DYNA
http://dyna.medellin.unal.edu.co/

UNIVERSIDAD NACIONAL DE COLOMBIA

# Cybersecurity in the maritime industry: an analysis of emerging threats and challenges

Alexander Palma-Chipana, Juan Villantoy-Echegaray, Javier Ccapcha-Cabrera & Carlos Neyra-Rivera

*Facultad de Ingeniería de Sistemas e Informática, Universidad Tecnológica del Perú, Lima, Perú, U21219084@utp.edu.pe, U20307124@utp.edu.pe, c24878@utp.edu.pe, c29136@utp.edu.pe*

Received: July 24th, 2024. Received in revised form: October 7th, 2024. Accepted: November 8th, 2024.

**Abstract**
The maritime industry faces increasing cyber threats that jeopardize the safety and efficiency of its operations. Therefore, the present study aims to analyze cybersecurity in this industry. We used SCOPUS databases and the PRISMA methodology, applying rigorous inclusion and exclusion criteria to select relevant articles. The results of these articles show that the most common threats include attacks on navigation systems and manipulation of cargo data. The reviewed studies indicate growing concern over insufficient regulations and lack of cybersecurity training. Additionally, it highlighted the need to improve cyber defenses through robust policies and international cooperation. In conclusion, the maritime industry must adopt a proactive and coordinated stance to address these challenges and ensure the resilience of its operations within the digital environment.

*Keywords*: cyber-attack; cyber-threat; maritime industry; risks; vessels.

# Ciberseguridad en la industria marítima: un análisis de las amenazas y desafíos emergentes

**Resumen**
La industria marítima enfrenta crecientes amenazas cibernéticas que ponen en riesgo la seguridad y eficiencia de sus operaciones. Por ello, el presente estudio tiene como objetivo analizar la ciberseguridad en la industria. Se utilizó la base de datos de SCOPUS y la metodología PRISMA aplicando criterios rigurosos de inclusión y exclusión para seleccionar los artículos relevantes. Los resultados de estos artículos muestran que las amenazas más comunes incluyen ataques a sistemas de navegación y manipulación de datos de carga. Los estudios revisados indican una preocupación creciente por la insuficiencia de normativas y la falta de formación en ciberseguridad. Además, se destaca la necesidad de mejorar las defensas cibernéticas mediante políticas robustas y cooperación internacional. Como conclusión, la industria marítima debe adoptar una postura proactiva y coordinada para enfrentar estos desafíos y asegurar la resiliencia de sus operaciones en el entorno digital.

*Palabras clave*: buques; ciberataque; ciber amenaza; industria marítima; riesgos.

## 1 Introduction

La industria naviera lleva consigo un rol importante para el desarrollo económico de los países en cuestión de mejores rendimientos de exportación tal como ocurrió con el crecimiento de exportaciones de Vietnam al permitirle a la empresa naviera Maersk operar en su territorio [1], para la modelización de la agitación marítima como una herramienta importante para ayudar al diseño de obras marítimas [2], para el desarrollo turístico [3,4], para definir la onda de diseño de un proyecto marítimo [5], para la mejora de la ingeniería naval [6] así como también podría tener un impacto en trabajos vinculados al submarinismo [7]. La ciberseguridad juega un rol importante en la resiliencia cibernética de las entidades, por ello, las organizaciones buscaron modelos y marcos de referencia que le ayuden a implementar una gestión de ciberseguridad dentro de sus estrategias [8]. A pesar de los aportes de la industria marítima para la economía de los países hay varias investigaciones que

**How to cite:** Palma-Chipana, A., Villantoy-Echegaray, J., Ccapcha-Cabrera, J., and Neyra-Rivera, C., Ciberseguridad en la industria marítima: un análisis de las amenazas y desafios emergentes DYNA, 91(234), pp. 157-162, October - December, 2024.

manifiestan que hay problemas en materia de ciberseguridad que se presentan en los diversos sistemas a bordo de los buques y aunque algunas proponen posibles soluciones se requiere de una mayor profundización sobre estos [9-13].

