Modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para contener amenazas del ciberespacio[1]

MYCIM Juan Pablo Gómez López[2]
Escuela Superior de Guerra General "Rafael Reyes Prieto"

Resumen

La presente investigación se desarrolla con el objetivo de proponer un modelo conceptual de ciberseguridad aplicable en el comercio marítimo en Colombia, por eso tiene un enfoque cualitativo aplicado por medio de instrumentos de investigación como la revisión documental en fuentes primarias que incluyen libros, informes, páginas web, crónicas, noticias; el segundo instrumento son entrevistas a personal que trabaja en áreas relacionadas con la ciberseguridad en la Armada Nacional, a partir de esta información, de la que se obtiene de documentos y de casos en otros países se elabora un modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para contener amenazas del ciberespacio que cuenta con tres componentes enfocados en la prevención y minimización de delitos como el narcotráfico y la piratería que están relacionados con este fenómeno a través de la contribución de la Armada; el modelo propuesto es verificado por expertos en el tema y contrastado a través de una matriz DOFA.

Palabras clave: Armada Nacional, Ciberamenazas, Ciberseguridad, Comercio Marítimo.

---

[1] El presente capítulo de investigación es presentado como opción de grado para optar al título de Magister en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, siendo producto del proyecto de Investigación titulado "Modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para la contención de amenazas provenientes del ciberespacio", vinculado al grupo de investigación Masa Crítica, categorizado en B COL0123247, inscrito en Minciencias.

[2]Estudiante que optará por el título de Magister en Ciberseguridad y Ciberdefensa. Especialista en Política y Estrategia Marítima, y Profesional en Ciencias Navales y Administración de la Escuela Naval "Almirante Padilla". Código ORCID: https://orcid.org/0000-0001-6657-5251

The present investigation is developed with the objective of proposing a conceptual model of cybersecurity applicable to maritime commerce in Colombia, for this reason it has a qualitative approach applied through research instruments such as documentary review in primary sources that include books, reports, pages web, chronicles, news; The second instrument is interviews with personnel who work in areas related to cybersecurity in the National Navy. Based on this information, which is obtained from documents and cases in other countries, a cybersecurity model applicable to maritime trade is developed. in Colombia to contain threats from cyberspace, which has three components focused on the prevention and minimization of crimes such as drug trafficking and piracy that are related to this phenomenon through the contribution of the Navy; the proposed model is verified by experts in the field and contrasted through a SWOT matrix.

Key Words: National Navy, Cyberthreats, Cybersecurity, Maritime Trade

Introducción

La globalización es uno de los fenómenos que cambio la dinámica del mundo haciendo posible la materialización de una sociedad interconectada a través de internet y otros sistemas de comunicación, así mismo, fue el punto de partida para el desarrollo de herramientas que han simplificado procesos logísticos en sectores como el comercio marítimo, en donde internet se complementa con el ciberespacio para ayudar en la digitalización de sistemas de navegación, radares y la implementación de otros instrumentos que mejoran la gestión y la seguridad de buques y barcos que transportan mercancía por el mundo; pero, lo que en un momento se reconoció como una ventaja, con el paso del tiempo ha expuesto también amenazas que a través del ciberespacio han afectado el funcionamiento y la seguridad del comercio marítimo en Colombia.

Entre tanto, el ciberespacio, reconocido como un mundo virtual en el que interactúan diferentes actores a través de herramientas tecnológicas en donde se forja un espacio relacional

(Aguirre, 2010), influye en la evolución de la sociedad, pero con el paso de los años este se ha transformado en una amenaza para actividades como el comercio marítimo, víctima de ataques que evidencian la vulnerabilidad de la seguridad marítima y cibernética, afectándolo con la irrupción de sistemas marítimos que se suman a la llegada de intrusos y de virus que a su vez exponen amenazas de otra naturaleza que pueden entorpecer el correcto funcionamiento de instituciones estatales.

El auge del ciberespacio, la aparición de herramientas que afectan el comercio marítimo y otros aspectos del mundo globalizado han sido analizados y explicados por varios autores; por ejemplo, Nieva Machín y Manuel Gazapo (2016) exponen que las amenazas del ciberespacio son el resultado del avance tecnológico y de la inminente necesidad que tienen las personas por utilizar internet en su vida diaria y en otros aspectos como el desarrollo de las economías y sociedades, pero, cuando esta tecnología es utilizada para intervenir bases de datos, sistemas y softwares de seguridad es posible afectar a través de la intrusión de redes que funcionan con la tecnología de la *big data* la actividad económica marítima del mundo y, por ende, de Colombia.

Esta problemática no es ajena al escenario colombiano, por eso, Catalina Grimalt y Bernat Baró (2021), muestran la manera como la ciberdelincuencia se posiciona en el contexto nacional por medio de la interceptación de los sistemas de seguridad de la actividad portuaria y marítima, razón por la que se han creado estrategias para hacer frente a flagelos como el narcotráfico, la migración ilegal, el hurto, entre otros delitos relacionados con archivos maliciosos para acceder a sistemas y datos importantes, la interferencia en los sistemas de identificación de los barcos, del seguimiento de las cargas a través de GPS y el impedimento para visualizar las cartas electrónicas (Grimalt y Baró, 2021).

El contexto actual de la problemática de las amenazas provenientes del ciber espacio en el comercio marítimo y la justificación que demuestra la necesidad de estudiar el problema es explicada por la Armada Nacional en el Plan Estratégico Naval (2015), documento en donde la Institución expone que las amenazas cibernéticas a la seguridad de la actividad marítima crecen constantemente, por eso se hace necesaria la búsqueda de modelos con los que desde su misión esperan intervenir el ciberespacio para neutralizar los ataques informáticos, defender los intereses marítimos y fluviales de Colombia haciendo uso del desarrollo del poder militar y naval que es representado por la Armada Nacional.

En tal sentido, al identificar las amenazas que puedan afectar el comercio marítimo de un país, se estipula como pregunta de investigación: ¿Cuál debe ser el modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para la contención de amenazas provenientes del ciberespacio?, mediante un análisis documental y fuentes de información que conlleven a identificar modelos que permitan contrarrestar dichas amenazas.

Por consiguiente, como tesis central se establece un modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para la contención de amenazas provenientes del ciberespacio, permitiendo desde el poder militar y naval que representa la Armada Nacional, intervenir todas las estrategias que afecten esta actividad económica marítima y los intereses de la Nación.

Finalmente, la metodología implementada en el desarrollo de la investigación es enfoque cualitativo con una orientación interpretativa, razón por la que se recolecta información que posteriormente se clasifica a través del método de la triangulación hermenéutica para luego, analizar los datos recolectados con el fin de dar respuesta al interrogante formulado como pregunta de investigación (Hernández Sampieri, Fernández Collado, y Baptista Lucio, 2014).

Metodología

El objetivo general de la investigación fue proponer un modelo conceptual de ciberseguridad para el comercio marítimo en Colombia. Para su desarrollo se establecieron tres objetivos específicos que se desarrollaron en tres fases respectivamente. La primera consistió en caracterizar las amenazas cibernéticas que afectan la seguridad de la información del comercio marítimo colombiano por medio de la revisión documental de fuentes primarias y secundarias tanto en primera y segunda fase que incluyen informes, artículos, trabajos de investigación y normatividad vigente, las cuales serán revisadas y analizadas por medio del método de triangulación hermenéutica, con el propósito de identificar dichas amenazas, caracterizarlas, puntualizar sobre cada una de ellas y establecer sus principales características.

Asimismo, la aplicación de entrevistas como instrumento de investigación al personal relacionado con la actividad en el mar, teniendo en cuenta variables como: Ciberseguridad en el comercio marítimo, comercio marítimo y amenazas del ciberespacio al comercio marítimo, arrojando como resultado una matriz de caracterización de amenazas cibernéticas y las necesidades de ciberseguridad para el comercio marítimo colombiano.

Posteriormente, continua la segunda fase que permite definir un modelo conceptual de ciberseguridad para contención de amenazas provenientes del ciberespacio en el comercio marítimo de Colombia, el cual se logra por medio de la recolección de información en motores de búsqueda, repositorios, portales web, entre otras herramientas; utilizando variables para su búsqueda como la ciberdelincuencia en el comercio marítimo, tipos de ciberataques y modelos de ciberseguridad en el comercio marítimo. La documentación consultada, permitirá establecer los criterios de selección del modelo, es decir, definir qué características debe tener el modelo teniendo en cuenta las necesidades identificadas en el objetivo anterior, de igual manera, identificar los

modelos de ciberseguridad implementados en el mundo para la contención de amenazas provenientes del ciberespacio, ponderar los modelos identificados para de esta manera definir cuál es el modelo más aplicable, o cual es la propuesta de modelo adaptado a la necesidad.

Es importante mencionar que en esta fase también se lleva a cabo el proceso de análisis documental para estudiar las normas NIST y así reconocer los puntos aplicables a la situación del comercio marítimo colombiano en materia de amenazas cibernéticas, de esta forma se crea un listado de acciones que pudieran aplicarse en la construcción de un modelo enfocado en el caso colombiano y mediante una estructura gráfica permita explicar y comprender el modelo a profundidad.

Por último, en la tercera fase se verifica el modelo conceptual para el comercio marítimo en Colombia a través de la validación con dos o tres expertos, siendo necesario definir la metodología empleada para dicha validación, así como el perfil del experto con conocimiento ya sea sobre seguridad cibernética o temas relacionados con el comercio marítimo entre otros, y como se llevara a cabo el análisis de los resultados obtenidos, la cual podría ser mediante la elaboración de una matriz DOFA en donde se determinen las debilidades, oportunidades, fortalezas y amenazas o dar como resultado los aspectos positivos y negativos del modelo propuesto.

