Universitat Abat Oliba CEU

Ciber Riesgo: el gran excluido del Derecho Marítimo

TRABAJO FIN DE MASTER

Autor: Yolanda María Pifarré Rivadulla

Tutor: Iñaki Zurutuza Arigita

Máster Universitario en: Derecho Marítimo

Año: 2023

DECLARACIÓN

El que suscribe declara que el material de este documento, que ahora presento, es fruto de mi propio trabajo. Cualquier ayuda recibida de otros ha sido citada y reconocida dentro de este documento. Hago esta declaración en el conocimiento de que un incumplimiento de las normas relativas a la presentación de trabajos puede llevar a graves consecuencias. Soy consciente de que el documento no será aceptado a menos que esta declaración haya sido entregada junto al mismo.

Firma: ……
Nombre y APELLIDOS (del alumno/a)
Yolanda María Pifarré Rivadulla

Todo es navegar, todo es una continuada lucha,
(…) arte y valor para no ahogarse

BENITO PÉREZ GALDÓS

A mi madre,
por luchar conmigo.

Resumen

El contrato de seguro constituye uno de los pilares básicos de la estabilidad socio económica global y desde su creación ha ido adaptándose a los acontecimientos históricos, no obstante, dentro del sector marítimo cuesta tomar conciencia sobre la importancia de los ciberataques.

Por ello, el presente trabajo se centra en los seguros marítimos y en saber por qué las aseguradoras no cubren los ciberataques, dirimir la responsabilidad de las partes y liberar de las navieras de no poder ser aseguradas. Además, se citan los criterios para que un buque pueda ser asegurado con la propuesta innovadora de una cláusula estándar que cubra el ciberriesgo: un buque ciberasegurado.

Resum

El Contracte d'assegurances constitueix un dels pilars bàsics de l'estabilitat social econòmica global i des de la seva creació ha anat adaptant-se als esdeveniments històrics, no obstant això, dins del sector marítim costa prendre consciència sobre la importància dels ciberatacs.

Per això, el present treball se centra en les assegurances marítimes i en saber perquè les asseguradores no cobreixen els ciberatacs, dirimir la responsabilitat de les parts i alliberar a les navieres de no poder ser assegurades. A més a més, es nomenen els criteris perquè un vaixell pugui ser assegurat gràcies a la proposta innovadora d'una clausula estàndard que cobreixi el ciberrisc: un vaixell ciberassegurat.

Abstract

The insurance contract constitutes one of the basic pillars of global socio-economic stability and since its creation it has been adapting to historical events, however, within the maritime sector it is difficult to become aware of the importance of cyber-attacks.

For this reason, the present work focuses on maritime insurance and the reasons why insurers do not cover cyber-attacks, settle the responsibility of the parties and free shipping companies from not being able to be insured. In addition, the criteria for a ship to be insurable under the innovative proposal for a standard clause covering cyber risk are cited: a cyber insured ship.

Palabras claves / *Keywords*

Seguro Marítimo – Ciberataque –– Propuesta innovadora – Seguro cibernético

Sumario

INTRODUCCIÓN 11
I. EL RIESGO CIBERNÉTICO EN LA INDUSTRIA MARÍTIMA 13
1. Importancia de la ciberseguridad 13
2. De qué manera son vulnerables los buques 17
2.1. Documentación de sistemas IT y OT 18
2.2. Sistemas típicamente vulnerables 18
3. Ataques cibernéticos más usuales en el sector marítimo 20
3.1. Ataques cibernéticos vía ramsomware 21
3.2. Ataques cibernéticos vía phishing y spear phishing 22
3.3. Ataques cibernéticos vía malware para manipular datos de la navegación 23
4. Panorama general del mercado de seguros cibernéticos 24
II. EL CONTRATO DE SEGURO MARÍTIMO 27
1. Características del contrato 27
2. Elementos del contrato de seguro marítimo 29
2.1. Elementos subjetivos 29
2.2. Elementos objetivos o reales 30
3. Elementos formales 32
4. Liquidación del siniestro 33
5. Tipología del contrato de seguro marítimo 34
5.1. Seguro de buques 34
5.2. Seguro de mercancías 35
5.3. Seguro de responsabilidad civil 35
III. PROBLEMAS JURÍDICOS DEL SEGURO DE RIESGO CIBERNÉTICO 37
1. Cobertura del riesgo cibernético 37
1.1. Cobertura cibernética silenciosa (no afirmativa). 39
2. Ciberexclusiones 40
4. Intentos legislativos para abordar las cuestiones legales del riesgo cibernético 44
IV. PROPUESTA INNOVADORA DE UNA CLÁUSULA ESTÁNDAR QUE CUBRA EL RIESGO CIBERNÉTICO 47
1. Cláusula previa sobre exigencias de Ciberseguridad 47
2. Cláusula de cobertura del riesgo cibernético en el contrato de seguro marítimo 49
V. CONCLUSIONES 52
VI. BIBLIOGRAFÍA 58

