Capítulo 10

La ciberseguridad marítima: una nueva dimensión de las relaciones internacionales en materia de seguridad marítima*

DOI: https://doi.org/10.25062/9786287602083.10

Daniel Alfonso Rojas Sánchez
Universidad de La Sabana

Samuel Rivera-Páez
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Los puertos son estructuras críticas cruciales para la gestión de la cadena de suministros global. Mejorar su eficiencia, hacer frente a los retos de la competencia y potenciar la sostenibilidad ambiental demanda del sector portuario usar tecnologías de la cuarta revolución industrial. La investigación sobre ciberseguridad en el sector marítimo y portuario ha iniciado estudios sobre los riesgos inherentes a la implantación de la Industria 4.0, la generación de políticas públicas y la regulación internacional para hacer frente a las nuevas amenazas. El objetivo de este trabajo es proporcionar una visión de la evolución y el progreso de la investigación sobre ciberseguridad en la industria portuaria, a través de un análisis bibliométrico. Los resultados de la investigación indican que el conocimiento de las ciberamenazas es todavía insuficiente para la industria portuaria. Es necesario identificar factores críticos de éxito (CSF), impulsores, barreras y conflictos para su aplicación, especialmente en las economías emergentes.

Palabras clave: Ciberseguridad, digitalización, industria 4.0, infraestructura crítica, puerto inteligente.

* Este capítulo presenta los resultados del proyecto de investigación "El poder marítimo como fundamento estratégico del desarrollo de la Nación", del grupo de investigación "Masa Crítica", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como A1 por MinCiencias y con código de registro COL0123247. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Daniel Alfonso Rojas Sánchez
Capitán de Navío (R) y magíster en Asuntos Marítimos, Shipping Management, de la Universidad Marítima Mundial, Malmö, Suecia. Candidato a doctor en Logística y Gestión de Cadenas de Suministros Universidad de La Sabana, ingeniero naval y profesional en Ciencias Navales de la Escuela Naval Almirante Padilla.

Samuel Rivera-Páez
Capitán de Navío (R) y doctor (cum laude) en Ciencias Sociales y Humanas de la Pontificia Universidad Javeriana. Profesor titular y líder del Grupo de Investigación "Masa Crítica", adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto" (Colombia).

Citación APA: Rojas Sánchez, D. & Rivera-Páez, S. (2022). La ciberseguridad marítima: una nueva dimensión de las relaciones internacionales en materia de seguridad marítima. En S. Rivera-Páez & J. R. Espinel Bermúdez (Eds.), *Asuntos marítimos y relaciones internacionales* (pp. 341-364). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602083.10

ASUNTOS MARÍTIMOS
Y RELACIONES INTERNACIONALES
ISBN impreso: 978-628-7602-07-6
ISBN digital: 978-628-7602-08-3
DOI: https://doi.org/10.25062/9786287602083

Colección Estrategia, Geopolítica y Cultura
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2022

Introducción

La industria marítima es vital para la economía global. Más del 85 % del volumen del comercio internacional pasa por las naves, puertos y terminales en todo el mundo, lo que los hace cruciales para la gestión de suministros internacionales y un elemento estratégico para la logística global. La actividad marítima es escencial en las actividades económicas de un país, ya que los puertos son plataformas logísticas que facilitan el flujo de mercancías abordo de las naves, proporcionando una interfaz entre el transporte oceánico y terrestre, e impulsando el comercio y la competitividad. Es muy claro que la industria marítima depende del comercio internacional, así como el comercio internacional depende de la producción global de bienes y servicios.

Böheim et al. (2015) pronosticó que la producción de la economía mundial se multiplicaría por siete en las próximas décadas. Aunque su proyección no consideró eventos aleatorios como la pandemia y sus efectos, la predicción aún parece posible. Su investigación también enfatizó en la necesidad de comprender la complicada relación entre la preocupación por el desarrollo sostenible, especialmente en lo ambiental, y los patrones de comercio internacional. La sostenibilidad ambiental estaría asociada con la integración de recursos humanos y tecnológicos que permitan a las empresas mejorar su eficiencia, ser más competitivas y, al mismo tiempo, ser amigables con el medio ambiente.

Para un eficiente comercio internacional, se requiere una logística marítima robusta, y la innovación en todo el proceso es decisiva para reducir el impacto del hombre sobre el medio ambiente (Golrizgashti et al., 2019). En este contexto, marcado por nuevos desafíos, el rápido pero incierto crecimiento económico global y la creciente preocupación por la sostenibilidad hacen que la actividad y

la competencia en el sector marítimo sean más exigentes. Para enfrentar estos desafíos, las tecnologías de punta de la cuarta revolución industrial parecen ser el camino, y la ciberseguridad muestra ser el antídoto para evitar el uso de estas capacidades para actividades ilegales o impactos corporativos.

La ciberseguridad comprende los esfuerzos realizados por una organización para evitar acciones cibernéticas maliciosas que afecten al funcionamiento normal de una organización o que afecten de otro modo el cumplimiento de su misión (Singer & Friedman, 2014). El interés reciente del tema ha llegado con la digitalización de nuestra sociedad, potenciada durante la pandemia de COVID-19 y el entusiasmo en las tecnologías emergentes asociadas a la sostenibilidad. La digitalización está presente en casi todas las actividades económicas, pero el interés particular de este documento se centra en la ciberseguridad y su influencia en las actividades marítimas. La investigación sobre ciberseguridad en la industria marítima ha crecido en número recientemente, pero faltan estudios sistemáticos, cronológicos y de síntesis que indiquen su evolución e implicaciones en su desempeño. Este trabajo tiene como objetivo revisar la literatura para obtener una mejor visión de la ciberseguridad en el medio marítimo. Para abordar lo anterior, se utiliza el análisis cuantitativo de los artículos publicados con miras a:

- Resumir los resultados más significativos de las publicaciones en materia de investigación sobre ciberseguridad marítima;
- identificar los temas centrales de la investigación realizada; y
- permitir a los lectores identificar las tendencias de la investigación y los retos futuros.

El capítulo está dirigido a los interesados en el tema, para brindarles una visión de la evolución y el progreso actual de la investigación sobre ciberseguridad en la industria portuaria. Para cumplir el objetivo, el documento está dividido en cinco secciones; la primera es la introducción, la segunda discute los materiales y los métodos, la tercera presenta los resultados y la discusión, la cuarta está dedicada a analizar los hallazgos con diversas herramientas de interpretación bibliométrica, y la última sección presenta las conclusiones y posibilidades de investigación. Para futuros estudios, la comprensión, evaluación y gestión del riesgo cibernético, sin disminuir el desempeño económico, ambiental y social de la actividad marítima, es la meta, así como su aplicación en el sector marítimo colombiano.

Materiales y métodos

Scopus se considera una de las fuentes de datos más importantes para el análisis bibliométrico científico. Es una base de datos que indexa artículos de investigación académica coproducido por Elsevier. Esta base de datos es fácil de consultar, y el aspecto multidisciplinario le da al investigador flexibilidad aún fuera de su disciplina (Burnham et al., 2010). Por lo tanto, se eligió Scopus como fuente de datos primaria para esta investigación. Además, se examinaron otras bases de datos y herramientas como Google Scholar, Web of Science e IEEE Xplore. Se han revisado las publicaciones de la UNCTAD, en particular la serie *Maritime Transport Review* del 2010 al 2020. Las expresiones *cybersecurity* o *ciber security; maritime industry* o *maritime sector;* y *port* o *seaport* se combinaron mediante operadores booleanos para buscar títulos, resúmenes y palabras clave de los autores desde el 2010 hasta el 2021.

