Gestión de la seguridad marítima en Venezuela ante las amenazas cibernéticas en la sociedad del riesgo

Gioyyanni Jesús, Calderón Domínguez
Marina Mercante
orcid: 0000-0002-8531-2665
gioyyanni@gmail.com
Venezuela

Fechas de recepción: 25/09/2021
Fecha de aceptación: 10/10/2021

Resumen

A partir del Comité Marítimo de Seguridad Nro. 98 de la Organización Marítima Internacional, surgió la resolución MSC.428(98) sobre la Gestión de los Riesgos Cibernéticos Marítimos en los Sistemas de Gestión de la Seguridad, en correspondencia con la circular MSC-FAL.1-Circ.3: Directrices sobre la Gestión de los Riesgos Cibernéticos Marítimos, cuyo propósito es coadyuvar en la generación de normas para mitigar los riesgos y amenazas cibernéticas a las cuales se encuentra expuesta la seguridad marítima a nivel global, generando así transformaciones en la habitual forma de gerenciar dentro del contexto de escenarios complejos vinculados a este tipo de seguridad. Los Estados miembros de este organismo multilateral han respaldado la necesidad de implementar estas medidas para mitigar los riesgos a los cuales se expone la interface buque-puerto durante el proceso comercial. En la realidad venezolana existen aspectos que dan cuenta de una ausencia regulatoria y una elevada desinformación en las instituciones vinculadas al sector. De ahí que el objetivo de esta investigación consiste en configurar los elementos teóricos de la gestión de la seguridad marítima en Venezuela como parte de la trama de la sociedad del riesgo en el contexto de la seguridad cibernética. El análisis de contenido cualitativo, es la técnica de investigación empleada para el análisis de los datos secundarios extraídos de 8 textos. Esta técnica permitió la construcción de tres categorías como nociones que permitieron agrupar los elementos con características comunes de acuerdo a su naturaleza y contenido. Los resultados demuestran que existen aspectos disruptivos en la gestión de las instituciones públicas y las empresas del sector privado en la adaptación de las normas prescritas.

Palabras clave:
Gestión de la seguridad marítima ; amenazas cibernéticas; sociedad del riesgo; convenios marítimos internacionales

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Maritime safety management in Venezuela against cyber threats in the Risk Society

Abstract

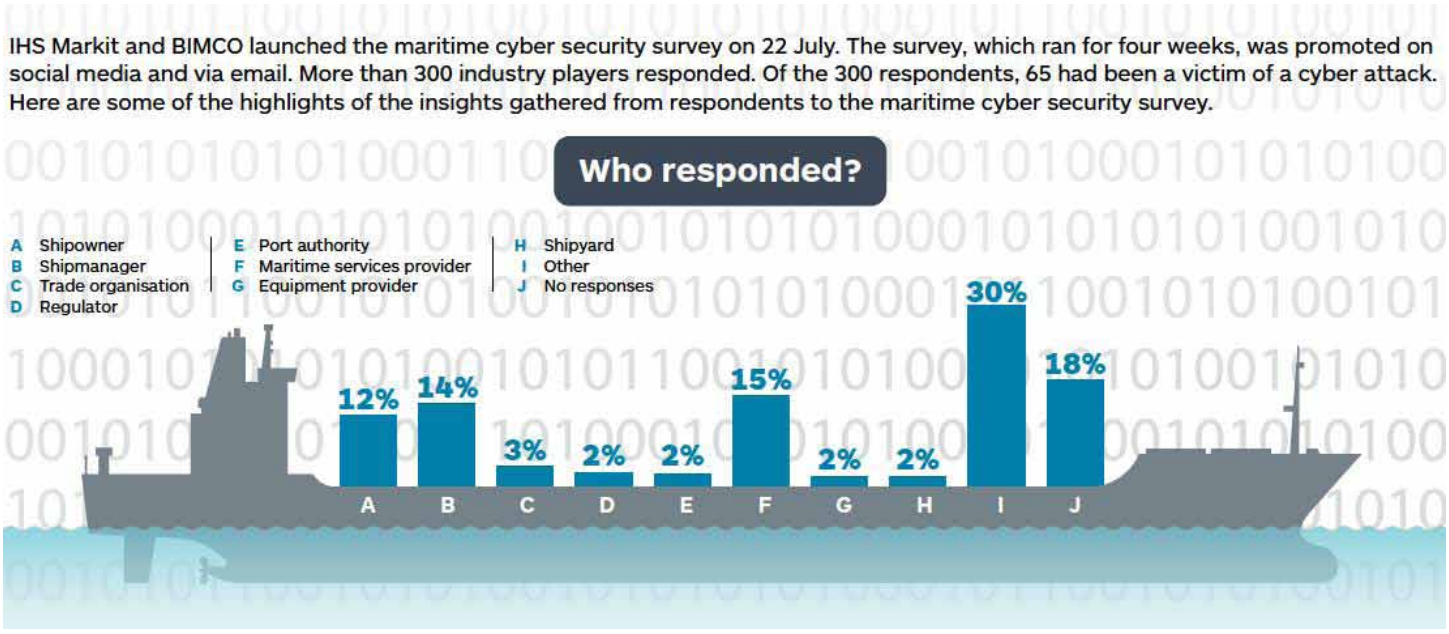
From the Maritime Safety Committee No. 98 of the International Maritime Organization, emerged the resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems in correspondence with the MSC-FAL.1-Circ.3: Guidelines on Maritime Cyber Risk Management; the purpose is to contribute to the generation of standards to mitigate cyber risks and threats to which maritime security is exposed in worldwide, generating transformations in the usual way of managing within the context of complex threat related to this security level. The member States of this multilateral organization have fostered the need to implement these measures to mitigate the risks to which the ship-port interface is exposed during the commercial process. In the Venezuelan reality there are aspects that account for a regulatory absence and high misinformation in the institutions related to the sector. The objective of this investigation is to configure the theoretical elements of maritime security management in Venezuela as part of the risk society in the context of cybersecurity. Qualitative content analysis is the research technique used to analyze secondary data extracted from 8 texts. This technique allowed the construction of three categories as notions that allowed grouping the elements with common characteristics according to their nature and content. The results show that there are disruptive aspects in the management of public institutions and private sector companies in the adaptation of prescribed standards.

Keywords:
Maritime security management ; cyber Threats; risk society ; international maritime agreements

Introducción

En el año 2017 IHS Markit en asociación con el Consejo Marítimo Internacional y del Báltico (BIMCO, siglas en inglés) realizó una encuesta de seguridad cibernética vía web y de acuerdo a los resultados, de las 300 empresas que participaron y respondieron a la investigación, 65 habían sido víctimas de un ataque cibernético. Entre las más destacadas se encontraban empresas de *armadores*[1], operadores de buques y agencias marítimas. Con un predominante 30% de los encuestados que no se ubicó en las alternativas señaladas y otro 18% que no respondió a la encuesta, como se puede ver en la Figura 1.

Figura 1.- Encuesta BIMCO sobre Ataques Cibernéticos



Fuente: Adaptado de IHS and BIMCO, (2017).

Es importante, tener presente que estas cifras contemplan únicamente los eventos denunciados, aunque se sabe que muchos de los incidentes ocurridos no son reportados para no dañar la reputación de la compañía y son tratados de manera privada, de allí la abstención y la no identificación de algunos encuestados.

