Revista de **Relaciones Internacionales, Estrategia y Seguridad**

2024
Vol. 19(1)

Editorial Neogranadina

enero-junio ■ ISSN: 1909-3063 · e-ISSN: 1909-7743 ■ **pp. 13–30**

DOI: https://doi.org/10.18359/ries.6634

Estrategia de ciberseguridad en la infraestructura portuaria colombiana*

Samir Andrés Lores Acosta[a]

Resumen: En el actual contexto del mundo y por la importancia del tráfico marítimo mundial en el ámbito colombiano, donde la carga exportada por vía marítima es aproximadamente el 98,8 % del total del comercio exterior del país, mientras que la importada es del 98,2 %, principalmente movilizada en contenedores, es fundamental adoptar tecnologías, como la adopción de ventanillas únicas para los trámites y pagos en línea de servicios en los puertos, gestiones de documentación electrónica y comunicaciones, la implementación de sistemas automáticos de carga y descarga de mercancía y automatización de la operación, las cuales, por su naturaleza, tienen riesgo en el ámbito cibernético, y se abordan desde la perspectiva de infraestructura portuaria como activo crítico de las naciones. En este artículo se identificaron diferentes estrategias de seguridad marítima, bajo una metodología cualitativa de selección de información mediante repositorios académicos y buscadores *web*, para seleccionar las estrategias de ciberseguridad marítima que algunos países como Estados Unidos han desarrollado, y, con estos documentos, se plantea una propuesta de estrategia para Colombia, que toma elementos relevantes y aplicables al país, dada su estructura de gobierno y las entidades involucradas en la infraestructura portuaria, como la Dirección General Marítima, el Ministerio de Defensa, el Ministerio de Transporte, el Ministerio de Comercio, Industria y Turismo y la Superintendencia de Transporte.

Palabras clave: sector portuario; ciberseguridad; estrategia; puerto inteligente; ciberseguridad marítima; infraestructura portuaria

* El presente artículo de investigación tiene fundamento en la revisión bibliográfica como opción de grado para optar al título de magíster de la Escuela Superior de Guerra.

a Magíster en ciberseguridad y ciberdefensa, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá, Colombia. Especialista en evaluación y gerencia de proyectos. Ingeniero mecatrónico.

Correo electrónico: samiroandres@gmail.com

ORCID: https://orcid.org/0000-0003-1604-0237

Recibido: 24/02/2023. **Aceptado:** 29/02/2024. **Disponible en línea:** 30/06/2024.

Cómo citar: Lores Acosta, S. A. Estrategia de ciberseguridad en la infraestructura portuaria colombiana. *Revista De Relaciones Internacionales, Estrategia Y Seguridad, 19*(1), 13-29. https://doi.org/10.18359/ries.6634

A Cybersecurity strategy for the Colombian port infrastructure

Abstract: In light of the global maritime context and Colombia's significant reliance on maritime shipping, which constitutes approximately 98.8 % of its foreign trade, with 98.2 % of imported goods primarily transported in containers (DIMAR, 2020), it is imperative to embrace technologies such as single windows for online procedures and payments of port services, electronic document management, and communications of strategic importance to the nation. Additionally, the implementation of automatic cargo handling systems and operational automation, inherently carrying cyber risks, is crucial and approached from the perspective of port infrastructure as a critical nations asset. Within this framework, this article aims to propose a cybersecurity strategy for Colombian port infrastructure, comparing it with other cybersecurity strategies in the global maritime sector. A qualitative methodology was employed for information selection, utilizing academic repositories and web search engines to identify cybersecurity strategies developed by countries such as the United States. The article is structured into four subsections covering the international scope, global port infrastructure, associated cyber risks, and finally, the Colombian Port Cybersecurity Strategy. The conclusion underscores the challenges posed by strategy implementation and the involvement of diverse organizations engaged in port and maritime operations as critical hurdles that the nation must address for the prevention of cyberterrorism in this vital infrastructure.

Keywords: Port Sector; Maritime Cybersecurity; Strategy; Smart Port; Port Infrastructure

Estratégia de cibersegurança na infraestrutura portuária colombiana

Resumo: No contexto atual do mundo e pela importância do tráfego marítimo mundial no âmbito colombiano, onde a carga exportada por via marítima representa aproximadamente 98,8 % do total do comércio exterior do país, enquanto a importada corresponde a 98,2 %, principalmente movimentada em contêineres, é fundamental adotar tecnologias, como a implementação de janelas únicas para os trâmites e pagamentos online de serviços nos portos, gestão de documentação eletrônica e comunicações, a implementação de sistemas automáticos de carga e descarga de mercadorias e automação da operação, as quais, por sua natureza, possuem risco no âmbito cibernético, e são abordadas desde a perspectiva de infraestrutura portuária como ativo crítico das nações. Neste artigo foram identificadas diferentes estratégias de segurança marítima, sob uma metodologia qualitativa de seleção de informações através de repositórios acadêmicos e buscadores web, para selecionar as estratégias de cibersegurança marítima que alguns países, como os Estados Unidos, desenvolveram. Com esses documentos, é proposta uma estratégia para a Colômbia, que incorpora elementos relevantes e aplicáveis ao país, dada sua estrutura de governo e as entidades envolvidas na infraestrutura portuária, como a Direção Geral Marítima, o Ministério da Defesa, o Ministério dos Transportes, o Ministério do Comércio, Indústria e Turismo e a Superintendência de Transportes.

Palavras-chave: setor portuário; cibersegurança; estratégia; porto inteligente; cibersegurança marítima; infraestrutura portuária

Introducción

En la actualidad, el 90 % del comercio mundial se realiza por vías marítima y fluvial, lo cual supone un desafío para la logística global, aunado al hecho de que en la Globalización podría aumentar la demanda de los países hacia los productos terminados, motivo por el cual esta cadena de suministro se consolida como un aspecto fundamental para el desarrollo y habitabilidad de los países.

En consecuencia, cualquier contratiempo sucedido en este sistema afecta las infraestructuras tecnológica, comercial e industrial, generando posibles daños a la calidad de vida de los ciudadanos y, a mayor escala, a las economías de los países. Un ejemplo de esto se puede observar en el bloqueo ocasionado por el encallamiento del buque *Ever Given*, lo que causó la obstrucción del canal de Suez, por el que circula más del 10 % del tráfico del comercio marítimo mundial (Yee y Glanz, 2021).

Según el Banco Interamericano de Desarrollo de América Latina (BID, 2016), en los últimos diez años, el tráfico portuario de Latinoamérica y el Caribe ha crecido aproximadamente un 6,3 %, aunque está por debajo del promedio mundial, representa una oportunidad para la región de poder aumentarlo y, en consecuencia, elevar su producto interno.

Lo anterior se debió a las exportaciones de productos a los demás países de la región y fuera de ella, razón por la cual es necesario diseñar estrategias preventivas para robustecer la infraestructura marítima regional, con el fin de contar con diferentes alternativas que permitan proteger de manera apropiada a la seguridad física y cibernética de este delicado ecosistema requerido para el crecimiento de toda la región.

Es por lo anterior que se requiere identificar la infraestructura clave, la cual se encuentra definida en el artículo 2.2.21.1.1.3 del Decreto 338 del 8 de marzo de 2022:

> […] son infraestructuras críticas, activos físicos o virtuales que usan y operan mediante tecnologías de la información y al ser afectadas tiene un impacto negativo en la sociedad y en la economía de la población y en el correcto funcionamiento del Estado en su conjunto.

Entre esta se incluye a la infraestructura portuaria que hace parte del sector transporte, ya que es un habilitador del comercio en la cadena logística que permite la importación y exportación de materias primas y productos especializados, para la transformación y uso local.

La anterior definición tiene claras coincidencias con lo descrito por el Congreso de los Estados Unidos (Moteff *et al*., 2003), para el que la infraestructura crítica, tras la discusión, está vinculada estrechamente con los objetivos del debate sobre el terrorismo y la seguridad nacional. Acota el Decreto 338, que la base técnica incluye carreteras, puentes, presas, sistemas de saneamiento básico, etc., que si se vieran afectados tendrían implicaciones importantes en la moral nacional.