El periodo seleccionado para el análisis se debe a que la escasa literatura anterior al 2010 no es relevante, pero ha crecido exponencialmente desde ese año, mostrando el creciente interés en el tema. Para la investigación sobre ciberseguridad en la industria marítima, el análisis de palabras clave de autor y de clústeres de palabras se realizó mediante la aplicación VOSviewer. La herramienta Analysis Research Results de Scopus, Scival de Elsevier, se emplea para analizar el impacto de la citación de cada publicación, establecer documentos por año, por fuente, por autor, por afiliación, por país/territorio, documentos por tipo y documentos por área temática.

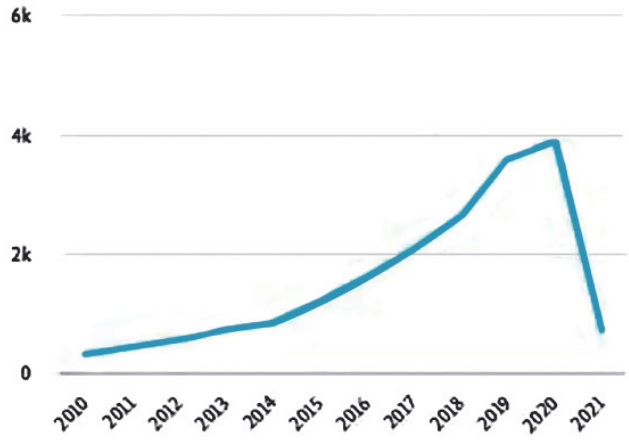
Resultados y discusión

El uso de Scopus como fuente primaria para la investigación bibliométrica comenzó con un barrido de la producción bibliográfica relacionada con la expresión *cybersecurity* o *cyber security.* La ciberseguridad parece ser el término más utilizado, pero muchas publicaciones siguen utilizando las dos palabras por separado. Los resultados de la consulta fueron 19.033 documentos. Este gran número de registros pone de manifiesto el vivo interés de la investigación académica sobre el tema. Contrasta con los registros encontrados relativos a la ciberseguridad y a la industria marítima y portuaria.

Las principales áreas temáticas en las que se estudia la ciberseguridad son la informática, la ingeniería, las ciencias sociales, las matemáticas, las ciencias de la

decisión y la energía principalmente. Cada día aumentan las áreas temáticas interesadas en este tema, lo que demuestra el impacto de la ciberseguridad en todas las esferas de la actividad humana, incluyendo los asuntos marítimos. Estados Unidos es, en general, el país donde se originan más publicaciones, seguido del Reino Unido, China e India. Otros países que destacan por el número de publicaciones son Australia, Italia, Alemania, Canadá, Federación Rusa y Japón. La figura 1 muestra un dato interesante, que hace referencia a que el interés académico y la investigación sobre el tema comenzaron a crecer con fuerza en el 2010.

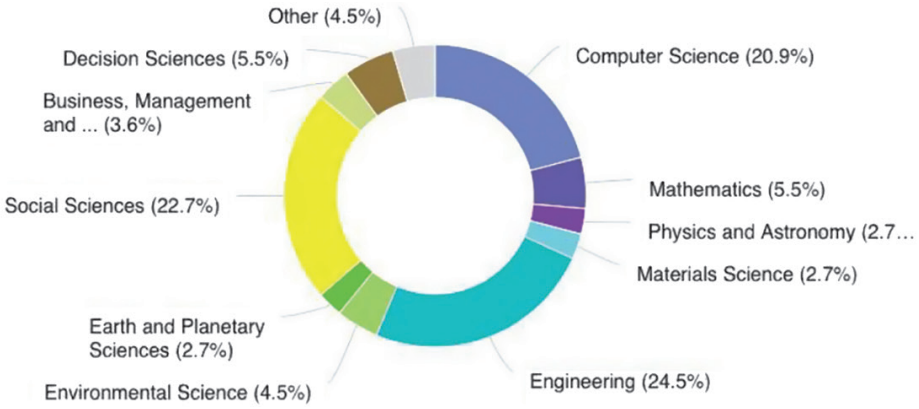
Figura 1. *Cantidad de publicaciones sobre ciberseguridad, 2010-2020*



Fuente: Scopus Analytics.

En este universo de documentos se buscaron publicaciones relacionadas con la industria o el sector marítimo. El resultado fue de 61 documentos que formaron una veintena de clústeres, de los cuales los diez más destacados son: delitos informáticos; derecho internacional; sistemas ciberfísicos; ingeniería social; sistemas de posicionamiento global; buques, estructuras offshore y navegación; criptografía; salud; Ártico, mares y piratería; modelación, y redes sociales. Los puertos no aparecen como un grupo independiente y se incluyen en el clúster de buques, estructuras marítimas y navegación. La figura 2 presenta las principales áreas temáticas en las que se desarrolla la investigación, en la que la ingeniería, la informática y las ciencias sociales se destacan sobre el resto.

Figura 2. *Principales temáticas de investigación en ciberseguridad en el medio marítimo*



Fuente: Scopus Analytics.

Entre los 61 documentos encontrados, se buscaron aquellos en los que incluyeran las palabras puerto o puerto marítimo ocupando un lugar destacado, lo que dio como resultado 30 publicaciones. A continuación se presenta la ecuación boleana que se utilizó para identificar las publicaciones analizadas.

((TITLE-ABS-KEY (*cybersecurity* OR *{Cyber security}*)) AND (*{Maritime industry}* OR *{Maritime sector}*)) AND (*port?* OR *seaport?*)

El término *maritime industry* se utiliza para dirigir la búsqueda hacia las actividades de las empresas navieras y portuarias directamente relacionadas con el comercio internacional, incluyendo los tipos de puertos y buques, la tripulación, la carga, las principales organizaciones marítimas y la normativa marítima, los seguros y el equipamiento náutico y portuario. El signo de interrogación (?) se utiliza para incluir el plural de las palabras *port* o *seaport* en la búsqueda.

Este resultado se divide en dos tipos de publicaciones: artículos, 46,7 %; documentos de conferencias, 43,3 %; libros y capítulos de libros, 10 % aproximadamente. La mayoría de los artículos son de ingeniería (24,5 %), seguidos de ciencias sociales (22,7 %), informática (20,9 %) y ciencias de la decisión (5,5 %). Otras áreas temáticas son las matemáticas (5,5 %), las ciencias ambientales (4,5 %) y las ciencias de la tierra y planetarias (2,7 %). Por países, Estados Unidos está a la cabeza con cinco publicaciones; Grecia, con cuatro; Italia y Reino Unido, con tres; Australia, Finlandia, Portugal, Sudáfrica y España, con dos; y Bélgica, con una. Los

años de mayor producción son 2018, 2019 y 2020, lo que demuestra el creciente interés al respecto. En la tabla 1 se muestran las publicaciones que han tenido mayor trascendencia, por ser las más citadas.