Como se puede ver en la Figura 2, Las pérdidas económicas por ataques de ciberseguridad se amplifican en la medida que la digitalización de los procesos avanza. Las estadísticas incluyen a las empresas e instituciones relacionadas a la logística y al transporte, "rubro que durante el año 2019 mostró una tasa de crecimiento interanual

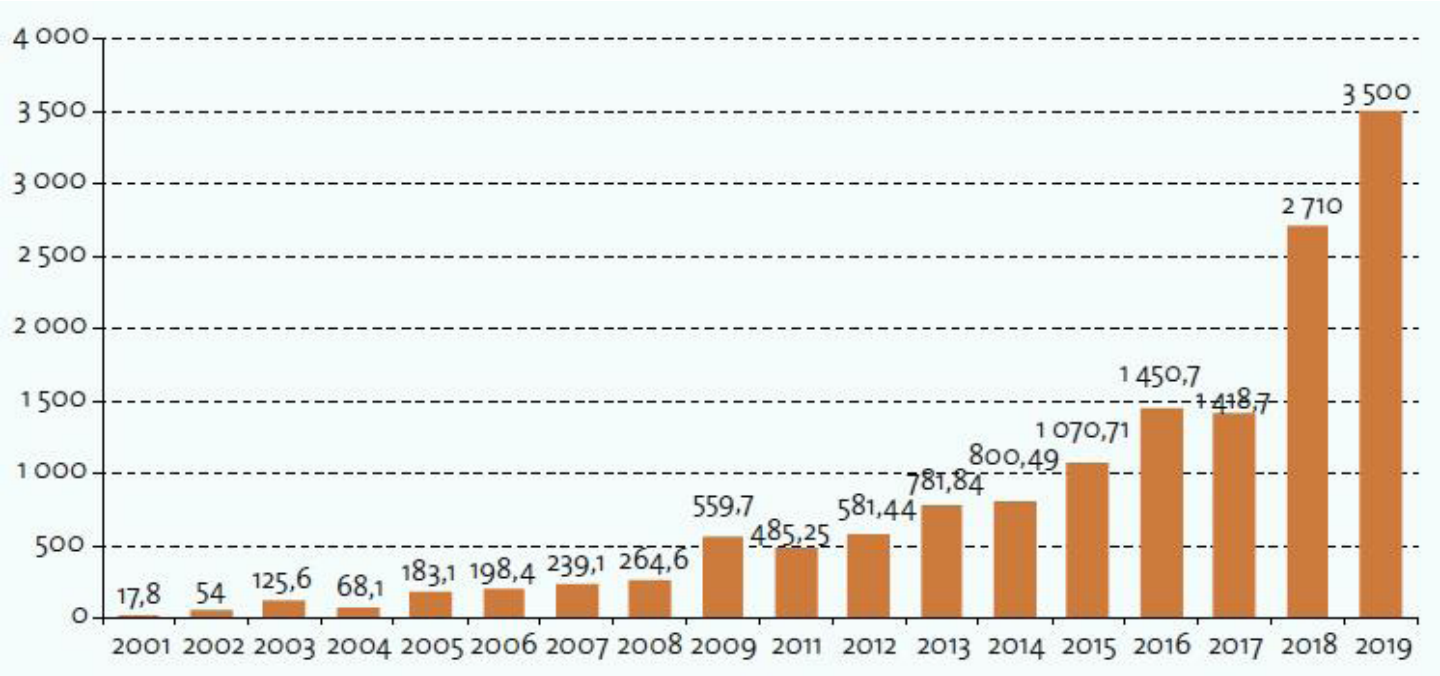
1 El Armador, es responsable de la gestión operativa del buque, es decir, quien lo equipa y pertrecha, lo prepara para prestar el servicio de transporte, es quien nombra al Capitán y pone la tripulación a bordo y lo provee del seguro marítimo más conveniente.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

del 78% en los ataques" que involucran a diferentes organizaciones de transporte marítimo, ubicándose de esta manera en el tercer lugar, con un 10% del total de los ataques a nivel global. (Comisión Económica para América Latina y el Caribe, 2020, p.10).

La logística y transporte, que se mantiene a lo largo de los años entre las primeras posiciones, realza el creciente valor de los datos de este sector para la industria del cibercrimen. Esta ubicación, se explica "debido al valor de los activos electrónicos y la posibilidad de manipular los datos de las cadenas de distribución, esto sin contar con el efecto dominó causado en el resto de los sectores y en otros servicios". (Comisión Económica para América Latina y el Caribe, 2020, p.10).

Figura 2.- Pérdidas Económicas Anuales debido al Cibercrimen. (En millones de dólares)



Fuente: Adaptado de Internet Crime Annual Report, por Federal Bureau of Investigation, Department of Justice, USA (FBI), (2020).

Rodríguez (2016), hace especial énfasis en que la actividad humana constituye el principal colaborador de las amenazas que se ciernen sobre los mares. Además reflexiona e incluye la cibernética como un elemento de riesgo en la seguridad, las actividades cibernéticas maliciosas a nivel global muestran un impacto extraordinario en términos de pérdidas y daños. De Izcue Arnillas, Arriarán y Tolmos (2012) expresan que:

> Estas nuevas amenazas, también denominadas amenazas no tradicionales, provienen por un lado de la conjunción de las fuerzas puestas en libertad por la repentina desaparición del formato bipolar del antiguo orden mundial, y, por otro lado del incremento del crimen organizado ante mayores facilidades tecnológicas en un ambiente globalizado (p. 263).

Depósito legal: PP201402DC4456
ISSN: 2343-6212

En este contexto, la convención de las Naciones Unidas sobre el Derecho del Mar de 1982 (CDM)[2], constituye la norma principal del marco jurídico internacional de los espacios marinos. Los derechos y obligaciones que la convención atribuye al Estado ribereño sobre los distintos espacios marinos frente a sus costas (aguas interiores, mar territorial, plataforma continental y zona económica exclusiva) y las reglas y principios que rigen la utilización de las zonas más allá de la jurisdicción estatal, son el punto de partida de cualquier esfuerzo, interno o externo, encaminado a resolver los desafíos que plantea la seguridad marítima.

Sobre este particular, el Estado venezolano, aun cuando no es signatario del convenio CDM, en el ejercicio de su papel como Estado ribereño y Estado rector del puerto[3], fija claramente en la Constitución de la República Bolivariana de Venezuela (1999), en su Artículo 11 la soberanía plena del territorio marítimo, cuando advierte:

> Sobre los espacios acuáticos constituidos por la zona marítima contigua, la plataforma continental y la zona económica exclusiva, la República ejerce derechos exclusivos de soberanía y jurisdicción en los términos, extensión y condiciones que determinen el derecho internacional público y la Ley (p.18).

En ese contexto, los distintos procesos internacionales de coordinación y cooperación en el ámbito de la seguridad marítima parten de asumir la importancia que tienen los mares y océanos del mundo para el bienestar y la prosperidad de los pueblos que de ellos dependen. Esta vinculación estrecha entre la seguridad de los mares, el desarrollo y el bienestar económico de sociedades enteras, se ve reflejada en diversos convenios[4] de organizaciones de alcance global como las Naciones Unidas, las resoluciones anuales de la Asamblea General sobre los océanos y el derecho del mar, al igual que en los de su organismo especializado, la Organización Marítima Internacional (OMI).

Venezuela progresivamente se ha incorporado a la unificación de criterios en materia del derecho marítimo internacional, esto se puede ratificar en el número de convenciones internacionales a las cuales se ha adherido, y por consiguiente asociado en el marco jurídico interno mediante la promulgación de leyes y sus respectivos reglamentos aprobatorios. Para poder avanzar en esta investigación, es importante resaltar las competencias del Ejecutivo Nacional en materia de la suscripción de los convenios internacionales, estas se encuentran descritas en la Constitución de la República Bolivariana de Venezuela (1999), en la forma siguiente:

---

2 La CDM es considerada uno de los tratados multilaterales más importantes de la historia, desde la aprobación de la Carta de las Naciones Unidas, siendo calificada como la Constitución de los océanos. Fue aprobada, tras nueve años de trabajo, el 30 de abril de 1982 en Nueva York y abierta a su firma por parte de los Estados, de los cuales 167 han firmado y ratificado. A pesar de haber sido en Caracas la primera sesión de discusión de la convención, esta no ha sido firmada ni ratificada por la República Bolivariana de Venezuela hasta la presente fecha.

3 El Estado Ribereño (soberanía y jurisdicción del Estado con respecto a sus espacios marítimos); es un argumento de la seguridad. Se distingue un espacio de soberanía como es el Estado ribereño, conocido como mar territorial, y un espacio común llamado alta mar, regido por el principio de libertad.