Las Amenazas del ciberespacio que afectan la seguridad del comercio marítimo en Colombia

La Teoría del ciberespacio aplicada a la ciberseguridad del comercio marítimo

Estudiar la seguridad ante amenazas provenientes del ciberespacio requiere de una perspectiva teórica que pueda explicar el fenómeno a estudiar, en este caso, la teoría sobre el ciberespacio propuesta por James Adams (2001), la cual es aplicable al tema de estudio teniendo

en cuenta que el autor afirma que “el ciberespacio se ha convertido en un nuevo campo de batalla internacional”, lo que se explica desde la perspectiva de la seguridad del comercio marítimo ante amenazas del ciberespacio como el establecimiento de un nuevo entorno de enfrentamiento en el que las armas y otros escenarios de confrontación pasan a un segundo plano para concentrarse en la evolución de la delincuencia que ahora se establece en un ambiente diferente en donde la confrontación no se da por medio de la guerra física o armamentista sino por medio del poder enmarcado en el manejo de la información y datos críticos.

Antecedentes de la Ciberseguridad y el comercio marítimo

En lo que respecta al comercio marítimo, el Capitán de Navío (RA) Héctor Mauricio Rodríguez (2016) publica los hallazgos de una investigación sobre la importancia del mar en el mundo contemporáneo y por ende, en el desarrollo del comercio marítimo de los Estados, también, relaciona el uso del océano con la necesidad de fortalecer la seguridad de los mares a través de un concepto de seguridad integral marítima que se interpreta como “un elemento sustantivo, relevante y estratégico para el desarrollo sostenible de los espacios y territorio marítimo nacional.” (p.41).

Alrededor del tema de la ciberseguridad en el comercio marítimo existen diferentes investigaciones que establecen las bases para otros estudios relacionados, por ejemplo, el texto “La estrategia de Seguridad Nacional. Ciberdefensa y seguridades marítimas energética.” (Moreno, 2015), explica la necesidad de manejar un nivel adecuado de ciberseguridad y resiliencia para superar las crisis que se dan a través de las TIC y otras herramientas con las que se consigue “potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación” de estos fenómenos que generan inseguridad para la población.

Otra investigación que proporciona datos necesarios para dar respuesta al interrogante de investigación es el de la Compañía Marsh McLennan (2014), en el que se contextualiza al lector acerca de los ataques cibernéticos a las organizaciones y las amenazas continuas que se presentan en un entorno en el que las organizaciones necesitan obtener información para conseguir datos que les permitan prevenir cualquier tipo de irrupción, lo anterior como consecuencia de un diagnóstico en el que se identifican estructuras preparadas para adaptarse a un espacio cibernético variable y continuo pero no están listas para enfrentar los ataques y amenazas que se desarrollan con la evolución de las tecnologías y su uso para fines no deseados.

Caracterización de las amenazas provenientes del ciberespacio que afectan la seguridad del comercio marítimo colombiano

Los ataques cibernéticos se pueden presentar por diferentes tipos o técnicas, por ejemplo, pueden ser ataques a contraseñas, ataques por spam, correo, phishing y ataques por malwares, este último el más común cuando se trata de redes que pertenecen a organizaciones, entidades y demás actores involucrados en la actividad comercial marítima y el que lleva al análisis de riesgos, el cual, está basado en la identificación de amenazas, vulnerabilidades y los riesgos mismos (Valbuena, 2022).

Así mismo, la revisión documental contribuye con la identificación de características relacionadas con las amenazas que, desde el punto de vista de autores como Mednikarov, Tsonev y Lázarov (2020), surgen en los procesos de intercambio de información y en la relación interconectada existentes entre los recursos y sistemas operativos integrados con las plataformas

de TI[3]. Para estos autores, las amenazas cibernéticas pueden ser dirigidas y no dirigidas[4], también, se desarrollan en cuatro etapas:

Figura 1. Etapas del ciberataque en la industria marítima

Nota. Estas etapas son aplicables a los buques utilizados para el transporte de mercancías

Por otro lado, de la Peña (2021), citando a Dingeldey (2017), muestra que los puertos son más vulnerables ante este tipo de ataque cibernéticos, lo anterior como resultado de la facilidad para ejecutar este tipo de acciones en contra de los sistemas de las navieras a través de Wi-Fi y otras redes, por lo tanto, este estudio se enfoca en las amenazas que se materializan a través de los hechos que afectan a los puertos.

Las amenazas a la seguridad y por lo tanto, aplicables en este estudio, se clasifican en humanas y lógicas, las primeras hacen referencia a los tipos de ataques provenientes de personas

[3] Tecnología de la información

[4] Los ataques dirigidos son "ataques cibernéticos en redes de Internet corporativas específicas y componentes de red con un propósito específico de penetración: acceso a información confidencial, obstrucción del funcionamiento normal de los sistemas del barco", mientras que los ataques no dirigidos son aquellos que se realizan por medio de "el entorno de Internet y herramientas de software para detectar componentes de comunicación desprotegidos" (Mednikarov, Tsonev, y Lázarov, 2020).

que aprovechan las vulnerabilidades detectadas en los sistemas para obtener información de su interés y beneficiarse de estos datos, es así como surge la figura del *Hacker* quien se enfoca en aprender por eso ingresa al sistema solo para satisfacer su curiosidad pero no para borrar alguna información o hurtarla y luego venderla (UNAM, 2009). Los *cracker* son otro tipo de personas que representan una amenaza para la seguridad cibernética y son quienes acceden a los sistemas para causar algún tipo de daño sin un fin determinado, finalmente están los *Phreakers* que aprovechan la vulnerabilidad de las compañías telefónicas en su beneficio (UNAM, 2009).

Las amenazas lógicas, las cuales están representadas técnicas; es decir, programas como malwares, Bugs, o agujeros que son creados con la intención de dañar los sistemas; algunos ejemplos son los *adware* o publicidad en ventanas emergentes, los *Backdoors* o puertas traseras que se muestran como atajos para ingresar a los sistemas operativos, también están las *bombas lógicas* que son códigos de los programas que al ser activados producen daños en ellos, continúan con los caballos de troya que hace referencia a programas que se hacen pasar por uno y en realidad es otro y con fines maliciosos, también es conocido como troyano (p.53).

Otros tipos de amenazas lógicas son los *exploits* que aprovechan las vulnerabilidades de los sistemas, los gusanos que se propagan por las redes para aprovechar las vulnerabilidades y crear acciones maliciosas, también están otros ya conocidos como el *malware*¸ el *phishing*, los *spam*, los programas espía y los virus (pp.53-54).

Ahora bien, el reconocimiento de las amenazas se realiza teniendo en cuenta los aportes de Rodríguez (2016), quien determina que existen amenazas materializadas en riesgos emergentes que siguen tendencias convertidas en retos enmarcados en fenómenos como el terrorismo que se evidencia en los ataques a buques en alta mar, que se suman a la piratería y otras actividades que hacen parte de la globalización y del incremento de la tecnología (pp.11,13), de la misma forma,

la clasificación va de acuerdo con su naturaleza, objetivo y recursos, por lo tanto, estas se registran como ciber espionaje, amenazas hibridas, cibercrimen y hacktivismo; de las cuales son aplicables en el comercio marítimo el ciber espionaje, el cibercrimen, el hacktivismo y las amenazas híbridas que buscan la manipulación de la información (pp.11,13).

A través del análisis documental se identifican amenazas como la extorsión, la piratería digital, el espionaje, la subversión y el terrorismo (Androjna, Brcko, y Greidanus, 2020), cada una de ellas presentes en diferentes situaciones que afectan en su mayoría a las navieras y por supuesto, a los puertos donde estas operan y en donde son manejados los sistemas que tecnifican los procesos de la actividad marítima. A estas se suman el manejo de información falsa, el narcotráfico y otros delitos trasnacionales (University of Miami, 2017).

Entre tanto, la información obtenida por medio de las entrevistas hechas a personal que labora en el Comando Conjunto Cibernético de las Fuerzas Militares y en el Comando Cibernético Naval, permite identificar otras amenazas y vectores de ataque, en primer lugar, las amenazas que a través de los tipos de ataques afectan a las plataformas tecnológicas de operación (TO), caracterizadas por ser más difíciles de proteger al tener menos protocolos comerciales y con menos estándares de ciberseguridad, lo que empeora con el uso de “cajas negras con mucha información para los operadores” y además, son utilizadas por organizaciones de alto nivel (Aponte, 2022). También están las plataformas de información (TI), que por medio de diferentes técnicas que afectan a los sistemas “soportan las operaciones de los puertos y el comercio marítimo para dar cumplimiento su naturaleza comercial” (Correa, 2022), de la misma forma, de acuerdo con otros entrevistados, es posible encontrar como amenazas comunes al narcotráfico, la ciberdelincuencia y la piratería como las principales amenazas que afectan al comercio y otras actividades marítimas que están relacionadas con las funciones de la DIMAR y del Ministerio de transporte, las cuales

son ejecutadas por medio de lo que los entrevistados llaman “Vectores de ataque” y que incluyen: códigos dañinos, intrusiones, compromiso de la información, contenido abusivo y obtención de información.

Así las cosas, es posible identificar casos relacionados con algunas de las principales ciberamenazas que afectan al comercio marítimo:

Tabla 1. Amenazas al comercio marítimo en el mundo y posibles casos

Amenaza	Tipo	Casos
Hacktivismo	Humana	2013: el White Rose of Drax recibe señales falsas al GPS para desviar su rumbo, pero esto no fue percibido en el radar (Crawford Crawford, 2019).
Narcotráfico	Humana - lógica	2011: En el puerto de Amberes (Bélgica) hackean los sistemas y ocultan droga en los contenedores que estaban registrados como carga legitima (Boyes, 2015).
Piratería digital (amenazas hibridas y terrorismo)	Humana – lógica	2022: Ataque a los sistemas del INVIMA para evitar el funcionamiento y las capacidades de almacenamiento del puerto (Portafolio.com, 2022)

Lo anterior aplicado a la seguridad de la información, lleva a realizar la caracterización de las amenazas tomando como punto de partida el nivel de importancia que cada de las amenazas tiene en las entidades y el proceso que debe llevar a cabo el sistema afectado en cada organización que se dedica al comercio marítimo en el país, es así como se caracterizan en un nivel inferior, bajo, medio, alto y superior, teniendo en cuenta el nivel de criticidad y de importancia para la gestión del comercio marítimo (Ver tabla 2).