Tabla 1. *Lista de las diez publicaciones más citadas sobre ciberseguridad en la industria marítima y portuaria*

Title	Authors	Year	Cited by	Author Keywords
Providing industry 4.0 technologies: The case of a production technology cluster	Dalmarco G., Ramalho F.R., Barros A.C., Soares A.L.	2019	13	Industry 4.0; Portugal; Technology adoption; Technology management; Technology provider companies
The little-known challenge of maritime cyber security	Direnzo J., Goward D.A., Roberts F.S.	2016	11	automatic identification system; cargo handling; cyber security; electronic chart display and information system; GPS jamming; port operations; shipboard systems
A new digital service quality model and its strategic analysis in aviation industry using interval-valued intuitionistic fuzzy AHP	Büyüközkan G., Havle C.A., Feyzioğlu O.	2020	6	Air transportation; Airlines; Digital service quality; Digital transformation; IVIF AHP; SERVQUAL
CYSM: An innovative physical/cyber security management system for ports	Papastergiou S., Polemi N., Karantjias A.	2015	6	Port's risk assessment; Safety; Security
Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains	Polemi N.	2017	6	
Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre	Jacq O., Boudvin X., Brosset D., Kermarrec Y., Simonin J.	2019	5	ICS-SOC-maritime-cyber situation awareness
Current efforts in ports and supply chains risk assessment	Polemi N., Papastergiou S.	2016	5	physical /cyber security; risk assessment; supply chain
Navigating the cyber sea: Dangerous atolls ahead	Greiman V.	2019	3	Admiralty law; Cyber security; Data breach; Maritime security; Shipping regulations
Effective maritime cybersecurity regulation–the case for a cyber code	Hopcraft R., Martin K.M.	2018	3	cybersecurity regulation; International Maritime Organisation; Maritime cybersecurity; maritime industry; port security; risk management
Trojan horse risks in the maritime transportation systems sector	Shapiro L.R., Maras M.-H., Velotti L., Pickman S., Wei H.-L., Till R.	2018	3	Cybersecurity; Emergency management; Maritime security; Maritime threat actors; Personnel security; Transportation security

Fuente: elaboración propia a partir de las herramientas de análisis documental de Scopus.

En este grupo de 30 publicaciones, se priorizaron para el análisis 13 con las palabras *port* o *seaport* en el título o en las palabras clave proporcionadas por el autor por tener una relación con el tema analizado (tabla 2). En este grupo, ciberseguridad y puertos, Nineta Polemi, de la Universidad del Pireo, Grecia, es la autora más prolífica con tres publicaciones. Le siguen con dos, Spyridon Papastergiou de la Universidad del Pireo, Bilhanan Silverajan de Tampereen Yliopisto de Finlandia (Universidad de Tampere) e Ignacio de la Peña Zarzuelo de la Escuela Técnica

Superior de Ingenieros de Caminos, Canales y Puertos de Madrid. Otros con una publicación son Chalermpong Senarak C, de la Universidad Kasetsart de Bangkok, Tailandia, Andrea Chiappeta A, de ASPISEC Srl, Roma, Italia, Duarte Lynce de la Faria de la Universidade Nova de Lisboa, Portugal, Rory Hopcraft y Keith Martin de Royal Holloway, Universidad de Londres, Philip McGillivary de la Guardia Costera de EE. UU., Joseph Direnzo de Ciencia y Tecnología, Dana Goward de la Fundación Resilient Navigation and Timing, y Fred Roberts de la Universidad de Rutgers, Estados Unidos, y finalmente, Yair Wiseman de la Universidad Bar-Ilam de Israel.

Tabla 2. *Publicaciones priorizadas en el estudio*

Title	Authors	Year	Cited by	Author Keywords
The little-known challenge of maritime cyber security	**Direnzo J., Goward D.A., Roberts F.S.**	**2016**	**11**	automatic identification system; cargo handling; cyber security; electronic chart display and information system; GPS jamming; port operations; shipboard systems
Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains	**Polemi N.**	**2017**	**6**	
CYSM: An innovative physical/cyber security management system for ports	**Papastergiou S., Polemi N., Karantjias A.**	**2015**	**6**	Port's risk assessment; Safety; Security
Current efforts in ports and supply chains risk assessment	**Polemi N., Papastergiou S.**	**2016**	**5**	**physical /cyber security; risk assessment; supply chain**
Effective maritime cybersecurity regulation–the case for a cyber code	**Hopcraft R., Martin K.M.**	**2018**	**3**	cybersecurity regulation; International Maritime Organisation; Maritime cybersecurity; maritime industry; port security; risk management
Port cybersecurity and threat: A structural model for prevention and policy development	**Senarak C.**	**2021**	**2**	Cybertechnology; Cyberthreat; Port cybersecurity hygiene; Port digitalization; Prevention and policy development; Structural equation modeling
Why maritime cybersecurity is an ocean policy priority and how it can be addressed	**McGillivary P.**	**2018**	**2**	Cybersecurity; Port security; Quantum encryption; Shipping
Industry 4.0 in the port and maritime industry: A literature review	**de la Peña Zarzuelo I., Freire Soeane M.J., López Bermúdez B.**	**2020**	**1**	Global supply chain; Internet of things; Port 4.0; Port connectivity; Port innovation; Smart port
Enabling cybersecurity incident reporting and coordinated handling for maritime sector	**Silverajan B., Vistiaho P.**	**2019**	**1**	Cybersecurity incident exchange; Maritime cybersecurity; Smart ports; Smart ships
Protecting seaport communication system by steganography based procedures	**Wiseman Y.**	**2014**	**1**	**We would like to encourage you to list your keywords in this section**
Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue	**de la Peña Zarzuelo I.**	**2021**		Cybersecurity; Port 4.0; Risk analysis; Smart ports
Cybersecurity benefits and resilience of ports	**Chiappetta A., Chiappetta A.**	**2020**		Critical infrastructure protection; Cybersecurity; Infrastructures; Ports; Public-prvate partnerhsip; Resilience
The impact of cybersecurity on the regulatory legal framework for maritime security	**De la Faria D.L**	**2020**		Cybersecurity; Flag State; Maritime safety; Maritime security; Port State

Fuente: elaboración propia a partir de las herramientas de análisis documental de Scopus.

Los cinco documentos más citados en este grupo son "The little-known challenge of maritime cyber security" (Direnzo, Goward, & Roberts, 2016) citado once veces, en el que los autores describen las vulnerabilidades cibernéticas del sistema de transporte marítimo, centradose en los sistemas de a bordo, las instalaciones *offshore,* la carga y las operaciones portuarias; en segundo lugar, "Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chain" (Polemi, 2017), citado seis veces.

Polemi (2017) identifica los escenarios más probables de las ciberamenazas en las estructuras portuarias y analiza sus efectos en sus cadenas de suministro. Asimismo, su documento examina las metodologías y herramientas de evaluación de riesgos, identificando su aplicación a las infraestructuras portuarias de información crítica. El tercero es "CYSM: An innovative physical/cyber security management system for ports" (Papastergiou et al., 2015). Esta publicación describe un proyecto europeo conocido como CYSM, cuyo objetivo es abordar los requisitos de seguridad y protección de las infraestructuras críticas de información (ICI) en los puertos comerciales. El proyecto introduce un sistema integrado de gestión de riesgos cibernéticos para modelar diferentes escenarios con el fin de identificar, evaluar y abordar sus problemas de seguridad y protección de manera eficiente, armonizada y unificada.

