE, CYBER DEFENSE, MULTIDOMAIN OPERATIONS, SECURITY AND DEVELOPMENT.

capacidades operacionales, logísticas, humanas, tecnológicas e interagenciales para sostener presencia efectiva en un ambiente de alta complejidad. Por ello, la innovación no debe concebirse como una aspiración abstracta, sino como una necesidad operacional y doctrinaria.

El problema central es que las amenazas contemporáneas han evolucionado con mayor rapidez que muchas estructuras tradicionales de respuesta. Redes vinculadas al narcotráfico, minería ilegal, tala ilegal, contrabando, trata de personas y delitos ambientales emplean movilidad, información, corrupción, tecnología comercial y conocimiento del terreno. Estas amenazas no se comportan como fuerzas convencionales; operan como redes adaptativas. Frente a redes adaptativas, el Estado requiere capacidades igualmente conectadas, inteligentes y resilientes.

La tesis de este artículo es que el poder fluvial peruano debe evolucionar hacia una Flotilla Inteligente Amazónica y Segura: una arquitectura de capacidades que integre plataformas tripuladas, sistemas no tripulados, sensores, inteligencia artificial, ciberdefensa, centros de fusión de información y cooperación interagencial. Este concepto no busca reemplazar la experiencia marinera ni la presencia física, sino multiplicarlas mediante información oportuna, vigilancia persistente y decisión operacional superior.

PROBLEMA ESTRATÉGICO Y JUSTIFICACIÓN

La defensa y seguridad en la Amazonía no pueden reducirse a la presencia episódica de unidades. La magnitud territorial, el dinamismo del entorno y la capacidad de adaptación de las amenazas obligan a construir un modelo de presencia persistente. La presencia persistente no significa ocupar todos los puntos de manera simultánea, sino disponer de una arquitectura capaz de observar, comprender, priorizar y actuar con oportunidad.

El Ministerio del Ambiente del Perú señala que una proporción sustantiva del territorio nacional está cubierta por bosques amazónicos, y el IIAP describe la Amazonía peruana como un ámbito superior al 60% del territorio nacional. Esta magnitud territorial convierte a la Amazonía en un espacio decisivo para el futuro del país, no solo por sus recursos naturales, sino por su valor estratégico, ambiental y humano (MINAM, s. f.; IIAP, s. f.).

Desde la perspectiva de la defensa, el Libro Blanco de la Defensa Nacional reconoce que la seguridad y defensa deben articular los esfuerzos del Estado y la población frente a riesgos y amenazas que afectan los intereses nacionales (Ministerio de Defensa, 2005). En el caso amazónico, esta articulación requiere un instrumento fluvial moderno, flexible, interoperable y tecnológicamente habilitado.

La justificación operacional de este artículo se sustenta en tres necesidades: primera, incrementar la conciencia situacional sobre corredores fluviales críticos; segunda, optimizar el empleo de unidades y personal en un entorno de recursos limitados; tercera, fortalecer la presencia estatal mediante acciones coordinadas de seguridad, desarrollo y protección ambiental. La justificación académica reside en proponer un modelo doctrinario propio para el contexto peruano, alineado con tendencias globales de operaciones multidominio, ciberseguridad y sistemas autónomos.

METODOLOGÍA

El artículo emplea un enfoque cualitativo, documental y propositivo. Es cualitativo porque analiza conceptos estratégicos, doctrinarios y operacionales; documental porque se sustenta en fuentes oficiales, marcos doctrinarios y literatura especializada; y propositivo porque formula un modelo aplicable al dominio fluvial amazónico.

Las fuentes empleadas se organizan en cuatro grupos. Primero, documentos nacionales de defensa, ambiente y acción social vinculados a la Amazonía peruana. Segundo, marcos internacionales de ciberseguridad y transformación digital, especialmente el NIST Cybersecurity Framework 2.0. Tercero, documentos doctrinarios y estratégicos sobre operaciones multidominio, mando y control, y transformación naval. Cuarto, fuentes sobre amenazas ambientales y criminales, con énfasis en cri-

men organizado, minería ilegal y convergencia de economías ilícitas.

La propuesta evita deliberadamente incluir información táctica sensible, rutas operacionales específicas, procedimientos internos, vulnerabilidades particulares o detalles que puedan comprometer la seguridad de unidades y personal. El nivel de análisis es estratégico-operacional y doctrinario.