Esta norma no solo la define, si no que la clasifica, crea una lista entre lo público y privado (sistemas sanitario, eléctrico y financiero, transporte, producción, transporte y procesamiento de crudo, servicios de emergencia, seguridad y defensa, entre otros), y advierte el esfuerzo de priorizar y crear una nueva infraestructura para la custodia y protección de las mercancías, haciendo uso de sistemas de datos, histórico de incidentes y otra suerte de acciones que propendan por la reducción del impacto sobre la seguridad nacional.

Para el caso de Colombia, lo expresado es replicable, ya que el principal material exportado corresponde a aceites crudos de petróleo o de mineral bituminoso, los cuales salen del país por vía marítima, principalmente, a Estados Unidos y China (Godoy, 2022); aplica, igual, a las importaciones de químicos, fertilizantes y víveres, así como de equipos electrónicos y vehículos, los cuales no son producidos en el país y se requieren para el consumo y mantenimiento de la calidad de vida de los colombianos. Dado el estrecho vínculo de Colombia con la logística marítima internacional y las previas consideraciones en términos de la infraestructura crítica del país, es de interés mencionar que, en términos logísticos regionales, América Latina y el Caribe son susceptibles de sufrir afectaciones, según el último reporte de la Comisión Económica para América Latina y el Caribe (Cepal) (Rodrigo, 2020), que define unas posibles pérdidas de hasta US$155 000, por la materialización de

ciberataques, y enfrentar daños colaterales como multas, bajas de la credibilidad en los mercados financieros y logísticos, disminución de las relaciones comerciales internacionales y otros.

Colombia, según el reporte, está en la segunda posición en cuanto al número de incidentes que afectaron la logística nacional, solo superado por Brasil. Lo que supone, según el reporte en mención, un cambio en la estrategia, con especial énfasis en la resiliencia cibernética, la cooperación global y la comprensión de las redes y nuevas tecnologías.

De este modo se evidencia la necesidad de identificar los documentos o lineamientos específicos para Colombia sobre ciberseguridad, como lo son políticas públicas, resoluciones y normatividad relacionadas con los sectores marítimo, de tecnologías e infraestructuras críticas definidas en el país, con el fin de proponer estrategias que adopten las buenas prácticas internacionales aplicables en el contexto colombiano y ofrecer algunas recomendaciones a entidades públicas competentes del sector de transporte, específicamente sobre infraestructura portuaria y empresas privadas, incluidos los concesionarios portuarios.

Metodología

La búsqueda, selección y análisis de fuentes de información se realizó por medio de repositorios académicos y bases de datos de documentos indexados, como *Web of Science*, *Scopus*, *Elevier*, *Springer*, entre otros; el método empleado es un análisis cualitativo de tipo descriptivo y comparativo, que consistió en establecer categorías de análisis relacionadas con la ciberseguridad marítima y estrategias de ciberseguridad; de igual forma se realizó la consulta, compilación y análisis de documentos técnicos relacionados con riesgos de seguridad de infraestructura portuaria y con vulnerabilidades de los sistemas utilizados en el sector marítimo, con la intención de respetar una lógica temporal, estratégica y regional. Es menester indicar que, como herramientas de análisis de recopilación de información, se recurrió a la entrevista semiestructurada. Para la sistematización se empleó el análisis documental.

Con referencia a la construcción del marco teórico y conceptual se recurrió a fuentes de información técnica sobre las primeras iniciativas relacionadas con la seguridad marítima internacional, y a entidades no gubernamentales como la Organización Marítima Internacional (OMI), para profundizar en estrategias globales y después nacionales; para esto se establecieron los principales países que han desarrollado estrategias de ciberseguridad marítima o que contemplan el campo marítimo dentro de su estrategia de ciberseguridad nacional.

Al final se redunda en la construcción de la estrategia, en contextualizar sobre los avances y falencias en América Latina y el Caribe, como marco de referencia, que con amplitud son descritos por Aguilar (2020) en su estudio sobre el estado actual de la ciberseguridad y el evidente rezago ante las ciberamenazas, en el que prioriza enfoques para comprender los niveles de riesgo y amenaza.

Posterior al anterior estudio, Aguilar (2021) puntualiza en las oportunidades que tiene la región para avanzar en sus estrategias de ciberseguridad, mediante el estudio estadístico y el posprocesamiento y análisis de datos basados en mediciones de Global Cybersecurity Index (GCI) y el National Cyber Security Index (NSCI), con énfasis en Colombia como eje central de este documento.

Marco teórico y conceptual

Ciberseguridad marítima en el ámbito internacional

Los primeros pasos intergubernamentales de cooperación en el ámbito de la seguridad marítima se dieron gracias a la Convención de las Naciones Unidas sobre el Derecho del Mar, en 1982, también conocida como Convemar, en la cual se definieron derechos y obligaciones de los Estados ribereños, incluyendo plataforma continental y mar territorial, así como las reglas, principios, jurisdicciones estatales de operación y explotación, en función de resolver los desafíos que suponía la seguridad marítima y con la intención de contar con un marco de referencia estandarizado que permitiera facilitar la interacción más fundamental entre los diferentes países: el transporte y el comercio internacional por vía marítima.

A pesar de lo anterior y de otros lineamientos intergubernamentales, el mar se constituye estratégicamente por usuarios ilícitos como el medio ideal para

mantener sus operaciones ilegales; en este sentido, hay organizaciones internacionales como la OMI, en el rol de autoridad mundial encargada de establecer normas para la seguridad, la protección y el comportamiento ambiental1, que deben observarse en el transporte marítimo internacional, con la función principal de establecer un marco normativo para el sector del transporte marítimo2 que sea justo y eficaz, y que se adopte y aplique en el plano internacional.

El desarrollo informático acelerado por las nuevas dinámicas de comercio exterior ha obligado a cambiar el panorama frente a la seguridad marítima y portuaria, debido a la necesidad de usar sistemas automáticos o semiautomáticos de manejo de información, en los que se incluyen bases de datos, operaciones remotas, información satelital y comunicaciones entre otras (Cepal, 2020), con el propósito de aumentar la eficiencia en la producción, disminuir costos fijos y variables, y asegurar la estandarización en los parámetros de calidad de los diferentes productos y servicios que son ofertados por las naciones, gestionando así una permanente evolución de los empleos hacia labores más especializadas y no reemplazables por tecnologías existentes.

Hasta noviembre de 2001, en Budapest, se firmó el primer tratado internacional sobre ciberdelincuencia, creado para la seguridad nacional de los delitos cibernéticos (Cepal, 2020), el cual es firmado por 50 países, ante el aumento de las ofertas en el mercado de la ciberdelincuencia y por el evidente uso y dependencia de los sistemas informáticos, *software*, datos y servicios en línea, resultante de la implementación de internet y el establecimiento de canales transaccionales que permiten la adquisición de bienes y servicios por esta vía.

Este convenio se destaca por los avances regulatorios sobre transferencia de información, datos personales y comunicaciones, con un importante enfoque en seguridades nacionales y sociales, en las que se incluyen almacenamiento y difusión de pornografía infantil, y acceso ilícito a sistemas informáticos y redes privadas (Aguilar, 2019).

Lo anterior revela que a lo largo de los años y tras el avance de la ciberdelincuencia, en paralelo se avanza en esfuerzos gubernamentales en el marco normativo global y en la adopción nacional de estrategias encaminadas a la seguridad del país.