Tabla 2. Caracterización de las amenazas teniendo en cuenta el nivel de criticidad del sistema afectado

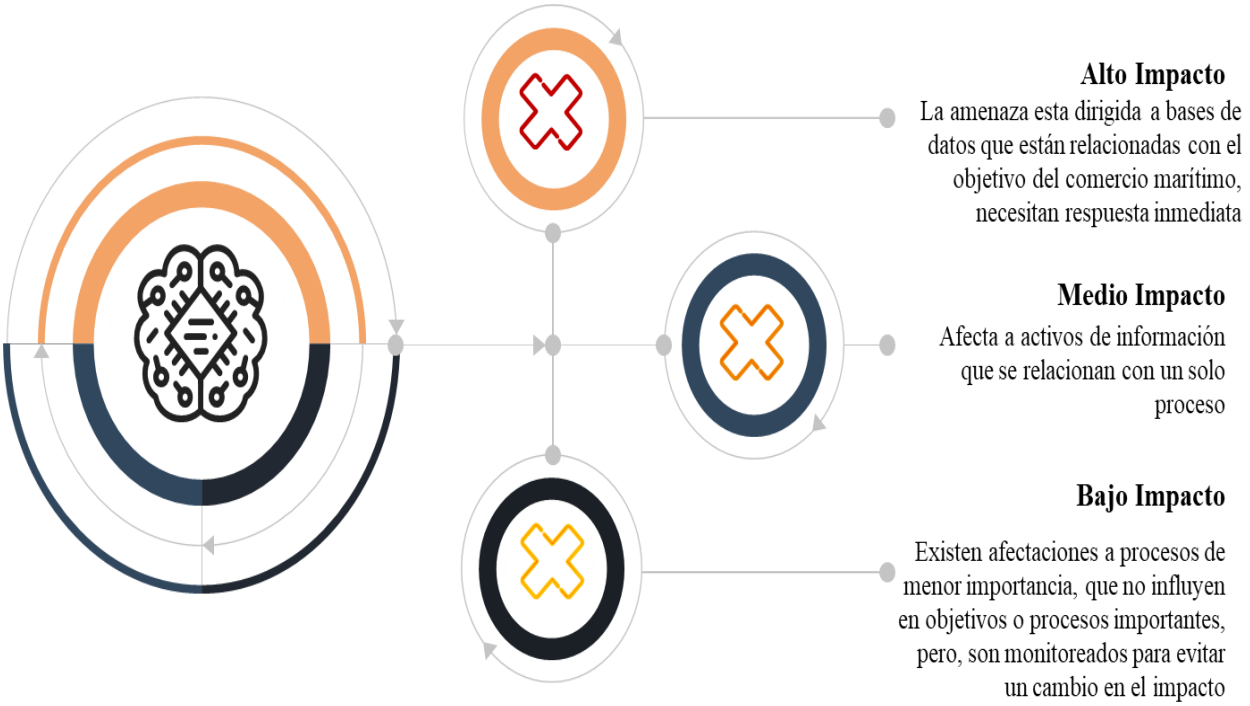
Nivel de Criticidad	Valor	Descripción
Inferior	0,10	Sistemas con funciones sustituibles o no críticas
Bajo	0,25	Sistemas que hacen referencia a un solo proceso

Medio	0,50	Hace referencia a los sistemas que apoyan a varios de los procesos del comercio marítimo
Alto	0,75	Sistemas que hacen parte del área de tecnología y estaciones con funciones importantes
Superior	1,00	Sistemas en estado crítico y con funciones importantes sino fundamentales para el comercio marítimo

Nota. Tabla elaborada con base en la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (s.f.)

De la misma forma, existen otros parámetros para caracterizar las amenazas, estos establecen el nivel de impacto que estas pueden tener en la gestión del comercio marítimo y en los procesos que se relacionan con este (transporte, logística, etc.), estos son: de Alto Impacto, de Medio Impacto y de Bajo Impacto, los cuales se describen de la siguiente manera:

Figura 2. Caracterización de amenazas según el impacto causado en los sistemas



Nota. Esquema elaborado con información obtenida de la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (s.f.)

A partir de la descripción hecha sobre las formas de caracterización, se establece que en esta investigación se realiza un proceso en el que se combina la caracterización; es decir,

inicialmente se identifica el nivel de criticidad y de importancia para la gestión del comercio marítimo y posteriormente, con base en los resultados obtenidos de este proceso, se determina el nivel de impacto que puede tener.

Matriz de Caracterización de Amenazas Cibernéticas

La investigación acerca de amenazas provenientes del ciberespacio es un campo de interés para muchos estudiosos como el Capitán de Navío (RA) Héctor Mauricio Rodríguez (2016), quien se ocupa de analizar la situación de la seguridad cibernética en el país y las amenazas que hacen parte del contexto de la ciberseguridad en las actividades marítimas en Colombia, no obstante y como lo menciona James Crawford Crawford (2019), la evidencia de publicaciones que hablen de las amenazas marítimas es escaso, por lo tanto, identificar las amenazas que afectan a este sector de la economía colombiana se torna en una labor difícil, no obstante, con datos obtenidos a través de la revisión documental es posible reconocer las más sobresalientes.

A continuación, se presenta la matriz de caracterización de las amenazas cibernéticas que afectan al comercio marítimo en el país, las cuales, son clasificadas teniendo en cuenta el nivel de criticidad y nivel del impacto que causan en esta actividad económica.

Tabla 3. Matriz de Caracterización de amenazas cibernéticas

Amenaza/Incidente	Tipo de Amenaza	Agente de la Amenaza	Método	Nivel de Criticidad	Impacto
Ciber espionaje (Acceso no autorizado para ver información de interés del adversario)	Humana	Phreaks, Hacker,	Troyano, Malware, programas espía, virus, adware	Superior	Alto
Amenazas Hibridas (Ciberterrorismo, interrupciones de actividades económicas, interrupción de procesos, virus, narcotráfico)	Lógica	Cracker	Exploits, Malware, adware	Superior	Alto

Cibercrimen (Daño a sistemas, robo de información)	Humana	Cracker, Phreakers	Bombas lógicas, Backdoors, Phishing, spam, bugs, adware	Superior	Alto
Hacktivismo (Buscan generar presión a través del bloqueo de sistemas, virus, robo de cuentas, etc.)	Humana	Hacker, Cracker, Phreakers	Malware, phishing, virus, adware	Alto	Alto

Nota. Matriz realizada con información obtenida de la revisión y análisis documental y a partir de la elaboración propia.

De acuerdo con la tabla 3, es evidente que cada una de estas amenazas afectan a este sector porque la mayoría de ellas impiden su correcto funcionamiento, perjudicando indirectamente la economía, desarrollo social y la seguridad del país, de los puertos y de los pueblos costeros que dependen del comercio marítimo, también, son un medio a través del que organizaciones criminales extienden su accionar y fortalecen indirectamente los crímenes trasnacionales, exponiendo vulnerabilidades y nuevas formas de delinquir que esta vez interfieren en la cuarta industria o en la tecnología.

Necesidades de ciberseguridad para el comercio marítimo colombiano

La revisión documental permite encontrar en países como España puntos de referencia que ayudan a entender aspectos de la ciberseguridad de buques y puertos, los cuales, están enfocados en sistemas de comunicación, administración y control que hacen parte de las Tecnologías de la Información, por lo tanto, muestran diferentes niveles de vulnerabilidad ante ataques cibernéticos que son explicados desde una óptica diferente para detectar cuáles son los puntos más vulnerables dentro del desarrollo de la actividad comercial marítima, los cuales, por lo general se concentran en los siguientes elementos: “información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos” (Grupo de Seguridad Marítima, 2020).

De la misma forma, teniendo en cuenta los aportes hechos por el Grupo de Seguridad Marítima de España (2020), se determina que las dimensiones de la seguridad que resultan afectadas a través de los ataques cibernéticos hechos a las actividades del comercio marítimo son:

- La confidencialidad: Indica que la información debe estar disponible solo para quien este autorizado,
- La integridad: Evita que los datos sean modificados,
- La disponibilidad: Permite el acceso a las bases de datos en el momento en el que es necesario,
- La autenticidad: Legitima la veracidad de cada una de las cifras e información que se encuentra en estas bases de datos,
- La responsabilidad de quien manipula estos datos,
- El no repudio: Previene la negación de la autoría de los datos y la fiabilidad que conlleva a evitar resultados poco confiables (p.6).

En Colombia, el interés por conocer, identificar y estudiar las amenazas que impactan la Seguridad Integral Marítima y Fluvial se evidencia en la Estrategia de Seguridad Nacional Marítima y Fluvial 2020-2030 creada por el Curso de Altos Estudios Militares (CAEM) No.61 (Curso de Altos Estudios Militares No.61, 2020), investigación que cuenta dentro de sus hallazgos, amenazas a la seguridad marítima y fluvial relacionadas con el Crimen Trasnacional Organizado y dentro de las que se encuentran algunas relacionadas con las amenazas que afectan la ciber seguridad (p.58).

La amenazas que son incluidas en este estudio del CAEM son, en primer lugar, los Grupos Armados Organizados que, si bien es cierto, basan su accionar en la violencia, en los últimos años han sido capaces de desarrollar estrategias para practicar el terrorismo por otros medios,

incluyendo los cibernéticos, lo que lleva a encontrar en el terrorismo otra de las amenazas que paulatinamente se materializa a través de otros delitos de naturaleza virtual (p.55). También existen otras amenazas como la vulnerabilidad de las infraestructuras críticas (security), el hurto en el mar y los ataques a la seguridad cibernética (p.55-58).