MARCO CONCEPTUAL

Poder fluvial como instrumento de soberanía y desarrollo

El poder fluvial puede definirse como la capacidad del Estado para ejercer presencia, control, movilidad, protección y apoyo al desarrollo en espacios articulados por ríos navegables. En el contexto amazónico, el río es simultáneamente vía logística, frontera, mercado, escuela, hospital, ruta de amenaza y símbolo de presencia estatal.

La experiencia de las Plataformas Itinerantes de Acción Social demuestra que las unidades fluviales pueden ser instrumentos de integración nacional. El Programa Nacional PAIS describe a las PIAS como plataformas móviles que acercan servicios del Estado a comunidades de Loreto, Ucayali y Puno; la información oficial de 2025 refiere atención a 235 comunidades y 68,670 personas, mientras que notas institucionales de la Marina resaltan campañas de acción social en cuencas amazónicas (Programa Nacional PAIS, 2025; Marina de Guerra del Perú, 2026).

Operaciones multidominio y decisión en red

El concepto de operaciones multidominio parte de una premisa central: las decisiones relevantes ya no dependen de un solo dominio físico, sino de la integración de información, comunicaciones, sensores, plataformas, ciberespacio y actores. La estrategia JADC2 del Departamento de Defensa de los Estados Unidos enfatiza la necesidad de dotar a los comandantes de capacidades para mandar y controlar fuerzas a través de dominios y del espectro electromagnético, buscando ventaja de información y decisión (Department of Defense, 2022).

Aunque JADC2 corresponde a una realidad estratégica distinta, su principio general es aplicable al escenario amazónico: conectar sensores, decisores y medios de acción para reducir el tiempo entre detección, comprensión y respuesta. En un ambiente fluvial disperso, esa reducción de tiempos puede marcar la diferencia entre presencia efectiva y reacción tardía.

Transformación naval, sistemas autónomos y flotas híbridas

La U.S. Navy ha priorizado la preparación, las operaciones marítimas distribuidas y la operacionalización de sistemas robóticos y autónomos dentro de su Navigation Plan 2024. Este énfasis refleja una tendencia global: las armadas buscan combinar plataformas tripuladas con medios no tripulados para ampliar alcance, persistencia, masa distribuida y reducción de riesgo para el personal (Chief of Naval Operations, 2024).

Trasladado al entorno amazónico, el concepto de flota híbrida no implica imitar modelos oceánicos, sino adaptar la lógica de integración tripulada-no tripulada al río. Un sistema aéreo no tripulado puede ampliar la observación de una patrullera; un sensor ribereño puede advertir patrones anómalos; una plataforma de superficie no tripulada puede explorar áreas de riesgo; y un centro de fusión puede convertir datos dispersos en alertas operacionales.

Ciberdefensa como condición de resiliencia operacional

La digitalización de las operaciones militares incrementa la eficiencia, pero también amplía la superficie de ataque. El NIST Cybersecurity Framework 2.0 plantea un marco flexible para gestionar riesgos de ciberseguridad mediante funciones de gobernanza, identificación, protección, detección, respuesta y recuperación (National Institute of Standards and Technology, 2024).

Una flotilla inteligente requiere redes, sensores, bases de datos, comunicaciones y sistemas de navegación. Por ello, su resiliencia no puede depender únicamente de medidas físicas. La ciberdefensa

FIGURA 2. MARCO CONCEPTUAL DE LA FLOTILLA INTELIGENTE AMAZÓNICA PARA OPERACIONES MULTIDOMINIO, VIGILANCIA PERSISTENTE Y SUPERIORIDAD INFORMACIONAL.

Fuente: Elaboración propia del autor, basada en conceptos de operaciones multidominio, inteligencia artificial, vigilancia persistente y transformación digital militar.

debe incorporarse desde el diseño, bajo el principio de seguridad por arquitectura: segmentación, redundancia, control de accesos, respaldo de información, procedimientos de continuidad y cultura de seguridad digital.