Los ataques a infraestructuras de interés nacional e internacional son más críticos si los objetivos se enfocan en la operación vital que depende de redes, internet, datos, accesos y otros, como es el caso de Estonia, país que sufrió un ciberataque en 2007 que dejó fuera de servicio las páginas *web* gubernamentales y el WannaCry; otro ciberataque de impacto mundial fue ejecutado en octubre de 2017, en por lo menos 150 países, que inhabilitó las operaciones de fábricas y sistemas de transporte, salud y de comunicación, y filtró información gubernamental, empresarial y personal, debido a fallas producidas en sistemas operativos de Microsoft (Departamento de Seguridad Nacional, 2019).

En ese sentido, algunas entidades no gubernamentales han orientado sus esfuerzos a dar lineamientos sobre ciberseguridad, en el caso del sector marítimo en el ámbito internacional, como la Organización Marítima Internacional (2017), que emite directrices sobre la gestión de los riesgos cibernéticos marítimos y con claridad establece una serie de orientaciones y normas no exhaustivas, entre las que se encuentran la norma ISO/IEC 27001, y la National Institute of Standards and Technology (NIST por sus siglas en inglés); lo anterior busca procurar que los países tengan en cuenta la ciberseguridad, resalta la importancia de la seguridad de las embarcaciones e instalaciones portuarias, con la intención de salvaguardar el transporte marítimo internacional, y propone metodologías de identificación, análisis, evaluación y comunicación de los riesgos cibernéticos, con enfoque en la proyección de las nuevas tecnologías.

1 La Organización de las Naciones Unidas para la Alimentación y la Agricultura (FAO) es un organismo especializado de la ONU que dirige las actividades internacionales encaminadas a erradicar el hambre.

2 La Organización Internacional del Trabajo (OIT), como un organismo especializado de las Naciones Unidas que se ocupa de los asuntos relativos al trabajo y las relaciones laborales, lleva a cabo un conjunto de acciones para incorporar mecanismos para la protección física de buques, puertos y usuarios marítimos, cuyos lineamientos se reúnen, incluyendo otros tantos, en el Código para la Protección de Buques e Instalaciones Portuarias, establecido en el 2001, posterior al atentado terrorista acontecido el 11 de septiembre de 2001 en Estados Unidos, en específico en el World Trade Center.

Es menester indicar que en la Resolución MSC.428(98), emitida por la Organización Marítima Internacional (OMI) (2021), se asevera que todo sistema de gestión de seguridad aprobado debe tener en cuenta la gestión de riesgos cibernéticos, alinearse con la preservación de la vida humana en el mar y mantener un nivel elevado de seguridad y protección del medio ambiente y de la seguridad nacional. Porque una ineficaz gestión de riesgos cibernéticos también tiene el potencial de acarrear accidentes que impacten el medio ambiente marino (OMI, 2021), generándole afectaciones irreparables, así como a las rutas de tráfico internacional y a la vida humana en el mar, aspectos que son prioritarios para el transporte marítimo internacional.

De igual forma, Bimco (2021) destaca la importancia del concepto de infraestructura portuaria, que incluye la interfaz buque-puerto.

A pesar de que la mayoría de sistemas de la industria marítima aún no están conectados con redes remotas, la amenaza y la vulnerabilidad derivadas de la implementación de nueva tecnología podrían aumentar en años venideros con los procesos de ejecución de sistemas y sus procedimientos de ciberseguridad (Bimco, 2021).

De modo que podría ser vulnerable ante diferentes eventos, entre otros, como secuestros cibernéticos o pérdida de información de manera intencional por partes ilícitas de la cadena logística de análisis, lo que tiene un claro impacto en la seguridad nacional.

Otra entidad que ha construido documentos sobre la ciberseguridad marítima es la Organización de Estados Americanos (OEA), de la cual hace parte Colombia, y que en 2021 publicó un documento llamado "La seguridad cibernética marítima en el hemisferio occidental: introducción y directrices", con el propósito de dar lineamientos y mejores prácticas a partir de las principales reglas y normas internacionales, recalcando la importancia del transporte marítimo para los Estados y la economía global (OEA, 2021).

Mientras que el BID, que entre sus objetivos declara la importancia de fomentar el desarrollo en los países de América Latina y el Caribe en materias económica y social, y propone el "Manual de puertos inteligentes" (BID, 2020), en el que define los componentes de un puerto inteligente que deben ser considerados para el establecimiento de cualquier estrategia de ciberseguridad en la infraestructura marítima.

Entre otros componentes, este Manual presenta diferentes lineamientos sobre la seguridad y la protección del ecosistema portuario y, al interior del apartado de marco conceptual, establece la problemática de la ciberseguridad para el desarrollo de los puertos inteligentes, la cual es un reto para los países que quieran desarrollar este tipo de infraestructura y aumentar su competitividad en el negocio de la logística marítima mundial, orientando a un diseño ecosistémico basado en la gestión de riesgos, de manera que sean mínimos una vez se alcancen las etapas de implementación y producción.

En junio de 2017, *NotPetya*, un *software* malicioso, se extendió por el mundo, afectando sistemas conectados a internet, incluida la compañía naviera *Moller-Maersk*, obligándola a detener sus operaciones en por lo menos 76 terminales portuarias (Departamento de Seguridad Nacional, 2019); las pérdidas calculadas por la Cepal alcanzan los US$ 300 millones (Cepal, 2020), sin contar con las no tangibles para la empresa, en materia de confiabilidad de las operaciones y de incumplimientos de los requisitos de calidad establecidos con los usuarios directos e indirectos.

América Latina y el Caribe, como macrorregión, no es ajena a eventos similares que afectan en especial a la cadena logística; según (Díaz, 2021), estos incidentes tienen una tendencia de crecimiento desde 2019 y resalta que los países que ha sufrido más percances son Brasil y Chile con once cada uno, Argentina y México con nueve y ocho, respectivamente. Colombia ocupa el octavo lugar con cuatro incidentes. Estos ataques registrados tienen un claro objetivo contra la infraestructura logística nacional, que afectan principalmente su infraestructura digital y su capacidad y tiempos de respuesta (comunicación interna-externa), con cerca de un 77,4 % de impacto, según (Díaz, 2021).

En el mismo año, Aguilar (2021) presentó un análisis sobre la evolución de las capacidades de Latinoamérica, y que sus avances son, según los datos revelados, un claro aumento de las

capacidades de ciberseguridad de países atacados. El autor destaca, tras su ponderación, a Uruguay, Colombia, Brasil, México y Chile. Al tomar en cuenta la ventana de análisis 2016-2020, todos los países de América Latina y el Caribe han realizado esfuerzos para aumentar sus capacidades.

Del mismo modo, la Cepal (2020) advirtió que en la red logística de América Latina, la mitad de los ciberataques denunciados corresponden a *ransomware*, modalidad en la cual existe la exportación de una gran cantidad de datos no cifrados, lo que afecta sobre todo la confidencialidad; estos datos no cifrados son después usados para sobornar o solicitar rescate de información a la víctima.

Estos ataques resuenan y crean tensión política y militar, de modo que Aguilar (2019) revela cómo impactan a países vecinos en medio de los esfuerzos propios para aumentar la seguridad cibernética, en lo que él ha denominado una "fuerza de inercia" que impulsa en bloque al apoyo internacional para la creación de políticas conjuntas.

Asimismo, el Departamento de Seguridad Nacional (2019) muestra las falencias de países de América Latina y el Caribe en la implementación de herramientas para la ciberseguridad, incluidos México, Colombia, Panamá, Paraguay, Chile y Costa Rica; pese a esto, países de la región se han unido progresivamente desde el 2006 a las reuniones de Ministerios de Justicia o de Fiscales Generales de las Américas (Remja / OEA), en las que se adelantan esfuerzos para implementar los principios del convenio de Budapest sobre el delito cibernético, entre los que están, Costa Rica, México, Argentina, Chile, Colombia, Panamá, República Dominicana, Paraguay y Perú (BID, 2016). Sus directrices sirven como referencia para robustecer las hojas de ruta de las naciones en materia de ciberseguridad y defensa de la cadena logística de análisis.