Por otro lado, las respuestas recibidas en medio del desarrollo de las entrevistas aplicadas a personas que tienen experiencia en ese medio, evidencian que los avances de las políticas públicas en materia de ciberseguridad en las actividades comerciales marítimas se encuentra en un proceso lento y que exterioriza varias necesidades; por ejemplo, la implementación de planes con los que sea posible, desde la labor de la Armada Nacional, llevar una estadística como parte de un sistema de alarmas y establecer cuál de las amenazas que pudieran estas afectado a los buques y demás embarcaciones, de esta forma es posible crear una base de datos que sea de conocimiento de las autoridades portuarias y marítimas y con la que es posible confirmar cuales son las actividades delictivas más recurrentes en los puertos y mares de Colombia.

También, expresan la necesidad de fortalecer el Comando Cibernético Naval en capacidades de ciberseguridad de unidades marítimas, de esta forma generan estrategias que indirectamente pueden ser útiles en la protección de los buques que transportan mercancía, además, es necesario el fortalecimiento de las capacidades de seguridad cibernética de la Dirección de Tecnologías de la Información que gestiona la Armada Nacional para operaciones navales orientadas al libre desarrollo del comercio marítimo, lo anterior teniendo en cuenta que el Comando cibernético Naval enfoca sus esfuerzos en la protección de la plataforma institucional (Jefatura de Planeación Naval y Dirección de Planeación Estratégica, 2021), pero no tiene programas para el apoyo de la ciberseguridad del comercio marítimo.

De la misma forma, es importante establecer medidas con las que se pueda proteger las bases de datos de las empresas que pueden parecer vulnerables ante ciberdelitos como el control y el monitoreo de cargas; también es necesario el fortalecimiento y consolidación del principio de corresponsabilidad que atañe a todas las autoridades responsables de la seguridad portuaria y marítima de este tipo de empresas que se encargan del transporte de mercancías por el mar.

Lo anterior es apoyado por el Capitán de Navío (RA) Samuel Rivera-Páez y por Juan Sebastián Pérez Morales (2012) , quienes afirman que existen necesidades que son notables, por ejemplo:

> el continuo intercambio de información entre las instituciones del Estado y sus pares en los estados que son socios comerciales marítimos. La adecuada integración entre las instituciones parte permitirá un intercambio fluido de información que contribuya a mejorar los controles y, por tanto, la seguridad de las actividades marítimas en Colombia. (p.161)

De la misma forma, se establece que en materia de ciberseguridad ante las amenazas que pueden afectar el comercio marítimo en el país, es necesario que en el país acelere la transformación tecnológica en el sector marítimo, lo que quiere decir que la necesidad de reforzar las medidas de seguridad implementadas por las autoridades competentes, incluyendo la Armada Nacional, las cuales son las responsables de prevenir cualquier tipo de ataque tecnológico que pudieran sufrir estas embarcaciones dentro de sus sistemas, o los puertos en materia de GPS.

Modelo conceptual de ciberseguridad para contención de amenazas provenientes del ciberespacio en el comercio marítimo de Colombia

Criterios de selección del modelo aplicable al comercio marítimo

Los elementos a tener en cuenta dentro del estudio para determinar cuál de los modelos aplicables al caso colombiano es el más apropiado, se tienen en cuenta los siguientes aspectos: Tiempo de implementación, resultados parciales o totales, recursos necesarios para su

implementación, contexto en donde es aplicado y proceso de implementación, los cuales se describen de la siguiente manera:

- Tiempo de implementación del modelo: Es cierto que un buen trabajo requiere de tiempo, también, de un proceso de pruebas y evaluaciones que permiten perfeccionarlo y adaptarlo a las necesidades de la problemática, que en este caso hace referencia a las amenazas cibernéticas que el comercio marítimo enfrenta en el país. El tiempo de implementación hace referencia al tiempo que tardó este modelo en ser implementado y perfeccionado ya que es innegable que a mayor tiempo mayores van a ser los costes de este.

- Resultados parciales o totales: Los resultados son uno de los criterios con mayor importancia dentro del análisis por cuanto a través de ellos es posible verificar la eficacia del modelo y de cada una de las acciones que hacen parte de él, el modelo que presente los mejores resultados a un menor costo puede ser el más conveniente para afrontar la problemática en Colombia.

- Recursos necesarios: Dentro de los dos criterios anteriores los costes han sido un factor importante a tener en cuenta en el momento de analizarlo, por eso, se establece este aspecto como parte del análisis del modelo ya que solo así se puede verificar si los recursos con los que cuenta la Armada Nacional y el país son suficientes, en otras palabras, de esta manera se confirma si este es un modelo económicamente viable para el país.

- Contexto en el que se aplica: Colombia es un país caracterizado por un conflicto armado constante, por lo tanto, cuenta con características y necesidades especiales que no están presentes en todas las Naciones y contextos, por lo tanto, es importante elegir o tener en cuenta un modelo que pueda ser adaptado al entorno colombiano y a las particularidades que genera el conflicto armado, la transición de gobierno y la situación de orden público en el país.

- Proceso de implementación: Este punto se refiere a las fases que deben ser puestas en marcha para aplicar el modelo en su totalidad, en este caso, aquel modelo que muestre un proceso más largo puede ser sinónimo de desventaja para Colombia ya que puede incurrir en mayores costos económicos y humanos.

La evaluación de cada uno de los modelos se realiza por medio de una ponderación, la cual, se presenta a través de una matriz (Ver tabla 4) que se explica de la siguiente manera: El peso de cada uno de los criterios se mide entre 1-10, donde los números del 1-3 representan que no tienen mayor importancia, los números del 4-7 que tienen una importancia media y del 8- 10 una importancia alta, así mismo, la puntuación dada a cada uno de los criterios evaluados dentro de cada modelo se basa en la similitud que el contexto tiene con el contexto colombiano, mayor o menor tiempo de aplicación, los costes y necesidades resueltas, por eso, la ponderación tiene una variación entre 1 y 10 donde los números del 1-3 representan una pertinencia poco favorable, los números del 4-7 que medianamente podría satisfacer las necesidades en la ciber seguridad del comercio marítimo en Colombia y del 8- 10 un nivel de pertinencia alto en cada uno de los aspectos analizados.

Modelos de Ciberseguridad aplicables en el comercio marítimo en Colombia

Los modelos de ciberseguridad son el resultado de las necesidades que se generan con la llegada de la pandemia, cuando el mundo para pero los ciberataques incrementan haciendo evidentes las vulnerabilidades de los sistemas (Banco Interamericano de Desarrollo - BID & Organización de Estados Americanos -OEA, 2020), es por esta razón que diferentes gobiernos y organizaciones los crean para hacer frente a las amenazas que provienen del ciberespacio y que se encuentran latentes en un mundo cada vez más tecnificado.

Los escenarios planteados en cada uno de los modelos a analizar guardan cierta similitud con la situación Colombiana, además, cumplen en su mayoría con los criterios de selección establecidos para determinar su pertinencia o la utilidad de sus acciones en el caso colombiano. Es a partir de la verificación de estos puntos que se considera pertinente tener en cuenta los siguientes modelos:

- Modelo de Cooperación en Ciberseguridad
- Modelo de Defensa en Capas
- Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)

En primer lugar, el Modelo de Cooperación en Ciberseguridad es creado para minimizar los efectos de los ciberataques a través de la implementación de mecanismos que ayuden a prevenir o minimizar el daño que trae consigo una amenaza de ciberataque, eliminando las posibilidades de convertirlas en un riesgo o un ataque real (Guiora, 2018, p.01).

Ante este modelo, Amos Guiora (2018) afirma que su propósito es:

> reducir los costes, tanto directos como indirectos, de las acciones en el ciberespacio. El modelo se fundamenta en una premisa: prevenir un ataque o, en el peor de los casos, llevar a cabo un esfuerzo concertado y decidido es preferible a asumir los costes de un ataque exitoso. (p.03)

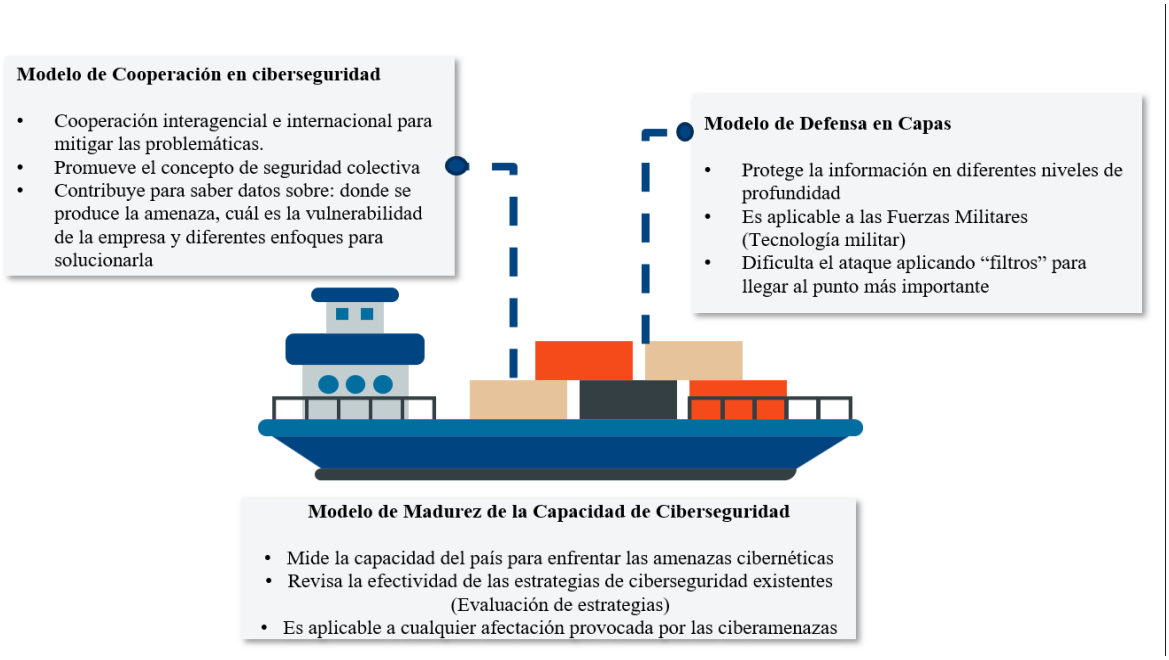
Existe otro modelo conocido como el “Modelo de Defensa en Capas” con el cual se pretende evitar que los ataques provocados en la red puedan expandirse para causar un daño de mayor impacto y además critico dentro de los procesos productivos (CEPAL, 2020) o, visto desde el caso del comercio marítimo, en los procesos de transporte y distribución de los productos hacía los diferentes puertos del mundo.