DIAGNÓSTICO ESTRATÉGICO DEL DOMINIO FLUVIAL AMAZÓNICO

El dominio fluvial amazónico presenta una tensión permanente entre vastedad territorial y disponibilidad limitada de medios. Este desbalance favorece a actores ilícitos que operan de forma descentralizada y aprovechan vacíos de presencia estatal. En términos estratégicos, el desafío no consiste solamente en incrementar patrullajes, sino en mejorar la calidad de la información que orienta dichos patrullajes.

Las amenazas más relevantes no actúan de forma aislada. La minería ilegal puede vincularse a tráfico de insumos, lavado de activos, contaminación por mercurio y coerción sobre comunidades. El narcotráfico puede utilizar rutas fluviales, economías locales, comunicaciones clandestinas y redes transfronterizas. La tala ilegal puede asociarse con ocupación informal, corrupción y violencia contra defensores ambientales. La UNODC ha destacado la convergencia entre economías ilícitas, delitos ambientales y crimen organizado, especialmente en contextos de débil presencia estatal (UNODC, 2024, 2025a, 2025b).

El diagnóstico, por tanto, exige entender la Amazonía como un sistema de seguridad multidimensional. La respuesta naval fluvial debe articular soberanía, legalidad, protección ambiental, apoyo al desarrollo e interoperabilidad interagencial. En términos de comando, el reto es pasar de una lógica de reporte fragmentado a una lógica de conocimiento operacional integrado.

CUADRO 1. DESAFÍOS ESTRATÉGICOS DEL DOMINIO FLUVIAL AMAZÓNICO

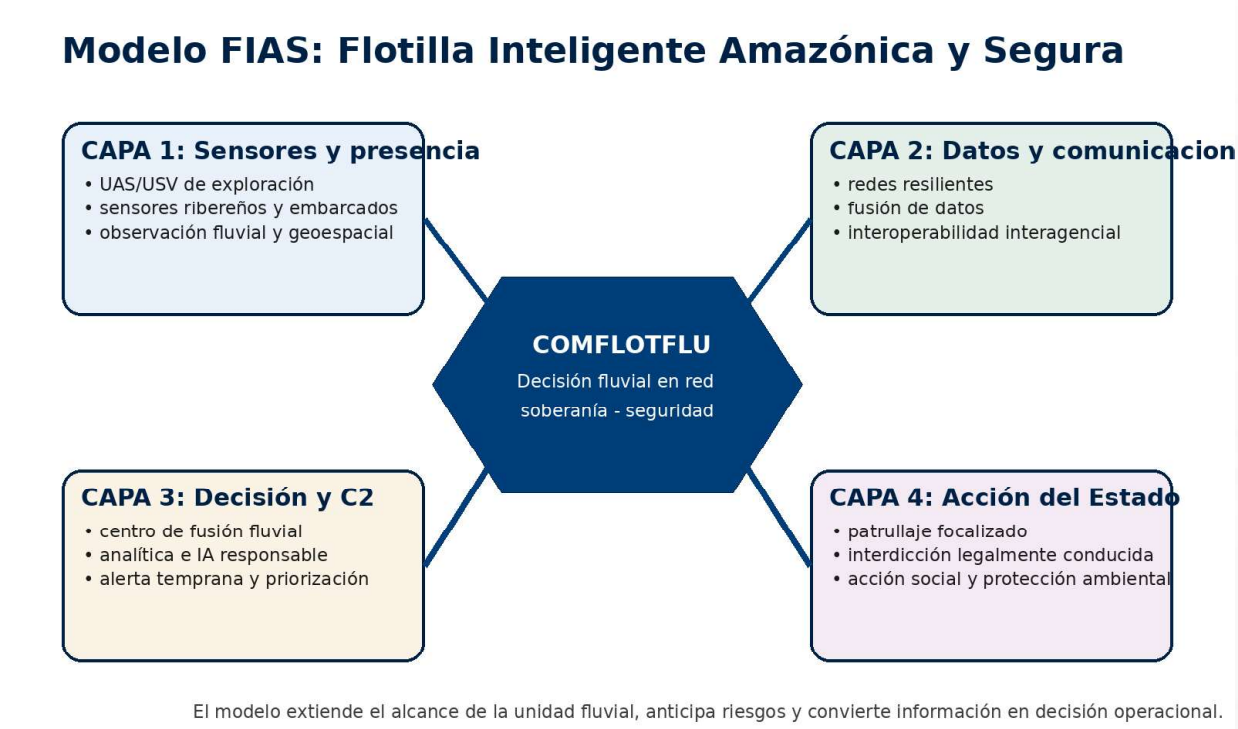
Desafío	Manifestación operacional	Riesgo estratégico	Respuesta FIAS
Dispersión territorial	Comunidades alejadas y extensas rutas fluviales	Presencia estatal intermitente	Vigilancia persistente y priorización de sectores
Amenazas híbridas	Actores ilícitos móviles, redes y economías convergentes	Pérdida de control efectivo	Fusión de información e interdicción focalizada
Limitada conectividad	Cobertura irregular de comunicaciones	Retardo en reporte y respuesta	Redes resilientes y protocolos redundantes
Recursos escasos	Alta demanda de unidades y personal	Sobrecarga operativa	Empleo inteligente de sensores y sistemas no tripulados
Riesgo digital	Dependencia creciente de sistemas conectados	Ataques o fallas de mando y control	Ciberdefensa desde el diseño