Las naciones de la macrorregión se han demorado en la implementación del convenio de Budapest, a pesar de las recomendaciones de la Remja / OEA (BID, 2020) para que sea usado como una directriz ante los delitos cibernéticos; en ese sentido, el BID (2016) advierte sobre las resistencias política, jurídica y procesal de las nuevas dinámicas y la tipificación de los delitos derivados de las conductas delincuenciales en el ciberespacio.

Colombia ha realizado un esfuerzo en la transformación del Estado a partir de políticas públicas que permiten dar lineamientos a las entidades gubernamentales para la adopción de nuevas tecnologías, a todos sus niveles, entre las que se destacan las políticas públicas contenidas en los Conpes 3701 de 2011, 3854 de 2016 y 3995 de 2020, los cuales dan cuenta de la intención política de blindar las cadenas económicas y productivas que afectan los intereses del Estado.

Mediante el Conpes 3701 de 2011 se dictaron lineamientos de política para ciberseguridad y ciberdefensa buscando "[…] una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país" (Conpes, 2011), debido a la creciente Globalización, la mejora en las tecnologías, los permanentes desarrollos tecnológicos y la creación de aplicaciones requeridas para asegurar los suministros y productos especializados generados por los países, en el marco de los diferentes acuerdos comerciales transnacionales suscritos por los Estados.

En concordancia con lo anterior y tomando en cuenta los lineamientos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el Gobierno nacional emitió el Conpes 3854 de 2016, con el que se creó la Política Nacional de Seguridad Digital, con el objetivo de "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia" (Conpes 2016), como un marco técnico de referencia que permita la adecuada gestión de riesgos en esta materia.

Estas políticas públicas permitieron que Colombia avanzara paulatinamente en el establecimiento de medidas para garantizar la seguridad digital; sin embargo, ante los retos que demanda el avance tecnológico fue necesario que se emitiera la Política Nacional de Confianza y Seguridad Digital, vigente en la actualidad, mediante la cual se proyecta "[…] establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital" (Conpes, 2020), objetivo que el Gobierno nacional trazó como carta de navegación en el Plan Nacional de Desarrollo 2018-2022 (Ley

1955 de 2019), específicamente en el "Pacto por la legalidad", que dispone en el objetivo séptimo el control integral marítimo, terrestre, aéreo, fluvial, espacial y ciberespacial (p. 68).

Estrategias de ciberseguridad que se han establecido en la infraestructura portuaria global

El Departamento de Seguridad Nacional (DHS) de los Estados Unidos advierte sobre el creciente incremento de las vulnerabilidades cibernéticas en infraestructuras críticas del país, con énfasis en la dependencia de las agencias clasificadas y no clasificadas de una infraestructura compleja que incluye "redes distribuidas, varias estructuras organizativas y modelos operativos (incluida la propiedad multinacional), funciones y sistemas interdependientes tanto en el espacio físico como en el ciberespacio, y la construcción de gobernanza que involucran autoridades, responsabilidades y regulaciones de varios niveles" (US Coast Guard, 2020)

En ese sentido, Wilshusen (2015) reporta un crecimiento lineal de los incidentes informados al equipo de preparación para emergencias informáticas de EE. UU., entre los años 2006 y 2014, el cual se evidencia como una interrelación de las constantes evoluciones de las tecnologías con las aperturas que generan a los diferentes ciberdelitos.

La infraestructura marítima se configura, según la USCG (2017), como uno de los ejes fundamentales de la seguridad y la prosperidad de la nación, debido a que de esta depende el transporte de personas, productos agrícolas y manufacturados, igual que de combustibles, de modo que permite y facilita la entrega de bienes, potencializando la economía de Estados Unidos, aspecto que es fácilmente extrapolable a cualquier país, lo cual obliga a los países a contar con un plan de tratamiento de los riesgos de seguridad física y digital de este ecosistema.

En ese sentido, la protección y seguridad tanto física como cibernética de una red integrada de

> […] 25.000 millas de vías navegables costeras e interiores, 361 puertos, 124 astilleros, más de 3.500 instalaciones marítimas, 20.000 puentes, 50.000 ayudas federales a la navegación y 95.000 millas de costa que se interconectan con carreteras, ferrocarriles, aeropuertos y oleoductos que representa aproximadamente unos $US 5.4 trillones/año. (Trump, 2020, p. 9)

La cantidad de dinero que está en peligro por ataques cibernéticos y las consecuencias de una parálisis parcial o total de la logística comercial debido a una mala gestión de seguridad, la convierte en una infraestructura crítica que debe ser priorizada por las agencias clasificadas para su protección y aseguramiento de su operación (USCG, 2017).

Se han ponderado los incidentes por categorías, y del 100 % reportado por Wilshusen (2015) se identificó que el 11 % correspondió a códigos maliciosos, 0,3 % a *phishing*, 6 % a ingeniería social, 13 % a equipamiento, 3 % a actividad sospechosa, 19 % a intentos de acceso no concedido y 17 % a violación de políticas. A partir de lo anterior, la Guardia Costera de Estados Unidos considera que ella misma se configura como un blanco de ataque cibernético, por su conexión estratégica entre las fuerzas militares, las fuerzas y agencias de seguridad, así como por el control, adquisición y administración de datos marítimos comerciales, civiles y estatales (USCG, 2017).

De esta manera se plantea la evaluación del riesgo, priorizando las medidas de seguridad y control interno, con un balance costo-beneficio para lo siguiente: 1) reconocer y comprender la dependencia del ciberespacio; 2) fomentar las asociaciones interinstitucionales e interdepartamentales; 3) usar inteligencia para priorizar y enfocar la implementación de mitigación de riesgos, y 4) monitorear y evaluar continuamente la efectividad de la mitigación de riesgos (USCG, 2017).

Es importante plantear la integración de la ciberseguridad en la planeación y adquisición de sistemas, enfocando los esfuerzos en comprender y gestionar los riesgos de la cadena de suministro a lo largo de todo el ciclo de vida; desarrollar políticas y prácticas de adquisición que fomenten las mejores prácticas para la seguridad, aumenten la seguridad y promuevan la eficiencia de las operaciones defensivas del ciberespacio, teniendo como pilares la mejora de la formación y la educación de los profesionales de la tecnología, vinculadas con los procesos de reclutar, educar, capacitar y

retener profesionales idóneos que prosperen en el campo de la tecnología, y promover asociaciones con departamentos de seguridad y el mundo académico, para así garantizar una formación y una educación de vanguardia en la materia, para defender los intereses estatales.

El último Plan Marítimo Nacional para la Ciberseguridad (Trump, 2020) reitera la importancia de proteger la infraestructura marítima y su interconexión, definiendo acciones prioritarias en el ámbito de "Riesgos y estándares", razón por la cual, como primera acción, se establece la eliminación del conflicto de intereses entre instituciones gubernamentales por roles y responsabilidades, como base fundamental para las siguientes acciones del mismo plan.

La segunda acción está encaminada al apoyo que recibe la Guardia Costera, entidad que interconecta física y cibernéticamente la red marítima de Estados Unidos mediante el desarrollo de modelos de riesgos y mejoramiento de los estándares de difusión de información y prácticas ciberseguras. La tercera acción tiene el objetivo de fortalecer los requisitos de ciberseguridad y la inspección de contratistas de los puertos; la cuarta y última acción prioritaria es el desarrollo de procedimientos para identificar, priorizar, mitigar e investigar los riesgos de ciberseguridad en sistemas de barcos y puertos críticos.

La segunda línea de trabajo definida en el mismo Plan Marítimo Nacional para la Ciberseguridad es la información e inteligencia compartida, que también plantea acciones prioritarias para avanzar en términos de ciberseguridad, como las siguientes:

1. La primera acción es compartir la información con la industria marítima por medio de agencias como la Guardia Costera, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Oficina Federal de Investigación (FBI) y la comunidad de inteligencia clasificada y no clasificada, para redistribuirla y prevenir ataques contra otra infraestructura interconectada.
2. La segunda acción es crear mecanismos que permitan compartir inteligencia con entidades no gubernamentales, para aumentar el acceso a información procesada o procesable, con la intención de proteger las redes que componen la red interconectada y la infraestructura marítima.
3. La tercera acción prioriza la adquisición y recopilación de inteligencia sobre la ciberseguridad marítima, lo que permite a los usuarios marítimos oficiales y civiles prepararse ante eventualidades físicas y cibernéticas, favoreciendo el modelado de riesgos, valoración y respuesta ante eventos.

