



LA GESTIÓN AMBIENTAL INTELIGENTE: IA Y AUTOMATIZACIÓN EN LA IMPLEMENTACIÓN DE LA ISO 14001 PARA LA ARMADA 2050

Introducción

EN enero de 2025 algo cambió silenciosamente en el Tercio de Levante: obtuvo la certificación ISO 14001:2015 por AENOR (Asociación Española de Normalización y Certificación). Para el observador casual, un logro administrativo más. Para la Armada, el nacimiento de un nuevo paradigma: la sostenibilidad como arma operativa.

No estamos hablando de «pintar los barcos de verde», sino de días adicionales de autonomía en el mar, de bases que pueden operar sin red eléctrica externa, de decisiones tácticas optimizadas por algoritmos que reducen nuestra huella de detección mientras ahorran combustible. Eso es proyección real de la Fuerza haciendo un uso optimizado y eficiente de los medios disponibles.

Bienvenidos a la era del Sistema de Gestión Ambiental Inteligente (SGAI), donde la inteligencia artificial (IA) convierte el cumplimiento normativo de la ISO 14001:2015 en ventaja estratégica y eficiencia en las operaciones.

¿Por qué la sostenibilidad importa en defensa?

La pregunta que muchos se hacen es legítima: ¿por qué una fuerza armada debería preocu-

parse por su huella de carbono cuando su misión es defender a la nación? La respuesta tiene tres niveles, todos estratégicos en el sentido siguiente:

—*La autonomía operativa.* La *Visión Armada 2050* plantea un escenario inquietante pero realista: España podría enfrentar amenazas «en solitario, sin apoyo externo». En ese contexto, cada litro de combustible ahorrado, cada día de autonomía energética ganada mediante paneles solares y baterías inteligentes, cada optimización logística que reduzca dependencias externas, se convierten en capacidad de combate real.

Si un buque consume un 20 por 100 menos de combustible porque la IA y el sistema de algoritmos han optimizado la velocidad y la ruta sin comprometer la misión, eso son días adicionales en patrulla sin necesidad de un petrolero de reabastecimiento. En una crisis en la que el enemigo puede interdecir nuestras líneas logísticas, eso marca la diferencia entre cumplir la misión o «abortarla».

—*La legitimidad internacional.* La OTAN declaró el cambio climático como «multiplicador de amenazas» en su Climate Change and Security Action Plan en la Cumbre de Bruselas de 2021. La Agencia Europea de Defensa vincula explícitamente la sostenibilidad con la resiliencia



de las fuerzas armadas. No es imperativo político: es alineamiento estratégico con aliados que definirán las coaliciones del futuro y las relaciones supranacionales entre los miembros de la organización.

—*El respaldo social.* En democracias avanzadas, el apoyo ciudadano a las fuerzas armadas no es automático: se construye. Una marina que demuestra responsabilidad ambiental fortalece su contrato social, mejorando su imagen pública y facilitando inversiones futuras y el reclutamiento de talento joven sensibilizado con estas cuestiones.

¿Qué es exactamente el Sistema de Gestión Ambiental Inteligente?

Este Sistema, también llamado SGAI, suena a tecnocracia; no obstante, ¿de qué estamos hablando realmente? En esencia, el SGAI es la fusión de dos mundos: la ISO 14001:2015, el estándar internacional de gestión ambiental que certifica a las organizaciones, desde hospitales hasta fábricas, y las capacidades de la inteligencia artificial, que están transformando industrias enteras.

La ISO 14001 funciona con el Ciclo PDCA: Planificar, Hacer, Verificar, Actuar. Es un sistema de mejora continua por el que una organización identifica sus impactos ambientales, esta-



Diagrama del Ciclo PDCA.
(Fuente abierta generada con IA)

blece objetivos de reducción, implementa controles, mide resultados y ajusta. Tradicionalmente, esto genera montañas de papel, hojas de cálculo interminables y personal dedicado a rellenar formularios.

Aquí es donde entra la IA en el funcionamiento de los sistemas

Imaginemos miles de sensores IoT (internet de las cosas) distribuidos en un arsenal: medidores de consumo eléctrico en cada edificio,

sensores de calidad del agua, detectores de emisiones, contenedores de residuos inteligentes que comunican su llenado. Todos generando datos en tiempo real. Ahora añadamos algoritmos de *machine learning*¹ capaces de:

- Predecir que un tanque de sentina tiene un 92 por 100 de probabilidades de incumplir normativas si su tasa de uso supera equis metros cúbicos por hora.
- Optimizar automáticamente las rutas de recogida de residuos para minimizar combustible.
- Detectar fugas en la red hídrica antes de que se conviertan en un problema grave.
- Ajustar en tiempo real la mezcla de energía solar, baterías y generadores para maximizar eficiencia.
- Recomendar al comandante de un buque la velocidad óptima que balancee la urgencia táctica con la eficiencia energética.

Lo que antes requería un equipo de personas revisando informes mensuales, ahora ocurre en tiempo real, 24/7, con una precisión imposible para humanos, y no es sólo monitoreo: el sistema aprende, predice y prescribe acciones.

¿Cómo funciona en la práctica?