Mientras que los constructores y stakeholders invierten en innovación tecnológica para mejorar las operaciones y la progresiva cimentación e integración de los buques autónomos a los mares aparece una creciente preocupación sobre la seguridad cibernética que compromete el progreso de la industria naviera [9,13]. En este sentido, se necesita de una revisión de toda evidencia y fuentes bibliográficas actuales que ayuden a entender la situación actual de la industria respecto a la seguridad de su infraestructura tecnológica, considerando los riesgos que se pueden presentar, las vulnerabilidades de los sistemas, las soluciones que se han propuesto y las recomendaciones que se han brindado. Existe un reducido número de artículos que tratan el tema de la ciberseguridad dentro de la industria naviera pero en los que existen se destaca la necesidad de mejorar la ciberseguridad marítima desde bases costeras, puertos, barcos y la comunicación satelital, la falta de preparación y sensibilización de la tripulación y agencias internacionales, federales e industriales que realizaron proyectos, investigaciones, guías y estándares de administración de ciber riesgos [14,15]. Actualmente, el problema se agrava considerando que nuevos riesgos y ciberataques se incrementarán a medida que la industria marítima dependa cada vez más de las tecnologías de la información y comunicación (TICs). El éxito de los ciberataques y la materialización de los riesgos en esta industria pueden conducir a catástrofes financieras y ambientales y esto hace incierto la inclusión de buques autónomos que hacen uso del ciberespacio ya que podrían ser más vulnerables a distintos tipos de ciberataques [13].

En la presente investigación, se identificaron revisiones sistemáticas de literatura respecto a la actividad marítima y los retos para la navegación marítima y la integración de barcos autónomos en puertos de contenedores que concluyen en que la industria marítima no es inmune a los ciberataques y que no está preparada para combatir los riegos del uso de sistemas obsoletos a lo que proponen establecer medidas de seguridad e integrar sistemas específicos para el aseguramiento de la navegación [16,17]. Estos hallazgos indican que hay una necesidad de conocer las vulnerabilidades, riesgos y soluciones que nos den un panorama de la situación actual de la industria naviera en ciberseguridad, a lo que se propone realizar una recopilación de estos.

Por lo indicado anteriormente, el objetivo de la presente Revisión Sistemática de Literatura (RSL) es identificar y clasificar las amenazas y desafíos en la ciberseguridad de los buques y agencias navieras y sintetizarlas, haciendo un acercamiento especial hacia los ataques de malware para conocer la naturaleza de estos y apoyar el diseño de soluciones informáticas sobre ciberseguridad que se ajusten a los requerimientos del sector naviero.

## 2 Metodología

Para el desarrollo de la presente RSL en el periodo 2020-2024 para identificar y clasificar las amenazas y desafíos en la ciberseguridad de los buques y agencias navieras. Para ello se se aplicó la metodología PRISMA [18]. La estrategia de búsqueda se realice en base a la pregunta PICO (Problema, Intervención, Comparador y Resultados) permitiendo realizar una búsqueda más rigurosa en la base de datos seleccionada.

La pregunta de investigación que guio el estudio fue ¿Qué amenazas y desafíos afectan a las operaciones principales de las empresas navieras? En base a la pregunta de investigación se genera la siguiente ecuación de búsqueda: (threats OR menance OR cyberdanger OR cyberrisk OR cybermenance OR cyberattack OR cybervulnerability OR cyberhazard OR cyberintrusion OR cyberperil OR cyberthreat OR cybersecurity OR "information security" OR "cyber defense" OR "cyber protection" OR "digital security" OR "computer security" OR "malicious software" OR "malicious code" OR malware OR "malicious program" OR "malicious script" OR "malicious application" OR "malicious payload" ) AND ( shipping OR shipment OR freight OR carriage OR conveyance OR ship OR vessel OR watercraft OR seacraft OR harbor OR docks OR terminals OR wharve OR marina OR berth OR quay ). Dicha búsqueda se realizó en la base de datos Scopus durante los meses de abril-junio del 2024 definiendo los criterios “year, subject area, document type, y open access con los valores 2020 – 2024, Engineering y Computer Science, Article, y All open access y Green”. Para la selección de artículos se establecieron los siguientes criterios de selección:

Criterios de Inclusión: CI-1 Estudios referente a malwares en la industria naviera, CI-2 Estudios que aborden la seguridad tecnológica en la industria naviera, CI-3: Estudios referente a navieras internacionales.

Criterios de Exclusión: CE-1 Estudios provenientes de entornos simulados, CE-2 Estudios de activos afectados diferentes de los procesos principales de las navieras y compañías de cruceros, CE-3 Estudios que se encuentren en un idioma diferente al español e inglés, CE-4: estudios anteriores al año 2020.