Finalmente, Trump (2020) abordó lo anteriormente descrito por la USCG (2017) respecto al personal y lo llamó "Creación del personal para la ciberseguridad marítima", haciendo énfasis en la formación de personal especializado en ciberseguridad marítima, en la colaboración con el sector privado, para aumentar la experiencia en ciberseguridad marítima y, por último, planteó como acción priorizada, el desarrollo y despliegue de una fuerza laboral de ciberseguridad marítima que opere dinámicamente en toda la red interconectada a la infraestructura crítica del país (US Department of Homeland Security, 2018).

Por su parte, la Unión Europea (UE) definió 22 criterios de seguridad clasificados en grupos para proteger el ecosistema marítimo, basados en cuatro escenarios de ataques identificados y priorizados, en los que incluye: el robo de datos críticos de alto valor, la propagación de *ransomware* que obliga al cierre de operaciones portuarias, el compromiso de la comunidad portuaria de evitar la manipulación y el robo de datos y, finalmente, el deber de los administradores de información de evitar accidentes en zonas portuarias (Drougkas *et al*., 2019)supply in energy, trade within the European Union and transport of passengers and vehicles. This activity relies on more than 1 200 seaports within the European Union, each with different organisation, interests, challenges and activities. The global digitalization trend and recent policies and regulations require ports to face new challenges with regards to information and communication technology (ICT.

En ese sentido, la UE, con el objetivo de salvaguardar su ecosistema marítimo de ciberataques, adelantó acciones que incluyen diseñar e implementar una política de seguridad de los sistemas de

información que aborde medios, procedimientos y técnicas que deben ser aprobados por la alta dirección de puertos; definir claramente roles y responsabilidades de la comunidad portuaria, incluidos operadores, terminales, prestadores de servicios y proveedores, entre otros; adoptar el enfoque basado en riesgos para la construcción, evaluación, identificación, actualización y mejora continua de la estrategia de ciberseguridad de puertos, de forma que se vigilen continuamente las amenazas actuales y futuras, para ejecutar acciones que impidan los objetivos de los ciberdelincuentes, promover el flujo de información y adoptar modelos colaborativos públicos-privados.

Otra acción priorizada y relevante es la identificación de datos críticos en las operaciones portuarias relacionados con embarcaciones y mercancías peligrosas; así mismo, la evaluación e identificación de vulnerabilidades en los procesos de adquisición y monitoreo de activos, manteniéndolos actualizados, con el fin de contar con una ciberseguridad que permita alcanzar cada vez más un punto de mayor blindaje ante ciberataques.

Debido a las actuales amenazas y vulnerabilidades, Drougkas *et al*., (2019) aceptan que la UE será atacada y afectada, de forma que añaden a las acciones prioritarias la ciberresiliencia de los sistemas portuarios, definida como la estrategia de la gestión de la recuperación de los sistemas y la continuidad del ecosistema portuario, y el diseño de una política específica de gestión de crisis cibernética que involucra a todos los actores marítimos y de aguas continentales.

En ese sentido, la UE planteó definir una arquitectura segmentada, de forma que se pueda limitar la expansión de los ataques dentro de los sistemas portuarios y restringir la afectación para enfocar esfuerzos en la defensa del sistema afectado, del mismo modo que analizar y monitorear la infraestructura para detectar redes no autorizadas y maliciosas, que permitan tener una estructura de control para facilitar la recuperación ante ciberataques; esto se vincula al desarrollo de cursos de capacitación específicos y obligatorios sobre ciberseguridad, igual que asegurar las capacidades profesionales para realizar auditorías de antecedentes y proteger desde el interior a las entidades gestoras de información marítima y portuaria que tienen incidencia en todo el ecosistema (Drougkas *et al*., 2019).

Otros países, a pesar de no tener directrices específicas sobre la ciberseguridad marítima, vinculan criterios y lineamientos para el aseguramiento y la protección de las operaciones de la cadena de suministro de bienes y servicios, como es el caso de Australia, que aborda en su estrategia de ciberseguridad el aumento de la investigación cibernética, el vínculo estrecho y el trabajo conjunto que debe existir entre la industria marítima y las entidades gubernamentales de control y administración de información sensible (Department of Home Affairs, 2020).

De igual modo, Canadá insiste en su estrategia nacional de ciberseguridad (Public Safety Canada, 2018), al robustecer la red de colaboradores entre fuerzas del orden, agencias, servicios federales, territoriales, nacionales e internacionales con la industria privada, para aumentar la resiliencia ante inminentes ataques cibernéticos, con un modelo piramidal que vincula a las pequeñas y medianas empresas.

Noruega es otra nación que ha adelantado esfuerzos en la implementación de acciones y la identificación de rutas de trabajo. En su último informe, denominado "Estrategia cibernética nacional para Noruega" (Norwegian Ministeries, 2019), enfatiza en áreas prioritarias de trabajo para la protección ante ataques cibernéticos, reconoce la conexión existente entre proveedores y contratistas civiles, a las fuerzas públicas y organismos gubernamentales, lo que evidencia, de igual forma, que promover la ciberseguridad en instituciones privadas restringe los ataques a los entes gubernamentales, como parte de un sistema económico integral.

Rumania ha ido un poco más allá de lo antes descrito, y en su informe "Romania's National Cybersecurity and Defense Posture" presenta los roles, responsabilidades y estructura organizativa y de cooperación entre entidades estatales y privadas para la ciberdefensa nacional, liderada por instituciones como el sistema nacional de seguridad cibernética, y vincula a la Fuerzas Armadas, al Departamento de inteligencia, el servicio espacial de telecomunicaciones, los ministerios del Interior y de Comunicaciones, y la comunidad internacional, entre otros (Norwegian Ministeries, 2019).

Por su parte, la macrorregión de América Latina y el Caribe está de forma general muy inmadura en temas de ciberseguridad, según afirman Zambrano y Hernández (2020), lo que es coherente con lo que plantea la OEA (2021), ya que países centroamericanos como Honduras, Guatemala, el Salvador y Nicaragua, y República Dominicana, no cuentan con unas estrategias nacionales de ciberseguridad o con un equipo de respuesta ante la ciberdelincuencia; del mismo modo, no poseen unas hojas de rutas pública, jurídica, militar y civil enfocadas en disminuir el riesgo de ataques cibernéticos.

A pesar de las recientes intenciones de las naciones centroamericanas por avanzar en la seguridad cibernética, países como Panamá, Costa Rica y México logran sobresalir en la región al presentar estrategias claras y principios rectores al respecto (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones [MICCITT], 2017), con énfasis en infraestructura crítica, modelos colaborativos, investigación y desarrollo, y desarrollo de capacidades cibernéticas (México, 2017).

De lo anterior, un claro ejemplo son los avances de México en la publicación de su propia estrategia institucional del ciberespacio (Semar, 2021).