Pongamos ejemplos concretos. ¿Qué hace el SGAI en un día normal?:

- En un arsenal: un día cualquiera a las 06:00 en el Arsenal de Cartagena. El SGAI ha estado trabajando toda la noche. Ha predicho que la generación solar será óptima entre las

11:00 y las 15:00. En consecuencia, ha programado tareas energéticamente intensas —como recarga de vehículos eléctricos y pruebas de equipos— para esas franjas horarias. Ha retrasado el arranque de un generador diésel porque las baterías tienen capacidad suficiente. Ahorro: 300 euros y 200 kg de CO₂.

- A las 09:00, un sensor detecta un pico anómalo de consumo en el Edificio 7. El sistema cruza datos: no hay actividad especial programada. Alerta al técnico de mantenimiento: posible fallo en el sistema de climatización. Se confirma: un compresor atascado consume el doble de lo normal. Reparación inmediata. Ahorro: 1.500 euros mensuales.

- A las 14:00 los contenedores inteligentes de residuos comunican sus niveles de llenado. La IA recalcula la ruta de recogida: hoy no es necesario visitar el sector norte, ahorro de 15 km. El camión hace su ronda optimizada. Ahorro: tiempo, combustible, emisiones.

- A las 18:00, el sistema genera un informe ejecutivo para el mando responsable: «Hoy hemos operado seis horas en modo isla [energía 100 por 100 renovable]. Consumo total: -12 por 100 respecto a la media. Un incidente detectado y resuelto. Tres contenedores de reciclaje presentan contaminación cruzada: recomiendo sesión de formación al personal del Sector 3».

- En un buque desplegado de misión: la fragata *F-105* navega en patrulla por el Mediterráneo Oriental. Su gemelo digital —la réplica virtual del buque— procesa datos en tiempo real. Su comandante recibe una orden: transitar a zona de operaciones a 400 millas con urgencia moderada y con una llegada deseada en 36 horas. El sistema de IA analiza:

1. Aprendizaje automático (*machine learning*): subcampo de la inteligencia artificial que se centra en el diseño y estudio de algoritmos que permiten a las computadoras aprender y mejorar su rendimiento en tareas específicas, como clasificación, regresión o *clustering*, a partir de la experiencia (datos), sin ser programadas explícitamente para esa tarea.

Fragata *Cristóbal Colón* (F-105).
(Fuente: Armada)



condiciones meteorológicas, estado de la mar, consumo de combustible a diferentes velocidades, regulaciones de emisiones en las aguas territoriales que atravesará y capacidad restante de los tanques. Y realiza la siguiente recomendación: «Velocidad 18 nudos en lugar de 22. Llegaremos con dos horas de retraso respecto a máxima velocidad, pero ahorraremos 8.000 litros de combustible y reduciremos emisiones de NOx en un 40 por 100. Nuestra firma acústica será un 30 por 100 menor, dificultando la detección por submarinos potencialmente hostiles. ¿Autoriza perfil optimizado?». El comandante acepta. No es sólo medioambiente y gestión eficiente de los medios, sino que al final se traduce en una operatividad también más inteligente y eficaz, optimizando los medios y recursos disponibles. Durante la singladura, el sistema de tratamiento de aguas residuales se autorregula. Los sensores miden la composición del efluente y la IA ajusta las dosis químicas al mínimo necesario. El buque cumple rigurosamente con MARPOL (Convenio Internacional para prevenir la Contaminación por Buques) sin intervención de la dotación.

¿Qué papel juega la ciberseguridad con un sistema de gestión tan complejo?

Miles de sensores conectados. ¿No es un problema grave de seguridad? Absolutamente. Y de hecho es el talón de Aquiles del SGAI si no se gestiona correctamente.

Tenemos que asumir que un adversario con capacidades cibernéticas avanzadas intentará comprometer estos sistemas. Imaginemos que manipulan los datos de consumo de combustible de un buque. El comandante cree que tiene autonomía para 10 días cuando en realidad tiene para siete. Puede ser catastrófico y dar lugar al incumplimiento inevitable de la misión encomendada. O peor: un ataque a los sistemas de control de la microrred energética de una base. Si consiguen acceso a los PLC (controladores lógicos programables) que gestionan la microrred, podrían provocar un apagón justo cuando más se necesita la energía. O sabotear las baterías de almacenamiento. Es un vector de ataque nuevo que no existía hace una década.

La respuesta a todos estos problemas es el diseño de una arquitectura de seguridad en capas, que consiste en una estrategia de defensa que protege sistemas críticos mediante múltiples niveles de control, desde lo físico hasta lo lógico, dificultando que un atacante comprometa todo el entorno. Esta arquitectura, también conocida como defensa en profundidad, se basa en el principio de que ningún mecanismo de seguridad es infalible por sí solo. Al combinar varias capas, se crea una red de protección que mitiga riesgos, incluso si una capa es vulnerada. Las capas de la arquitectura de ciberseguridad son las siguientes:

Física:

- Protege el acceso físico a infraestructuras críticas: servidores, PLC, baterías, centros de datos.
- Ejemplos: cerraduras, vigilancia, control de acceso biométrico.
- Sin esta capa, un atacante podría manipular directamente los dispositivos sin necesidad de jaquearlos.