Un tercer modelo es el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), con el cual se espera medir las capacidades de los Estados miembro de la OEA

para enfrentar las amenazas provenientes del ciberespacio; este modelo se concentra en cinco dimensiones: "(i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías" (Banco Interamericano de Desarrollo - BID y Organización de Estados Americanos -OEA, 2020).

Por último, la elección de estos modelos depende, además de la revisión de los criterios de selección de características que aplican al estudio y al contexto colombiano, los cuales se explican de la siguiente manera:

Figura 3. Razones para la elección de los modelos



Ponderación de los modelos

Tomando como referencia los criterios de evaluación planteados de acuerdo con las necesidades de la ciber seguridad del comercio marítimo en los puertos de Colombia, la ponderación de cada uno de los modelos es el siguiente:

Tabla 4. Ponderación de los modelos de ciberseguridad analizados

Factores		**Opción**					
Criterio	**Peso**	**Modelo de Cooperación en Ciberseguridad**		**Modelo de Defensa en Capas**		**Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)**	
			Total		**Total**		**Total**
Tiempo de implementación	7	8	56	8	56	8	56
Resultados	8	8	64	7	56	9	72
Recursos necesarios	8	8	64	7	56	7	56
Contexto en el que se aplica	8	7	56	6	48	8	64
Proceso de implementación	7	7	49	6	42	7	49
Total			289		258		297
Promedio			57,8		51,6		59,4

Nota. *El peso de cada uno de los criterios se mide entre 1-10, donde los números del 1-3 representan que no tienen mayor importancia, los números del 4-7 que tienen una importancia media y del 8- 10 una importancia alta.
** La puntuación dada a cada uno de los criterios evaluados dentro de cada modelo tiene una variación entre 1 y 10 donde los números del 1-3 representan que no tiene similitud, los números del 4-7 que tienen una similitud media y del 8- 10 una similitud alta.
***La calificación dada a cada modelo varía entre 1-10, donde los números del 1-3 representan la peor calificación, los números del 4-7 una calificación media y del 8- 10 un calificación importancia alta.

De acuerdo con los resultados obtenidos en esta matriz, es posible afirmar que el modelo que cuenta con un mayor número de características que pudieran ser aplicables para la ciber seguridad en el comercio marítimo de Colombia es el de la Madurez de la Capacidad de Ciberseguridad para las Naciones, esto se debe a que analiza cinco dimensiones con las que es posible identificar las debilidades del Estado Colombiano para enfrentar este tipo de amenazas y con base en esta información, crear estrategias a través de las que se consiga prevenir cualquier tipo de ataque y en casos extremos, evitar que estas amenazas se transformen en riesgos.

Modelo aplicable: Modelo de ciberseguridad para el comercio marítimo en los puertos de Colombia

Aspectos Generales

La misión de la Armada Nacional determina que esta institución debe "Desarrollar operaciones navales para la defensa y seguridad nacional, y la protección de los intereses marítimos y fluviales, contribuyendo al desarrollo sostenible del Estado" (Armada Nacional, 2022), por lo tanto, hace parte de las funciones de esta institución el desarrollo de estrategias que coadyuven con la protección de los intereses nacionales, los cuales, están dirigidos a la promoción de la cultura marítima colombiana y de su apropiación para crear oportunidades de crecimiento económico sostenible e inclusivo que contribuyan con el desarrollo del país (Ramírez, Pedroza, y Forero, 2021).

El Comercio Marítimo y los Intereses Marítimos en Colombia

El transporte marítimo es una de las actividades que hacen parte de las principales tendencias en la actualidad, su nivel de importancia llega a un punto en el que el 98% del comercio internacional circula por vías marítimas y fluviales del país (Nyman, 2019). Aunque en el año 2018 el comercio marítimo se dio a la baja, de acuerdo con la United Nations Conference on Trade and Development (UNCTAD) cree en la posibilidad de una proyección orientada a un crecimiento del 3,5% entre 2019 y 2024 (United Nations Conference on Trade and Development (UNCTAD), 2019).

Respecto a Colombia, es posible afirmar que

> por sus características geográficas y posición estratégica, se convierte en un país marítimo; en el mar Caribe tiene 658 000 km2 y 330 000 km2 en el Pacífico, lo que representa el 44,8% de la extensión total del territorio, y le da una proyección

> internacional importante, si se desarrollan las estrategias adecuadas. (Comisión Colombiana del Océano, 2014).

Hasta ahora ha sido posible explicar la importancia que el comercio marítimo tiene para el país desde el punto de vista económico, no obstante, su relevancia también es visible desde la perspectiva institucional, en la que se determina que como parte de la inteligencia naval, enmarcada en las acciones implementadas por la Jefatura de Inteligencia Naval, se buscan oportunidades que contribuyan con el desarrollo de factores relacionados con la defensa y seguridad de Colombia, por eso, dentro de sus objetivos se encuentra:

> el ingreso al sistema de puertos y la protección del comercio ante la intención de las organizaciones de delincuencia trasnacional de contaminar la carga lícita con estupefacientes. Ese es un fenómeno que de continuar podría tener repercusiones en el comercio exterior y la economía del país. (Jefatura de Planeación Naval y Dirección de Planeación Estratégica, 2021)

Así mismo, la Jefatura de Inteligencia Naval considera que:

> La defensa y seguridad tienen nuevos campos de guerra como el ciberespacio, en ese sentido la Armada Nacional, ha conseguido avances en materia de ciberseguridad, ciberdefensa y ciberinteligencia, que han ayudado al aumento en las capacidades de detección, gestión y análisis de eventos e incidentes cibernéticos en la red de datos de la Armada Nacional.(p.52)

Es evidente entonces que el interés de la Armada Nacional está orientado a la minimización de elementos que desde el ciberespacio afectan la defensa y seguridad de los mares y ríos, así mismo, han entrado en funcionamiento el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM), desde donde la evaluación y revisión de vulnerabilidades es posible, pero, es importante generar estrategias con las cuales, esa intención de detener la expansión de la criminalidad a través del espacio marítimo y cibernético se dirija al

comercio marítimo, unas de las actividades más importante para la economía colombiana y que pudiera resultar más afectado por estas actividades cibernéticas ilícitas.

Por otro lado, dentro del documento "Intereses Marítimos de Colombia", la Vicepresidencia de la República representada por la Comisión Colombiana del Océano se establece una lista de 18 intereses, de la misma forma que establecen una clasificación y ejes que se relacionan con estos intereses y, por ende, con la labor de la Armada Nacional (pp. 22-37).

Teniendo en cuenta lo anterior, este modelo se formula enfocándose en la contribución que la Armada Nacional da a la defensa y seguridad de los mares, haciendo énfasis en dos intereses específicos: La seguridad Integral Marítima y Fluvial (SIMF)[5] y el Transporte y comercio marítimo[6], los cuales, se complementan con los siguientes ejes y objetivos CONPES 3990[7] (Ramírez, Pedroza, y Forero, 2021, p.39):

- Ejes estratégicos Política Nacional del Océano y los Espacios Costeros: Integridad y Desarrollo del territorio marítimo y Desarrollo Económico.
- Ejes Estratégicos de la Comisión Colombiana del Océano: Desarrollo fluvial, Seguridad Marítima Integral y Abanderamiento de buques.

---

[5] Es incluida dentro de los intereses marítimos nacionales, este se define como: la gestión conjunta, coordinada e interinstitucional, con la participación de los usuarios, para articular esfuerzos y capacidades, con el propósito de prevenir, proteger y responder ante los riesgos, amenazas y delitos en el dominio marítimo y fluvial que afectan las condiciones de seguridad de las personas, los bienes, los activos y el medio ambiente. (Ramírez, Pedroza, y Forero, 2021, p. 31).

[6] El interés enfocado en el transporte y comercio marítimo es explicado como la "Utilización del mar para el transporte seguro de mercancías, sustancias y/o elementos a través de buques versátiles, infraestructura portuaria eficiente, localizada y segura." (p. 32).

[7] El Documento CONPES 3990 "Colombia Potencia Bioceánica Sostenible 2030" (2020), posiciona a los océanos dentro de la agenda pública nacional como factores que contribuyen con el desarrollo sostenible del país en los próximos 11 años, lo anterior basados en la siguiente consigna: los estados ejercen soberanía; aprovechan su posición geopolítica, sus ecosistemas marinos y su biodiversidad; hacen uso de los accesos a los océanos y las líneas marítimas; realizan actividades marítimas sostenibles y competitivas; generan capacidad naval, conocimiento y conciencia nacional oceánica; defienden los intereses marítimos nacionales, y gestionan interinstitucionalmente de los océanos (Mahan, 1980; Till, Seapower: A Guide for the Twenty-First Century, 2004). (Consejo Nacional de Política Económica y Social CONPES, 2020)

- Objetivos CONPES 3990: Incrementar la capacidad del Estado para velar por la soberanía, defensa, vigilancia, control, y seguridad integral marítima e Impulsar las actividades económicas marítimas en función del desarrollo sostenible local y nacional.