Riesgos cibernéticos de la infraestructura portuaria colombiana

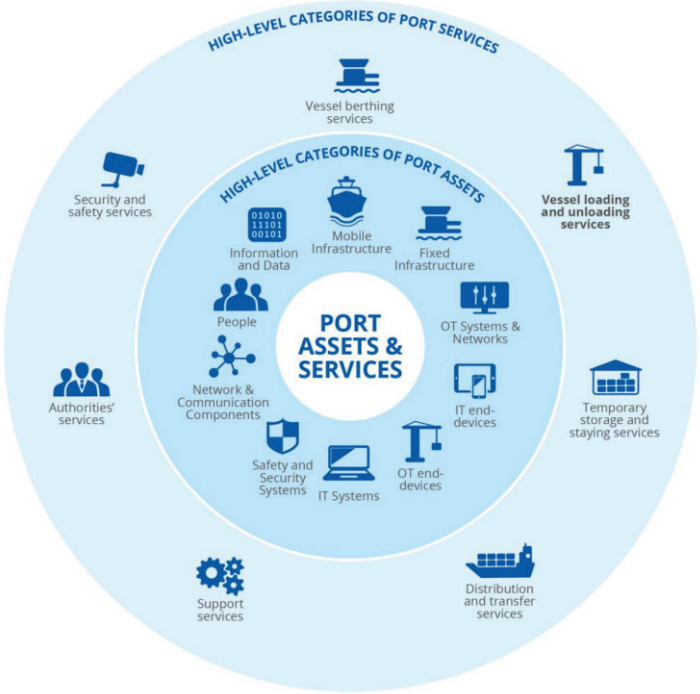
Como cualquier otra infraestructura crítica, los puertos usan tecnologías de información (TI) y tecnologías de operación (OT); en específico, en el sector marítimo hay unos riesgos debidos a los sistemas que utilizan y a las comunicaciones que se tienen con los diferentes actores que intervienen en el proceso logístico y de carga y descarga de mercancías, empezando por los buques, los cuales utilizan Global Navigation Satellite System (GNSS) y se apoyan en el Electronic Chart Display and Information System (Ecdis), el cual permite la visualización de las cartas náuticas electrónicas fundamentales para la navegación.

Así mismo, son vulnerables los sistemas electrónicos de pagos a los que las embarcaciones acceden, prestados por las instalaciones portuarias; en estos servicios interactúan varios actores, como la autoridad marítima, que en el caso de Colombia es la Dirección General Marítima (Dimar), los operadores, las terminales y los proveedores de servicios portuarios, los cuales intercambian información sensible, financiera, de coordinación portuaria, para que la interacción frecuente entre cada uno de estos actores genere una confianza, al recibir y entregar información que puede ser usada por los atacantes para explotar alguna vulnerabilidad de los sistemas, tanto de la instalación portuaria como de proveedores y terceros que hacen parte de la cadena logística.

De igual manera, algunos de los sistemas que pueden ser objetivos de ataque son el Sistema Mundial de Socorro y Seguridad Marítima (smssm), equipos de radares, el Sistema de Alarma de Guardia de Navegación del Puente (BNWAS), Cargo Control Room (CCR) y su equipo a bordo de computadoras, los sistemas de vigilancia como la red CCTV y los sistemas de propulsión, gestión de maquinaria y control de potencia, entre otros (Bimco, 2021), lo cual evidencia que las instalaciones portuarias también se pueden ver afectadas por el intercambio de información de alguno de estos sistemas.

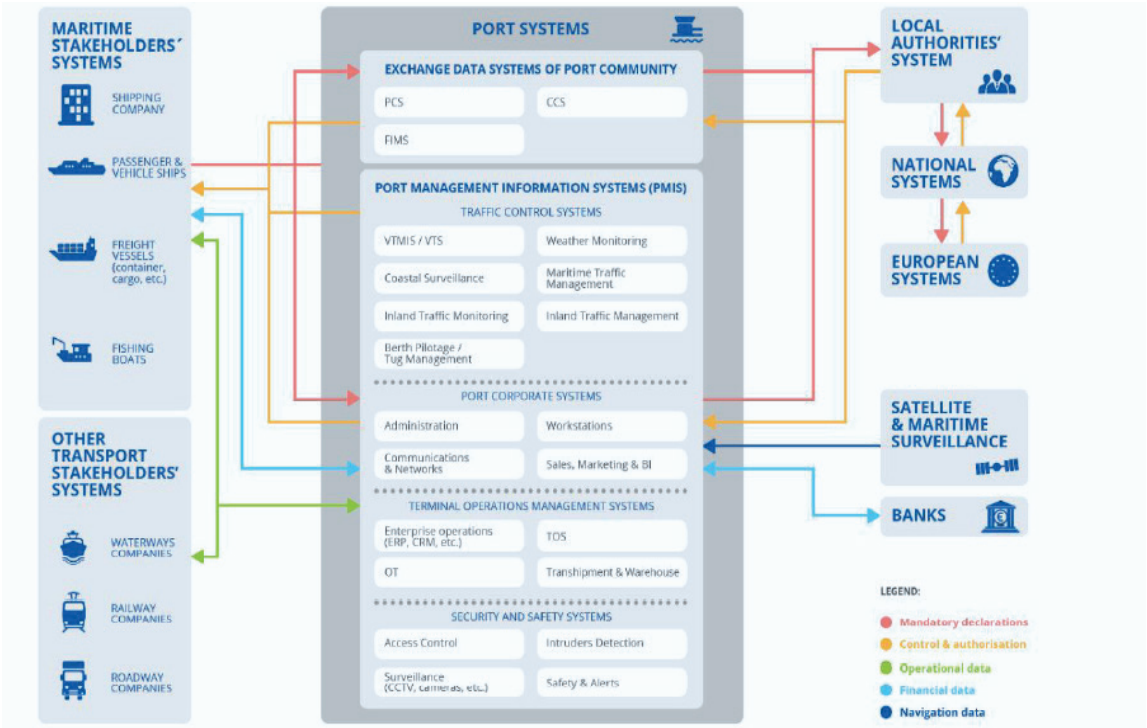
Los puertos también tienen sistemas ciberfísicos conectados a internet y, por tanto, son vulnerables a ciberataques, según la Agencia Europea de Seguridad de las Redes y de la Información (Drougkas *et al*., 2020), que generó un modelo de referencia de alto nivel (figura 1) para la identificación de los sistemas y actores involucrados de manera general, pero hizo la salvedad de que cada ecosistema portuario es muy específico, dependiendo de los servicios que preste y de la carga que maneje (Drougkas *et al*., 2020).

Figura 1. Categorías de alto nivel de activos y servicios portuarios



Fuente: Drougkas et al. (2020).

Figura 2. Modelo de referencia de alto nivel de los sistemas portuarios



Fuente: Drougkas et al. (2020).

En la figura 2 es apreciable la relación de los principales actores que interactúan con el puerto y los sistemas por los cuales se comunican e intercambian información, entre ellos se encuentran los sistemas utilizados por actores marítimos (compañías navieras, consignatarios, capitanes y tripulación de embarcaciones, etc.), los aplicados por otros transportistas para compartir información de carga o pasajeros y para permitir el transbordo (transporte fluvial empresas de transporte, empresas de carreteras, empresas ferroviarias, etc.), los utilizados por las autoridades locales, nacionales y regionales, y los sistemas empleados para la vigilancia marítima satelital.

Estas vulnerabilidades y necesidades tecnológicas son las mismas a las que se encuentra sujeta la infraestructura marítima colombiana, dadas las necesidades existentes en la prestación del servicio, su interrelación interna como país y la externa con los diferentes países con los cuales realiza actividades de intercambio comercial, entre otras. Las vulnerabilidades cibernéticas derivadas de la complejidad de la infraestructura tanto física como inmaterial de los puertos plantea nuevos desafíos, como lo identifica (Drougkas *et al*., 2020).

Los puertos se caracterizan por una gobernanza muy fragmentada y distribuida, en especial en el sector privado. Con frecuencia, las organizaciones o entidades responsables de las operaciones parciales o totales en los puertos comprenden múltiples partes interesadas, y las responsabilidades de seguridad cibernética no están claras y son complejas de implementar (Drougkas *et al*., 2020).