El cuarto, con tres citas, es "Current efforts in ports and supply chains risk assessment" (Polemi & Papastergiou, 2015). En este trabajo, Polemi continúa estudiando las infraestructuras críticas de información portuaria y su relación con las TIC, presentando los esfuerzos de investigación existentes sobre la naturaleza ciberfísica de los sistemas portuarios y otros actores relacionados dentro de la cadena de suministro. El quinto, "Effective maritime cybersecurity regulation-the case for a cyber code" (Hopcraft & Martin, 2018), con tres citas, describe la necesidad de crear regulaciones de ciberseguridad robustas y resistentes. Se sugiere que la Organización Marítima Internacional (OMI) considere la promulgación de un código cibernético independiente, basándose en códigos anteriores como el Código Polar. Dado que la OMI busca que sus códigos sean legalmente vinculantes, esto podría impulsar la seguridad y la eficiencia operativa de la industria marítima frente a las amenazas cibernéticas.

Otras publicaciones con la palabra *port, maritime port* o *container port* en el título o en las palabras clave son, en primer lugar, "Port cybersecurity and threat: A structural model for prevention and policy development" (Senarak, 2020). El documento analiza la ciberseguridad con el fin de desarrollar una política pública que

se concentre en las dimenciones de la ciberseguridad (humana, infraestructura y medidas). En segundo lugar, "Protecting seaport communication system by steganography-based procedures" (Wiseman, 2014), que estudia los problemas de seguridad de los datos en un puerto, la importancia y valor de la información, la falta de ciberseguridad adecuada, y propone una forma criptográfica de compartirla basada en el formato JPEG. En tercer lugar, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue" (De la Peña Zarzuelo, 2021), que aborda la transformación digital que están experimentando los puertos, el nivel de integración de los diferentes dispositivos, agentes, actividades, y la ciberseguridad como el principal reto que la industria y los responsables políticos deben abordar para que las infraestructuras críticas estén bien protegidas. En cuarto lugar, "Industry 4.0 in the port and maritime industry: A literature review" (De la Peña Zarzuelo et al., 2020). El artículo señala y explora los nueve pilares de la Industria 4.0 en la industria portuaria y marítima, señalando que algunos de ellos están suficientemente maduros, pero otros se encuentran en sus primeras etapas, entre ellos la ciberseguridad.

Para confirmar los hallazgos, se consultó la base de datos Web of Science utilizando la ecuación equivalente para la investigación, como resultados, cuatro documentos. El primero, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue", de Ignacio de la Peña Zarzuelo; el segundo, "Industry 4.0 in the port and maritime industry: A literature review", de la Peña Zarzuelo et al.; el tercero, "Risks and threats of the maritime industry functioning in conditions of the world economy digitizing", de Baburina y Gurieva (2019); y "Effective maritime cybersecurity regulation: The case for a cyber code", de Hopcraft et al. (2018). Salvo la tercera, todas están ya registradas desde Scopus.

Barburina y Gurieva señalaron que la industria marítima fue una de las primeras en experimentar las vulnerabilidades de la digitalización de la economía global y destacaron la importancia de una gestión eficaz de los riesgos y de la coordinación nacional e internacional, pública y privada, para garantizar la seguridad de la navegación y el funcionamiento de los puertos y terminales marítimos.

Hay otra base de datos consultada: IEEE Xplore. IEEE Xplore se promociona como "La mayor organización profesional técnica del mundo para el avance de la tecnología" (Eichenhofer et al., 2020). Contiene resúmenes, registros de citas y textos completos en PDF de todas las revistas y conferencias del IEEE publicadas desde 1988 (Durniak, 2000). La búsqueda utiliza la misma metodología descrita, con lo que se obtienen cinco documentos, cuatro documentos de conferencias y

un artículo de revista. Los documentos de la conferencia, enumerados por orden de relevancia, son: "A framework for cybersecurity assessment of critical port infrastructure", de Trimble y Monken (2017), presentado en la Conferencia Internacional sobre Ciber Conflicto; "Enabling cybersecurity incident reporting and coordinated handling for maritime sector", de Silverajan y Vistiaho (2019), presentado durante la 14.ª Conferencia sobre Seguridad de la Información; "Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport", de Chiappetta y Cuozzo (2017), presentado en la 5.ª Conferencia Internacional del IEEE sobre modelos y tecnologías para sistemas de transporte inteligentes (MT-ITS); y "SecureAIS: Securing pairwise vessels communications", de Aziz et al. (2020), presentado en la Conferencia del IEEE sobre Seguridad de las Comunicaciones y las Redes. El artículo "Mining channel water depth information from IoT-based big, automated identification system data for safe waterway navigation", de He et al. (2018), editorial IEEE.

Por otro lado, Google Scholar enumeró al menos 110 resultados para el mismo método de búsqueda. Se incluyen la mayoría de los documentos encontrados en las otras bases de datos analizadas, además de trabajos de todo tipo. Los resultados de Google Scholar son significativos porque nos dan una idea clara de la importancia del tema en la actualidad y de cómo el interés, no solo académico, sino también práctico, aumenta cada día.

Tras revisar los títulos, resúmenes y palabras clave de los artículos identificados en las últimas bases de datos, se seleccionaron los directamente relacionados con la ciberseguridad marítima y los puertos y se añadieron a las publicaciones que figuran en la tabla 2. A continuación, se analizó la versión completa de cada uno de ellos para asegurar su relevancia y extraer novedades e ideas originales que permitieran conocer mejor el estado del arte para responder a los objetivos de investigación. Sin embargo, dado el escaso número de publicaciones, se decidió analizar todas las publicaciones relacionadas con la ciberseguridad, la industria marítima y los puertos para evaluar la relevancia del sector portuario en el sector marítimo en su conjunto.

El estudio de los trabajos seleccionados permitió identificar la evolución, las tendencias y los retos de la ciberseguridad en el sector portuario, temas de interés para profesionales y académicos. Un hecho relevante que se desprende de este estudio es que a partir del 2017 se observa un interés creciente por el tema. Como se ilustra en la tabla 3, los países en los que ha habido más inquietudes en cuanto a la investigación de ciberseguridad, industria marítima y puertos son los siguientes:

Estados Unidos, con cinco publicaciones; Grecia, con cuatro; Italia y Reino Unido, con tres; Australia, Finlandia, Portugal, España y Sudáfrica, con dos. En la lista también aparecen Brasil, Colombia, Croacia, Francia, Kazajistán, Eslovenia, Corea del Sur, Turquía y Ucrania, con una.