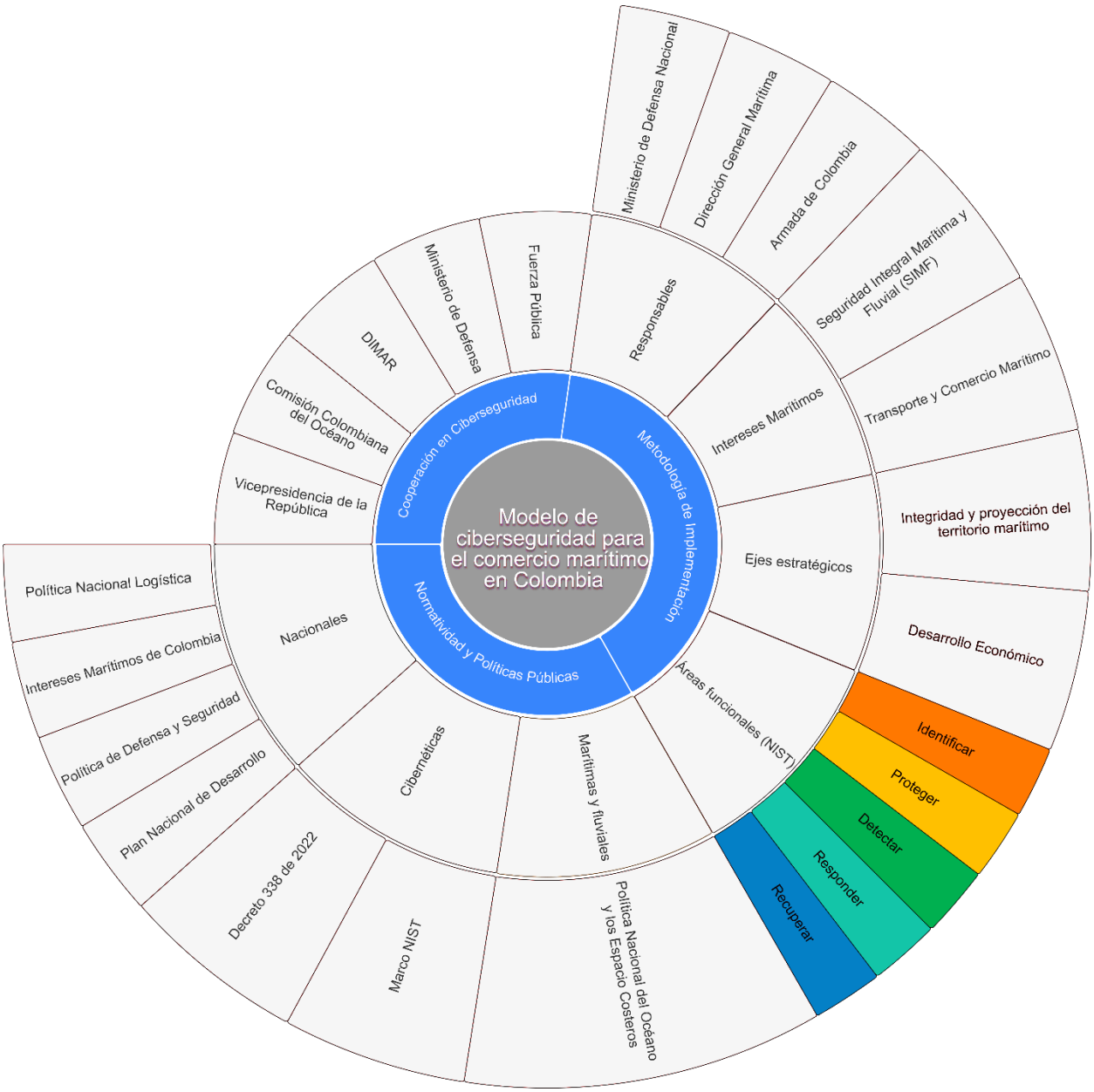
Sin embargo, ninguno de los intereses marítimos está relacionado con la seguridad cibernética, razón por la que esta información tuvo que ser adaptada a las necesidades cibernéticas del comercio marítimo colombiano.

Descripción del Modelo

En el siguiente gráfico se describen los elementos, políticas, entidades, estrategias y planes o campañas que se vinculan a este modelo que tiene como principal objetivo: Definir acciones para la disminución y prevención de amenazas cibernéticas que afecten la operación del comercio marítimo en Colombia.

El modelo está organizado en tres componentes: Metodología de implementación, la Cooperación en ciberseguridad y la Normatividad y Políticas públicas en las que se apoya el desarrollo de las acciones implementadas dentro de este. En primer lugar, la metodología de implementación busca relacionar la misión de la Armada Nacional con la ciberseguridad adaptada a los intereses marítimos de la Nación: Seguridad Integral Marítima y Fluvial (SIMF) y el Transporte y Comercio Marítimo, por lo tanto, los ejes estratégicos a los que se dirige el modelo son: Integridad y proyección del territorio marítimo y el desarrollo económico.

Figura 4. Esquema gráfico del Modelo de ciberseguridad para el comercio marítimo en los puertos de Colombia



Nota. Elaboración propia

Componente: Metodología de implementación

Dentro del componente de la metodología de implementación también se habla de los gerentes del modelo, en otras palabras, los responsables, quienes teniendo en cuenta lo establecido en el documento “Intereses Marítimos de Colombia” (2021) son: Ministerio de Defensa Nacional,

la Dirección General Marítima y la Armada de Colombia. El componente que habla de la implementación del modelo se basa en el Marco de Seguridad Cibernética de NIST[8] Cibersecurity Framework, razón por la que se desarrolla por medio de cinco áreas estratégicas, cada una de ellas con acciones específicas que se crean a partir de las necesidades en materia de ciberseguridad para el comercio marítimo en Colombia (Ver tabla 5).

Tabla 5. Áreas funcionales y acciones para implementar en el modelo

Función	Acción
Identificar	Identificación y clasificación de sistemas e información sensible de las navieras y puertos. Identificación de vulnerabilidades y amenazas en los sistemas de los puertos. Identificación de procesos, permisos de acceso y personas responsables a las bases de datos y sistemas de los puertos.
Proteger	Proteger el acceso a información sensible de navieras y puertos. Proteger Servicios operacionales importantes dentro de los procesos logísticos del comercio marítimo Proteger sistemas de información y operacionales relacionados con las plataformas operativas y de la información de los puertos. Proteger cuentas y bases de datos que pueden ser vulnerables
Detectar	Detectar los intentos de ataques cibernéticos llevados a cabo en los últimos seis meses a través de la conexión existente con el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM). Detectar los Ataques cibernéticos efectuados en el último semestre por medio del trabajo interagencial y la conexión con el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM). Detectar cuantas, y cuales amenazas emitidas son dirigidas a entidades estatales, empresas que trabajan en el puerto e incluso, a la Armada de Colombia a través de elementos relacionados con el comercio marítimo y que pudieron ser detectadas en el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM).

[8] El NIST es una "infraestructura de seguridad cibernética" que tiene como finalidad ayudar a las organizaciones a mejorar o implementar acciones para la ciberseguridad a través de la gestión de riesgos y la resistencia de sus sistemas (Amazon Web Services, Inc, 2019).

Responder	Elaborando informes y mostrando pruebas con las que se certifique la existencia de los incidentes de ciberseguridad detectados.
Recuperar	Recuperar cuentas y acceso a sistemas bloqueados en el menor tiempo posible y generando un bloqueo para que solo puedan acceder con un código especifico. Recuperar el acceso a las bases de datos que han sido irrumpidas en el menor tiempo posible, evitando que los datos puedan ser vistos o extraídos por algún método. Recuperar el control para garantizar la continuidad de los procesos del comercio marítimo.

Nota. Elaboración propia

Componente: Cooperación en ciberseguridad

La cooperación en ciberseguridad es un proceso que depende del trabajo interinstitucional, es decir, de las estrategias o planes implementados por la DIMAR y la Armada Nacional y que necesitan del apoyo de otras instituciones como la Comisión Colombiana del Océano, la Vicepresidencia de la República, organizaciones dedicadas al comercio marítimo y al trabajo en los puertos, el Ministerio de Defensa a través de la Fuerza Pública (Policía Nacional, Fuerza Aérea) y la Dirección Marítima por medio de otras unidades que no se ocupen de la ciberdefensa y la ciberseguridad, las cuales cuentan con información, herramientas o incluso, tecnología, que pueda ser de ayuda para la prevención e irrupción de delitos cometidos en contra del comercio marítimo a través del ciberespacio.

Es importante mencionar que dentro de la Cooperación en Ciberseguridad existe la necesidad de establecer contacto con las entidades y gobiernos de otros países para que se logre hacer un trabajo coordinado cuando se trata de organizaciones que irrumpen en los sistemas nacionales y operan desde otras partes del mundo, o, cuando el caso es al contrario, el trabajo coordinado con otros países permite a la Armada Nacional al defensa de los intereses marítimo de Colombia y con ello, salvaguardar la soberanía del país.