Red:

- Controla el tráfico entre dispositivos y sistemas.
- Incluye *firewalls*, segmentación de red, detección de intrusos (IDS/IPS).
- Evita que un atacante se mueva lateralmente dentro de la red tras comprometer un punto.

Perímetro:

- Protege el borde entre la red interna y el exterior (internet).
 - Se usan *proxies*, VPN, filtrado de contenido y *gateways* seguros.
- Es la primera línea de defensa contra ataques externos como *malware* o *phishing*.

Aplicación:

- Asegura el *software* que gestiona funciones críticas (como los sistemas de navegación o control energético).
- Incluye validación de entradas, actualizaciones seguras y pruebas de vulnerabilidades.
- Un fallo aquí podría permitir manipular datos como el consumo de combustible.

Datos:

- Protege la integridad, confidencialidad y disponibilidad de la información.
- Se usan cifrado, *backups*, control de versiones y monitoreo de accesos.
- Evita que se alteren datos sensibles, como la autonomía de buques o el estado de las baterías.

Identidad y acceso:

- Controla quién puede acceder a qué recursos y bajo qué condiciones.
- Se implementan autenticación multifactor, gestión de privilegios y auditorías.
- Un atacante que accede como administrador podría sabotear sistemas enteros.

(Fuente abierta generada con IA)



Supervisión y respuesta:

- Monitorea continuamente el entorno para detectar y responder a incidentes.
- Incluye análisis de comportamiento y planes de contingencia.
- Permite reaccionar ante ataques, como el acceso a PLC o la manipulación de datos.

¿Cómo se materializa la arquitectura de ciberseguridad en capas?

La teoría es clara: proteger los sistemas críticos requiere una arquitectura de seguridad en capas. Pero, ¿cómo se traduce esto en acciones concretas? En el terreno operativo, la seguridad no se logra con buenas intenciones, sino con procedimientos rigurosos y tecnologías avanzadas que refuercen cada eslabón de la cadena digital. Éstos son los pilares que hacen posible esa protección:

Microsegmentación de redes

La primera línea de defensa es la separación física y lógica entre los sistemas de tecnología operacional (OT) —como sensores y PLC— y las redes de tecnología de la información (IT) e internet. Incluso dentro del entorno OT, se aplican segmentaciones internas: los sistemas que gestionan la microrred energética de una base no comparten red con los sensores de residuos. Esta compartimentación limita el alcance de cualquier intrusión.

Modelo Zero Trust²

En este paradigma no existe la confianza por defecto. Cada dispositivo, cada conexión, cada solicitud debe ser verificada de forma continua. El acceso se concede no por ubicación o rol, sino por autenticación constante y contextual. Es un enfoque que asume que la amenaza puede estar en cualquier parte, incluso dentro del perímetro.

Detección de anomalías con inteligencia artificial

La misma inteligencia artificial que optimiza el consumo energético se convierte en centinela digital. Algoritmos entrenados para reconocer patrones normales de comportamiento detectan desviaciones sospechosas: un sensor que cambia súbitamente su frecuencia de comunicación, por ejemplo, puede activar una alerta de posible intrusión. La IA permite una vigilancia proactiva, adaptativa y en tiempo real.

Blockchain³ para trazabilidad

Los datos críticos —especialmente aquéllos que deben ser auditados por organismos externos— se registran en *blockchain*, garantizando su integridad. Esta tecnología hace que la información sea inmutable: aunque un atacante logre comprometer un sensor, no podrá alterar retroactivamente el historial

2. *Zero Trust* es un modelo de seguridad que se basa en el principio de «nunca confiar, siempre verificar». En lugar de asumir que todo dentro de la red corporativa es seguro, este enfoque asume que cualquier usuario, dispositivo o conexión podría estar comprometido y, por lo tanto, exige una verificación explícita de identidad y autorización antes de otorgar acceso a cualquier recurso.

3. El *blockchain* (cadena de bloques) es una tecnología de registro distribuido (DLT) que permite almacenar información de manera segura, descentralizada e inmutable.

registrado. Es una garantía de transparencia y resiliencia frente a la manipulación.

recomendación de velocidad óptima, es más probable que la acepte.

Una carrera que no podemos perder

La ciberseguridad en entornos militares y estratégicos ya no es una cuestión técnica, sino una necesidad existencial. Cada avance en protección es respondido por nuevas tácticas de ataque. Es una carrera armamentística silenciosa, pero decisiva, y debemos ganarla no por ventaja, sino por supervivencia.

¿Cuáles son los mayores desafíos? Nada es perfecto. ¿Qué puede salir mal?

El factor humano

La tecnología es la parte fácil, lo difícil son las personas, el recurso humano con su complejidad y variabilidad.

Cambiar culturas organizacionales profundamente arraigadas en sistemas de operaciones obsoletos es el verdadero reto. Oficiales y suboficiales que llevan décadas haciendo las cosas de cierta manera deben ahora confiar en recomendaciones algorítmicas. No es trivial, es crucial; la adaptación es clave para la supervivencia. Es un cambio generacional: los jóvenes que ingresan hoy han crecido con *smartphones* y algoritmos. Para ellos es natural, pero para las generaciones anteriores y para el personal más antiguo es incómodo.