Luego de aplicar la ecuación de búsqueda se identificaron 529 publicaciones las que siguieron el diagrama de flujo PRISMA y los criterios de inclusión y exclusión seleccionándose finalmente 6 artículos (Figura 1).

## 3 Resultados

Los resultados de la presente RSL se han dividido en análisis descriptivo de datos bibliométricos y análisis detallado de las características de interés según el objetivo de la presente investigación.

### *3.1. Análisis bibliometrico*

En la Tabla 1 se resumen los principales datos bibliométricos de las publicaciones identificadas en la temática de estudio. Hasta junio del 2024 solo se identificaron 6 publicaciones que cumplían con los criterios de inclusión y exclusión indicados en la presente RSL. El artículo que tuvo mayor cantidad de citas fue el de Caprolu et al. [24] mientras que el que tuvo menor cantidad de citaciones fue el de Pawelski [20].

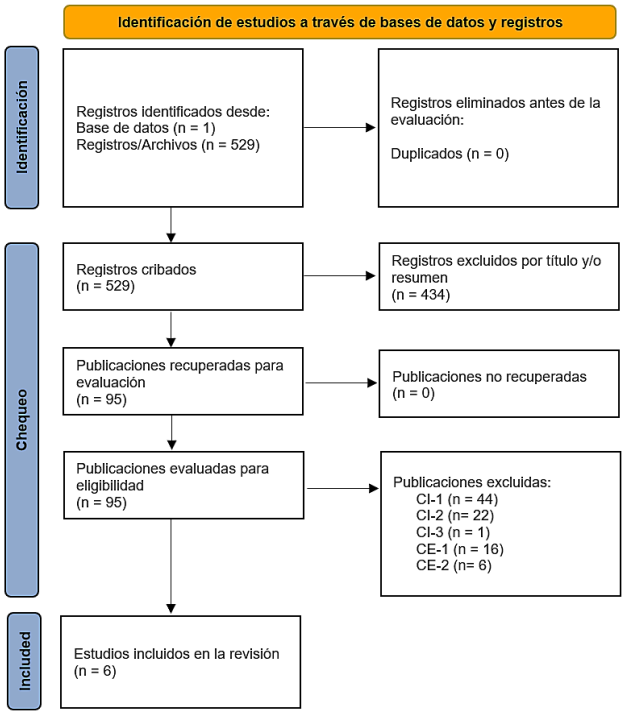


Figura 1. Flujograma PRISMA para la filtración y selección de fuentes. Fuente: [18].

Tabla 1.
Datos bibliometricos de artículos seleccionados

| Ref. | Título | Año | Revista | Citas |
|---|---|---|---|---|
| [19] | Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule- based Bayesian network modelling | 2024 | Reliability Engineering and System Safety | 15 |
| [20] | Cyber Threats for Present and Future Commercial Shipping | 2023 | TransNav | 0 |
| [21] | Ensuring Cyber Resilience of Ship Information Systems | 2022 | TransNav | 23 |
| [22] | Discussing cybersecurity in maritime transportation | 2022 | Maritime Technology and Research | 2 |
| [23] | Maritime Cyber(in) security: A Growing Threat Imperils EU Countries | 2021 | Connections | 1 |
| [24] | Vessels Cybersecurity: Issues, Challenges, and the Road Ahead | 2020 | IEEE Communicati ons Magazine | 61 |

Fuente: Elaboración propia

### *3.2 Ciber amenazas y ciberataques en sistemas a bordo*

Pawelski [20] indica que los barcos actuales llevan consigo una gran variedad de sistemas a bordo y cada uno tiene sus respectivos propósitos. Acerca de los sistemas digitalizados se pueden categorizar en dos grupos, las tecnologías de información y tecnologías de operaciones. Algunas de las redes (sistemas) a bordo de los barcos se encuentran las redes de comunicaciones, los sistemas de control industrial, red y carga y estabilidad, sistemas de seguridad de barcos, sistemas de protección de barcos y sistemas de navegación integrado (INS). Los sistemas AIS (Sistema de Identificación Automática) son vulnerables ante amenazas como accesos no autorizados; spoofing; DoS, por medio de la inundación de la red AIS con sobrecarga de tráfico o interferencia de las señales de radio; o ataques de malware, infectando la red con virus o gusanos, causando la interrupción o destrucción de sistemas y/o datos críticos. Uflaz et al. [19] menciona que los mensajes transmitidos por el sistema AIS son planos y no están encriptados, generando más problemas como técnicas de eavesdropping, inyección de información falsa sobre el tráfico marítimo, y la eliminación y modificación de mensajes. El protocolo de comunicación que usa el sistema AIS no posee propiedades de seguridad como la autenticación y la confidencialidad, y no posee mecanismos de verificación de datos [23,24].