4 La OMI cuenta en su haber con aproximadamente unos 53 convenios internacionales. De todos estos convenios la gran mayoría han entrado en vigor y han hecho del transporte marítimo el modo de transporte más seguro, más eficiente y mucho más amigable con el ambiente.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

> Artículo 217. La oportunidad en que deba ser promulgada la Ley aprobatoria de un tratado, de un acuerdo o de un convenio internacional, quedará a la discreción del Ejecutivo Nacional, de acuerdo con los usos internacionales y la conveniencia de la República.

Para el desarrollo y regulación de todo lo concerniente al derecho marítimo internacional público, el ordenamiento jurídico venezolano concentra normas de carácter tanto internacionales como internas, y dentro de éstas últimas, las normas de rango constitucional y de rango legal, considerándose los convenios internacionales de la Organización Marítima Internacional de rango supralegal. La OMI tiene como parte fundamental de su precepto, el deber de velar por la seguridad del transporte marítimo. Para gestionar y mitigar los riesgos que puedan poner en peligro la protección marítima, la Organización elabora la normativa y orientaciones adecuadas a través del Comité de Seguridad Marítima, Comité de Facilitación y el Comité Jurídico (MSC, FAL y LEG) asumiendo plenamente la incorporación de aspectos de protección física de buques y puertos a sus normativas, estableciendo mecanismos de cooperación con otras agencias internacionales que se ocupan de actividades vinculadas al mar.

La Asociación Peruana de Agentes Marítimos, (2019) señala que en el año 2008, la OMI inició un programa para la facilitación y transacción electrónicas aprobado por el FAL 28. La información contenida en los formularios normalizados incluidos en los formularios FAL, ha sido diseñada utilizando los códigos normalizados correspondientes que pueden encontrarse en los directorios del intercambio electrónico de datos para la administración, el comercio y el transporte de las Naciones Unidas.

Como consecuencia de lo anterior y ante el enorme incremento en el uso de los sistemas de tecnología cibernética en el sector marítimo, en el año 2016 el Comité FAL 39 acordó incluir un nuevo asunto en el orden del día de la asamblea: "Directrices sobre los aspectos de la facilitación relacionados con la protección de la red de transporte marítimo contra las amenazas cibernéticas". Tanto el FAL 39 como el FAL 40 examinaron los aspectos de la facilitación para proteger la red de transporte marítimo contra las amenazas cibernéticas, incluyendo la necesidad de abordar los riesgos concretos, los procedimientos correspondientes a los certificados electrónicos y el intercambio de datos entre buques y tierra; y la información previa a la llegada basada en el Convenio FAL y los procedimientos que hacen uso de la interfaz buque-puerto. (Asociación Peruana de Agentes Marítimos, 2019).

En esta materia la Ley General de Marina y Actividades Conexas (2002), estableció las bases para la correcta implementación de los convenios de facilitación, y señala en su Artículo 16 que:

> Se crea la Comisión Nacional para la Facilitación del Sistema Buque-Puerto, con el objeto de dar cumplimiento a las acciones para optimizar el tráfico marino internacional. Dicha comisión será presidida por el Presidente del Instituto Nacional de los Espacios Acuáticos, quien instalará las comisiones locales en cada una de las circunscripciones acuáticas de la República, las cuales serán presididas por los respectivos capitanes de puerto.

Paralelamente, la Presidencia de la República (2008) dictó el Decreto número 6.265 con Rango, Valor y Fuerza de Ley de Simplificación de Trámites Administrativos (2008), donde se establecen las bases para la simplificación de

los trámites administrativos, como el máximo uso de las tecnologías de información, la incorporación de controles automatizados, la implementación de base de datos automatizadas, la creación de un sistema de información centralizado y automatizado para integrar y compartir información (Artículos 6º, 11º y 44º).

De acuerdo a la organización del Estado, las competencias para el sector acuático según al ordenamiento jurídico interno tienen un órgano rector y un órgano administrativo, con funciones diferentes y con competencias muy similares en cuanto a la seguridad marítima, estas están descritas en la Ley Orgánica de los Espacios Acuáticos (2014), de acuerdo al artículo siguiente:

> Artículo 71. El Ministerio del Poder Popular con competencia en materia de transporte acuático, es el órgano rector de la navegación marítima, fluvial y lacustre destinada al transporte … así como, lo relacionado a la materia portuaria, y cualquier otra que señale la ley; y tiene las siguientes competencias:…14. Vigilar, fiscalizar y controlar la aplicación de las normas para la seguridad del transporte acuático nacional.

El extinto Ministerio del Poder popular para el Transporte y Comunicaciones para atender funciones especializadas de administración acuática creó el Instituto Nacional de los Espacios Acuáticos (INEA) como órgano adscrito, comenzando sus funciones el 15 de enero del año 2002, posterior a la promulgación de la primera Ley Orgánica de los Espacios Acuáticos del año 2001.

El INEA, es el ente del Estado que ejercer la autoridad acuática en todo el territorio; el ejercicio de la administración acuática; y la ejecución de las políticas navieras y portuarias del órgano rector, el control de la navegación y del transporte acuático, tal como lo establece el Decreto con Rango, Valor y Fuerza de Ley Orgánica de los Espacios Acuáticos vigente en su Artículo 73 numerales 1, 2 y 4.

Este órgano administrativo y de gestión de los Espacios acuáticos, es el garante de la verificación, inspección y auditoria de todos los aspectos de seguridad concernientes al sector marítimo, entre sus facultades está la de establecer las normas correspondientes a objeto de garantizar la seguridad marítima, en correspondencia con la Ley General de Marinas y Actividades Conexas según Gaceta Oficial de la República Bolivariana de Venezuela (2002).

> Artículo 81. La Autoridad Acuática fijará políticas y establecerá normas, para que la materia referente a la seguridad y navegabilidad del buque, sea tratada de manera continua y permanente, que se extienda a los aspectos propios de la seguridad y operatividad del buque.

Definida y delimitada la responsabilidad del Estado en materia de seguridad marítima, a través de su órgano rector y de gestión administrativa, se hace inevitable revisar el marco jurídico (Gacetas oficiales) vigentes en materia de seguridad informática. A tal efecto, para esta investigación solo se evidencian la Ley de infogobierno (2013), Ley sobre Acceso e Intercambio electrónico de datos entre los Órganos y entes del Estado (2012) y la Ley de delitos informáticos (2001) como instrumentos jurídicos que regulan el manejo de la información electrónica en la República.

Tomando en consideración que el comité FAL 28 exhorta a los Estados miembros de la OMI a utilizar la certificación electrónica de documentos con el objeto de facilitar la llegada a puerto, es preciso

Depósito legal: PP201402DC4456
ISSN: 2343-6212

considerar la Ley de Infogobierno (2013, p.406.189) y su ámbito de aplicación a través de la superintendencia de certificación electrónica, tendrá según lo plasmado en su Artículo 55 las siguientes competencia:

> : …1. Desarrollar, implementar y coordinar el Sistema Nacional de Seguridad Informática.
> (….) 3. Establecer los mecanismos de prevención, detención y gestión de los incidentes generados en los sistemas de información y en las infraestructuras críticas del Estado, a través del manejo de vulnerabilidades e incidentes de seguridad informática.

La Ley Especial contra Delitos Informáticos, que se encuentra en la Gaceta Oficial de la República Bolivariana de Venezuela. (2001), establece el régimen de sanciones en todo lo referente a la violación de la seguridad informática. Este instrumento jurídico es el más importante de la República en materia de mitigación de riesgos en el plano de las tecnologías de la información y la comunicación y la transferencia de información electrónica, a pesar de no haber sido modificada y aun cuando ha tenido poca aplicación, el objeto principal, se describe en su Artículo 1:

> La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley (p.1).

A los efectos de la ley, se entiende por tecnología de información: "rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática" (artículo 2, ejusdem).