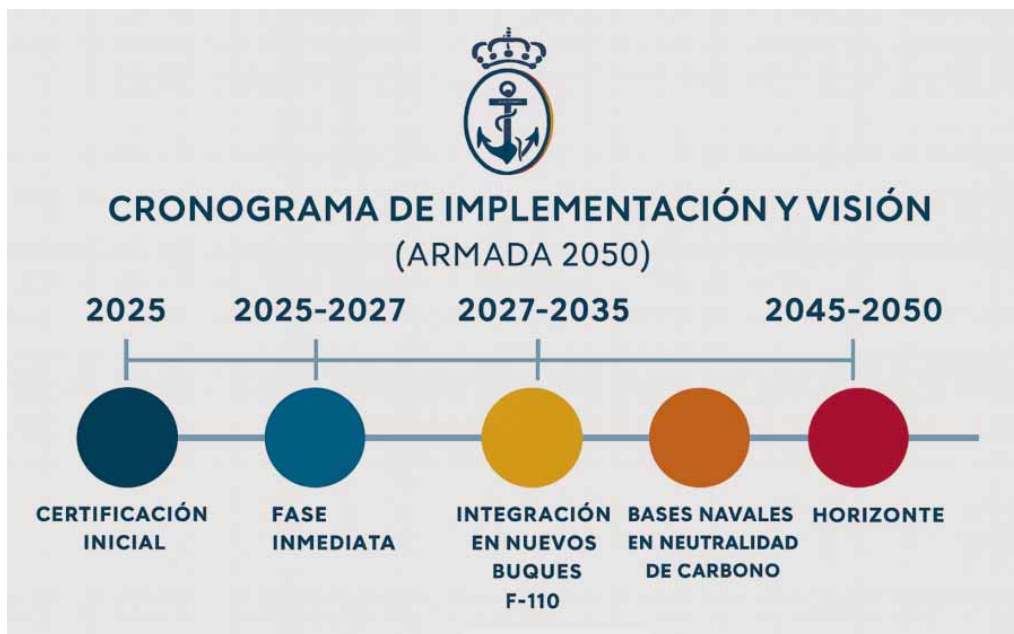
La solución: formación masiva y continua, no sólo sobre cómo usar el sistema, sino por qué funciona. Cuando el comandante de un buque entiende la matemática que hay detrás de la

La brecha de competencias

La Armada necesita urgentemente perfiles híbridos: ingenieros con conocimiento operacional naval, oficiales con formación en ciencia de datos, técnicos capaces de mantener sensores IoT en un ambiente marino hostil. Estamos compitiendo por el talento con empresas del nivel de Google o Amazon, y el sector privado paga mejor, por lo que necesitamos hacer atractiva la carrera militar para estos perfiles, y la estrategia para conseguirlo incluye becas para formación especializada, colaboraciones con universidades y la promesa de trabajar en tecnologías punteras que no están disponibles en el sector civil.

El coste inicial

Implementar el SGAI en toda la Armada requiere costes significativos: cientos de millones de euros en sensores, infraestructura computacional, *software*, formación y ciberseguridad. Es una inversión, no un gasto, pues el retorno llegaría en tres o cinco años vía ahorros operativos. Y lo que compramos no es sólo eficiencia ambiental: es resiliencia, autonomía y capacidad operativa mejorada. Intentar poner precio a eso es complejo, y justificar su utilidad, aún más teniendo en cuenta los objetivos estratégicos de la Armada para 2050. Además, en tiempos de presupuestos ajustados cada euro de inversión en SGAI es un euro que no va a otros programas. La priorización es inevitable y dolorosa, es un proceso de transformación forzosa.



(Fuente abierta generada con IA)

¿Qué sigue después? Si el SGAI es el presente, ¿cuál es el futuro?

Fase inmediata (2025-2027): escalado

Extender el modelo de la Armada a todas las dependencias subordinadas presenta desafíos únicos: Rota, con su alta actividad de repostaje; Ferrol, con sus astilleros; Cartagena, con su polígono de tiro. Cada unidad o arsenal tiene una configuración y una idiosincrasia que lo hacen singular, dificultando la aplicación de un modelo único común a todos, con el consiguiente coste que supone esta variabilidad.

Fase media (2027-2035): integración en buques

Las fragatas *F-110* podrían incluir una arquitectura de SGAI desde el diseño. No sería un

añadido, sino parte del sistema de combate. Imaginen un buque en el que la IA gestiona simultáneamente el combate, la navegación y el impacto ambiental de manera integrada, o la modernización (*retrofitting*) de unidades existentes cuando ello sea técnica y económicamente viable y necesario desde el punto de vista operativo. Una *F-100* modernizada podría ganar capacidades SGAI mediante la actualización de sensores y *software* sin inversiones muy elevadas.

Fase avanzada (2035-2045): autonomía total

Bases navales operando en neutralidad de carbono: 100 por 100 de energía renovable con almacenamiento suficiente para días de autonomía completa. Microrredes tan inteligentes que pueden vender excedentes a la red civil en tiempos de paz. Buques con propulsión híbrida diésel-eléctrica o incluso



Recreación de la futura base naval de La Algameca. (Fuente abierta generada con IA)

totalmente eléctrica para patrullas de baja intensidad. La IA gestionando cada vatio para maximizar sigilo y autonomía.