Acerca de los equipos GPS (Sistema de Posicionamiento Global), Bielawski et al. [22], mencionan que son vulnerables ante ataques de spoofing, que consisten en la transmisión de señales GPS falsas para que los receptores a bordo de los barcos reciban información incorrecta sobre el posicionamiento del barco. Uflaz et al. [19] mencionan que otro tipo de ataque es jamming de señales GPS, que consiste en la saturación de las señales GPS con ruido excesivo o interferencia de radio para que los receptores GPS pierdan la señal o la capacidad de obtener información precisa y se identificaron ataques DoS que sobrecargan las señales con tráfico excesivo para interrumpir la navegación y comunicación, y accesos no autorizados, que implican la extracción o modificación de datos críticos como las variables de ubicación, velocidad y curso.

Bielawski et al. [22] estudiaron el ECDIS (Sistema Electrónico de Navegación), siendo un sistema que se encarga de la recolección de información proveniente de varios sistemas instalados en el barco y muestran los mapas digitales para asistir a los oficiales en la navegación. Para hacer uso de estos mapas el sistema necesita estar conectado a internet para poder descargar las últimas versiones más actuales, aunque también se puede hacer uso de dispositivos USB. Es por esta característica que este sistema es vulnerable ante infecciones de malware. Otras amenazas identificadas son los ataques de repudio, tampering, spoofing y DoS. Pawelski [20] encuentra que estos componentes funcionan en computadoras con sistemas operativos comerciales propensos a ciberataques inclusive si están actualizados o protegidos con software anti-malware. Además, se encontró que la mayoría de los sistemas operativos empleados para correr el software de ECDIS, eran antiguos, tales como Windows NT y menciona que el GNSS (Sistema Global de Navegación por Satélite) permite el control de datos de

navegación y mostrar el estado y datos de navegación. Este es el pilar de los INS y que permite el funcionamiento de los demás componentes. En contraste, Caprolu et al. [24], indican que puede ser atacado por métodos de spoofing por medio de SDR'S comerciales, que aprovechan las vulnerabilidades propias del sistema. Las señales legítimas son débiles y los mensajes falsos pueden superponerse, haciendo que los receptores de señal estimen localizaciones falsas. Los ataques de jamming son también otra amenaza que se realiza aproximando dispositivos que emitan ruido en las frecuencias de comunicación GNSS. Este sistema carece de propiedades de seguridad como la confidencialidad, autenticación y disponibilidad.

Bielawski et al. [21] indican que el GMDSS (Sistema Mundial de Socorro y Seguridad Marítimos) es un sistema diseñado para la obtención de asistencia temprana en casos de emergencia. Sus potenciales amenazas son los ataques de repudio, spoofing, tampering y divulgación de información (information disclosure). Según Uflaz et al. [19], otras amenazas identificadas son los accesos no autorizados, DoS, spoofing, y ataque de malware, que consiste en la infección del sistema con software malicioso generando mal funcionamiento o entrega de datos no precisos.

Respecto a los componentes PLC, Pawelski [20] menciona que las primeras generaciones de malware tenían como objetivo a las tecnologías de operaciones OT y se llevaban a cabo en sistemas SCADA basados en Windows, debido a que los componentes PLC fueron considerados por largo tiempo seguros contra malwares, estos eran fabricados con características básicas de seguridad. En pocos años los investigadores descubrieron un hack de PLC que les permitiría obtener información importante y enviarlo por frecuencia de radio originadas por el PLC mismo. También se desarrollaron puertas traseras (rootkits) que se alojan en memorias dinámicas con el que se puede manipular los dispositivos PLC. Con esto se logra afectar el control de los procesos industriales.

Todorov [23] indica que los sistemas ESD (Emergency Shut Down System) sirven para el bloqueo de la gestión de la propulsión y maquinaria del marco en casos de emergencia. Se identificó que su única vulnerabilidad es que es accesible desde la costa.

### *3.3 Niveles de impacto*

Pawelski [20], menciona que los ataques de malware en los sistemas ECDIS pueden hacer que este se vuelva inservible y afectar de la misma manera a los demás equipos conectados debido a la expansión de la infección de malware. Todorov [23] destaca que falta de propiedades de autenticación puede conducir a la alteración de rutas de navegación.