Tabla 3. *Producción académica e impacto en los países*

COUNTRY/REGION	SCHOLARLY VIEWS		FIELD-WEIGHTED CITATION IMPACT	CITATION COUNT
	OUTPUT	COUNT		
United States	5	327	1,13	21
Greece	4	170	0,74	13
Italy	3	124	0,39	3
United Kingdom	3	103	0,35	4
Australia	2	67	0,14	1
Finland	2	66	0,35	1
Portugal	2	162	1,44	13
Spain	2	160	0,39	1
South Africa	2	31	1,28	3
Belgium	1	69	1,14	6
Brazil	1	140	2,88	13
Colombia	1	5	0,00	0
Croatia	1	25	1,18	2
France	1	37	3,86	5
Kazakhstan	1	37	1,39	2
Slovenia	1	25	1,18	2
South Korea	1	48	0,00	0
Turkey	1	99	4,44	6
Ukraine	1	37	1,39	2

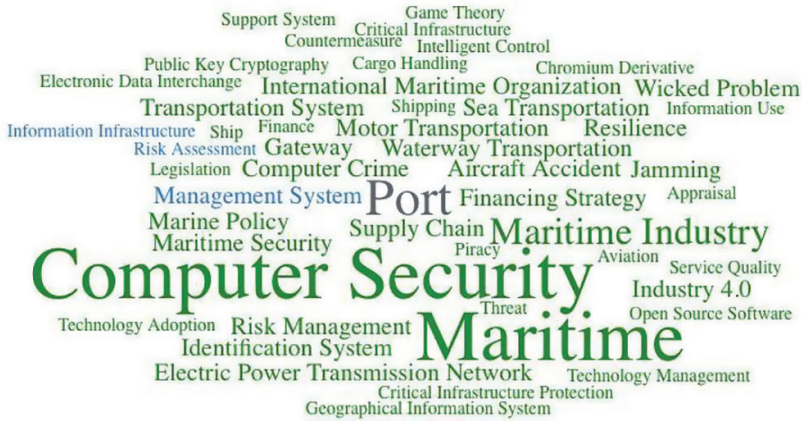
Fuente: elaboración propia a partir de las herramientas de análisis documental de Scopus.

La tabla destaca los países que han tenido más influencia dada su producción académica, el número de veces que el trabajo ha sido consultado, sus citas y su peso en otras investigaciones. Dentro de estos parámetros, destacan las publicaciones

de Estados Unidos, Francia, España y Corea del Sur. El Scholarly Output de América Latina se limita a Gamboa et al. (2020), de Colombia, y a Dalmarco et al. (2019). Sobre el primer trabajo, su incidencia ha sido apenas marginal, mientras que el segundo ha tenido más de 140 visitas y un Field Weighted Impact Citation de 2,88.

El análisis de palabras clave de las publicaciones seleccionadas se muestra en la figura 3. Dos expresiones dominan el grupo de palabras clave: *seguridad informática* y *marítimo,* seguidas de la palabra *puerto.* Salvo por la primera expresión, el resultado es el esperado dada la intención de la búsqueda. La relevancia del término *seguridad informática* dentro de las palabras clave es un indicio de que los temas de ciberseguridad en esta área de investigación se centran en el papel de los computadores, las redes que forman y la información que contienen. Palabras como *gestión de la tecnología, gestión del riesgo, protección de las infraestructuras críticas, Industria 4.0, sistemas de identificación, cadena de suministro y resiliencia* atraen la atención. Es probable que estas palabras asocien los riesgos cibernéticos en el sector marítimo y portuario con la adopción de tecnologías digitales emergentes y la necesidad de mitigar los posibles impactos en la cadena de suministro global. Otras palabras clave identificadas como *teoría de juegos, evaluación de riesgos, organización marítima internacional, legislación y política marítima* muestran un esfuerzo de investigación en la exploración de nuevas normativas y soluciones prácticas para controlar los riesgos potenciales.

Figura 3. *Palabras clave más relevantes*



Fuente: elaboración propia a partir de las herramientas de análisis documental de Scopus.

Hallazgos

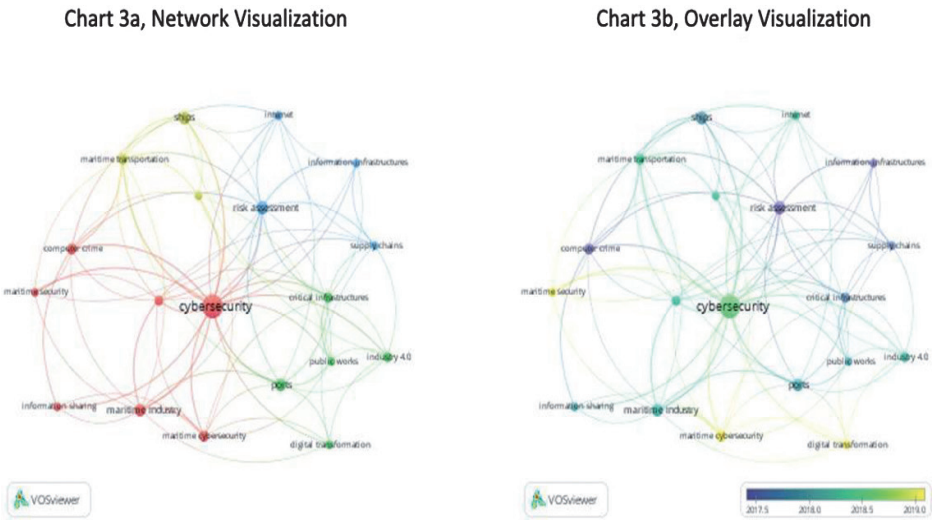
El estudio bibliográfico se realizó con dos herramientas de análisis: Scival de Scopus y VOSviewer. La primera analiza los datos almacenados en la base de datos de Scopus para encontrar la preeminencia de las principales palabras utilizadas en la investigación, visualiza las principales áreas de investigación de forma más comprensible, además de mostrar la investigación de los temas, el análisis de las citas de los artículos y la investigación, coincidencia y colaboración de los autores. La segunda permite encontrar las relaciones y correlaciones de las palabras clave de los artículos seleccionados, las tendencias de investigación y la agrupación de los investigadores según el grado de coincidencia de sus trabajos.

Para utilizar VOSviewer, las tres bases de datos seleccionadas, Scopus, WoS e IEEE Xplore, fueron convertidas al formato RIS y compiladas en una única base de datos con la ayuda de la aplicación Mendeley. Una vez hecho esto, se analizaron todas las publicaciones posibles, normalizando las palabras sinónimas o de significado similar para mayor rigor; el resultado está en la figura 4. En la primera representación se muestra la red superpuesta; se identifican 34 artículos en 4 clústers; cada clúster tiene un color. El clúster 1, en rojo, reúne siete ítems: delincuencia informática, ciberseguridad, intercambio de información, ciberseguridad marítima, industria marítima, seguridad marítima y gestión de riesgos. Clúster 2, en verde, infraestructuras críticas, transformación digital, industria 4.0, puertos, obras públicas. Clúster 3, en azul, infraestructuras de información, Internet, evaluación de riesgos y cadena de suministro. Clúster 4, en amarillo, Organización Marítima Internacional, transporte marítimo y buques. La investigación en ciberseguridad es el elemento central de la red que aglutina todos los componentes y en torno al cual se forman los clústeres.

En el primer clúster, la investigación sobre ciberseguridad se concentra en la delincuencia informática y sus efectos en la industria marítima. En el segundo clúster, la investigación hace hincapié en los efectos de los riesgos cibernéticos en las infraestructuras marítimas críticas, especialmente los puertos y en las naves, dada su creciente transformación digital. La Industria 4.0, la automatización naviera y los puertos inteligentes son el nuevo paradigma de la competitividad y la sostenibilidad que tienen como objetivo tener una cadena de suministro más eficiente. En el tercer clúster, la investigación se focaliza en la relación entre la ciberseguridad, las infraestructuras de la información y el uso de Internet. En este caso, preocupan las posibles consecuencias de un ataque cibernético sobre las infraestructuras críticas y la cadena de suministro. En el último clúster, el centro

es la relación entre los esfuerzos para lograr una ciberseguridad robusta y organizaciones como la Organización Marítima Internacional, encargada de liderar el esfuerzo, en particular sobre las normas y regulaciones internacionales para la industria marítima y portuaria.