El horizonte (2045-2050): integración estratégica

Una IA capaz de optimizar no ya un buque o una base, sino toda la flota simultáneamente. Sistemas que recomiendan redistribución de unidades considerando no sólo factores tácticos, sino también eficiencia logística y huella ambiental. Computación cuántica para resolver problemas de optimización que hoy son imposibles y, por otro lado, la IA generativa creando planes de contingencia ambiental para escenarios que ni siquiera hemos imaginado. Robótica autónoma realizando inspecciones ambientales en espacios peligrosos sin exponer personal.

Y en el horizonte más lejano: las marinas que no sólo minimizan su impacto, sino que activamente contribuyen a la regeneración ambiental marina como parte de su misión. Buques que monitorizan y protegen ecosistemas mientras patrullan. Ésa es la visión última y el objetivo a alcanzar.

¿Qué significa esto para España? Y más allá de la Armada, ¿cuál es el impacto nacional?

Liderazgo internacional

Si España ejecuta correctamente esta visión, se posiciona como líder global en sostenibilidad militar. Eso se traduce en influencia en la OTAN, en la Agencia Europea de Defensa y en foros de Naciones Unidas. Seríamos el país al que otros acuden para aprender: *softpower* real, visible y alcanzable. Todo ello abriría las puertas para la exportación de tecnología.

Industria dual

Las tecnologías desarrolladas para el SGAI tienen aplicación inmediata en el sector civil: puertos comerciales, flotas pesqueras, gestión de ciudades costeras, industria naval civil. Estamos creando un ecosistema de empresas especializadas en IA para gestión ambiental en entornos marinos hostiles. Eso es empleo cualificado, exportación de tecnología e incremento sustancial del PIB. Empresas españolas podrían convertirse en proveedores preferenciales de marinas aliadas que busquen soluciones similares. Un mercado global de miles de millones.

Resiliencia nacional

En un escenario de crisis —desastre natural, ataque cibernético a infraestructuras civiles...—, las bases navales con microrredes autónomas pueden servir como nodos de resiliencia para comunidades locales. Una base que puede operar en modo isla no sólo se protege a sí misma: puede proporcionar energía de emergencia a hospitales o centros de coordi-

nación de crisis cercanos. Eso es defensa integral del territorio.

La última pregunta: ¿vale la pena?

En una era en que las amenazas se multiplican —terrorismo, Estados revisionistas, crimen organizado, ciberataques...— y los presupuestos son finitos, ¿es realmente prioritario que la Armada sea «verde»? La respuesta, paradójicamente, es que formular la pregunta así es un error categórico. No se trata de elegir entre capacidad operativa y sostenibilidad, sino de entender que en el siglo XXI la sostenibilidad es capacidad operativa, y ambos conceptos van de la mano.

Una Armada que consume menos combustible es una Armada con mayor autonomía estratégica. Una Armada con bases energéticamente autónomas es una Armada más resiliente ante ataques asimétricos. Una Armada que optimiza cada recurso mediante IA es una Armada que puede hacer más con menos. Y una Armada que demuestra responsabilidad ambiental es una Armada que mantiene el contrato social con los ciudadanos que la financian y cuyos hijos sirven en ella.

No estaríamos sacrificando capacidad por sostenibilidad, sino que usaríamos la sostenibilidad para multiplicar nuestra capacidad. Ésa es la diferencia fundamental.

¿Qué están haciendo otras marinas del mundo?

«El mar, que durante siglos fue la ruta fundamental para la expansión de imperios, es ahora también indicador de nuestra responsabilidad

colectiva. La Armada que entienda esto primero no sólo será más sostenible: será la más poderosa.»

(Armada 2050)

España no está sola en esto. ¿Cómo se compara con otras potencias navales? La carrera por la sostenibilidad militar es global y cada vez más compleja y competitiva, siendo el factor tiempo crucial. Cada marina aborda el desafío desde su propia perspectiva estratégica y capacidades tecnológicas; cada país desarrolla sus capacidades en función de sus intereses estratégicos.

tienen un volumen de datos que nosotros no podemos igualar, pero también una complejidad burocrática que los ralentiza. Somos más ágiles al ser menos compleja nuestra organización.

La Marina estadounidense ha logrado reducir su consumo energético en instalaciones terrestres en un 35 por 100 desde 2010. Ha desplegado microrredes en bases clave y está probando biocombustibles avanzados en sus buques, aunque con resultados mixtos por problemas de coste y logística de suministro.

Estados Unidos: la potencia del big data⁴

La US Navy, con un presupuesto descomunal y 290 buques, ha apostado por la escalada masiva. Su programa Energy, Environment and Climate Change gestiona datos de más de 400 instalaciones navales mediante plataformas de analítica de datos centralizadas. Ellos

Reino Unido: innovación en propulsión

La Royal Navy ha tomado un camino diferente: la innovación radical en propulsión. Sus destructores *Type 45* ya tienen propulsión eléctrica integrada, aunque con problemas técnicos iniciales que han requerido costosas actualizaciones.