Los ataques dirigidos al componente GPS termina en una mayor dificultad de navegación y compromete la seguridad de la navegación del barco [3].

Si no se logran superar las vulnerabilidades de los sistemas AIS la introducción de los buques autónomos en la industria naviera demorará [9]. Afectan a la confidencialidad, integridad, disponibilidad, posesión, autenticidad y facilidad para la utilización de información, así se pueden generar desviación del curso de los barcos [21]. También puede conducir a la alteración de rutas de navegación [23].

La materialización de las amenazas en GNSS comprometería a los barcos no tripulados, puesto estos dependerían del GNSS, por lo que se haría imposible la inclusión de este nuevo tipo de barcos [9]. Además, las operaciones de estos barcos se verían comprometidos [22].

Pawelski [20] indica que los ataques dirigidos tanto a líneas navieras y compañías que ocurrieron en los últimos años originaron pérdidas financieras a pesar de que las compañías posean profesionales de red e IT, que los problemas en la comunicación pueden repercutir seriamente en las operaciones del barco y acceso a los equipos de OT, y que en caso las tecnologías usadas a bordo no se vuelven lo suficientemente resilientes la introducción de buques autónomos tardará [20]. Según Uflaz et al. [19], otras consecuencias son el incremento de la vulnerabilidad de los sistemas hacia ataques físicos, pérdidas de información comercial o militar valiosa, daño a propiedad, contaminación ambiental y, la pérdida de vidas humanas, incremento de los riesgos de accidentes y colisiones, pérdida de la funcionalidad e incremento de los costos de operaciones y mantenimientos, toma de decisiones equivocadas, disminución de la alerta situacional, y demora en la respuesta a situaciones de emergencia.

### *3.4 Desafíos identificados*

Uflaz et al. [19] revela que los componentes del INS, como el AIS y el GPS son altamente vulnerables y los modos de falla críticos incluyen el spoofing de AIS y GPS así como la manipulación de datos del VDR (Registrador de Datos del Buque).

Pawelski [20] destaca cómo varios componentes de la red de los barcos, como los PLC, que se creían seguros, pueden ser afectados por rootkits indetectables, que los sistemas de navegación críticos como AIS, GPS y ECDIS son susceptibles a ataques de malware, y que pueden propagarse a través de la red de la nave.

Onishchenko et al. [21] enfatizan la falta de atención que las empresas navieras otorgan a la defensa contra ciber amenazas y la filtración de información confidencial, como bajos niveles de conocimiento entre los profesionales a bordo sobre la complejidad de las redes de los barcos, la incapacidad del personal para detectar correos electrónicos de phishing y la mala gestión de los sistemas pueden abrir puertas a los hackers, como conectar un teléfono al terminal ECDIS, permitiendo el acceso a sistemas críticos.

Bielawski [22] discuten que los problemas potenciales asociados con tendencias emergentes en el transporte marítimo como la alta vulnerabilidad de los sistemas AIS, GPS y ECDIS, con este último especialmente propenso a infecciones de malware tanto a través de la red como de conexiones USB, e indican que las amenazas pueden ser indiscriminadas, apuntando a los sistemas sin un objetivo específico, usando técnicas comunes como el malware.

Caprolu et al. [24] señalan la falta de armonización y estandarización en los marcos de ciberseguridad marítima como una vulnerabilidad significativa, indica la necesidad de un código global de ciberseguridad marítima para mejorar la

resiliencia y seguridad, enfocándose en la compartición de información, aumento de la alerta, certificaciones y resiliencia, y resalta la importancia de establecer normas y guías técnicas coherentes para los sistemas de buques.

### *3.5 Ataques de malware y evidencias*

Uflaz et al. [19] mencionan que los ataques de malware son parte de los modos de falla del INS pero no son los más destacados en términos de criticidad ya que sus valores de riesgo y consecuencias son comparables a otros riesgos significativos. Pawelski [20] identificó que los sistemas de navegación como ECDIS son vulnerables a ataques de malware ya que pueden desplegarse a través de la red de la embarcación resultando en consecuencias similares a las que ocurren en sistemas informáticos personales. Onishchenko et al. [21] reportan casos reales donde empresas navieras fueron víctimas de ataques de malware debido a la falta de conocimiento y capacitación del personal y al mal uso de los sistemas como la conexión de dispositivos no autorizados.