Figura 4. *Visualización de los clústeres según vosviewer*



Fuente: elaboración propia a partir de las herramientas de análisis documental de Scopus.

La figura 4b muestra la visualización de superposición en la que los nodos y los enlaces de la red se muestran con diferentes tonos de color, representando el año de publicación. En este caso, los tonos amarillos representan las publicaciones más recientes a partir del segundo semestre del 2019, y los tonos más oscuros, las más antiguas. La transformación digital y la ciberseguridad marítima son los nodos más llamativos en amarillo, que conectan con una serie de nodos más pequeños en verde y azul, entre los que se encuentran la industria marítima, los puertos, la Industria 4.0 y las obras públicas. Cuanto más cercanos son los nodos, más significativa es su correlación.

Las conexiones más cercanas del nodo de puertos corresponden a la industria 4.0, la transformación digital, la ciberseguridad y la evaluación de riesgos. Se puede deducir que el interés por la industria marítima y portuaria y la ciberseguridad se

fortaleció a partir del 2019; esta preocupación aumentó con la llegada de la transformación digital y la industria 4.0 que apunta a puertos inteligentes o puertos 4.0. En este sentido, como afirman De la Peña Zarzuelo et al. (2020), la principal barrera para esta implantación es la preocupación por la ciberseguridad.

De lo anterior se deduce que el foco de la investigación sobre ciberseguridad en el sector marítimo se encuentra en el segundo clúster. En cambio, cuando se analizan solo los documentos que conciernen directamente a la ciberseguridad en el sector portuario, los resultados difieren un poco. En este escenario, hay diecinueve elementos agrupados en tres clústeres. El clúster 1 abarca seis elementos: transformación digital, tecnologías emergentes, Industria 4.0, Internet de las cosas y Puerto 4.0. El clúster 2 está conformado por cinco elementos: infraestructuras críticas, ciberseguridad, obras públicas, riesgos y sistemas SCADA. Por otra parte, el Clúster 3 lo conforman el transporte marítimo, los puertos y la evaluación de riesgos.

El clúster 1 se centra en la aplicación de las nuevas tecnologías digitales en la industria marítima para mejorar su competitividad y cumplir con los nuevos requisitos medioambientales. La aplicación del Internet de las cosas, los puertos inteligentes y los buques autónomos son los temas principales de este grupo. En este sentido, Gunes et al. (2021), De la Peña Zarzuelo et al. (2020), y De la Peña Zarzuelo et al. (2021) sostienen que la industria marítima está en constante evolución, y esta evolución conlleva cambios drásticos. Algunos de estos cambios están en las capacidades operativas y de infraestructura, los modelos de gobernanza y los marcos administrativos. El sistema ciberfísico (CPS) es un buen ejemplo, ya que se refiere a la interfaz entre el mundo digital y físico que se manifiesta en la industria marítima en el control de las naves autónomas o de los procesos automatizados de los puertos. En esto, la ciberseguridad y la desconfianza para compartir información parecen ser los principales obstáculos, aunque también representan vacíos de conocimiento que son una oportunidad para futuras investigaciones.

El Clúster 2 presenta los riesgos de la aplicación de las tecnologías emergentes en la industria marítima. La focalización está en la importancia de la ciberseguridad y sus efectos en las infraestructuras críticas, destacando las responsabilidades del sector público en su preservación. En ese sentido, Chiappetta & Cuozzo (2017) presentan una descripción de las principales vulnerabilidades relacionadas con el transporte marítimo y aéreo para el sector público y privado, particularmente en las vulnerabilidades de firmware vinculados a los sistemas SCADA (control de supervisión y adquisición de datos). En la misma línea, De la Peña Zarzuelo (2021)

afirma que la digitalización se convierte en la mayor vulnerabilidad del sistema portuario, mientras que Gunes et al. (2021) insisten en la necesidad de una evaluación constante de los riesgos, para lo cual presentan un método de gestión integrada y un plan que minimiza el ciberriesgo.

Para Trimble et al. (2017) y Polemi (2017), la regulación de las medidas y protocolos de ciberseguridad para las infraestructuras marítimas y portuarias es aún insuficiente. Destaca el interés del sector público por mitigar los riesgos cibernéticos, para lo cual se hacen imprescindibles los marcos estandarizados de evaluación de riesgos. Polemi, además, examina las metodologías y herramientas en la evaluación de los riesgos cibernéticos de las infraestructuras portuarias de información crítica (ICI) e identifica las barreras y las debilidades en las políticas, la legislación y de los marcos normativos existentes.

El clúster 3 plantea la necesidad de evaluar constantemente los riesgos cibernéticos para evitar interrupciones en el transporte oceánico y, en consecuencia, en la logística marítima. Para Lesniewska et al. (2019), Senarak (2021) y De la Peña Zarzuelo (2021), una parte esencial de la industria del transporte marítimo es afrontar y superar los retos. La pandemia del COVID-19 o las amenazas cibernéticas son solo dos ejemplos. Las nuevas tecnologías hacen que los buques y los puertos estén cada vez mejor conectados, para lo cual el control de riesgos cibernéticos es vital. Las recientes resoluciones de la Organización Marítima Internacional animan a los Estados y a los agentes privados a garantizar que los riesgos de ciberseguridad se aborden de manera adecuada para asegurar la continuidad de la cadena de suministro global. La oportunidad de investigación en este grupo está en el análisis de procesos y normas para lograr medidas eficaces de ciberseguridad sin afectar a la eficiencia operativa de la industria marítima.

Estos tres clústeres constituyen las tres líneas centrales de la investigación en ciberseguridad en el sector marítimo. Esto indica que los esfuerzos en materia de ciberseguridad van de la mano de la aplicación de tecnologías emergentes, en particular la Industria 4.0. Estas tecnologías le apuntan a la evolución de naves autónomas y puertos inteligentes con un impacto contundente y positivo en la logística marítima y, en general, en la cadena de suministro global. No obstante, la preocupación por la ciberseguridad se convierte en la principal barrera para la evolución digital, ante la escasa concientización, la inadecuada regulación y el insuficiente cumplimiento de los protocolos básicos en la aplicación de las tecnologías emergentes.

A pesar de la relevancia y el impacto de la ciberseguridad en el sistema portuario

y la industria marítima, una de las conclusiones más relevantes es que el interés académico por el tema ha sido escaso. Sin embargo, ha ido creciendo paulatinamente, asociado a la implementación de nuevas tecnologías digitales en puertos y terminales. Esto significa que surgen oportunidades de investigación para explorar este tema. Por ejemplo, las nuevas investigaciones podrían centrarse en el desarrollo de estrategias eficaces de ciberseguridad, estableciendo una tipología y una taxonomía adecuadas de los planes de preparación para los ciberataques (Ahokas et al., 2017). Sobre esto, Ahokas et al. (2017) afirman que se necesita más información sobre cómo se han aplicado dichas estrategias de forma empírica y cuán eficaces han sido para mitigar las ciberamenazas. También es necesario desarrollar nuevos métodos de evaluación de riesgos y mitigación de sus efectos, lo que ayudaría a los empresarios y a los responsables políticos a tomar mejores decisiones (Senarac, 2020; De la Peña, 2020; Gunes et al., 2021).