MODELO FIAS: FLOTILLA INTELIGENTE AMAZÓNICA Y SEGURA

La Flotilla Inteligente Amazónica y Segura (FIAS) se define como una arquitectura operacional, doctrinaria y tecnológica orientada a extender el alcance del poder fluvial mediante la integración de medios tripulados, sistemas no tripulados, sensores, ciberdefensa, inteligencia artificial y coordinación interagencial.

FIAS no es un proyecto exclusivamente tecnológico. Es un modelo de conducción. Su valor reside en convertir datos dispersos en conocimiento operacional, conocimiento en decisión y decisión en acción estatal legítima. La unidad fluvial continúa siendo el nú-

FIGURA 3. MODELO FIAS: FLOTILLA INTELIGENTE AMAZÓNICA Y SEGURA



Fuente: elaboración propia.

cleo de presencia, mando y autoridad; la innovación actúa como multiplicador de alcance, persistencia y oportunidad.

El modelo se sustenta en siete principios: legalidad, soberanía, interoperabilidad, resiliencia, proporcionalidad, innovación gradual y protección de la población. Estos principios permiten evitar dos riesgos frecuentes: tecnificar sin doctrina o doctrinar sin capacidades reales. La innovación debe ser útil, gradual, auditable y compatible con las capacidades institucionales existentes.

ARQUITECTURA OPERACIONAL PROPUESTA

La arquitectura FIAS se organiza en seis capas funcionales. Esta estructura permite ordenar la implementación sin depender de grandes adquisiciones iniciales. Cada capa puede desarrollarse de manera progresiva, empezando por procedimientos, estandarización de reportes, entrenamiento y uso de capacidades disponibles.

La primera capa corresponde a sensores y observación. Incluye medios embarcados, observación visual sistematizada, registros digitales, sistemas aéreos no tripulados cuando estén disponibles, sensores ribereños y fuentes abiertas autorizadas. La segunda capa corresponde a comunicaciones resilientes, entendidas como la combinación de medios principales, alternos y de contingencia.

La tercera capa es la fusión de información. Allí se integran reportes de unidades, información interagencial, datos geoespaciales, antecedentes de incidentes y patrones históricos. La cuarta capa corresponde a analítica e inteligencia artificial responsable, orientada a apoyar la priorización de patrullajes y detección de patrones, sin sustituir el juicio del comandante.

La quinta capa es la decisión operacional, que traduce información en órdenes, coordinaciones, alertas o recomendaciones. La sexta capa es la acción estatal, que puede adoptar forma de patrullaje, presencia disuasiva, apoyo a acción social, coordinación ambiental o respuesta ante emergencia. Cada capa debe estar protegida por una capa transversal de ciberseguridad.