Bielawski et al. [22] subrayan la vulnerabilidad de sistemas como AIS, GPS y ECDIS a infecciones de malware, que pueden ocurrir a través de la red o mediante dispositivos USB conectados. Todorov [23] menciona numerosos incidentes de malware en sistemas GNSS, AIS y GMDS1S, indicando que los tripulantes desprevenidos suelen ser la fuente de estos ataques.

## 4 Discusión

La RSL ha revelado una variedad de desafíos y vulnerabilidades en la ciberseguridad de la industria naviera. A través del análisis de múltiples estudios y artículos se destacan varios puntos clave que merecen ser discutidos en profundidad.

Los sistemas de navegación y comunicación a bordo de los barcos, como AIS, GPS y ECDIS [12], presentan vulnerabilidades significativas. Estos sistemas, que son cruciales para la operación segura y eficiente de los barcos son susceptibles a ataques de spoofing, jamming y malware [20]. Los ataques a estos sistemas pueden resultar en la manipulación de datos críticos, pérdida de señales y en última instancia en la navegación incorrecta o pérdida de control del barco [13]. La investigación muestra que estas vulnerabilidades son consecuencia tanto de la falta de encriptación y autenticación en los protocolos de comunicación así como también del uso de sistemas operativos obsoletos que son más propensos a ser explotados [21].

La creciente digitalización y conectividad de los sistemas de TI y OT a bordo de los barcos han aumentado las vulnerabilidades cibernéticas [19]. La integración de redes y sistemas digitales, mientras mejora la eficiencia operativa, también abre nuevas vías para los ciberataques. El uso de dispositivos USB y la conectividad a Internet para actualizaciones de software son ejemplos de cómo el malware puede introducirse en los sistemas críticos del barco [11]. Este fenómeno se ve exacerbado por la falta de medidas de seguridad robustas y actualizadas en muchos de estos sistemas [16].

La falta de conciencia y capacitación en ciberseguridad entre el personal marítimo es otro desafío crítico identificado [13]. La revisión indica que los profesionales a bordo a menudo no están suficientemente entrenados para identificar y responder a ciber amenazas [14]. Esta falta de preparación puede llevar a errores humanos que facilitan los ciberataques, como la apertura de correos electrónicos de phishing o la conexión de dispositivos no seguros a los sistemas del barco. Por lo tanto, es crucial implementar programas de capacitación y sensibilización que aborden estas deficiencias [13].

La industria marítima no solo enfrenta amenazas actuales, sino también futuras tendencias que pueden agravar las vulnerabilidades existentes. La adopción de buques autónomos, por ejemplo, depende en gran medida de la robustez de los sistemas de ciberseguridad [22]. Sin una ciberseguridad adecuada la operación de estos buques puede estar comprometida poniendo en riesgo no solo las operaciones comerciales sino también la seguridad y el medio ambiente. Las tendencias emergentes en ciberataques también sugieren que los atacantes están desarrollando técnicas cada vez más sofisticadas para explotar las vulnerabilidades marítimas [23].

La falta de regulación y estandarización en ciberseguridad marítima representa un desafío significativo [8]. Aunque existen marcos y guías para la ciberseguridad, la revisión señala la necesidad de un código global y armonizado que establezca estándares claros y coherentes para la protección cibernética en la industria naviera. Un enfoque estandarizado permitiría una mejor coordinación internacional, intercambio de información y respuesta a incidentes, aumentando la resiliencia cibernética del sector.

Los ataques de malware en la industria naviera han demostrado tener un impacto significativo, desde la interrupción de las operaciones hasta pérdidas financieras y daños ambientales [10]. Los estudios revisados documentan casos donde el malware ha comprometido sistemas críticos, resultando en fallos operativos y riesgos para la seguridad marítima. La discusión destaca la necesidad de adoptar medidas preventivas y de respuesta eficaces para mitigar estos riesgos y proteger tanto los activos físicos como digitales de las navieras.

Para futuras investigaciones, sería crucial abordar varias áreas que aún no han sido completamente exploradas. Por ejemplo, sería beneficioso investigar más sobre la efectividad a largo plazo de las soluciones de ciberseguridad implementadas en la industria marítima. Estudios longitudinales podrían proporcionar insights sobre cómo estas soluciones evolucionan con el tiempo y cómo responden a nuevas amenazas emergentes. Además, explorar la integración de tecnologías emergentes como la inteligencia artificial y el machine learning en los sistemas de ciberseguridad marítima podría mejorar significativamente la detección temprana y la respuesta a amenazas avanzadas. También sería crucial investigar más sobre la efectividad y la viabilidad de estrategias de concientización y capacitación en ciberseguridad para el personal marítimo.