Componente: Normatividad y Políticas Publicas

En este componente se incluyen las políticas y normas que rigen el modelo y sirven como punto de partida para la formulación del modelo y la definición de las acciones que hacen parte de cada una de las áreas funcionales de este, las políticas y normas vinculadas al modelo se clasifican según su ámbito de aplicación en nacionales, cibernéticas y marítimas o fluviales. A este componente pertenecen:

- Nacionales: El Plan Nacional de Desarrollo, la Política de Defensa y Seguridad, la Política Nacional Logística y el documento que consigna los intereses marítimos de Colombia.
- Marítimos y fluviales: Política Nacional del Océano y los Espacios Costeros
- Cibernéticos: Marco NIST y el Decreto 338 de 2022

Evaluación de la aplicación del modelo

Una vez implementado el modelo se realizará un seguimiento trimestral y semestral para revisar qué parte del modelo muestra mayor efectividad y si existe una minimización de los incidentes y ataques que hasta el momento habían sido detectados gracias a las alertas tempranas o a las denuncias hechas por las navieras y trabajadores de los puertos. Es así como se establece que los indicadores para determinar cuáles son los cambios que se generan alrededor de este y los que permiten disminuir el impacto que la delincuencia causa en la seguridad cibernética de los puertos de Colombia, estos son:

$$\frac{\#\ de\ ataques\ identificados\ en\ el\ SOC\ y\ SIEM}{\#\ de\ ataques\ prevenidos}$$

De esta manera será posible revisar de forma continua, la efectividad de las acciones implementadas como parte del modelo, claro está, la evaluación del modelo en esta oportunidad

se hace desde la perspectiva de la prevención de problemáticas que pudieran relacionarse con amenazas como narcotráfico, ciberdelincuencia, hacktivismo, entre otros.

$$\frac{\#\ de\ denuncias\ recibidas\ por\ ataques\ identificados}{\#\ de\ ataques\ presentados\ durante\ tres\ meses}$$

Verificar semestralmente el número de ataques perpetrados y con resultados negativos para el comercio marítimo establece un punto de partida para determinar la existencia del trabajo coordinado con los empresarios y las directivas de los puertos, así mismo, teniendo en cuenta que dentro del modelo existe un componente enfocado en la cooperación en ciberseguridad, por medio de la conexión con el Centro Cibernético Policial y la Unidad de Delitos Cibernéticos, para saber cuántas denuncias por estos hechos se están presentado forja el trabajo interinstitucional con la Policía Nacional, de esta manera es posible confirmar que la cooperación en ciberseguridad es una herramienta efectiva cuando se trata de reducir la presencia de organizaciones criminales que operan en los sistemas de los puertos, también, revisar cuantas personas cumplen con la denuncia y contribuyen con ella para que las autoridades procedan de inmediato.

Dentro de la evaluación de la efectividad del modelo también se tendrán en cuenta, de forma trimestral, la discriminación de las novedades dependiendo el tipo de ataque que es llevado a cabo, el sistema que ha sido atacado y la cantidad de veces que han intentado vulnerarlo, de esta forma serpa posible identificar los punto débiles dentro del sistema del puerto y también, la manera como la ciberdelincuencia está siendo ejecutada, también si existe la posibilidad que está utilice más de un tipo de ataque al mismo tiempo y de qué forma la DIMAR e incluso, la misma Armada Nacional a través de los centros estratégicos que ahora trabajarían de forma coordinada con los de la DIMAR, han logrado impedir al menos con la alerta, posibles ataques cibernéticos.

Estos indicadores funcionan como un plan piloto y guía para desarrollar otros que permitan ver la efectividad del modelo y también, realizar un proceso de retroalimentación semestral para

que contribuya con la disminución de irrupciones hechas en los sistemas del comercio marítimo en los puertos de Colombia.

Validación del modelo

La validación del modelo se realiza desde dos puntos de vista, el primero de ellos es el que aporta una matriz DOFA, con la cual se revisan las debilidades, oportunidades, fortalezas y amenazas para esta propuesta. La segunda perspectiva la proveen las opiniones de expertos que son docentes y conocedores de la materia que han trabajado con temas relacionados al objeto de este estudio.

Matriz DOFA

Tabla 6. Matriz DOFA Modelo

MATRIZ DOFA	**FORTALEZAS (F)**	**DEBILIDADES (D)**
	1. Análisis de amenazas nacionales teniendo en cuenta sucesos recientes (INVIMA), también la perspectiva de personal que labora en unidades relacionadas con la ciberseguridad.	1. Escasez de documentación o investigaciones previas que proporcionen información relacionada con el tema de las ciberamenazas al comercio marítimo y de la Ciberseguridad en el mar
	2. Experiencia y conocimiento del personal entrevistado y que aporta información para crear el modelo.	2. El enfoque del modelo inicialmente se concentra solo en los puertos y en las novedades relacionadas con la ciberseguridad en sus sistemas
	3. La creación del Centro de Operación de Seguridad (SOC) y del Sistema de Información y Gestión (SIEM), con los que la Armada Nacional puede contribuir en materia de ciberseguridad en el mar.	3. En la implementación del modelo, la falta de capacitación del personal para el manejo de sistemas y equipos que puedan establecer alguna conexión con otras entidades, instituciones y navieras
OPORTUNIDADES (O)	**ESTRATÉGIA (FO)**	**ESTRATÉGIAS (DO)**
1. Normatividad y programas gubernamentales relacionados con la gobernabilidad cibernética.	1. Aprovechar la experiencia y el conocimiento del personal entrevistado para identificar las necesidades en materia de ciberseguridad del comercio marítimo, a partir del trabajo coordinado, las iniciativas gubernamentales y los planes de la Armada Nacional para ampliar el alcance de la labor de la institución llegando a la	1. Incentivar la investigación desde la Armada Nacional dirigida a la ciberseguridad en espacios marítimos, lo anterior teniendo en cuenta que es importante tener datos e información que pueda aportar pistas sobre las amenazas que no solo afectan al comercio marítimo, también pueden ser amenazas para la Institución y otras entidades gubernamentales que
2. El Plan de Desarrollo Naval que con miras al año 2042 plantea estrategias que se orientan a la seguridad cibernética y cómo debe ser implementada en favor de los intereses de los colombianos		

3. Vinculación de las autoridades y entidades competentes dentro del modelo para realizar un trabajo coordinado que complemente actividades y fortalezca los procesos de protección de la ciberseguridad.	ciberseguridad de las navieras y otras instituciones que podrían resultar afectadas por amenazas cibernéticas desde la labor hecha en el SOC y en el SIEM	son vulnerables ante este tipo de ataques.
AMENAZAS (A)	**ESTRATEGIAS (FA)**	**ESTRATEGIAS (DA)**
1. Con la llegada de un nuevo gobierno puede haber cambios en las políticas públicas relacionadas con la ciberseguridad, la protección de los intereses marítimos y otros aspectos relacionados con la ciberseguridad y el comercio marítimo.	1. La experiencia y el conocimiento del personal entrevistado y que labora en las unidades relacionadas con la ciberseguridad de la Armada Nacional puede llevar a establecer estrategias y acciones con las que se fomente la ciberseguridad y la cooperación en ciberseguridad, está última vista como una opción para prevenir la mutación del ciberdelito y del cibercrimen que afectan en la actualidad a las navieras y con ello, a la ciberseguridad, un nuevo espacio que debe ser protegido para ver por la seguridad nacional.	1. Buscar la oportunidad en medio de las políticas gubernamentales y la normatividad nacional para generar investigaciones que fortalezcan la ciberseguridad en el espacio marítimo colombiano, también, para capacitar al personal en la manera como deben manejar la información que se encuentra en el ciber espacio, como blindarla y eliminar las vulnerabilidades que pudieran ser la puerta de entrada para hackers, evitando así la proyección de sus delitos y del desarrollo de las ciberamenazas.
2. Negación a la cooperación interagencial e internacional para proporcionar información o trabajar de forma coordinada.		
3. Proyección y mutación del ciberdelito basados en los avances tecnológicos, el acceso a programas e información para bloquear la actividad marítima comercial		

Fuente: Elaboración propia

El segundo punto de vista en la validación del documento es aportado por personal experto o conocedor del tema teniendo en cuenta que laboran en unidades relacionadas con la ciberseguridad de alguna de las Fuerzas Armadas de Colombia o cuentan con estudios relacionados en el tema, estas personas evalúan la viabilidad y pertinencia del modelo teniendo en cuenta el objetivo de la investigación y la problemática planteada en este, la evaluación se realiza sobre ítems como los componentes del modelo, la aplicación del Marco Normativo NIST y su pertinencia teniendo en cuenta la situación actual de la seguridad cibernética en el comercio marítimo del país.

Conclusiones

El proceso de caracterización de las amenazas que en la actualidad afectan la ciberseguridad en el espacio marítimo fue llevado a cabo teniendo en cuenta la opinión de los

entrevistados y expertos en el tema, lo anterior como consecuencia de la carencia de documentación que muestre datos recientes relacionados con este tipo de problemáticas; sin embargo, también se tomaron como punto de referencia casos en otros países del mundo. Es importante mencionar que dentro de la caracterización de las amenazas fue posible encontrar que las amenazas cibernéticas dirigidas a navieras e incluso a entidades gubernamentales se intensificaron luego del año 2020 ya que con la llegada de la pandemia la mayoría de procesos fueron vinculados a algún sistema o proceso cibernético, también, que va más allá del robo de información porque existen delitos trasnacionales como la extorsión o el narcotráfico, los cuales se han beneficiado de estas amenazas para manipular la información del sistema y la información relacionada con la carga de los contenedores o simplemente, saber sus rutas para retener la carga y extorsionar a las navieras.

Por otro lado, la definición del modelo de ciberseguridad es un proceso en el que se toma como punto de referencia modelos de seguridad marítima de países como España, encontrando diferencias en el manejo que cada país tiene frente a este tipo de situaciones, también mostrando el alcance que la ciberdelincuencia y el cibercrimen han logrado en los últimos años, mostrando que dentro del modelo es importante vincular otras entidades y lograr que la Armada Nacional haga parte de este grupo de autoridades para proteger el espacio cibernético que atañe al mar, pensando en crear un modelo que también se fundamente en el Marco Normativo NIST que tiene sus inicios en Estados Unidos y que puede ser aplicable a empresas como las navieras de Colombia que pudieran resultar afectadas con estas ciberamenazas cuando se materializan a través de riesgos, lo que lleva a construir un modelo basado en las lecciones aprendidas de otros países y en la información proporcionada por los expertos sobre las ciberamenazas al comercio marítimo en Colombia, por eso busca prevenirlas y trabajar de forma coordinada para detener las existentes.