CUADRO 2. ARQUITECTURA POR CAPAS DEL MODELO FIAS

Capa	Función	Capacidades asociadas	Producto esperado	Control de riesgo
1. Observación	Captar señales del entorno	UAS, sensores, reportes embarcados	Datos primarios	Validación y trazabilidad
2. Comunicaciones	Transmitir información	Redes principales y alternas	Conectividad operacional	Redundancia y disciplina COMSEC
3. Fusión	Integrar fuentes	Centro de fusión fluvial	Panorama operacional	Control de calidad de datos
4. Analítica	Detectar patrones	IA asistiva, georreferenciación	Alertas y prioridades	Supervisión humana
5. Decisión	Asignar medios y coordinar	C2 fluvial e interagencial	Órdenes y acciones	Legalidad y proporcionalidad
6. Acción estatal	Producir efectos legítimos	Patrullaje, acción social, protección ambiental	Presencia efectiva	Evaluación posterior

MATRIZ DE AMENAZAS, CAPACIDADES E INDICADORES

Un artículo orientado a generar impacto académico y utilidad institucional debe traducir conceptos en herramientas. Por ello, se propone una matriz que relaciona amenazas, efectos deseados, capacidades FIAS e indicadores de desempeño. Esta matriz no reemplaza el planeamiento operacional; lo orienta desde una perspectiva estratégica y medible.

Amenaza / problema	Efecto deseado	Capacidad FIAS	Indicador sugerido	Horizonte
Tránsito ilícito fluvial	Detección temprana y disuasión	Vigilancia persistente + análisis de patrones	Alertas validadas / patrullajes focalizados	Corto plazo
Minería ilegal ribereña	Apoyo a interdicción y protección ambiental	Georreferenciación + coordinación interagencial	Zonas críticas monitoreadas	Mediano plazo
Tala ilegal	Identificación de patrones de movilidad	Sensores, reportes y fuentes autorizadas	Reportes integrados por cuenca	Mediano plazo
Baja conectividad	Continuidad de mando y reporte	Comunicaciones resilientes	Tiempo de transmisión de reportes	Corto plazo
Ciberincidentes	Resiliencia de sistemas	CSF 2.0 adaptado al entorno fluvial	Incidentes detectados/ resueltos	Corto-mediano plazo
Demanda social dispersa	Presencia estatal articulada	PIAS + datos de necesidades	Servicios coordinados por campaña	Permanente

HOJA DE RUTA DE IMPLEMENTACIÓN

La implementación de FIAS debe ser gradual, realista y sostenible. Un error común en procesos de innovación militar es iniciar por la adquisición de equipos sin haber definido doctrina, procedimientos, datos, responsabilidades y métricas. En la Amazonía, donde las condiciones logísticas exigen pragmatismo, la secuencia debe partir de lo disponible y avanzar hacia pilotos controlados.

Se propone una hoja de ruta en tres fases. La fase inicial prioriza ordenamiento de información, capacitación interna, estandarización de reportes y diagnóstico de brechas. La fase piloto incorpora capacidades de vigilancia, fusión de datos y ciberseguridad básica en sectores seleccionados. La fase de institucionalización formaliza doctrina, presupuesto, entrenamiento, interoperabilidad y evaluación permanente.

Fase	Periodo referencial	Objetivo	Acciones principales	Resultado esperado
I. Ordenamiento	0-90 días	Crear base doctrinaria y de datos	Inventario de medios, formatos únicos, capacitación, matriz de riesgos	Modelo operativo inicial sin gasto mayor
II. Piloto	3-12 meses	Probar vigilancia y fusión	Sector piloto, reportes georreferenciados, protocolos ciber, coordinación interagencial	Lecciones aprendidas y métricas
III. Escalamiento	12-24 meses	Institucionalizar capacidades	Manual FIAS, centro de fusión, entrenamiento regular, presupuesto progresivo	Capacidad permanente
IV. Consolidación	24+ meses	Integrar innovación continua	Laboratorio fluvial, cooperación regional, actualización doctrinaria	Sistema adaptable y sostenible

GOBERNANZA, RIESGOS Y LÍMITES ÉTICO-LEGALES

La innovación militar debe estar subordinada a la legalidad, la conducción del mando y el respeto de los derechos fundamentales. En el entorno amazónico, ello adquiere especial relevancia por la presencia de comunidades nativas, poblaciones vulnerables y ecosistemas de alto valor ambiental.

El empleo de sistemas autónomos, sensores e inteligencia artificial debe regirse por principios de supervisión humana, necesidad, proporcionalidad, trazabilidad y protección de datos. La IA debe utilizarse como apoyo a la decisión, no como sustituto del criterio del comandante ni de los procedimientos legales aplicables. La confianza en la tecnología debe construirse mediante auditoría, entrenamiento y reglas claras de empleo.