Ahora bien, el marco jurídico descrito aunque endeble, corresponde a la protección, responsabilidad y régimen de sanciones del Estado venezolano en materia de seguridad marítima y seguridad informática. Para efectos de la seguridad de los procedimientos electrónicos de la interfaz buque-tierra implementados por las directrices del comité FAL 40, el Estado resguarda sus intereses y responsabilidades dentro de las aguas jurisdiccionales de la República, ejerciendo la soberanía en esta materia. Sin embargo, a efectos de garantizar la seguridad marítima en el contexto de los riesgos y amenazas emergentes en el uso las tecnologías de la información y el uso de medios electrónicos y tecnologías cibernéticas en aguas jurisdiccionales de la República, el marco jurídico internacional es predominante, prevaleciendo el Estado de abanderamiento del buque.

En ese sentido, los convenios internacionales garantizan la responsabilidad del Estado del pabellón en aguas jurisdiccionales de Venezuela, con especial preferencia sobre la normativa legal vigente, para prevenir los riesgos y amenazas de la seguridad marítima incluidas las recientes directrices en seguridad cibernética. La responsabilidad de la República Bolivariana de Venezuela en esta materia, residirá por consiguiente en su órgano de administración acuática INEA, en todo lo referente al refrendamiento de la certificación de los buques que enarbolen el pabellón venezolano, y a través de auditorías y la verificación documental en todo lo referido a los buques con otros Estados de abanderamiento.

Dicho lo anterior, para efectos de protección en materia de seguridad marítima a bordo de buques de pabellón venezolano, el Estado ha reconocido y suscrito el Convenio Internacional para la Seguridad de la Vida en el Mar (SOLAS[5], en inglés) del año 1974 con sus sucesivas enmiendas en el año 1998. La República de Venezuela (1982), lo publica en Gaceta Oficial Nº: 32.597, de 1982. El objetivo principal del Convenio SOLAS es establecer normas mínimas relativas a la construcción, equipo y la utilización de los buques, compatibles con su seguridad.

Los Estados de abanderamiento son responsables de asegurar que los buques que enarbolen su pabellón cumplan las disposiciones del Convenio, el cual prescribe la expedición de una serie de certificados como prueba de acatamiento. Las disposiciones relativas a la supervisión permiten también a los gobiernos signatarios inspeccionar los buques de otros Estados contratantes, si hay motivos fundados para creer que un buque y su correspondiente equipo no cumplen sustancialmente las prescripciones del convenio. A este procedimiento se le conoce como supervisión por el Estado rector del puerto.

El control por el Estado rector del puerto hace referencia a las inspecciones que se realizan sobre buques extranjeros en los puertos, con la finalidad de comprobar si se cumplen o no las prescripciones sobre seguridad marítima. Se configura como un mecanismo de protección de los Estados frente a buques de bandera extranjera, que pueden suponer un riesgo para la seguridad marítima. Y, sin duda, es una muestra de la desconfianza de los Estados en el proceso de abanderamiento de buques extranjeros; bien sea porque sus legislaciones presentan distintos niveles de severidad o bien porque se presume el incumplimiento de los requisitos mínimos por parte de los Estados cuyo pabellón enarbolan.

Del Capítulo IX del convenio SOLAS se desprenden las directrices para la gestión operacional del buque, el Código Internacional de Gestión de la Seguridad operacional del buque y prevención de la contaminación (ISM Code). Este fue adoptado en 1993 por resolución A.741(18) y entra en vigencia el 1 de julio de 1998, por lo que se hace de cumplimiento obligatorio para todos los Estados miembros. El referido código ISM obligatoriamente exige a los Armadores la elaboración de los respectivos Sistemas de Gestión de la Seguridad (SGS) según la especificación y propósito del buque. Recientemente, por la resolución del Comité MSC se emite la resolución MSC.428(98) sobre la gestión del riesgo cibernético marítimo en los SGS en junio de 2017. La resolución establece que un SGS aprobado, debe tener en cuenta la gestión del riesgo cibernético de acuerdo con los objetivos y requisitos del Código. (Organización Marítima Internacional. ,2017).

> A los efectos de las presentes directrices, se entiende por gestión de los riesgos cibernéticos el proceso de identificación, análisis, evaluación y comunicación de riesgos de índole cibernética y de aceptación, evitación, transferencia o mitigación de esos riesgos hasta un nivel aceptable, teniendo en cuenta los cos-

5 El Convenio SOLAS en sus versiones sucesivas está considerado como el más importante de todos los tratados internacionales relativos a la seguridad de los buques. La primera versión fue adoptada en 1914, en respuesta a la catástrofe del Titanic, la segunda en 1929, la tercera en 1948, y la cuarta en 1960. En la versión de 1974 se incluye el procedimiento de aceptación tácita por el que se establece que una enmienda entrará en vigor en una fecha determinada a menos que, antes de esa fecha, un determinado número de Partes haya formulado objeciones. (Organización Marítima Internacional, s.f).

Depósito legal: PP201402DC4456
ISSN: 2343-6212

> tos y las ventajas para los interesados de las actuaciones emprendidas (Organización Marítima Internacional, 2017, p.3).

El Código para la Protección de Buques e Instalaciones Portuarias (ISPS, siglas en inglés) que entró en vigor en julio 2004, constituye el segundo código en importancia con respecto a la seguridad y protección marítima. El propósito del código es proveer un sistema estandarizado de evaluación de riesgos que permita a los gobiernos reaccionar ante un cambio en el nivel de amenaza con cambios apropiados en la protección de buques e instalaciones portuarias.

> El Código se divide en dos secciones: Parte A y Parte B. La parte A, obligatoria, proporciona una reseña detallada de prescripciones de protección marítima y portuaria que los gobiernos contratantes del Convenio SOLAS, las autoridades portuarias y las compañías navieras han de observar, de manera que se puedan cumplir el Código. La Parte B del Código facilita una serie de directrices de carácter recomendatorio sobre cómo cumplir las prescripciones y obligaciones especificadas en las disposiciones de la Parte A. (Organización Marítima Internacional, s.f, párr.1)

De esta manera, en la parte "A" se exponen las prescripciones obligatorias, requerimientos detallados relativos a la protección, dirigidos a los gobiernos, las autoridades portuarias y las compañías navieras; junto con una serie de orientaciones sobre cómo alcanzar estos requerimientos en una segunda sección parte "B" de cumplimiento voluntario, considerado como recomendaciones.

Las directrices sobre gestión del riesgo cibernético marítimo, emanados de la resolución MSC-FAL.1-Circ.3, tienen alcance sobre este código al igual que las directrices de la resolución MSC.428 (98) y entraron en vigencia a partir del 1 de enero del año 2021. Dicho lo anterior, con el propósito de dar cumplimiento a lo señalado por el organismo multilateral, el Ministerio del Poder Popular para Relaciones Exteriores acordó en el año 2017, el memorándum de entendimiento entre la República Bolivariana de Venezuela y la OMI sobre su participación en el plan de auditorías de los Estados miembros, utilizando como norma de auditoria el Código III[6] para la implantación de los instrumentos de la OMI, resolución A.1070 (28)[7], señala que la auditoría debe abarcar los diversos instrumentos obligatorios con el fin de determinar la forma en que la República Bolivariana de Venezuela ejerce, como Estado de abanderamiento, como rector del puerto y Estado ribereño, las obligaciones y responsabilidades pertinentes relativas a la seguridad marítima y a la protección del medio ambiente establecidos en el código ISM. (Gaceta oficial de la República Bolivariana de Venezuela, 2017, p. 436.004).

No obstante, aún se desconoce por diversas autoridades, según las observaciones registradas[8] en el transitar en las instituciones, esta demanda internacional, entre otros elementos asociados a la

6 Código III: Implantación de normas OMI por los Estados miembros.

7 La Resolución A.1070 (28), del 4 de diciembre de 2013, adoptó el Código para la implantación de los instrumentos de la OMI (Código III), y pidió tanto al Comité de seguridad marítima como al Comité de protección del medio marino que mantengan el código sometido a examen y, en coordinación con el Consejo, propongan a la Asamblea General del organismo enmiendas al mismo.