1. Doctrina 58
2. Referencias bibliográficas web 59
3. Listado legislativo 65
4. Listado jurisprudencial 66

INTRODUCCIÓN

La elección del presente tema de estudio viene motivada por la inminente necesidad de modernización que presenta el sector marítimo. Especialmente, sobre la figura del seguro en atención a los riesgos cibernéticos.

Actualización necesaria para salvaguardar la seguridad de los agentes intervinientes en la cadena logística marítima, ya que actualmente están indefensos en el ciberespacio. Indefensión provocada por la falta de actualización del sector en sus prácticas laborales, en su esfera comercial y, sobre todo, en su seguridad.

A juicio de los profesionales que trabajan en la industria marítima, el seguro marítimo es considerado como un seguro eficiente que protege a los asegurados ante los riesgos más relevantes que pueden sufrir en este transporte. No obstante, nada les protege de los riesgos cibernéticos. De forma sencilla podemos asimilarlo a una cadena de engranajes, los profesionales del sector marítimo no realizan mejoras en sus sistemas de ciberseguridad y, en consecuencia, los aseguradores no quieren asegurarles.

"Ciber Riesgo: el gran excluido del Derecho Marítimo" pretende dar a conocer la imperiosa necesidad del sector a adaptarse a los nuevos tiempos. Propone, en última instancia, una cláusula estándar que dé cobertura al riesgo cibernético y pueda ser incorporada en cualquier seguro marítimo tradicional.

Como a nivel global no existe ninguna cláusula estándar que regule el riesgo cibernético y que pueda incorporarse en una póliza de seguro marítimo, se estudia también la influencia del Derecho Marítimo Inglés sobre el contrato de seguro marítimo español, con la intención de poder aplicar los criterios que brinda el Derecho Anglosajón.

Pasando a analizar la estructura del trabajo, en primer lugar, se presentan las razones por las que la ciberseguridad comienza a ganar interés en el Derecho Marítimo. A continuación, se estudian las vulnerabilidades cibernéticas que tienen los buques. Estudio necesario para comprender la razón de ser de los ciberseguros.

Seguidamente, con el fin de plasmar la urgente necesidad de poder contar con una cobertura que cubra el riesgo cibernético, se presentan los ciberataques más relevantes que el sector ha sufrido hasta la fecha. Tras ello, se estudia el grado de importancia que se le otorga al ciberseguro en la actualidad del sector marítimo.

El siguiente apartado es inminentemente teórico pues estudia el contrato de seguro marítimo en la legislación española y sus características esenciales, influenciadas por el Derecho Marítimo Inglés.

Como núcleo del presente Trabajo Final de Máster (en adelante, TFM) se sitúan los tres capítulos que prosiguen. El primer capítulo realiza un estudio sobre los problemas jurídicos que se enfrentaría un seguro que cubriese el riesgo cibernético en el sector marítimo. Además, se tratan las barreras con las que se toparían los aseguradores si cubriesen un riesgo de esta tipología. Además, se mencionan las distintas cláusulas de exclusión de cobertura por siniestros causados a causa de ataques cibernéticos y los intentos legislativos para abordar las cuestiones legales del riesgo cibernético en los seguros marítimos.