La validación del modelo elaborado se realiza desde dos puntos de vista, el primero de ellos es a través de una matriz DOFA con la que se evalúa teniendo en cuenta el entorno, la situación actual de estas amenazas en el país y los hallazgos de esta investigación, el segundo es el punto de vista de expertos que consideran viable el modelo teniendo en cuenta la posibilidad de que la Armada Nacional intervenga en esta problemática siempre y cuando cuente con el apoyo de entidades y organizaciones vinculadas con este sector y así trabajar de forma eficiente.

Finalmente, se realiza una propuesta de un modelo de ciberseguridad aplicable en el comercio marítimo en Colombia y las amenazas provenientes del ciberespacio, el cual, cuenta con tres componentes que promueven acciones para prevenir y detener este tipo de novedades, también vincula la normatividad y políticas existentes en los que se fundamenta para siempre actuar acorde a lo establecido con la Ley y promueve el trabajo coordinado con otras entidades, de esta forma logra cubrir la mayoría de áreas relacionadas y actuar desde todos los frentes posibles para reducir la actuación de estos grupos delincuenciales que actúan a través del ciberespacio.

Recomendaciones

Con el desarrollo de la investigación fue posible percatarse de la inexistencia de estudios en la Armada Nacional que vayan más allá de los intereses institucionales, por eso, se sugiere la promoción de la investigación enfocada en fenómenos que afectan la seguridad y ciberseguridad marítima desde otras perspectivas como la de las navieras y de esta forma identificar que problemas pueden representar una amenazas para la Armada Nacional y la seguridad nacional, también, para crear una base de datos que pueda ser consultada a la hora de revisar antecedentes que sirvan como punto de partida para la creación de estrategias de seguridad y para próximos estudios.

Referencias

Adams, J. (2001). Virtual Defense. *Foreing Affairs, 80*(3), 98-112. doi:https://doi.org/10.2307/20050154

Aguirre, J. (2010). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. *Espéculo. Revista de Estudios literarios*, 33. https://biblioteca.org.ar/libros/150717.pdf

Amazon Web Services, Inc. (2019). *Marco de Seguridad Cibernética NIST (CSF, por sus siglas en inglés). Alineación con el NIST CSF en la nube de AWS.* Amazon Web.

Androjna, A., Brcko, T., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation [On line]. *Journal of Marine Science and Engineering*.

Aponte, J. D. (31 de Julio de 2022). Jefe del Departamento de Prospectiva Cibernética. (J. Gómez, Entrevistador)

Armada Nacional. (2015). *Plan Estratégico Naval 2015-2018.* Armada Nacional de Colombia.

Armada Nacional. (2022). *Misión y Visión*. https://www.armada.mil.co/es/content/mision-y-vision-armada-nacional#:~:text=Ser%20una%20Armada%20de%20proyecci%C3%B3n,contribuci%C3%B3n%20al%20progreso%20del%20pa%C3%ADs.

Banco Interamericano de Desarrollo - BID, & Organización de Estados Americanos -OEA. (2020). *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe.* Banco Interamericano de Desarrollo.

Becerra, J., Sánchez, M., Castañeda, C., Bohórquez, A., Páez, R., Baldomero, A., & León, I. (2019). La Seguridad en el Ciber espacio, Un desafío para Colombia. Bogotá, Colombia: Escuela Superior de Guerra.

Boyes, H. (2015). Cyber security and cyber-resilient supply chains. *Technology Innovation, 5*(4), 28-34.

CEPAL. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad.* CEPAL. https://repositorio.cepal.org/bitstream/handle/11362/46275/1/S2000679_es.pdf

Comisión Colombiana del Océano. (2014). Construyendo País Marítimo: http://www.cco.gov.co/docs/publicaciones/libro_construyendo_pais_maritimo.pdf.

Consejo Nacional de Política Económica y Social CONPES. (2020). *Documento CONPES 3990 "Colombia Potencia Bioceánica Sostenible 2030"*. Bogotá: Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3990.pdf

Correa, J. (2022). Entrevista investigación. (J. Gómez, Entrevistador)

Crawford Crawford, J. (2019). Ciberataque al Transporte Marítimo: ¿Una Amenaza Real o Ciencia Ficción? *Revista de Marina*(970), 15-23. https://revistamarina.cl/revistas/2019/3/jcrawfordc.pdf

Curso de Altos Estudios Militares No.61. (2020). Estrategia de Seguridad Nacional Marítima y Fluvial. *Primera Edición,* 115. Bogotá, Colombia: ESDEGUE - Graphic Motion.

de la Peña, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue ¨[Online]. *Transport Policy*, 1-4.

Dingeldey, P. (2017). Port Automation and Cybersecurity Risks [On line]. *The Maritime Executive*. https://www.maritime-executive.com/editorials/port-automation-and-cybersecurity-risks

Dirección General Marítima. (2021). *Estadísticas Anuales de Transporte Marítimo en Colombia 2020 [Formato Digital]* (Primera edición ed.). Bogotá, Colombia: Dimar.

Fitton, O., Germond, B., & Lacy, M. (2016). El futuro de la ciberseguridad marítima. Bogotá, Colombia.

Franco, M. (diciembre de 2018). *Acción responsable del Estado. Una visión en el horizonte 2050.* Madrid, España: Instituto Español de Estudios Estratégicos.

Grimalt, C., & Baró, B. (2021). *Seguridad marítima y portuaria en la era 4.0*. https://www.mapfreglobalrisks.com/gerencia-riesgos-seguros/articulos/seguridad-maritima-y-portuaria-en-la-era-4-0/

Grupo de Seguridad Marítima. (2020). *Guía de Buenas Prácticas para la Gestión de Riesgos de Ciberseguridad en Buques e Instalaciones Portuarias.* Madrid, España: Consejo Nacional de Seguridad Marítima.

Grupo Editorial Extra. (18 de febrero de 2022). *Varios contenedores están retrasados por ciberataque del Invima*. https://extra.com.co/noticias/varios-contenedores-estan-retrasados-por-ciberataque-del-invima

Guiora, A. (2018). Ciberseguridad: un modelo de cooperación. *OpenMind*, 29. https://www.bbvaopenmind.com/wp-content/uploads/2018/12/BBVA-OpenMind-Amos-Guiora-Ciberseguridad-un-modelo-de-cooperacion.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). *Metodología de la Investigación* (Sexta Edición ed.). México D.F., México: McGrawHill Education.

Jefatura de Planeación Naval, & Dirección de Planeación Estratégica. (2021). *Plan de Desarrollo Naval 2042.* https://www.armada.mil.co/sites/default/files/descargas/Plan%20Desarrollo%20Naval%202042%2007042021.pdf

Marsh McLenann Company. (Julio de 2014). El riesgo del ciberataque al sector marítimo.

Mednikarov, B., Tsonev, Y., & Lázarov, A. (2020). Analysis of Cybersecurity Issues in the Maritime Industry. *Information & security, 41*(1), 27-43. doi:https://doi.org/10.11610/isij.4702

MINTIC, Centro Cibernético Policial, Vive Digital, & Presidencia de la República. (s.f.). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* Bogotá: MINTIC. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Moreno, A. (2015). La Estrategia de Seguridad Nacional. Ciberdefensa y Seguridades Marítimas y Energéticas.

Nyman, E. (2019). Techno-optimism and ocean governance: New trends in maritime monitoring. *Marine Policy*, 30-33. doi:https://doi.org/10.1016/j.marpol.2018.10.027

Portafolio.com. (2022). *Por qué el ataque cibernético al Invima encarecería más los productos*. https://www.portafolio.co/economia/finanzas/invima-ataque-cibernetico-encareceria-los-productos-en-colombia-561912

Presidente de la República. (2012). *Decreto 2078 de 2012 "Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), y se determinan las funciones de sus dependencias."*. http://www.secretariasenado.gov.co/senado/basedoc/decreto_2078_2012.html

Ramírez, F., Pedroza, W., & Forero, J. (2021). *IMC - Intereses Marítimos de Colombia.* Bogotá D.C.: Vicepresidencia de la República-Comisión Colombiana del Océano-Armada de Colombia.

Rivera, S., & Pérez, J. (2012). El Transporte Marítimo y las Fronteras Portuarias: Contenedores y Narcotráfico. En Escuela Superior de Guerra, *Crimen Organizado Transnacional y Conflictos Ambientales en América* (págs. 121-163). México D.F.

Rodríguez, H. (2016). Seguridad Integral Marítima, Reto Estratégico. En H. Rodríguez, L. Osorio, S. Uribe, & L. Chávez, *Seguridad Marítima: Retos y Amenazas* (Primera Edición ed., págs. 9-44). Bogotá: Escuela Superior de Guerra. doi: https://doi.org/10.25062/9789585605480

UNAM. (2009). *Capítulo 2. Amenazas y vulnerabilidades de la seguridad informática.* http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217/A5.pdf?sequence=5

United Nations Conference on Trade and Development (UNCTAD). (2019). *Review of maritime transport*. https://unctad.org/system/files/official-document/rmt2019_en.pdf

University of Miami. (2017). Global Threats: Cybersecurity in Ports (Donald Duck, Daughters & Dollars). Miami, Estados Unidos: Center for International Business Education & Research (CIBER).

Valbuena, M. (2022). MUSD Caracterización de las Ciberamenazas . España: Universidad de Nebrija.

Valvuena, M. (2022). Mundo Cibernético. Unidad Didáctica 2: Caracterización de las ciberamenazas. Madrid, España: Universidad de Nebrija.