8 Registro del investigador en el cuaderno de campo, este es el instrumento de registro de datos propio del investigador llamado el "cuaderno de campo", donde se anotarán las observaciones (notas de campo) de forma completa, precisa y detallada (Amezcua 2000).

Depósito legal: PP201402DC4456
ISSN: 2343-6212

problemática de la gestión de la seguridad marítima que limitan la trascendencia del problema planteado hacia el Estado.

En atención a estas consideraciones, la administración marítima nacional, como órgano administrativo de gestión, representada por el INEA, operadores de buques y agentes navieros, deben asumir la responsabilidad de tomar las medidas pertinentes para salvaguardar el transporte marítimo y el puerto ante las amenazas de las tecnologías cibernéticas emergentes, así como, dar respuestas a los requerimientos de la OMI para el año 2021. Para ello, es necesario profundizar en el ámbito de las instituciones en la búsqueda de ese conocimiento implícito o explícito sobre la seguridad marítima en Venezuela como parte de la trama de la sociedad del riesgo en el escenario mundial.

En este orden de ideas, se formula el siguiente objetivo: Configurar los elementos teóricos de la gestión de la seguridad marítima en Venezuela como parte de la trama de la sociedad del riesgo en el contexto de la seguridad cibernética. Partiendo, como lo señala Argentina.gob.ar (s.f, párr.1) que la "vulnerabilidad generada por el acceso y la interconexión de redes entre estos sistemas da lugar a riesgos cibernéticos" y otras concepciones que deben abordarse profundamente. Representa además una exigencia del comité de facilitación FAL 28 de la OMI donde se solicita a los Estados miembros la incorporación al compendio sobre facilitación y transacción electrónica para alentar al uso de las nuevas tecnologías de la información (TI) y en particular, el intercambio electrónico de información para transmitir todo lo relacionado con el transporte marítimo, incluyendo el Intercambio Electrónico de Datos (EDI, siglas en inglés).

En consecuencia, en su 96º período de sesiones, el Comité de Seguridad Marítima (MSC) aprobó unas directrices provisionales sobre la gestión de los riesgos cibernéticos marítimos. En esta línea, esta investigación configura y profundiza las dimensiones teóricas de la gestión de la seguridad marítima en Venezuela como parte de la trama de la sociedad del riesgo en el contexto de la seguridad cibernética con el propósito de explicar la realidad del transporte marítimo de las vulnerabilidades y amenazas cibernéticas emergentes por el constante incremento del uso de tecnologías a bordo de los buques, y de los posibles ataques cibernéticos contra estos.

Aspectos metodológicos

Es necesario resaltar que se utilizó el análisis de contenido, como técnica de investigación en el análisis de datos secundario, siguiendo a Mayntz, Holm, y Hübner, (1980), es: "una técnica de investigación que identifica y describe de una manera objetiva y sistemática las propiedades lingüísticas de un texto con la finalidad de obtener conclusiones sobre las propiedades no-lingüísticas de las personas y los agregados sociales". (p. 198). El Análisis de Contenido, hace referencia a cualquier procedimiento ideado para examinar el contenido profundo y las ideas expresadas en uno o varios documentos, en este estudio los textos se representan bajo la figura de unidades documentales.

El análisis permitió así, dar significado a las categorías deductivas de esta investigación. Las categorías de análisis para Abbagnano (1994) Una categoría de análisis, es la "abstracción de una o varias características comunes de un grupo de objetos o situaciones, que permite clasificarlos (p. 112). Una vez clasificada la información, ésta se agrupa de acuerdo a su naturaleza y contenido. Inicialmente las categorías obtenidas son deductivas y estas proceden del análisis teórico

Depósito legal: PP201402DC4456
ISSN: 2343-6212

y bibliográfico efectuado durante la investigación.

Las categorías de análisis en este estudio se asumieron como aquellas que agruparon a elementos con características comunes, se les aplico un conjunto de criterios para la emisión de juicios de valor, tomando en cuenta, que se establecieron tres categorías a indagar: Por otra parte, las categorías inductivas se derivaron de los resultados obtenidos de unidades documentales, además de la experiencia del investigador como auditor de los sistemas de gestión de la seguridad marítima para construir la categorización y el análisis correspondiente a los datos. Hessen (1925), mencionando a Kulpe en relación a la producción de la categorías insiste que: "no sólo tiene parte el pensamiento, sino también la experiencia" (p. 131). En este caso, para el manejo eficiente de los datos cualitativos desde los 8 textos consultados que sirvieron para extraer los datos que permitieron construir los resultados.

Los datos cualitativos se consideraron relativos a "cualidades" y son subjetivos y no numéricos, por tanto , no se orientaron a datos medibles para formular hechos y descubrir patrones en la investigación. Destacándose que esta investigación no se enmarca dentro de la dicotomía investigación cualitativa o cuantitativa, por el contrario, se comparte con Monasterio (2016, p.62) cuando refiere los planteamientos de Hashimoto y Saavedra al señalan que la clasificación entre investigación cualitativa y cuantitativa se constituye en un error categorial, y agrega:

> … A juicio de la tradición Wittgensteniana los falsos problemas surgen cuando se intenta reducir una forma de descripción a otra, o también cuando se emplea el vocabulario mental en el contexto equivocado". Además, acotan que el significado léxico de "investigación cualitativa o investigación cuantitativa" "no tiene correspondencia de lo que sucede en la realidad, a lo que se realiza en la investigación científica, antes bien, dichos adjetivos son distorsiones del propio quehacer científico.

Una vez constituidos y ordenados los datos en forma coherente, se clasificaron por contenidos y aspectos recurrentes que fueron pertinentes para responder al objetivo del estudio.

Resultados

En este apartado se presentan los resultados encontrados y agrupados en tres categorías que explican la gestión de la seguridad marítima en el país en el entramado de la sociedad del riesgo y la seguridad cibernética.

Categoría 1. Marco Jurídico

De acuerdo al resultado obtenido en la investigación, la gestión de seguridad marítima ante las amenazas cibernéticas se concentra en el marco legal regulatorio de la República. Coincidentemente el marco jurídico es la primera categoría deductiva de este trabajo de investigación, y sobre este particular escasamente se contemplan en Venezuela la Ley Especial contra los Delitos Informáticos que tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas; también destaca la Ley de infogobierno, la cual tiene por objeto establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información, garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la Nación. No obstante, no existe aún legislación

para la privacidad y protección de datos ni un conjunto de normas apropiadas para la prevención de ataques cibernéticos en el territorio. (Gaceta Oficial de la República Bolivariana de Venezuela, 2001).

Asimismo, destaca Venezuela entre los países de la región que no se han adherido a la Convención de Budapest[9], que facilita la cooperación internacional en la lucha contra el crimen informático. Dada la naturaleza sin fronteras de las redes de información digital, el marco de cooperación internacional provisto por el Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa ofrece promover una política penal común contra el cibercrimen, brindando un marco común de legislación y cooperación internacional entre un grupo diverso de países, a objeto de utilizar un estándar legal óptimo para las diferentes legislaciones nacionales de los países que abordan el delito informático. De este modo, como se observa en la Figura 3, los marcos legales y regulatorios de cooperación formal e informal para combatir el delito cibernético son prácticamente inexistentes en Venezuela.

Por otro lado, en cuanto al sistema de justicia penal venezolano, este es muy limitado, y precariamente éste cuenta en las fuerzas del orden con la División de Investigación de Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC) como la única fuerza de seguridad que realiza investigaciones en materia de seguridad informática y cibercrimen (véase Figura 3). Los datos han sido tomados para ésta y sucesivas adaptaciones del reporte de indicadores en seguridad cibernética presentado por la Organización de Estados Americanos (OEA) del año 2020. Esta información se considera confiable, a pesar de que Venezuela solicitó su retiro formal de la Organización de Estados Americanos en el año 2017, hasta el 27 Abril del año 2019 no se formalizo su desincorporación, debiendo cumplir con lo establecido en el artículo 143 de la Carta de la OEA (1948)[10].