El HMS *Daring* Type 45.
(Fuente: www.wikipedia.org)



4. El *big data* (macrodatos) se refiere a un conjunto de tecnologías y metodologías diseñadas para almacenar, gestionar y, principalmente, analizar volúmenes de datos extremadamente grandes y complejos que los sistemas tradicionales de gestión de datos no pueden procesar eficientemente.

El programa más ambicioso es la clase *Dreadnought* de submarinos nucleares de nueva generación, diseñados desde cero con criterios de eficiencia energética incluso en el reactor nuclear. Parece contradictorio hablar de sostenibilidad en un submarino nuclear, pero el reactor Rolls-Royce PWR3 es significativamente más eficiente que las generaciones anteriores, produce menos residuos radiactivos y tiene ciclos de mantenimiento más largos.

En instalaciones terrestres, la Royal Navy está probando sistemas de almacenamiento de energía mediante baterías de flujo de vanadio, una tecnología más cara que las baterías de litio pero con ciclos de vida de 20+ años, ideal para infraestructuras militares permanentes.

Francia: el enfoque nuclear en Europa

La Marine Nationale tiene una ventaja única: su flota de submarinos y el portaviones *Charles de Gaulle* son nucleares, lo que le confiere autonomía estratégica sin dependencia de combustibles fósiles en sus unidades principales. Pero la energía nuclear convencional no resuelve todos los problemas ambientales: genera residuos sólidos y consume agua, y entre tanto sus buques convencionales siguen dependiendo de combustibles fósiles. Además, el coste de desarrollo y mantenimiento de la propulsión nuclear es prohibitivo para la mayoría de países.

Francia está invirtiendo fuertemente en IA para gestión logística, aplicando algoritmos de optimización para reducir los movimientos innecesarios de su flota en tiempos de paz. Cada hora de navegación que se pueda evitar mediante una mejor planificación es ahorro directo y emisiones no producidas.

Alemania: liderazgo en submarinos convencionales eficientes

La Deutsche Marine ha desarrollado los submarinos *Type 212* y *214* con propulsión AIP (*air independent propulsion*), que combina pilas de combustible de hidrógeno con diésel. Pueden permanecer sumergidos semanas sin esnórquel, operando silenciosamente con cero emisiones. Es la tecnología más madura de propulsión alternativa en submarinos y varios países han adoptado este diseño precisamente por esa combinación de sigilo operativo y eficiencia ambiental.

Pero, ¿dónde está España en este mapa?

No tenemos el presupuesto de Estados Unidos ni la tradición nuclear de Francia ni la industria de submarinos de Alemania, pero sí algo valioso: agilidad y experiencia mediterránea en operaciones complejas. Además, con la reciente implantación de un SGAI, España gozaría de un enfoque integrado que ninguna otra marina ha implementado a día de hoy, dándole una ventaja estratégica incluso frente a otras con presupuestos más elevados.

¿Cómo se adiestra y se forma al personal para este nuevo paradigma?

Una cosa es tener la tecnología y otra muy distinta es que la gente sepa usarla. ¿Cómo se forma al marino del siglo XXI?

En la Escuela Naval Militar de Marín, Pontevedra, entre clases tradicionales de Navegación, Táctica Naval y Armamento, sería conveniente incluir una nueva asignatura en el Grado: Análítica de Datos Aplicada a Operaciones

Navales. Ésta no pretendería formar a científicos de datos, sino crear alfabetización digital crítica en los futuros cuadros de mando: entender qué puede hacer la IA, cuáles son sus limitaciones, cuándo confiar en una recomendación algorítmica y cuándo cuestionarla. Es un pilar básico en la formación que los mandos tengan los conocimientos de uso de la IA aplicada a la Armada.

Simulación con realidad virtual: otra herramienta de formación en buques, unidades y arsenales

La realidad virtual (VR)⁵ nos permite entrenar en situaciones ambientales críticas sin riesgo real ni coste de desplegar un buque, pudiéndose simular 50 escenarios diferentes en una jornada laboral, lo que en una formación tradicional se tardaría meses.

Los datos de desempeño en VR alimentan el sistema de IA que personaliza la formación continua. Si un miembro de la dotación mostrara dificultades en la gestión de residuos peligrosos, el sistema le programaría módulos de refuerzo específicos.

La resistencia de los veteranos

La estrategia para estos casos no es la imposición, sino la demostración gradual. Se le pediría probar el sistema en situaciones de bajo riesgo para facilitar el proceso de apren-

dizaje y adaptación, comparando su decisión con la recomendación de la IA. Con el tiempo, los más veteranos verían que el algoritmo tiene información que ellos no poseían: datos meteorológicos más precisos, consumo histórico detallado, proyecciones del tráfico marítimo, generando una mayor confianza en el algoritmo.

El punto de inflexión llegará cuando la IA detecte algo que el comandante de un buque pasó por alto en su momento, como por ejemplo que el sistema alerte de un consumo anómalo de agua cuando realmente se trata de una fuga en un baño que ha pasado inadvertida durante semanas. Este caso tan habitual podría suponer el ahorro de miles de litros de agua.