Por otro lado, se sugiere que para futuras investigaciones se analicen los nueve pilares de la Industria 4.0 considerando los elementos prácticos de las actividades marítimas, incluyendo la ciberseguridad (De la Peña Zarzuelo et al., 2020; Gundu et al., 2019; Kouhizadeh et al., 2020). Hasta ahora, se han realizado muy pocas investigaciones sobre la tecnología Blockchain en el entorno de la logística marítima. Saber hasta qué punto la ciberseguridad y las preocupaciones medioambientales son factores que obstaculizan la implementación de esta tecnología es un tema actual de potencial interés académico (Hackius y Petersen, 2017; Yoon et al., 2020).

Desde el punto de vista social, se necesitan más esfuerzos en el estudio de iniciativas de formación y sensibilización cultural que consideren las dimensiones culturales y la exploración de la interacción entre los aspectos técnicos y su vínculo con los comportamientos humanos en el contexto de la Industria 4.0 (Gundu et al., 2019). Sobre esto, hay varios desafíos relacionados con la gestión de la información crítica y las competencias de ciberseguridad. El equilibrio adecuado entre la eficiencia empresarial y operativa con la aplicación de medidas de ciberseguridad y la interconexión entre la tecnología de la información (TI) y la tecnología operativa (OT) son otras áreas potenciales de investigación. Por último, Androjna y Twrty (2020) subrayan que el estudio de las herramientas de las que disponen los ciberdelincuentes para llevar a cabo sus ataques y el impacto que alcancen es otra área en la que queda mucho por aprender.

Para la industria portuaria, la comprensión de las ciberamenazas es todavía insuficiente, la identificación de los factores críticos de éxito (CSF) para fomentar la ciberseguridad en la industria marítima no están totalmente identificados, y es

difícil hacer una evaluación adecuada de los riesgos cibernéticos de los puertos para obtener el nivel mínimo requerido en términos de seguridad.

Conclusiones

El sector marítimo es esencial para el desarrollo de las actividades económicas de un país; como sistema proporciona las naves, las plataformas logísticas y los procesos que facilitan el flujo de mercancías, proporcionan la interfaz entre el transporte oceánico y el terrestre y mejoran la competitividad del país. A pesar de los desafíos que se presentan, se espera que la producción de la economía mundial crezca más rápidamente en las próximas décadas, lo que generará una creciente preocupación por mejorar la competitividad sostenible, lo que impulsará a que las actividades del sector marítimo sean más exigentes. La mayoría de los operadores marítimos y portuarios están integrando la Industria 4.0 y otras tecnologías digitales en sus actividades para hacer frente a estos desafíos. Con esta integración, los puertos tienen el deber ineludible de integrar la ciberseguridad en sus procesos.

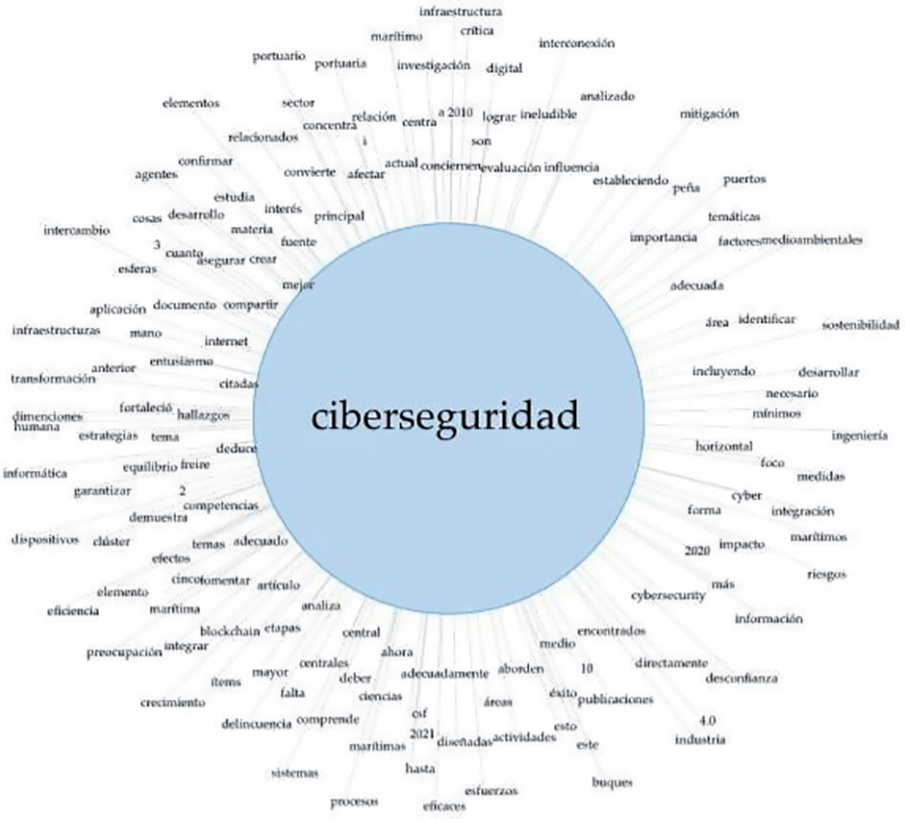
Este artículo ha tenido como objetivo revisar la literatura para encontrar vacíos para futuras investigaciones, ampliar la comprensión del tema, resumir los resultados más significativos, señalar los temas centrales, equipar a los lectores para identificar las tendencias y los desafíos futuros. Se eligió Scopus como fuente de datos principal para la investigación. Sin embargo, se examinaron otras bases de datos como Web of Science, e IEEE Xploreare, Google Scholar y las publicaciones de la UNCTAD sobre transporte marítimo. Las dos herramientas principales de análisis fueron la aplicación VOSViewer y la herramienta Scival de Elsevier.

Tras revisar los títulos, resúmenes y palabras clave de los documentos identificados, se seleccionaron solo aquellos directamente relacionados con la ciberseguridad y la industria marítima y portuaria, resultando treinta y cuatro publicaciones. De lo anterior se desprende una de las conclusiones más destacadas: el notable contraste entre el dinamismo de la investigación en temas de ciberseguridad y la falta de entusiasmo del mundo académico en su aplicación en la industria marítima. Un dato relevante es que solo a partir del 2016 comienza el interés por el tema, aunque ha ido creciendo desde entonces.

El análisis bibliométrico muestra que las áreas temáticas de mayor interés en ciberseguridad marítima son las ciencias de la computación, la ingeniería y las ciencias sociales, como se muestra en la figura 5. Este resultado es coherente con los resultados del análisis SciVal y Vos Viewer. Las investigaciones en la primera

área temática tratan de las vulnerabilidades de los sistemas y del control de los códigos maliciosos. En ingeniería, sobre la evolución y aplicación de nuevas tecnologías en la industria marítima a pesar de los ciberriesgos, y los de las ciencias sociales sobre el desarrollo de legislación, normas y guías para el control de las ciberamenazas y a afectación de los grupos humanos con el desarrollo tecnológico.