Al respecto, la Carta de la OEA (1948, s.p) por el que se rige el ente desde 1948, establece en su artículo 143 que: Esta Carta regirá indefinidamente, pero podrá ser denunciada por cualquiera de los Estados miembros, mediante comunicación escrita a la Secretaría General, la cual comunicará en cada caso a los demás las notificaciones de denuncia que reciba". Pasados dos años a partir de la fecha en que la "Secretaría General reciba una notificación de denuncia, la presente Carta cesará en sus efectos respecto del Estado denunciante, y éste quedará desligado de la Organización después de haber cumplido con las obligaciones emanadas de la presente Carta"

9 El Convenio sobre ciberdelincuencia o Convenio de Budapest es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes. El convenio fue aprobado por el Comité de Ministros del Consejo de Europa el 8 de noviembre de 2001 y entró en vigor el 1 de julio de 2004. Los siguientes delitos están definidos por el Convenio: acceso ilícito, interceptación ilícita, ataque a la integridad de datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática y fraude informático.

10 Carta de la Organización de los Estados Americanos (o simplemente Carta de la OEA) es un tratado interamericano que crea la Organización de los Estados Americanos. Fue firmada en la IX Conferencia Internacional Americana del 30 de abril de 1948, celebrada en Bogotá. Entrando en vigencia el 13 de diciembre de 1951.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Figura 3.- Indicador: Marco legal y Regulatorio en Venezuela para el año 2020

Fuente: Adaptación y elaboración propia, (2021) de los datos tomados de la Organización de Estados Americanos y el Banco Interamericano de Desarrollo,(2020). Reporte de Ciberseguridad 2020.

La norma jurídica es una prescripción concreta, es decir, una regla que ordena o prohíbe sucesos sociales, económicos, políticos y técnicos concretos y establece los efectos jurídicos del cumplimiento o incumplimiento de tales regulaciones. Una norma por amplia que sea se establece para un determinado número de hechos y actos. Para Navarro (1998) las normas, regulan hechos que pronto son superados por nuevas realidades, generalmente más complejas, se compone de una estructura proposicional, donde se encuentra un supuesto de hecho y un efecto o consecuencia jurídica. En el supuesto de hecho encontramos tipificado el hecho o fenómeno social al que el Derecho condiciona un efecto, consecuencia o solución jurídica. En el supuesto de hecho encontramos generalmente un sujeto o sujetos productores, realizadores o soportadores de las conductas o hechos que allí se tipifican. Ese hecho puede ser una conducta humana, un hecho de la naturaleza, la existencia de alguna

cosa (fáctica o jurídica) e incluso una creación o ficción jurídica.

Las normas tienen generalmente una eficacia directa, ellas vinculan directa e inmediatamente a los sujetos que se encuentran bajo los supuestos de hecho por ella establecidos. Las normas tienen el valor jurídico o rango que la fuente formal a la que pertenecen tiene, y este valor está determinado en primer lugar, por la distancia que con respecto de la Constitución tiene cada una de esas fuentes y en segundo lugar, por la resistencia de esa norma o frente a otras y por el poder que la misma norma tiene para imponerse a otras de inferior rango y fuerza. Tal es el caso de los convenios internacionales reconocidos por la República.

Categoría 2. Nivel de Organización

Los resultados del análisis demuestran que, de acuerdo a la Organización de Estados Americanos y el Banco Interamericano de Desarrollo (2020) por su siglas, OEA (Brasil, Colombia, Uruguay y México son los países de la región mejor dotados y organizados en defensa cibernética. Venezuela, de acuerdo con el documento, se encuentra entre los países que aún no dan cuenta de un progresivo desarrollo en cuanto al tema cibernético, además mantiene una muy baja o casi nula interrelación con los países de la región en ese particular. Sin embargo, en ese contexto, destaca el Plan de la Patria 2019-2025 que fue convertido en ley según Gaceta Oficial Nº 6.118 de fecha 4 de diciembre de 2013 y que contempla cinco grandes objetivos históricos entre los cuales destaca el objetivo de: Contribuir al desarrollo de una nueva Geopolítica Internacional en la cual tome cuerpo un mundo multicéntrico y pluripolar que permita lograr el equilibrio del Universo y garantizar la Paz planetaria. (Gaceta Oficial de la República Bolivariana de Venezuela, 2019).

En este sentido, los riesgos asociados con la falta de un mecanismo institucionalizado para compartir información sobre vulnerabilidades descubiertas y políticas sobre piratería ética, podrían verse agravados por la poca capacidad de respuesta interna, incluyendo organización de protección de infraestructura, gestión y manejo de crisis, gestión de riesgos y controles criptográficos, ubicados en la parte inferior de la Figura 4:

Figura 4.- Indicador: Nivel de Organización en Venezuela para el año 2020

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Fuente: Elaboración y adaptación propia, (2021). Datos tomados de Organización de Estados Americanos y el Banco Interamericano de Desarrollo (2020). Reporte de Ciberseguridad 2020.

Categoría 3. Formación, Capacitación y Entrenamiento

La formación es la tercera dimensión que componen estos resultados de la investigación y es el "entrenamiento" que da cuenta de un escaso o nulo avance en lo concerniente a la educación, capacitación y desarrollo de habilidades en ciberseguridad.

El Consejo Marítimo Internacional y del Báltico (BIMCO) ha publicado una Cláusula de seguridad cibernética que requiere que las partes firmantes en los contratos de flete implementen procedimientos y sistemas de seguridad cibernética para ayudar a reducir el riesgo comercial de incidentes y responder de manera eficiente si tales incidentes ocurrieran. Para dar cumplimiento a la cláusula, BIMCO reconoce que la formación es una medida clave de mitigación de riesgos; si se formalizan los requisitos de formación, deben incluirse soluciones pragmáticas para tener en cuenta la amenaza cibernética que cambia rápidamente.

Empresas privadas que operan en el sector marítimo han prioriza-

Depósito legal: PP201402DC4456
ISSN: 2343-6212

do la formación y capacitación en seguridad cibernética atendiendo los requerimiento de la Organización Marítima Internacional (OMI), entre estas se encuentra la naviera alemana Bernhard Schulte Shipmanagement (BSM)[11] del grupo Schulte por ejemplo, que ha iniciado la campaña "Conciencia sobre seguridad cibernética" y que tiene como propósito capacitar a los tripulantes ante amenazas de cib erseguridad. Con especial énfasis en el personal de gestión y de dirección. (Véase Figura 5).

Figura 5.- Indicador: Formación y Capacitación en Venezuela para el año 2020

Fuente: Adaptación y elaboración propia, (2021) de los datos tomados de la Organización de Estados Americanos y el Banco Interamericano de Desarrollo,(2020). Reporte de Ciberseguridad 2020.

11 Bernhard Schulte Shipmanagement (BSM) es un proveedor de soluciones marítimas integradas y uno de los principales gestores de buques del mundo en los sectores de gas, petroleros, offshore, contenedores, a granel y cruceros. BSM gestiona actualmente una flota de 400 embarcaciones en plena gestión y adicionalmente 200 solo en gestión de tripulaciones. Cuenta con su propio centro de formación en más de 30 ubicaciones con 18.000 marinos de todo el mundo.(Bernhard Schulte Shipmanagement, 2021).

