Ciberseguridad en el sector marítimo: Riesgos, afectaciones y cómo afrontar el reto

Cámara Marítima de Panamá

La digitalización acelerada de los procesos logísticos y los avances en tecnologías emergentes y disruptivas, como blockchain y la inteligencia artificial, no solo han traído eficiencias operativas al sector, sino que también han abierto la puerta a nuevos riesgos que no deben ser ignorados por Panamá, como hub marítimo y logístico.

En los últimos años, varios actores clave de la cadena logística —incluidos puertos estratégicos de alto tráfico— han sido blanco de ciberataques que paralizaron operaciones, desviaron buques y afectaron servicios logísticos críticos. De igual forma, nuestro país ha registrado un aumento sustancial de ciberdelitos. El período 2020-2021 fue uno de los más intensos, con más de 767 millones de intentos de ciberataques según cifras de la compañía FORTINET, y en 2023 se reportaron aproximadamente 8,000 casos de ataques de ransomware.

El estudio titulado *"Un estudio de las afectaciones en las empresas panameñas a causa de los ciberdelincuentes y el uso de ransomware para el robo de información"*, publicado este año en la **Revista Colón, Ciencias, Tecnología y Negocios, de la Universidad de Panamá**, ofrece una radiografía realista de la situación de ciberseguridad que enfrentan las empresas en Panamá. Basado en encuestas estructuradas a 34 compañías, distribuidas entre Ciudad de Panamá (50%), la provincia de Colón y en particular la Zona Libre (44.1%), y el interior del país (5.9%), el informe revela que el 29.4% de las empresas fueron víctimas de ransomware durante el último año. Un porcentaje igual manifestó desconocer si habían sido atacadas.

Otro dato alarmante del estudio: el 55.9% de las empresas encuestadas indicaron estar poco o nada preparadas para enfrentar un ataque de este tipo.

A nivel internacional, se han registrado casos relevantes que evidencian la magnitud del riesgo cibernético en el sector marítimo y logístico:

- **DP World Australia (2023)**: sufrió un ataque masivo que paralizó operaciones en cuatro de sus principales terminales, afectando más de 3,000 movimientos diarios de carga.
- **Puerto de Nagoya (2023)**: el más activo de Japón quedó fuera de línea tras un ransomware que comprometió sus sistemas operativos.
- **KNP Logistics (2023)**: uno de los mayores grupos logísticos del Reino Unido, fue víctima de un ataque de ransomware que obligó al cierre indefinido de operaciones.
- **Maersk (2017)**: registró pérdidas estimadas en $300 millones por el ataque de NotPetya, según información verificada por el portal "Mundo Marítimo".

- **Puerto de Los Ángeles (2024)**: reportó más de 60 millones de intentos de ciberataque por mes, según Tony Zhong, Jefe de Seguridad de la Información del Puerto de los Ángeles.

Ante este panorama, la Cámara Marítima de Panamá hace un llamado urgente al Estado, a la Autoridad Marítima de Panamá (AMP), y a los operadores portuarios y logísticos para fortalecer la defensa digital del país.

Propuestas concretas:

1. **Creación del Comité Técnico Nacional de Ciberseguridad Marítima y Portuaria**, que trabaje de forma colaborativa con otros sectores críticos en la definición de una estrategia nacional de ciberseguridad.
2. **Adopción progresiva de estándares internacionales**, como NIST e ISO/IEC 27001, para fortalecer capacidades, reducir riesgos y promover un desarrollo económico digital seguro.
3. **Formación técnica inmediata**, mediante diplomados cortos en ciberseguridad para el sector marítimo, impartidos por centros educativos con trayectoria y prestigio.

"La ciberseguridad es tan crítica como el dragado, las grúas o el combustible. La continuidad operativa de nuestro sistema logístico depende también de la fortaleza de nuestros sistemas digitales." — Junta Directiva, CMP

"Fortalecer sistemas y procedimientos de ciberseguridad, gestión de riesgos y protección del valor de la información sensible, con capacidad para administrar datos y modelos predictivos, garantizará la confidencialidad, integridad y disponibilidad de datos críticos, protegiendo a nuestro sector y asegurando un flujo seguro de información." — Visión Marítima País 2024–2029, Cámara Marítima de Panamá

La amenaza es real y creciente. No actuar pone en juego la competitividad y seguridad del país. Es momento de invertir con decisión en ciberseguridad: sin protección digital, no hay futuro logístico. Ante este panorama, la Cámara Marítima de Panamá extiende una invitación al Estado, a la Autoridad Marítima de Panamá (AMP), y a los operadores portuarios y logísticos, para trabajar conjuntamente en el fortalecimiento de la defensa digital del país, promoviendo una estrategia coordinada y proactiva que asegure la resiliencia de nuestro sistema logístico-marítimo.

Artículo en colaboración con la Comisión de Innovación Empresarial