Figura 5. *Ciberseguridad en el medio marítimo y palabras frecuentemente asociadas*



Fuente: elaboración propia a partir de las herramientas de análisis de datos Voyant Tools.

En cuanto a las oportunidades de investigación, se identificaron los siguientes temas:

- El desarrollo de estrategias eficaces de ciberseguridad diseñadas para el sector marítimo.

- Nuevos métodos de evaluación de riesgos y desarrollo de planes de mitigación
- la relación entre ciberseguridad, industria 4.0, Blockchain y sostenibilidad en la logística marítima.

El estudio del elemento humano y su interacción cultural y competencias como fortaleza o vulnerabilidad en el sector y, las cuestiones relacionadas con el equilibrio entre la eficiencia portuaria y la ciberseguridad.

Para el sector marítimo, la comprensión de las ciberamenazas es todavía insuficiente. Para aplicar con éxito las medidas de ciberseguridad es necesario identificar los factores críticos de éxito (CSF). Las metodologías de evaluación de riesgos cibernéticos para obtener niveles mínimos de seguridad portuaria aún no son adecuadas y forman parte de campos de investigación que siguen ampliándose. La actividad académica por regiones muestra poca actividad en América Latina, lo que constituye otra oportunidad de investigación. El estudio académico rigurosa y su aplicación práctica son la única forma de enfrentar los desafíos que se avecinan.

Referencias

Ahokas, J., Kiiski, T., Malmsten, J., Ojala, & L., M. (2017): Cybersecurity in ports: A conceptual approach. En K. Wolfgang Blecker, & C. M. Thorsten Ringle (Ed.). En *Digitalization in supply chain management and logistics: Smart and digital solutions for an industry 4.0 environment. Proceedings of the Hamburg International Conference of Logistics (HICL)* (vol. 23, pp. 3-18). epubli GmbH.

Proceedings of the Ham burg International Conference of Logistics (HICL), 23, 343-359, https://doi.org/10.15480/882.1448

Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure. En *Cyber terrorism and extremism and threat to critical infrastructure protection* (pp. 163-171). Ministry of Defense Republic of Slovenia, Joint Special Operations University from Tampa, Institute for Corporative Security Studies.

Aziz, A., Tedeschi, P., Sciancalepore, S., & Pietro, R. D. (2020). SecureAIS: Securing pairwise vessels communications. *2020 IEEE Conference on Communications and Network Security,* 1-9. https://doi.org/10.1109/CNS48642.2020.9162320

Baburina, O., & Gurieva, L. (2019). Risks and threats of the maritime industry functioning in conditions of the world economy digitizing. *Maritime Intellectual Technologies,* 2(2), 109-115.

Böheim, M., Strauss, A., & Weiss, T. (2015). *Moving towards a new growth model: Policy options*. WWWforEurope, WelfareWealthWork. http://hdl.handle.net/10419/125627

Burnham, J., Lemley, T., & Brotton, R. (2010). Citation analysis: Comparison of Web of Science®, Scopus™, SciFinder®, and Google Scholar. *Journal of Electronic Resources in Medical Libraries,* 7(3), 196-217. https://doi.org/10.1080/15424065.2010.505518

Chiappetta, A., & Cuozzo, G. (2017). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS),* 206-211. https://doi.org/10.1109/MTITS.2017.8005666

Dalmarco, G., Ramalho, F., Barros, A., & Soares, A. (2019). Providing industry 4.0 technologies: The case of a production technology cluster. *Journal of High Technology Management Research,* Article number 100355.

De la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy, 100,* 1-4. https://doi.org/10.1016/j.tranpol.2020.10.001

Direnzo, J., Goward, D., & Roberts, F. (2016). The little-known challenge of maritime cyber security. *IISA 2015 - 6th International Conference on Information, Intelligence, Systems and Applications 20 January 2016, Article number 7388071* (p. Article number 7388071). Corfu, Greece: Institute of Electrical and Electronics Engineers Inc.

Durniak, A. (2000). Welcome to IEEE Xplore. *IEEE Power Engineering Review, 20*(11), 12.

Eichenhofer, J. O., Heymann, E., Miller, B. P., & Kang, A. (2020). An in-depth security assessment of maritime container terminal software systems. *IEEE Access, 8,* 128050-128067. https://doi.org/10.1109/ACCESS.2020.3008395

Golrizgashti, S., Piroozfar, S., & Dehghanpoor, A. (2019). Product innovation and supply chain sustainability. *IEEE Engineering Management Review, 15,* 128-136.

Gundu, T., & Maronga, V. (2019). IoT Security and privacy: Turning on the human firewall in smart farming. *ICICIS,* 95-104.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers and Security, 103.* https://doi.org/10.1016/j.cose.2021.102196

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? En *Digitalization in supply chain management and logistics: Smart and digital solutions for an industry 4.0 environment. Proceedings of the Hamburg International Conference of Logistics (HICL)* (vol. 23, pp. 3-18). epubli GmbH.

He, Z., Yang, F., Li, Z., Liu, K., & Xiong, N. (2018). Mining channel water depth information from IoT-based big, automated identification system data for safe waterway navigation. *IEEE Access, 6,* 75598-75608. https://doi.org/10.1109/ACCESS.2018.2883421

Hopcraft, R., & Martin, K. (2018). Effective maritime cybersecurity regulation: The case for a cyber code. *Journal of the Indian Ocean, 14*(3), 354-366.

Kouhizadeh, M., Zhu, Q., & Sarkis, J. (2020). Blockchain and the circular economy: Potential tensions and critical reflections from practice. *Production Planning & Control, 31*(11-12), 950-966.

Lesniewska, F., Ani, U., Carr, M., & Watson, J. (2019). In the eye of a storm governance of emerging technologies in UK ports post Brexit. *IET Conference Publications, 2019*(CP756). https://doi.org/10.1049/cp.2019.0165

Papastergiou, S., Polemi, N., & Karantjias, A. (2015, August). CYSM: An innovative physical/cyber security management system for ports. En *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 219-230). Springer, Cham.

Polemi, N. (2017). *Port cybersecurity: Securing critical information infrastructures and supply chains.* Elsevier.

Polemi, N., & Papastergiou, S. (2015). Current efforts in ports and supply chains risk assessment. *10th International Conference for Internet Technology and Secured Transactions* (pp. 349-354). Institute of Electrical and Electronics Engineers.

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *Asian Journal of Shipping and Logistics, 37*(1), 20-36. https://doi.org/10.1016/j.ajsl.2020.05.001

Silverajan, B., & Vistiaho, P. (2019, agosto). Enabling cybersecurity incident reporting and coordinated handling for maritime sector. En *14th Asia Joint Conference on Information Security* (AsiaJCIS) (pp. 88-95). IEEE.

Singer, P., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone need to know.* Oxford University Press.

Trimble, D., Monken, J., & Sand, A. F. L. (2017). A framework for cybersecurity assessments of critical port infrastructure. *2017 International Conference on Cyber Conflict (CyCon U.S.),* 1-7. https://doi.org/10.1109/CYCONUS.2017.8167506

Wiseman, Y. (2014). Protecting seaport communication system by steganography-based procedures. *International Journal of Security and its Applications, 8*(4), 25-36.

Yoon, A., Jeong, D., & Chon, J. (2021). The impact of the risk perception of ocean microplastics on tourists' pro-environmental behavior intention. *Science of the Total Environment, 774,* 144782.