Estrategia de ciberseguridad a la infraestructura portuaria colombiana

A partir del 2004, mediante el Decreto 730, del Ministerio de Defensa Nacional, se reglamentó de manera parcial el capítulo 11 del convenio internacional para la Seguridad de la Vida Humana en el Mar, de 1974 (Solas), aprobado mediante la Ley 8ª de 1980), el cual en su artículo sexto dicta lo siguiente:

> Artículo 6. La Dirección General Marítima del Ministerio de Defensa Nacional será la autoridad designada por el Gobierno Colombiano para desempeñar las funciones de protección en relación con las instalaciones portuarias y de los buques, indicadas en el Capítulo XI-2 o el denominado Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP).
>
> 1.17 La evaluación de la protección de la instalación portuaria es fundamentalmente un análisis de riesgos de todos los aspectos de las operaciones de la instalación portuaria para determinar qué elemento o elementos de éstas son más susceptibles, y/o tienen más probabilidad de sufrir un ataque. En este contexto, el riesgo es función de la amenaza de que se produzca un ataque, unida a la vulnerabilidad del blanco y a las consecuencias de tal ataque. La evaluación incluirá lo siguiente: determinar la amenaza percibida para las instalaciones portuarias y la infraestructura; identificar los posibles puntos vulnerables; y calcular las consecuencias de los sucesos. Una vez llevado a cabo el análisis, será posible realizar una evaluación general del nivel de riesgo. La evaluación de la protección de la instalación portuaria ayudará a determinar qué instalaciones deben designar un oficial de protección de la instalación portuaria y preparar un plan de protección de la instalación portuaria.

Aunque en Colombia no se ha establecido una estrategia formal para la ciberseguridad, el Gobierno ha impulsado desde el plan nacional de desarrollo el Pacto por la Transformación Digital de Colombia, el cual busca la masificación del servicio público de internet, y dentro de esas estrategias se encuentra el uso de tecnologías emergentes y la seguridad digital; aunque no es una estrategia dirigida específicamente a la ciberseguridad marítima, el Gobierno nacional, en cabeza del Ministerio de Tecnologías de la Información y las Comunicaciones, expidió el Decreto 338 del 8 de marzo del 2022, con el cual estableció los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital, los que definen el modelo de gobernanza de seguridad digital, y dentro de este, en el artículo 2.2.21.1.2.3. Niveles del Modelo de Gobernanza de la Seguridad Digital, se definen los niveles para la

implementación, entre los que se encuentra como primero el estratégico.

Al efectuar un paralelo con estrategias de ciberseguridad de países como Canadá, se tienen en común el liderazgo y la colaboración, que es la articulación de las entidades gubernamentales para poder contrarrestar las amenazas existentes en el ciberespacio, orientada hacia un único enfoque nacional: identificar la infraestructura crítica cibernética para analizar sus vulnerabilidades y realizar el debido plan de contención y respuesta ante posibles materializaciones.

Una vez sean definidas dentro de las infraestructuras críticas del país las infraestructuras portuarias, se tendrá que dar cumplimiento a este Decreto y vincularse el Ministerio de Tecnologías de la Información y las Comunicaciones al grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), con la responsabilidad de implementar un plan de seguridad digital para la protección de su infraestructura tecnológica y cibernética.

La definición de la estrategia integra a varias entidades que participan y se articulan con diferentes roles y competencias en los sectores transporte y defensa en el dominio cibernético, la cual queda condensada en lo siguiente:

> Definición: La Estrategia Colombiana de Ciberseguridad marítima es un mecanismo que dicta lineamientos y traza el rumbo a corto, mediano y largo plazo, liderado por el Ministerio de Defensa Nacional (MDN, con el apoyo del Departamento Nacional de Planeación (DNP), Ministerio de Tecnologías de la Información y los otros Ministerios Sectoriales de Colombia, que buscando la defensa y continuidad de las operaciones de transporte marítimo e infraestructura portuaria del país, mantener la logística nacional como parte del desarrollo económico, por medio del diseño y la implementación de planes, proyectos y políticas que tiendan a la protección de las infraestructuras críticas del sector transporte en su modalidad de transporte marítimo y simultáneamente, fortalezcan el crecimiento social. Y económico del país y las regiones costeras e insulares.

Al dar cumplimiento a los lineamientos nacionales, como objetivo de la estrategia de ciberseguridad de la infraestructura portuaria del país, se propone fortalecer esta infraestructura y aumentar las capacidades de ciberseguridad de manera conjunta con los organismos gubernamentales, para reducir las posibles afectaciones a la logística del transporte marítimo y sus servicios conexos, y permitir el desarrollo económico del país y de sus ciudadanos. De igual manera, se proponen unas líneas estratégicas que consideran factores clave identificados en otras estrategias de ciberseguridad, como los siguientes:

Anticipación, prevención y cultura de ciberseguridad: esta línea estratégica tiene como objetivo que el sector pueda anticiparse a las amenazas que pudieran materializarse en afectaciones a la infraestructura portuaria y generar programas de capacitación y de apropiación de la cultura de ciberseguridad entre el personal que interactúe y opere sistemas relacionados con la operación logística de los puertos.

Este enfoque es incluido por Siegel y Sweeney (2023), para quienes el éxito de la estrategia del Departamento de la Marina de los EE. UU. (DON) depende fundamentalmente de mejorar y respaldar a su fuerza laboral cibernética. Sin un personal cibernético robusto, ágil y capacitado, no puede avanzar en la mejora de su seguridad, resiliencia o capacidad de combate en el ciberespacio.

Esta estrategia destaca la gestión de la fuerza laboral, el desarrollo del talento cibernético y la promoción de la conciencia de ciberseguridad. Esta primera sección tiene el objetivo de garantizar la correcta gestión, el reclutamiento, el desarrollo, la retención y la conciencia de ciberseguridad en su fuerza laboral.

Aumento de las capacidades de atención y respuesta: tiene como objetivo elevar la capacidad de respuesta táctica y operacional, en caso de surgir un incidente cibernético que ponga en riesgo la continuidad de sus operaciones. Del mismo modo, el DON, según Siegel y Sweeney (2023), ha cambiado del enfoque centrado en el cumplimiento a uno en la preparación cibernética. Y se destaca la necesidad de una evaluación en tiempo real de la efectividad de los controles de seguridad, las evaluaciones adversariales y las buenas prácticas de ciberseguridad.

De modo que los actores involucrados incrementarán sus capacidades cibernéticas de talento humano profesional y técnico, con el fin de que se reduzca la probabilidad de que la infraestructura portuaria y sus servicios conexos sufran afectaciones significativas.

El DON destaca la medición del riesgo, preparar a la fuerza laboral y adoptar la mentalidad de "cibermoneda", lo que otorgaría una mayor capacidad conjunta de respuesta ante un evento.

Coordinación y cooperación internacional: comprende, como objetivo, la generación de alianzas estratégicas con las partes interesadas, y su coordinación armónica, comunicación constante e intercambio de información en los ámbitos nacional e internacional, con el fin de consolidar esfuerzos y capacidades conjuntas en la lucha contra las amenazas cibernéticas que afecten la operación de la infraestructura portuaria y sus actividades asociadas.

Igual que el DON, que ha establecido una estrategia para defender la tecnología de la información (TI), los datos y las redes empresariales, implica identificar y gestionar activos de TI, detectar con celeridad incidentes de ciberseguridad y responder a ellos (Siegel y Sweeney, 2023).

Del mismo modo, en la séptima estrategia de Siegel y Sweeney (2023) se vinculan la cooperación y la colaboración, que se centran en trabajar e interactuar con diversos socios y partes interesadas, instituciones y entidades no gubernamentales, y aprovechar alianzas y asociaciones.

Recuperación y resiliencia: esta línea busca que el sector tenga la capacidad de adoptar rápido las directrices o políticas expedidas por el Estado colombiano y entes internacionales, así como mantener sus operaciones, a pesar de las afectaciones originadas por eventos que perturben la prestación del servicio de transporte y sus actividades conexas, mediante planes de acción que contrarresten los posibles efectos de la materialización de un riesgo de seguridad digital, y que la respuesta a los eventos también sirva para fortalecer el sector y articular la línea estratégica de coordinación y cooperación internacional.