«Gamificación»⁶ y competencia entre unidades para mejorar la operatividad

La Armada tiene a su disposición herramientas para la mejora de la competitividad corporativa. Por ejemplo, se podría establecer un elemento de competencia amistosa: un *ranking* de desempeño ambiental entre unidades similares. Las fragatas compiten entre sí: ¿cuál consume menos combustible por milla navegada? Por otro lado, los arsenales y bases también podrían rivalizar: ¿cuál genera menos residuos por persona?, y las unidades de Infantería de Marina por cuál tiene mejor récord de cumplimiento normativo.

5. La realidad virtual (VR) es una tecnología que utiliza el *hardware* y el *software* para crear un entorno o mundo simulado de escenas y objetos que tiene una apariencia real, logrando que el usuario sienta que está totalmente inmerso en ese espacio digital.

6. La gamificación (ludificación) es una técnica que consiste en la aplicación de elementos, mecánicas y principios de diseño propios de los juegos en contextos que no son inherentemente lúdicos, con el objetivo principal de motivar, aumentar el compromiso y generar un cambio de comportamiento en las personas.



HMAS Hobart en la fase final de acondicionamiento. (Fuente: www.wikipedia.org)

¿Qué oportunidades crea para la industria española? Navantia y la ventaja competitiva internacional

El astillero estatal Navantia, constructor de las fragatas *F-110* y exportador de buques a Australia, Arabia Saudí y otros países, puede encontrar en el SGAi un argumento comercial diferenciador. Así, cuando presente la *F-110* a clientes internacionales ya no debería hablar sólo de capacidades de combate, sino también de eficiencia operativa certificada, de costes de ciclo de vida reducidos y del cumplimiento automático de regulaciones ambientales cada vez más estrictas, lo que redundará especialmente en las marinas europeas preocupadas por los mandatos parlamentarios de sostenibilidad y compromiso con el medio ambiente.

Australia, que ya compró destructores clase *Hobart* a Navantia, ha expresado interés en incorporar capacidades SGAi en las futuras actualizaciones. Si podemos exportar no

sólo el buque sino el sistema de gestión inteligente, estamos hablando de contratos de mantenimiento y actualización de *software* durante 30 años.

La oportunidad de la formación

Varias universidades españolas —Politécnica de Madrid, Politécnica de Cataluña y Universidad de Cádiz— han lanzado másteres especializados en gestión ambiental inteligente para sectores marítimos, en colaboración directa con la Armada. Estos programas combinan ingeniería ambiental tradicional con ciencia de datos, IoT, ciberseguridad y conocimiento específico del entorno marítimo.

¿Cómo afecta esto a las operaciones expeditivas?

Una cosa es gestionar el ambiente en una base permanente y otra muy distinta es

hacerlo en una misión expedicionaria en territorio hostil.

¿Es viable el SGAi en esos contextos?

Pongamos de ejemplo un hipotético escenario de operaciones: Mali 2030. Una unidad de Infantería de Marina es desplegada como parte de una operación de estabilización de la UE. No hay infraestructuras, el campamento se monta sobre terreno árido, las temperaturas superan los 45° C. En teoría, todas las normativas ambientales se siguen aplicando. En la práctica, las prioridades operativas suelen relegar el cumplimiento ambiental a un distante segundo plano.

Módulos logísticos inteligentes

El destacamento se despliega con los siguientes contenedores modulares especializados:

—Módulo de tratamiento de agua: convierte el agua local no potable en agua de consumo mediante filtración y purificación UV (ultravioleta) gestionada por IA, que ajusta automáticamente los ciclos según calidad del agua de entrada. Capacidad: 5.000 litros/día. Ahorra la necesidad de transportar agua embotellada desde Europa.

—Módulo de gestión de residuos: compactadora de alta eficiencia con clasificación automática mediante visión artificial. Separa reciclables, incinerables y peligrosos. Reduce

Diagrama virtual de flujos. (Fuente abierta generada con IA)



el volumen de residuos un 70 por 100, minimizando la necesidad de evacuación logística. —Módulo energético híbrido: paneles solares plegables + baterías + generador diésel de apoyo. La IA gestiona la mezcla para minimizar horas de funcionamiento del generador, que consume combustible precioso y es ruidoso, comprometiendo seguridad operacional.

El desafío de las «zonas grises»

No todo está técnicamente resuelto. En zonas de conflicto activo, las prioridades pueden entrar en tensión. Un ejemplo: una operación de evacuación de personal bajo fuego. ¿Priorizo cumplir los procedimientos de gestión de residuos o priorizo sacar a la gente? Es obvio: la vida humana primero. Pero luego viene la documentación del incidente, la justificación del incumplimiento temporal, el plan de corrección...

El SGAI ayuda incluso aquí: documenta automáticamente las circunstancias del incumplimiento, genera el informe de excepción y propone el plan de remediación poscrisis. Convierte una pesadilla burocrática en un proceso gestionable.

¿Qué papel juegan los aliados y la OTAN?

La interoperabilidad militar es clave. ¿Cómo se coordina esto a nivel multinacional? Retos y desafíos

Cuando desplegamos en una operación multinacional, cada país reporta datos ambientales en formatos diferentes, con metodologías incompatibles. Resultado: es imposible calcular la huella ambiental de la operación e identificar mejores prácticas que

se puedan seguir. La solución sería adoptar un Perfil OTAN de Gestión Ambiental basado en ISO 14001 con extensiones militares específicas y métricas estandarizadas: consumo de combustible por día/buque, generación de residuos por persona/día, emisiones de CO₂ equivalentes por hora de vuelo, etcétera.

