EL MERCURIO
DE VALPARAÍSO

Fecha: 29/06/2025 Audiencia: 33.000 Sección: ESPECIALES
Vpe: $1.696.097 Tirada: 11.000 Frecuencia: OTRAS
Vpe pág: $2.164.500 Difusión: 11.000
Vpe portada: $2.164.500 Ocupación: 78,36%

Los retos de la automatización en el transporte marítimo

Los sistemas integrados de monitoreo en tiempo real, el mantenimiento predictivo y el uso de IA permiten hoy operar embarcaciones con dotaciones mínimas. Con todo, faltan normas que regulen el tráfico de naves autónomas, acuerdos sobre responsabilidad legal, protocolos frente a emergencias y, en especial, mecanismos efectivos de ciberseguridad.

La automatización industrial no es novedad. Nació al calor de la Revolución Industrial, cuando los telares automáticos y las líneas de ensamblaje cambiaron la historia. Luego vino la automatización informática, en el siglo XX, con PLCs (Controladores Lógicos Programables) que comenzaron a tomar el control de procesos antes manuales. En el sector marítimo, las primeras señales aparecieron en la automatización de motores, sistemas de navegación y carga. Ya no era necesario un enjambre de marineros para verificar la presión del vapor o calcular la posición con sextante: la máquina tomaba el timón.

En pleno siglo XXI, los puertos se convierten en hormigueros robotizados, donde grúas autónomas descargan contenedores sin intervención humana. Buques como el Yara Birkeland, lanzado en 2021 con una capacidad de 120 Teus, que navega en las aguas de Noruega y es el primer carguero completamente eléctrico y autónomo, marcan un antes y un después. Los sistemas integrados de monitoreo en tiempo real, el mantenimiento predictivo y el uso de Inteligencia Artificial permiten operar embarcaciones con dotaciones mínimas.

¿Está el mundo preparado para una automatización total del transporte marítimo? En la teoría, sí. En la práctica, no del todo. Faltan normas internacionales que regulen el tráfico de naves autónomas, acuerdos sobre responsabilidad legal, protocolos frente a emergencias sin dotación y, sobre todo, mecanismos efectivos de ciberseguridad.

Chile, pese a su vocación portuaria y marítima, tampoco está completamente preparado. La infraestructura digital de muchos puertos aún es limitada, las normativas locales no contemplan naves no tripuladas y los marinos mercantes todavía no reciben formación masiva en ciberdefensa. El país corre el riesgo de ver pasar la revolución... desde el muelle.

Reducir la tripulación por razones de eficiencia puede traer consecuencias graves en situaciones de emergencia. Imaginemos un incendio en la sala de máquinas de un buque autónomo: sin personal a bordo, cada segundo cuenta y no hay manos que actúen. Un algoritmo no improvisa, un humano sí. Averías, abordajes, tormentas súbitas o fallos de propulsión son otras situaciones donde la ausencia de dotación embarcada puede marcar la diferencia entre un incidente menor y una catástrofe.

La mayor amenaza no proviene del mar... sino de una computadora. La digitalización y automatización han abierto un frente vulnerable: la ciberseguridad marítima, el talón de Aquiles de la flota del futuro.

Porque cada radar, cada compás electrónico, cada sistema de navegación, cada motor controlado por software es una puerta. Y todo lo que está conectado a internet puede ser intervenido, manipulado o bloqueado.

¿Qué puede ocurrir?

- Secuestro digital (ransomware): piratas del siglo XXI que cifran los sistemas críticos de un buque o puerto y exigen un rescate.
- Interferencia GPS (spoofing): alterar la señal GPS de una nave para desviarla de su ruta sin que lo note el sistema.
- Desactivación remota de motores, grúas o bombas de achique.
- Infiltración en el software de carga, que puede provocar distribución insegura de peso y comprometer la estabilidad de la nave.

En 2017, el gigante logístico Maersk fue víctima del malware NotPetya, que paralizó sus operaciones globales durante días y causó pérdidas estimadas en US$300 millones. Y en 2021, la Autoridad Portuaria de Sudáfrica sufrió un ataque que interrumpió operaciones marítimas claves. No son casos aislados, sino señales de advertencia.

La Organización Marítima Internacional (OMI) ya exige que las navieras incorporen la gestión del riesgo cibernético en sus sistemas de seguridad operacional (Código ISM). Varios países han desarrollado centros de respuesta ante incidentes cibernéticos (CSIRTs) especializados en logística y transporte.

Pero la carrera es desigual: los atacantes evolucionan más rápido que las normativas. Y muchos armadores todavía ven la ciberseguridad como un "gasto extra" o una carga administrativa y no como parte del casco del buque.

En Chile, La Ley Marco de Ciberseguridad (Ley N°21.663), promulgada el 26 de marzo de 2024, establece el marco legal para proteger la infraestructura crítica y mejorar la resiliencia digital del país. Su objetivo central es el de proteger la confidencialidad, integridad y disponibilidad de los sistemas gubernamentales y privados críticos (energía, transporte, salud, telecomunicaciones, finanzas) frente a amenazas cibernéticas, pero aún está en etapa de implementacion en puertos, embarcaciones y centros de formación marítima.

La automatización industrial en el transporte marítimo promete eficiencia, sustentabilidad y menor exposición humana al peligro. Pero también exige responsabilidad, regulación, inversión y visión de Estado. Porque un buque sin timonel humano, pero sin defensa digital, es un blanco flotante.

Mientras el océano sigue marcando el pulso del comercio global, la Inteligencia Artificial toma el timón. Pero no olvidemos: incluso el mejor sistema automático necesita que alguien lo entienda, lo proteja y lo controle. Porque en los mares del siglo XXI, la nueva brújula no apunta al norte... apunta al código fuente. ◆