Desde la perspectiva de ciberseguridad, el modelo FIAS requiere una gobernanza mínima: responsables definidos, inventario de activos digitales, clasificación de información, controles de acceso, respaldo de datos, respuesta a incidentes y capacitación continua. El CSF 2.0 de NIST aporta una lógica útil para adaptar estos controles a diferentes niveles de madurez institucional (NIST, 2024).

Riesgo	Impacto	Medida de control	Responsable sugerido
Dependencia excesiva de tecnología	Pérdida de criterio operativo	Supervisión humana obligatoria	Comando y Estado Mayor
Datos incompletos o erróneos	Decisiones mal priorizadas	Validación y trazabilidad	Centro de fusión
Ciberincidente	Interrupción de mando y control	CSF 2.0, respaldo y segmentación	Responsable TIC/Ciber
Afectación a derechos	Pérdida de legitimidad	Legalidad, proporcionalidad y coordinación	Asesoría jurídica y comando
Falta de sostenibilidad	Proyecto no institucionalizado	Fases, métricas y presupuesto gradual	Escalón superior

DISCUSIÓN

La propuesta FIAS no pretende presentar la tecnología como solución automática a problemas estructurales. La innovación solo produce efectos cuando se integra con doctrina, liderazgo, entrenamiento y legitimidad. En la Amazonía, un dron sin análisis, un sensor sin red, una base de datos sin disciplina de reporte o una plataforma sin mantenimiento pueden convertirse en capacidades simbólicas, no en capacidades reales.

El verdadero salto cualitativo consiste en transformar la cultura operacional: pasar de reportar eventos a producir conocimiento; de patrullar por rutina a patrullar por inteligencia; de operar por unidades aisladas a operar como sistema; de responder tarde a anticipar patrones; y de ver la acción social como actividad separada a entenderla como parte de la presencia estatal integral.

La FIAS, además, permite vincular defensa y desarrollo sin confundir funciones. La Marina mantiene su rol institucional de defensa y seguridad, pero lo ejerce en un ecosistema donde la salud, identidad, inclusión social, protección ambiental y control territorial son dimensiones interdependientes. La Amazonía exige una seguridad con rostro humano, pero respaldada por capacidades reales.

Desde una perspectiva académica, la contribución del artículo radica en adaptar conceptos globales -operaciones multidominio, flotas híbridas, ciberresiliencia e inteligencia artificial- a un escenario fluvial latinoamericano. Esta adaptación es relevante porque la mayor parte de la literatura sobre sistemas autónomos y mando en red se concentra en escenarios oceánicos, aéreos o terrestres de alta intensidad, mientras que la Amazonía demanda soluciones híbridas, graduales y culturalmente sensibles.

CONCLUSIONES Y RECOMENDACIONES

1. La Amazonía peruana debe ser entendida como un espacio estratégico donde soberanía, seguridad, desarrollo y ambiente se articulan a través del dominio fluvial.
2. El modelo tradicional de presencia fluvial, aunque indispensable, resulta insuficiente frente a amenazas híbridas, móviles y tecnológicamente adaptativas.
3. La Flotilla Inteligente Amazónica y Segura constituye una propuesta doctrinaria aplicable al contexto peruano, basada en vigilancia persistente, sistemas no tripulados, inteligencia artificial, ciberdefensa e interoperabilidad.
4. La tecnología debe actuar como multiplicador del liderazgo naval y de la experiencia marinera, no como reemplazo del criterio del comandante.
5. La ciberdefensa debe incorporarse desde el diseño de cualquier arquitectura fluvial inteligente, pues la digitalización sin resiliencia genera vulnerabilidad.
6. La acción social y la seguridad no son dimensiones excluyentes: en la Amazonía, la presencia estatal efectiva requiere ambas.
7. La implementación debe ser gradual, medible y sostenible, iniciando con capacidades disponibles, estandarización de información y pilotos controlados.