Por último, se crea la primera propuesta de una cláusula estándar que cubra los ataques cibernéticos en el contrato de seguro marítimo ya que, por el momento, no existe una cláusula que le dé cobertura. En consecuencia, de forma detallada, dentro del canon que permite el formato de un TFM, se realiza una propuesta innovadora de una cláusula estándar que cubra el riesgo cibernético en los diversos contratos de seguros marítimos tradicionales.

Para ello, con anterioridad a la misma, se elabora una cláusula de ciberseguridad con las obligaciones que debe cumplir el asegurado para que la cobertura que ofrece la cláusula que cubre el ciberataque pueda llevarse a cabo. Ya que la intención final del presente trabajo es la posible aplicación práctica de la cláusula en un contrato de seguro marítimo, de forma que se centra en elaborar una cláusula con un riesgo equilibrado entre asegurador y asegurado para poder brindar al sector de una protección eficaz y posible.

El trabajo finaliza con un listado de conclusiones fruto de un análisis global de la institución del seguro marítimo, el riesgo cibernético y el conjunto de problemáticas legislativas planteadas. En función de su objetivo, el presente TFM es un trabajo de documentación realizado a través de una metodología de búsqueda pura. Sobre la propuesta de la cláusula estándar que cubre el riesgo cibernético se lleva a cabo una metodología científico-analítica.

I. EL RIESGO CIBERNÉTICO EN LA INDUSTRIA MARÍTIMA

1. Importancia de la ciberseguridad

La ciberseguridad marítima es de vital importancia para una correcta circulación de personas y mercancías. Es notorio que la industria marítima sustenta la economía mundial y es la vía más utilizada para transportar la mayor parte de alimentos, medicamentos y energía (Comisión Europea, 2023).

En esta tesitura, la United Nations Conference on Trade and Development (2021) (en adelante, UNCTAD) afirma que más del 80% de los bienes que consumimos se transportan a través de este medio de transporte.

Prueba de la relevancia de la industria marítima es el notorio crecimiento que ha sufrido en los últimos 25 años, a nivel mundial las toneladas de mercancía transportadas por mar se han visto incrementadas en un 2,9% (UNCTAD, 2021).

Desgraciadamente, la creciente digitalización y automatización en todos los sectores y los esfuerzos por encontrar el justo equilibrio entre seguridad y rapidez empiezan a convertirse en una tarea peliaguda para la industria marítima. Ésta se caracteriza por ser reticente a modernizarse por lo que no se adecua con rapidez a los nuevos tiempos. Bajo esta idea Crawford (2019) sustenta la razón por la que la protección cibernética de la industria marítima queda obsoleta frente a los nuevos riesgos cibernéticos.

Así, Det Norske Veritas group [DNV] (2023) explica que a medida que el sector marítimo depende cada vez más de las nuevas tecnologías, también aumentan las vulnerabilidades cibernéticas y las posibilidades de ser víctimas de un ciberataque.

La marea de transformación digital que gobierna este siglo provoca que el mundo empresarial se enfrente a nuevos retos que exigen una visión global de todos los sectores (European Union Agency for Cibersecurity [ENISA], 2020). Dicha transformación se puede resumir en integrar la tecnología en todos los aspectos y elementos de cualquier modelo de negocio (International Association of Classification Societies [IACS], 2020, 3).

Partiendo de la base que el sector marítimo es sin duda un sector clave para el futuro de la economía global, es preciso entender que la seguridad y estabilidad del comercio mundial depende en gran medida, de él. Por ello, son necesarias inversiones que se centren en mejorar la protección del sector para que alcance la actualización necesaria frente a los nuevos riesgos cibernéticos (Comisión Europea, 2023).

Antonio Guterres, en calidad de secretario general de la Organización Nacional de Naciones Unidas (en adelante, ONU), reconoció en febrero de 2018 que se espera un aumento de ataques y guerras cibernéticas que enfrentarán a Estados y Gobiernos (Crawford, 2019).

En este sentido, cabe preguntar, ¿Cuántas industrias siguen con el mismo proyecto de trabajo desde hace más de 4 siglos?

A pesar que nos encontremos en la era de la tecnología y tengamos a mano las últimas novedades digitales, el seguro marítimo, una institución clave para la estabilidad del comercio global, sigue siendo una industria vetusta basada en los hábitos analógicos. Por tanto, pocos son los recursos disponibles para mitigar la responsabilidad frente a los ciberataques y la fricción que puede provocar en el comercio mundial (ENISA, 2020).