## 5 Conclusiones

Los hallazgos principales indican que los sistemas AIS, GPS y ECDIS son susceptibles a ataques de spoofing, jamming y malware, lo que puede resultar en navegación incorrecta o pérdida de control del barco. La creciente

digitalización y conectividad de los sistemas a bordo han incrementado las vulnerabilidades, facilitando la introducción de malware a través de redes y dispositivos USB. El personal a bordo destaca como una vulnerabilidad importante y que requieren capacitaciones sobre ciberseguridad. Por último, no existe un marco regulatorio global y estandarizado en ciberseguridad marítima, dificultando la coordinación internacional y la respuesta eficaz a incidentes.

Se proporcionar una visión comprensiva de las vulnerabilidades actuales en la ciberseguridad marítima y al resaltar la necesidad de una mayor estandarización y regulación. Se enfatiza la importancia de la capacitación continua del personal y la adopción de nuevas tecnologías para mejorar la resiliencia cibernética.

## Referencias


[1] Krase, V., Bente, S., Kowalsky, U., and Dinkler, D., Modelling the stress-deformation behaviour of municipal solid waste, Geotechnique, 61(8), pp. 665–675, 2011. DOI: https://doi.org/10.1680/geot.8.P.140.

[2] Hansen, M., and Wendelboe, M., The role of shipping and logistics MNCs in economic development: a case study of how Maersk contributed to Vietnam's ascendence to an export-oriented economy. Journal of Shipping and Trade, 9(4), pp. 1-30, 2024. DOI: https://doi.org/10.1186/s41072-023-00161-w

[3] Gonçalves, R.S., Camacho, R.F., Lousada, S., Castanho, R.A., Modeling of maritime agitation for the design of maritime infraestructures: the case study of Madeira Archipelago. Revista Brasileira de Planejamento e Desenvolvimento, 7(1), pp. 29-50, 2018. DOI: https://doi.org/10.3895/rbpd.v7n1.7136

[4] Lousada, S., Castanho R.A., The role of ports in tourism: Porto Santo Harbour. Water, 14(19), art. 3176, 2022. DOI: https://doi.org/10.3390/w14193176

[5] Lousada, S., and Castanho, R.A., Port Structures, Maritime Transport, and Tourism. Water, 15, 3898, 2023. https://doi.org/10.3390/w15223898.

[6] Lousada, S.A.N., and Gonçalves, R., Metodologias de determinação de alturas de onda. Dimensionamento de obras marítimas. Novas Edições Acadêmicas, Portugal, 2019, 253 P. ISBN 978-613-9-61105-8,

[7] Lousada, S.A.N., and Hassan, N.M.S., New innovations in engineering education and naval engineering. Ed. IntechOpen, Inglaterra, 2020, 164 P. ISBN: 978-1- 78984-037-7

[8] Lousada, S.A.N., Underwater Work., Ed. Intech Open, Inglaterra, 2021, 88 P. ISBN: 978-1- 78985-229-5

[9] Valkenburg, B., and Bongjovanni, I., Unravelling the three lines model in cybersecurity: a systematic literature review. Computers and Security, 139, art. 103708, 2024. DOI: https://doi.org/10.1016/j.cose.2024.103708

[10] Pawelski, J., Cyber threats for present and future commercial shipping. The International Journal on Marine Navigation and Safety of Sea Transportation, 17(2), pp. 261-267, 2023. https://doi.org/10.12716/1001.17.02.01

[11] Soner, O., Kayisoglu, G., Bolat, P., and Tam, K., Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. Applied Ocean Research, 142, art. 103855, 2024. DOI: https://doi.org/10.1016/j.apor.2023.103855

[12] Beradi, D., Giallorenzo, S., Melis, A., Melloni, S., Onori, L., and Prandini, M., Data flooding against ransomware: concepts and implementations. Computers & Security, 131, pp.1-15, 2023. DOI: https://doi.org/10.1016/j.cose.2023.103295

[13] Oruc, A., Kavallieratos, G., Gkioulos, V., and Katsikas, S., Cyber Risk Assessment for Ships (CRASH). TransNav, 18(1), pp. 115- 124, 2024. DOI: https://doi.org/10.12716/1001.18.01.10