RECOMENDACIONES ESTRATÉGICAS

1. Desarrollar una Directiva o Lineamiento de Innovación Fluvial para orientar la implementación progresiva del modelo FIAS.
2. Crear un repositorio de información fluvial no clasificada y estandarizada que permita análisis histórico, georreferenciación y evaluación de patrones.
3. Implementar un piloto de vigilancia persistente en un sector seleccionado, con indicadores claros y evaluación posterior.
4. Fortalecer la capacitación del personal en ciberseguridad operacional, análisis de información, empleo responsable de sistemas no tripulados y protección de datos.
5. Impulsar cooperación interagencial con entidades de desarrollo, ambiente, inteligencia y control, preservando la conducción naval del componente fluvial.
6. Promover investigación aplicada con escuelas militares, universidades y centros tecnológicos nacionales para adaptar soluciones de bajo costo al ambiente amazónico.
7. Elaborar una doctrina peruana de operaciones fluviales multidominio, tomando como base la experiencia nacional y las tendencias internacionales.

APORTE ORIGINAL DEL ARTÍCULO

El aporte original de este artículo consiste en formular un modelo conceptual y operativo denominado FIAS, diseñado específicamente para el contexto amazónico peruano. A diferencia de enfoques genéricos sobre transformación digital militar, FIAS parte de la realidad fluvial: ríos como corredores estratégicos, unidades como presencia estatal, comunidades como centro de gravedad humano y amenazas como redes adaptativas. Su valor reside en proponer una arquitectura escalable, medible y doctrinariamente coherente con la función de una flotilla fluvial moderna.

REFERENCIAS

Chief of Naval Operations. (2024). Navigation Plan for America's Warfighting Navy 2024. U.S. Navy. https://www.navy.mil/Portals/1/CNO/NAVPLAN2024/Files/CNO-NAVPLAN-2024-high-res-v2.pdf

Department of Defense. (2022). Summary of the Joint All-Domain Command and Control Strategy. U.S. Department of Defense. https://media.de-

fense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf

DCAF. (2024). Artificial Intelligence (AI) and the Defence Sector. Geneva Centre for Security Sector Governance. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BKG_30_AI-DefenceSector.pdf

Instituto de Investigaciones de la Amazonía Peruana. (s. f.). Institución: ámbito de acción. IIAP. https://portal.iiap.gob.pe/institucion

Marina de Guerra del Perú. (2026). Marina de Guerra del Perú iniciará campaña de acción social en la Amazonía en beneficio de más de 800 mil habitantes. Gob.pe. https://www.gob.pe/institucion/marina/noticias/1357178-marina-de-guerra-del-peru-iniciara-campana-de-accion-social-en-la-amazonia-en-beneficio-de-mas-de-800-mil-habitantes

Ministerio de Defensa del Perú. (2005). Libro Blanco de la Defensa Nacional. Gob.pe. https://www.gob.pe/institucion/mindef/informes-publicaciones/334409-libro-blanco-de-la-defensa-nacional

Ministerio del Ambiente del Perú. (s. f.). Perú, país de bosques. MINAM. https://www.minam.gob.pe/programa-bosques/peru-pais-de-bosques/

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29 https://doi.org/10.6028/NIST.CSWP.29

OECD. (2025). Governing with Artificial Intelligence. OECD Publishing. https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report.html

Programa Nacional PAIS. (2025). PIAS - Plataformas móviles. Gob.pe. https://www.gob.pe/66629-programa-nacional-plataformas-de-accion-para-la-inclusion-social-pias-plataformas-moviles

Programa Nacional PAIS. (2026). Plataformas Itinerantes (PIAS). Gob.pe. https://www.gob.pe/institucion/pais/tema/plataformas-itinerantes-pias

United Nations Office on Drugs and Crime. (2024). World Drug Report 2024. UNODC. https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2024.html

United Nations Office on Drugs and Crime. (2025a). The Global Analysis on Crimes that Affect the Environment: Part 2a - Forest Crimes: Illegal Deforestation and Logging. UNODC. https://www.unodc.org/unodc/en/data-and-analysis/statistics/publications.html

United Nations Office on Drugs and Crime. (2025b). The Global Analysis on Crimes that Affect the Environment: Part 2b - Minerals Crime: Illegal Gold Mining. UNODC. https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/ECR25_P2b_Minerals_Crime.pdf.

Nota

El presente artículo ha sido formulado a nivel estratégico-operacional. No contiene información clasificada, rutas, procedimientos tácticos específicos, vulnerabilidades particulares ni datos cuya divulgación pueda comprometer la seguridad de unidades, personal o instalaciones. Su finalidad es académica, doctrinaria y propositiva.