Sin embargo, el sector sí ha sabido adaptarse a los avances tecnológicos relacionados con la comunicación e interconexión entre las empresas del sector (IACS, 2020). Por contra, no ha sabido adaptarse al progreso que han sufrido los sistemas de seguridad y protección provocando brechas franqueables en sus sistemas y, en consecuencia, publicitándose como víctimas posibles de ser atacadas (ENISA, 2020).

Gürses (2023) explica que los aseguradores están realizando intentos por adecuarse a las nuevas necesidades propiciadas por el sector, pero por falta de adecuación de las empresas y de cláusulas reguladoras del riesgo cibernético, los aseguradores son reticentes a incorporar el riesgo cibernético en la cobertura de los seguros marítimos. La práctica usual tal y como plasma Fotinopoulou Basurko (2017) es incorporar el riesgo cibernético en el clausulado de sus pólizas como exclusión a través de la famosa cláusula CL380, entre otras. Estas exclusiones se explican en el capítulo III del presente trabajo, al cual me remito para su estudio.

Por su parte, la Comisión Europea (2023), tras el alarmante aumento de ciberataques en los últimos años, plasma su preocupación sobre la inexistencia de protección del riesgo cibernético en el sector. Siete de las navieras más prestigiosas del sector ya han sido víctimas de ciberataque, entre ellas A.P. Møller-Mærsk (Møller-Mærsk, 2017) y Mediterranean Shipping Company (Mediterranean Shipping Company [MSC], 2020).

A pesar que solo se conocen aquellos ciberataques publicitados por las víctimas, ya que muchas empresas optan por gestionar el ciberataque de forma interna, sin publicitarlo, por miedo a la posible pérdida de potenciales clientes (DNV, 2023). Por

tanto, en el mundo se han producido aún más ciberataques de los que se tienen constancia.

Sobre la importancia de la ciberseguridad se pronuncia la Comisión Europea (2023) en su Estrategia de Seguridad Marítima de la UE (p. 2) estableciendo que los riesgos cibernéticos deben ser identificados, evitados, analizados y mitigados con el fin de proteger el colapso de la economía mundial.

Como cita Baltic and International Maritime Council, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners, InterManager, International Association of Independent Tanker Owners, International Chamber of Shipping, International Union of Marine Insurance, Oil Companies International Marine Forum, Superyacht Builders Association y World Shipping Council (2023) (en adelante, BIMCO et.al.) los ciberataques pueden llegar incluso a afectar los sistemas de navegabilidad del buque y dejarlo a la deriva (p.14).

En resumidas cuentas, la columna vertebral de toda empresa marítima debe ser un proyecto de seguridad basado en la prevención, detección y gestión del riesgo cibernético. La Resolución MSC 428 (98) Gestión del riesgo cibernético marítimo en los sistemas de gestión de la seguridad, de 16 de junio de 2017, hecha por la *International Maritime Organization* (en adelante, IMO), advierte de la importancia de poder contar con un protocolo de ciberseguridad eficaz y critica la falta de conocimiento de las empresas del sector marítimo. La industria marítima no está preparada para poder hacer frente a los ataques cibernéticos.

Pues bien, después de todo lo expuesto es necesario definir qué se entiende por riesgo cibernético. Según la IMO (2023) el riesgo cibernético es el siniestro ocasionado en un activo tecnológico que genera la pérdida de datos empresariales, fallos en la logística operacional o una brecha en el sistema de seguridad.

Por consiguiente, el objetivo de la ciberseguridad según DNV (2023) es mantener a salvo la seguridad del sector en el ciberespacio. Para ello deben emplearse instrumentos digitales como *firewalls*, programas de encriptación de datos y programas de detección de intrusos en el sistema.

De ahí las enmiendas elaboradas por la IMO al Convenio Internacional para la Seguridad de la Vida Humana en el Mar, hecho en Londres el 1 de noviembre de 1974 para abordar la ciberseguridad en los buques, establezcan nuevos requisitos de ciberseguridad y hayan generado la creación de estándares de buenas prácticas sobre cómo el sector marítimo puede protegerse ante los ciberataques.