Conclusiones

La modernización y adopción de tecnología por parte de los puertos necesita la implementación de medidas de seguridad alineadas con una estrategia conjunta entre el Gobierno, los puertos, sus proveedores y demás actores que interactúan en el proceso logístico de transporte de mercancías, ya sea por vía marítima u otras modalidades conexas a la infraestructura portuaria. Para Colombia es un desafío integrar a todos estos actores de manera coordinada y que cada uno cumpla las políticas y lineamientos que deberá establecer el Ministerio de Tecnologías de la Información y las Comunicaciones, y el futuro Comité Nacional de Seguridad Digital, establecido en el Decreto 338 de 2022.

En los aspectos técnicos y dentro de su competencia, entidades como la Dimar, al tener que inspeccionar el sistema de gestión de protección marítima, en el que la evaluación de riesgos de las instalaciones portuarias tendrá que contemplar los riesgos cibernéticos, tiene el reto de obtener las capacidades para realizar estas inspecciones y asegurar que se cumpla, en el ámbito cibernético, el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias, y se responda a los riesgos de seguridad digital.

De igual manera, las instalaciones portuarias tienen el reto de cumplir con las recomendaciones y la normatividad que se expida en cuanto al tratamiento de riesgos de seguridad de la información, por instituciones como el Ministerio de Defensa Nacional, que está encargado de la formulación y adopción de políticas, planes generales, programas y proyectos del sector Defensa, para resguardar la soberanía, la independencia y la integridad territorial, en el que el ciberespacio es un dominio del cual también se tiene que hacer responsable dentro de sus competencias y, en específico, en el sector del transporte marítimo asegure que el comercio exterior y la economía del país no se verán afectados por una interrupción del servicio, como consecuencia de una operación cibernética.

Con las iniciativas del Gobierno en materia digital y la integración de ventanillas únicas es aún más relevante la apropiación de una estrategia de ciberseguridad para las infraestructuras portuarias, en la que confluyen la mayoría de los actores del sector; con la implementación de esta clase de servicio aumenta el área expuesta a ataques cibernéticos y las vulnerabilidades que se pueden explotar para afectarlo.

El Ministerio de Defensa Nacional es un actor principal en la articulación de las entidades estatales que dentro de sus competencias tienen incidencia en el sector del transporte marítimo y la infraestructura portuaria del país, ya que la información recolectada por medio de organismos de inteligencia y contrainteligencia es una fuente principal para prevenir, combatir y contrarrestar las amenazas emergentes que pongan en riesgo la seguridad y la defensa nacional.

Referencias

Aguilar, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales*, *53*(198). http://dx.doi.org/10.5354/0719-3769.2021.57067

Aguilar, J. M. (2020). Brecha de ciberseguridad en América Latina. *Revista de Estudios en Seguridad Internacional (RESI)*, 6(2). http://dx.doi.org/10.18847/1.12.2

Aguilar, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *Urvio. Revista Latinoamericana de Estudios de Seguridad*, 4299(25), 24-40. https://doi.org/10.17141/urvio.25.2019.4007

Banco Interamericano de Desarrollo (BID). (2020). *Manual de Puertos Inteligentes*.

Banco Interamericano de Desarrollo (BID). (2020). Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe. *BID-OEA*, 1, 116-119. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

BID. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?: Informe Ciberseguridad 2016*. Observatorio de la Ciberseguridad en América Latina y el Caribe, 193. https://www.observatoriociberseguridad.com

Bimco. (2021). The Guidelines on Cyber Security Onboard Ships. *International Chambber of Shippinger of Shipping*, 4, 1-53.

Cepal. (2020). *La ciberseguridad en tiempos del covid-19 y el tránsito hacia una ciberinmunidad*. FAL, Boletín 382. Cepal. (Internet). https://repositorio.cepal.org/bitstream/handle/11362/46275/S2000679_es.pdf?sequence=1&isAllowed=y

Departamento Nacional de Planeación (DNP). (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. Conpes 3701-2011. Consejo Nacional de Política Económica y Social. (Internet), 43.

Departamento de Seguridad Nacional-Gobierno de España. (2020). *Informe Anual de Seguridad Nacional 2019*. Defensa de Seguridad Nacional, 280. https://www.cisco.com/web/offer/gist_ty2_asset/Informe_anual_de_seguridad_de_Cisco_de_2013.pdf

Departamento de Seguridad Nacional. (2019). *Estrategia Nacional de Ciberseguridad*, 1-68. https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Department of Home Affairs. (2020). *Australia's 2020 Cyber Security Strategy: Industry Advisory Panel Report*. (Internet). https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf

Díaz, R. M. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe 228*. Desarrollo productivo. Cepal, 1-68.

Drougkas, A., Sarri, A. y Kyranoudi, P. (2020). *Cyber Risk Management For Ports*.

Drougkas, A., Sarri, A., Kyranoudi, P. y Zisi, A. (2019). *Port cybersecurity: good practices for cybersecurity in the maritime sector*. In Enisa.

Departamento de Estado (EE. UU.). (2015). *DOD Cyber Strategy*, 91.

Godoy, L. (2022). *Observatorio de Economía Compleja*. https://oec.world/es/profile/country/col

Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICCITT). (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica*. (Internet). http://www.conicit.go.cr/ver/sic/biblioteca_virtual/publicaciones/publica_cyt/otros_doc_cyt/Estrategia-Nacional-Ciberseguridad-CR-19-10-17.pdf

Moteff, J., Copeland, C., Fischer, J., Ave, I. y Washington, S. E. (2003). Report for Congress Received through the CRS Web Critical Infrastructures: What Makes an Infrastructure Critical? *Time*, 21. /https://irp.fas.org/crs/RL31556.pdf

Norwegian Ministeries. (2019). *National Cyber Security Strategy for Norway*. (Internet). https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

Organización de Estados Americanos (OEA). (2021). *Marítima: la seguridad cibernética en el hemisferio occidental. Introducción y directrices*. Organización de Estados Americanos.

Organización Marítima Internacional (OMI). (2017). *Directrices sobre la gestión de los riesgos cibernéticos marítimos*. Documento OMI, MSC-FAL. 1(0), 7. http://www.imo.org/es/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3 - Directrices Sobre La Gestión De Los Riesgos Cibernéticos Marítimos (Secretaría) (1).pdf

Organización Marítima Internacional (OMI). (2021, junio). *Resolución MSC*.428(98). https://wwwcdn.imo.org/localresources/es/OurWork/Security/Documents/Pages from MSC 98-23-Add.1 - Anexo 10.pdf

Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. In *Public Safety Canada*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx?wbdisable=true

Rodrigo, G. N. (2020). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe*. 60.

Secretaría de la Marina. (2021). *Estrategia Institucional en el Ciberespacio 2021-2024*. Armada de México.

Siegel, C. A. y Sweeney, M. (2023, noviembre). *Cyber Strategy*. 1ª. edición. Auerbach Publications. https://doi.org/10.1201/9780429323003

Trump, D. J. (2020). *National Strategy for Maritime Security*. (Internet). https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf

US Coast Guard. (2020). *Vessel Cyber Risk Management Work Instruction*. 027(1), 1-7. https://safety4sea.com/wp-content/uploads/2020/11/USCG-CVC-WI-027-"Vessel-Cyber-Risk-Management"-2020_10.pdf

US Department of Homeland Security. (2018). *DHS cybersecurity strategy*. 35. https://www.dhs.gov/publication/dhs-cybersecurity-strategy

Yee, V. y Glanz, J. (2021). Así fue como el Ever Given se atascó en el Canal de Suez. *New York Times*. https://www.nytimes.com/es/2021/07/19/espanol/canal-suez-evergiven.html

Wilshusen, G. C. (2015). *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*. (Internet). https://oversight.house.gov/wp-content/uploads/2015/04/Wilshusen-Testimony.pdf

Zambrano, A. y Hernández, L. (2020). *Centroamérica Cibersegura*. 43.