Resistencias y oportunidades

No todos los aliados están entusiasmados con la idea. Siempre habrá preocupaciones sobre confidencialidad operacional, pues los datos granulares de consumo pueden revelar patrones operativos que no queremos hacer públicos. Es una preocupación legítima. Un adversario que analice los datos de consumo de combustible de una fuerza naval puede inferir el *tempo* operativo, predecir cuándo necesitará reabastecimiento e identificar vulnerabilidades logísticas.

Solución propuesta: datos agregados y anonimizados a nivel de operación, no de unidad individual, y sistemas de compartición con control de acceso estricto, sólo entre aliados certificados.

Los países nórdicos —Noruega, Dinamarca— son los más avanzados en este sentido y tienen todos sus procedimientos estandarizados, lo que les ayuda a demostrar el cumplimiento de sus objetivos en operaciones internacionales.

¿Qué riesgos imprevistos pueden surgir?

Todo esto suena muy optimista. ¿Qué puede salir mal? Murphy es el patrón de los marinos: si algo puede fallar, fallará. Y, probablemente, en el peor momento posible.



Recreación de la futura base naval de La Algameca. (Fuente abierta generada con IA)

La paradoja de la dependencia tecnológica

Cuanto más sofisticado es el sistema, más vulnerable puede ser a fallos catastróficos. Un escenario adverso: conflicto de alta intensidad. Un adversario con capacidades cibernéticas avanzadas compromete los sistemas SGAI de la flota mediante un *malware* insertado meses antes a través de una actualización de *software* aparentemente legítima. Súbitamente, los comandantes no pueden confiar en los datos de sus sensores. ¿El contador de combustible es real o está manipulado? ¿Los niveles de consumo de agua son correctos o falsificados? ¿Las alertas ambientales son genuinas o son ataques de denegación de atención?

En ese escenario, tendríamos que revertir a procedimientos manuales. Una generación joven que creció formada en este tipo de

sistemas confiando en ellos puede no tener la competencia para operarlos manualmente bajo estrés.

La mitigación: mantener capacidad de operación degradada. El personal debe entrenarse regularmente en procedimientos manuales, en ejercicios sorpresa en los que se «apagan» los sistemas inteligentes y las tripulaciones deben gestionarlo todo de manera convencional.

El sesgo algorítmico⁷

Los algoritmos de IA aprenden de datos históricos. ¿Pero qué pasa si esos datos contienen sesgos? Pongamos un ejemplo hipotético e ilustrativo: un algoritmo de optimización de rutas que tiende a recomendar sistemáticamente velocidades más bajas para buques más antiguos,

7. El sesgo algorítmico ocurre cuando un sistema de IA o de *machine learning* produce resultados sistemáticamente injustos, discriminatorios o desiguales debido a la influencia de datos, diseño o procesos sesgados.

asumiendo que consumen más combustible. Problema generado: que algunos buques hayan sido remotorizados con motores más eficientes, y el algoritmo, entrenado con datos históricos prerremotorización, no lo sepa y los penalice injustamente. Lección aprendida: auditoría continua de algoritmos. Se trata no sólo de verificar que funcionen, sino que sus recomendaciones sean justas, lógicas y no perpetúen ineficiencias históricas que ya no se aplican.

El riesgo de la complacencia y la desidia

El mayor peligro del éxito es la complacencia: si el sistema funciona bien durante años, la gente deja de cuestionarlo. Ejemplo hipotético: el SGA recomienda repetidamente una ruta

específica para patrullas en cierta zona porque históricamente ha demostrado óptima eficiencia. Pero las condiciones han cambiado: un adversario ha identificado el patrón y está preparando una emboscada.

La eficiencia ambiental no debe anular nunca el juicio táctico. Un comandante debe tener autoridad para desviarse de la recomendación algorítmica si su intuición operativa o inteligencia clasificada así lo requieren. Y no debe sentir presión burocrática por hacerlo.

La cultura organizacional debe proteger explícitamente el derecho del comandante a ignorar al algoritmo cuando sea necesario, sin penalización ni cuestionamiento retrospectivo injusto.

BIBLIOGRAFÍA

Armada (2020): *Visión Armada 2050*. Directiva del almirante jefe de Estado Mayor de la Armada (AJEMA). Ministerio de Defensa, Madrid.

Asociación Española de Normalización (2023): *UNE-EN ISO 14001:2015. Sistemas de gestión ambiental. Requisitos con orientación para su uso*. AENOR, Madrid.

European Defence Agency (2022): *Defence and climate change: Building resilient armed forces*. EDA, Bruselas.

International Organization for Standardization (2015): *ISO 14001:2015. Environmental management systems. Requirements with guidance for use*. ISO, Ginebra.

Ministerio para la Transición Ecológica y el Reto Demográfico (s. f.): *Planes estratégicos de sostenibilidad y cambio climático*. Gobierno de España, Madrid.

North Atlantic Treaty Organization (2021): *NATO's Climate Change and Security Action Plan*. NATO, Bruselas.

Naciones Unidas (2015): *Transforming our world: The 2030 Agenda for Sustainable Development*. Nueva York.