[14] Oruc, A., Chowdhury,N., and Gkioulos, V., A modular cyber security training programme for the maritime domain. International Journal of Information Security, 23(2), pp. 1477-1512, 2024. DOI: https://doi.org/10.1007/s10207-023-00799-4

[15] McGillivary, P., Why maritime cybersecurity is an ocean policy priority and How it can be addressed. Maritime Technology Society Journal, 52(5), pp. 44-57, 2018. DOI: https://doi.org/10.4031/MTSJ.52.5.11

[16] Cabuya, D., Alvarado, C., Carrascal, R., Escandón, S., Riola, J., and Fajardo-Toro, C., Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990 – 2021. Risti Revista Iberica de Sistemas r Tecnologias de Informacao, 49(4), pp.197-210, 2022. DOI: https://doi.org/10.17013/risti.43.314-326

[17] Hirata, E., and Hansen, A.S., identifying key issues in integration of autonomous ships in container ports: a Machine-Learning-Based systematic literature review. Logistics, 8(1), pp. 1-15, 2024. DOI: https://doi.org/10.3390/logistics8010023

[18] Androjna, A., Brcko, T., Pavic, I., and Greidanus, H., Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering, 8(10), pp. 1-21, 2020. DOI: https://doi.org/10.3390/jmse8100776

[19] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., … Moher, D., Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. Revista Panamericana de Salud Pública, 46, art. 112, 2020. DOI: https://doi.org/10.26633/RPSP.2022.112

[20] Olapoju, O., Autonomous ships, port operations, and the challenges of African ports. Maritime Technology and Research, 5(1), pp. 1-16, 2023. DOI: https://doi.org/10.33175/mtr.2023.260194

[21] Uflaz, E., Sezer, S., Tunçel, A., Aydin, M., Akyuz, E., and Arslan, O., Quantifying potential cyber-attack risks in maritime transportation under Dempster-Sahafer theory FMECA and rule-based Bayesian network modelling. Reliability Engineering and System Safety, 243, art. 109825, 2024. DOI: https://doi.org/10.1016/j.ress.2023.109825

[22] Onishchenko, O., Shumilova, K., Volyanskyy, S., Volyanskaya, Y., and Volianskyi, Y., Ensuring cyber resilience of ship information systems. TransNav, 16(1), pp. 43-50, 2022. DOI: httpS://doi.org/10.12716/1001.16.01.04

[23] Bielawski, A., and Lazarowska, A., Discussing cybersecurity in maritime transportation. Maritime Technology and Research, 4, art. 252151, 2022. DOI: https://doi.org/10.33175/mtr.2022.252151

[24] Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S., and Tedeschi, P., Vessel's cybersecurity: issues, challenges, and the road ahead. IEEE Communications Magazine, 58(6), pp. 1-8, 2020. DOI: https://doi.org/10.1109/MCOM.001.1900632

[25] Todorov, Y., Maritime Cyber(in) security: a growing threat imperils EU countries. Connections QJ, 20(3-4), pp. 73-93, 2021. DOI: https://doi.org/10.11610/Connections.20.3-4.04



**A. Palma-Chipana,** es estudiante de último ciclo de la carrera de Ingeniería de Sistemas de la Universidad Tecnológica del Perú.
ORCID: 0009-0001-0992-1805

**J. Villantoy-Echegaray,** es estudiante de último ciclo de la carrera de Ingeniería de Sistemas e Informática de la Universidad Tecnológica del Perú.
Orcid: 0009-0004-7033-1160

**J. Ccapcha-Cabrera,** es MSc. en Ing. de Sistemas e Informática con Mención en Tecnologías de la Información. Ing. de Sistemas y Cómputo. Coordinador Especialista en Asistencia y Asesoramiento Tecnológico. Docente tiempo parcial de la carrera de Ingeniera de Sistemas y Redes en la Universidad Tecnológica del Perú.
ORCID: 0000-0003-1713-0648

**C. Neyra-Rivera,** Dr. en Biología Molecular y Biotecnología. Investigador en el área de Ciencias de la Salud, Ciencias Básicas y Ciencias Forenses. Ha desarrollado proyectos de investigación a nivel nacional (Perú) e internacional y es docente universitario tanto a nivel de pregrado como de posgrado en asignaturas relacionadas con Biología Celular, Bioquímica e Investigación.
ORCID: 0000-0003-1594-4947