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Ahora, en cuanto a la educación superior en ciberseguridad, se considera el Indicador: Formación y Capacitación en Venezuela para el año 2020, algunas instituciones del país que ofrecen su apoyo en una variedad de programas, desde la provisión de preparación de seguridad tecnológica hasta el nivel de estudios superiores. Una muestra de ello es la Universidad Nacional Experimental Marítima del Caribe (UMC), creada según Gaceta Oficial de la República Bolivariana de Venezuela, (2000), se encuentra ubicada en la ciudad Catia La Mar, Edo. La Guaira. Está adscrita al Ministerio del Poder Popular para la Educación Universitaria, Ciencia y Tecnología, y entre sus orientaciones y objetivos destaca en su reglamento interno el Artículo 9 numeral 7, referido a "promover la protección y mejoramiento del ambiente marino y la seguridad marítima, para coadyuvar al ejercicio óptimo de la Administración Marítima Venezolana" y el numeral 9, que establece "promover el desarrollo tecnológico en todos los ámbitos de su competencia orientados a la solución de los problemas del sector marítimo en el país". (Gaceta Oficial de la República Bolivariana de Venezuela, 2014, p.630).

Según Drucker, (1969) la formación se refiere a una nueva sociedad del conocimiento, en la que las nuevas formas de producción están directamente vinculadas a la formación del individuo en su oficio. Tanto la organización como el individuo son mutuamente dependientes, por lo que existe una necesidad en su preparación. En una economía basada en el conocimiento, donde la tecnología cambia vertiginosamente, la seguridad en todos los aspectos viene de la capacidad de aprender con agilidad y tener una buena base intelectual. Sobre ese particular, el subcomité de factor humano, formación y guardia (HTW, en inglés) que asiste directamente al Comité de Seguridad Marítima (MSC) de la Organización Marítima Internacional, implantó en 1978 el Convenio internacional sobre normas de formación, certificación y guardia para la gente de mar (Standards of Training, Certfication, and Watchkeeping, en inglés) en lo sucesivo STCW 78[12]. Al respecto, la Organización Marítima Internacional (s.a) señala que el "Convenio prescribe normas mínimas relativas a la formación, la titulación y la guardia para la gente de mar que los países están obligados a cumplir o superar" (s.p).

Asimismo, con el paso del tiempo, van apareciendo cambios en variados aspectos del mundo marítimo, a veces de orden tecnológico, en la operación de los buques, de carácter jurídico y de exigencias medioambientales, por lo que, en general, el convenio ha sufrido algunas enmiendas en su texto para acomodarlo a una realidad diferente de la que existía cuando inicialmente se adoptó. Ejemplo de ello son las enmiendas del año 1995 y la segunda implantada en el año 2010 en Manila, capital de Filipinas.

En la Ley Orgánica de los Espacios Acuáticos en Gaceta Oficial de la República Bolivariana de Venezuela (2014), refiere en su Artículo 74 sobre el ejercicio de la administración acuática, el numeral 2 indica que debe "Coadyuvar y supervisar la formación y capacitación del personal de la marina mercante". Señala además que a través de un órgano asesor como el Consejo

12 Una característica especialmente importante de la Convención STCW es que aplica a barcos de Estados no miembros cuando estos visitan puertos de Estados miembros de la convención. El convenio ha tenido una aceptación muy amplia. En 2014, la convención STCW fue suscrita por 161 países, que representan el 98.8 por ciento de las naciones del mundo. (Fairplay.IHS and BIMCO, 2017).

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Nacional de los Espacios Acuáticos según el Artículo 81 se debe fomentar y desarrollar entre otros aspectos la investigación científica y tecnológica del sector acuático, la formación, capacitación, actualización y certificación del talento humano de dicho sector.

Conclusiones

En cuanto a los elementos complejos que afronta la gestión de la seguridad marítima en Venezuela como parte de la trama de la sociedad de riesgo en el escenario de la ciberseguridad, se determinó que dada la naturaleza sin fronteras en el intercambio electrónico de datos, el marco de cooperación internacional provisto por el Convenio de Budapest sobre Ciberdelincuencia representa la oportunidad idónea de utilizar un estándar legal óptimo para las diferentes legislaciones nacionales que abordan el delito informático. La estabilidad cibernética global se basa en la capacidad local y nacional para prevenir y reaccionar ante incidentes cibernéticos e investigar y procesar casos de delitos cibernéticos.

Se demanda en Venezuela construir una mayor autonomía estratégica, aumentar las capacidades en términos de tecnología y habilidades, conformar un mercado fuerte para la seguridad cibernética, y desarrollar e implementar un enfoque integral para la ciberdiplomacia[13] a nivel mundial. Para "La diplomacia digital, también conocida como Digiplomacia y eDiplomacia (ver más abajo), se ha definido como el uso de Internet y las nuevas tecnologías de la información y comunicación para ayudar a lograr los objetivos diplomáticos" (Frantz Ryan, 2014, s.p).

En Venezuela, la oferta de formación especializada en seguridad digital es inexistente o tiene carácter de incipiente, y usualmente se considera sólo la extensión técnica de la ciberseguridad. Estos resultados nos invitan a repensar las estrategias que deberían adoptarse en el sector público y privado, junto con la promoción de mecanismos de cooperación internacional, tanto a nivel regional como subregional.

Por tanto, contar con profesionales más capacitados se ha tornado fundamental para diseñar e implementar políticas y medidas de seguridad cibernética que son necesarias para garantizar la resiliencia del país frente a ciberataques cada vez más sofisticados y complejos. Los resultados que se revelan invitan a repensar las estrategias que deberían adoptarse en las organizaciones públicas y privadas para mejorar y sensibilizar la concepción de la formación y la capacitación como un medio idóneo para responder a las necesidades de protección cibernética.

Finalmente, para contrarrestar las amenazas cibernéticas en rápida evolución, se debe contar con políticas de gestión, legislación y capacitación, resiliencia nacional, así como con equipos de respuesta a emergencias informáticas y unidades de ciberdelincuencia. La estrategia nacional de seguridad cibernética marítima debe contemplar el establecimiento de alianzas estratégicas entre el sector público y privado, con el propósito de fortalecer la cooperación y sincronizar los esfuerzos para dar respuesta a los incidentes que se produzcan en materia de seguridad cibernética.

---

13 La diplomacia digital , también conocida como Digiplomacia y eDiplomacia , se ha definido como el uso de Internet y las nuevas tecnologías de la información y comunicación para ayudar a lograr los objetivos diplomáticos. La ciberdiplomacia es la evolución de la diplomacia pública para incluir y utilizar las nuevas plataformas de comunicación en el siglo XXI. La ciberdiplomacia "vincula el impacto de las innovaciones en la tecnología de la información y la comunicación con la diplomacia". También se conoce como parte de la diplomacia pública 2.0 , la diplomacia electrónica y la diplomacia virtual. Tiene como fundamento que "reconoce que las nuevas tecnologías de la comunicación ofrecen nuevas oportunidades para interactuar con un público más amplio adoptando un enfoque de red y aprovechando al máximo un sistema interdependiente global. (véase en Artículo Ciber Diplomacia en Estados Unidos, s.f).)

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Referencias

Argentina.gob.ar.(s.f) Recomendación para la gestión de los riesgos cibernéticos marítimos. Recuperado en: https://www.argentina.gob.ar/prefecturanaval/seguridadnavegacion/buques/recomendacion-riesgos-ciberneticos-maritimos[Artículo Ciber Diplomacia en Estados Unidos]. (s.f). Recuperado en:https://hmong.es/wiki/United_States_cyber-diplomacy#tit

Abbagnano, N. (1994). Historia de la Filosofía. 4ta. Edición, Barcelona España.

Asociación Peruana de Agentes Marítimos. (2019) OMI: Promociona Comercio Electrónico – Intercambio Electrónico de Información. Recuperado en: https://apam-peru.com/web/

Bernhard Schulte Shipmanagement (2021). Un océano de experiencia. Recuperado en: https://www-bs--shipmanagement-com.translate.goog/en/services?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

Carta de la Organización de los Estados Americanos. (1948). Bogotá, Colombia, 30 de Abril. Recuperado en: https://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_A-41_carta_OEA.pdf.

Comisión Económica para América Latina y el Caribe. (2020). La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. Boletín FAL No 382. Boletín FAL No 382. Recuperado en: https://repositorio.cepal.org/bitstream/handle/11362/46275/1/S2000679_es.pdf.

Constitución de la República Bolivariana de Venezuela (2000). Gaceta Oficial Nº 5.453. Extraordinario .

De Izcue Arnillas. C.; Arriarán Schäffer A. y Tolmos Mantilla Y. (2012). Apuntes de estrategia naval. Editada por la Oficina de Desarrollo Bibliográfico de la Marina. Recuperado en: http://virtual.esup.edu.pe/bitstream/ESUP/33/1/Apuntes%20Estrategia%20Naval.pdf.

Drucker, P. (1969). La Sociedad del Conocimiento. Barcelona, España: Editorial Sudamericana S.A.

Federal Bureau of Investigation. (2020). Internet Crime Report. Department of Justice, USA. Recuperado en: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Frantz, D. y Ryan, E. (2014). Diplomacia digital: hacer que la política exterior sea menos extranjera. Videoconferencia digital, el 18 de febrero de 2014. Moderado por Emily Parker, New York City. Recuperado en: https://hmong.es/wiki/EDiplomacy.

Gaceta Oficial de la República Bolivariana de Venezuela (2001). Ley Especial Contra los Delitos Informáticos. No. 37.313 del 30 Octubre. Recuperado en: http://www.conatel.gob.ve/ley-especial-contra-los-delitos-informaticos-2/

Gaceta Oficial de la República Bolivariana de Venezuela (2002). Ley general de marina y actividades conexas .Caracas 14 noviembre de 2002. N° 37.570.Recuperado en:http://www.bolipuertos.gob.ve/descargas/G.O%20N%C2%BA%2037.570%0Ley%20General%20de20Marinas20y20Actividades20Conexas.pdf.

Gaceta Oficial de la República Bolivariana de Venezuela (2008). Ley de Simplificación de Trámites Administrativos. No. 38.984 del 31 Julio. Decreto N° 6265 con Rango, Valor y Fuerza de Ley. Recuperado en: http://www.onapre.gob.ve/index.php/publicaciones/descargas/finish/38-ley-de-simplificacion-de-tramites-administrativos/204-ley-de-simplificacion-de-tramites-administrativos.

Gaceta Oficial de la República Bolivariana de Venezuela (2012). Ley sobre Acceso e Intercambio electrónico de datos entre los Órganos y entes del Estado. Gaceta Oficial No. 39.945 de 15 de Junio 2012. Decreto N° 9.051 con Rango, Valor y Fuerza de Ley. Recuperado en: https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/ve_1170.pdf

Gaceta Oficial de la República Bolivariana de Venezuela (2013). Ley de infogobierno. Gaceta Oficial No. 40.274 de 17 de Octubre 2013. Recuperado en:https://dhqrdotme.files.wordpress.com/2013/02/ley-de-infogobierno.pdf

Gaceta Oficial de la República Bolivariana de Venezuela (2014). Ley Orgánica de los Espacios Acuáticos (2014). Gaceta Oficial No. 6.153 Extraordinario, de 18 de noviembre de 2014. Decreto No. 1.446, de 17 de noviembre de 2014. Recuperado en: https://www.un.org/Depts/los/LEGISLATIONANDTREATIES/PDFFILES/Ley_Org%C3%A1nica_de_los_Espacios_Acuaticos%202014.pdf.

Gaceta Oficial de la República Bolivariana de Venezuela (2019). Proyecto Nacional Simón Bolívar, Tercer Plan Socialista de Desarrollo Económico y Social de la Nación 2019-2025. Hacia la Prosperidad Económica AÑO CXLVI - MES VI. Caracas, lunes 9 de abril de 2019 N° 6.446 Extraordinario. Recuperado en: https://pandectasdigital.blogspot.com/2019/04/proyecto-nacional-simon-bolivar-tercer.html.

Gaceta Oficial de la República Bolivariana de Venezuela. (2017). Ministerio del Poder Popular para Relaciones Exteriores. Memorando de Entendimiento entre la República Bolivariana de Venezuela y la Organización Marítima Internacional (OMI) sobre la Participación en el Plan de Auditorías de los Estados Miembros de la OMI. Caracas, viernes 9 de Junio de 2017. Número 41.169.En: https://www.ghm.com.ve/wp-content/uploads/2017/06/41169.pdf.

Gaceta Oficial de la República Bolivariana de Venezuela, (2014). Ministerio del Poder Popular para la Educación Universitaria. Reglamento General de la Universidad Nacional Experimental Marítima del Caribe (UMC) Caracas, 1 de diciembre. Nº 40.487. Recuperado en http://www.umc.edu.ve/pdf/reglamentos/Reglamento%20General%20UMC.pdf.

Gaceta Oficial de la República Bolivariana de Venezuela. (2000). Caracas, 7 de julio. Nº 36.988. Recuperado en: http://www.mpppst.gob.ve/mpppstweb/wp-content/uploads/2016/08/2000_Decreto892.pdf

Gaceta Oficial de la República Bolivariana de Venezuela. (2001). Ley Especial contra los Delitos Informáticos. Nº 37.313. Caracas, 30 de octubre de 2001. Recuperado en: https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Gutierrez, D. (2018). Qué es la convención STCW? Diario Oficial

Depósito legal: PP201402DC4456
ISSN: 2343-6212

de la Federación. Recuperado en: https://sites.google.com/site/elrincondelnautico/home/que-es-la-convencion-stcw.

Hessen, J. (1925). Teoría del Conocimiento. Caracas, Venezuela: Ediciones ERA-LUZ.

IHS and BIMCO. (2017). Cyber security survey in association with BIMCO. Fairplay.IHS.com www.maritime.IHS.com Integrando el poder de Seaweb y AISLive. Recuperado en: https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf

Mayntz, R.; Holm, K. y Hübner, P. (1980). Introducción a los Métodos de la Sociología Empírica. Madrid: Alianza Editorial. Recuperado en: http://www.trabajosocial.unlp.edu.ar/uploads/docs/mayntz__holm_y_hubner__introduccion_a_los_metodos_de_la_sociologia_empirica_.pdf.

Mayntz, R., Holm, K. y Hübner, P. (1980). Introducción a los Métodos de la Sociología Empírica. Madrid: Alianza Editorial. Recuperado en: http://www.trabajosocial.unlp.edu.ar/uploads/docs/mayntz__holm_y_hubner__introduccion_a_los_metodos_de_la_sociologia_empirica_.pdf.

Monasterio, D. (2016). El Desarrollo Local desde las Lógicas complementarias en el Municipio Páez del Estado Miranda. Trabajo de ascenso no publicado). UNEFA, Caracas. Venezuela.

Navarro, R. (1998). Los Principios Jurídicos. Estructura, Caracteres y Aplicación en el Derecho. Universidad para la Cooperación Internacional. [Archivo PDF].

Organización de Estados Americanos y el Banco Interamericano de Desarrollo (2020). Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe. Recuperado en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Organización Marítima Internacional.(s.a). Convenio internacional para la seguridad de la vida humana en el mar, 1974 (Convenio SOLAS). Recuperado en: https://www.imo.org/es/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS)%2C-1974.aspx

Organización Marítima Internacional. (s.f). Convenio internacional sobre normas de formación, titulación y guardia para la gente de mar (STCW). Recuperado en: https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Conv-LINK.aspx

Organización Marítima Internacional. (s.f). El Código PBIP y el capítulo XI -2 del Convenio SOLAS. Recuperado en: https://www.imo.org/es/OurWork/Security/Paginas/SOLAS-XI-2%20ISPS%20Code.aspx

República de Venezuela. (1982). Ley Aprobatoria del Convenio de Seguridad de la Vida Humana en el Mar. Gaceta Oficial Nº 32.597 del 08-11-1982.

Rodríguez, Ruiz, H. (2016) Seguridad integral marítima, retos y amenazas. Escuela Superior de Guerra de Colombia. Recuperado en: https://issuu.com/estrategia-maritima/docs/seguridad_mar__tima_retos_y_amenaza