En definitiva, los últimos ciberataques demuestran la urgente necesidad de que la industria se adapte a las actualizaciones de ciberseguridad en todos sus ámbitos y, evidentemente, tal y como explica la IMO (2023) también en la parte que corresponde al seguro marítimo. Una brecha en uno de los engranajes puede generar la vulnerabilidad de toda la cadena.

El sector marítimo utiliza el contrato de seguro para protegerse económicamente ante un riesgo. Así, la importancia del seguro marítimo dentro del sector es manifiesta, su finalidad es la protección tanto del buque, de la mercancía que transporta éste y de liberar de responsabilidad a los profesionales durante el trayecto.

Dicho esto, es oportuno comentar las cuestiones que se suscitaron en la Cámara Marítima Internacional, reunida el 21 de febrero de 2021, en torno a los desafíos que presentan los riesgos cibernéticos en el sector marítimo (Mundo Marítimo, 2021).

Con el propósito de criticar la inexistencia de una cobertura en el contrato de seguro marítimo que proteja al riesgo cibernético y enfatizar la necesidad de su creación, expusieron los conflictos de diligencia debida que podrían ocasionarse en un seguro que no cubra el riesgo cibernético.

A título de ejemplo, crearon una situación hipotética en la que, por culpa del propio sistema de un buque de nueva construcción, dicho buque sea víctima de un ciberataque. En este sentido, se debatió sobre cuál sería la esfera de diligencia del responsable y si se tratase del propietario, cuales serían sus obligaciones (Mundo Marítimo, 2021).

Como actualmente no se puede dar respuesta a la pregunta anterior, únicamente pudieron estar de acuerdo en que para llegar a una solución justa es necesaria una conducta proactiva del legislador y de los profesionales del sector para poder mejorar los conocimientos tecnológicos en todos los aspectos del mundo marítimo (Mundo Marítimo, 2021).

En este sentido, Soyer (2018) establece que la velocidad con la que surgen nuevos conflictos cibernéticos en la vida real es superior a la rapidez con la que los altos legisladores dan respuesta a los mismos.

A continuación, en los siguientes apartados se realiza un estudio sobre el impacto que la digitalización ha provocado en el sector marítimo a través de sus nuevas vulnerabilidades en el aspecto de la seguridad en el ciberespacio, los sistemas y programas que integran actualmente un buque y la recopilación sobre los ataques cibernéticos más relevantes que ha sufrido el sector hasta la fecha.

2. De qué manera son vulnerables los buques

La logística de la industria marítima siempre se ha caracterizado por ser compleja. Sin embargo, tras la incorporación de los activos tecnológicos, las operaciones marítimas se han convertido en un entramado de conexiones con elementos distintos que deben funcionar a la perfección para su correcto desarrollo. Para ello se utilizan programas informáticos, activos fijos, tecnológicos, de comunicación y, por último, de carga. (Pawelski, 2023).

En este sentido, la hiperconexión entre los elementos que configuran el sector marítimo es una realidad. Esta hiperconexión ha generado que pueda surgir una automatización de ciertas operaciones. Sin embargo, como ha sido comentado con anterioridad en el presente trabajo, mientras se ha avanzado mucho en la digitalización de varios aspectos del sector, se ha dejado de lado el más importante, relativo a la ciberseguridad (BIMCO et.al., 2023).

En consecuencia, la digitalización y la automatización provocan una exposición mayor a los ciberataques y, por tanto, generan vulnerabilidades en la cadena logística (Subero, 2019). Por consiguiente, se citar cuáles son actualmente las vulnerabilidades cibernéticas de los buques y los buques de nueva construcción (BIMCO et. al., 2023):

- Sistemas operativos no compatibles y obsoletos (IACS, 2020, 6).
- Sistemas con *software* sin parches y con brechas (DNV, 2023).
- Antivirus o *sofwares* contra programas maliciosos obsoletos o directamente, inexistentes (IMO, 2023, 5).
- Configuraciones de seguridad inadecuadas con la utilización de la contraseña del administrador por defecto.
- Sistemas críticos de seguridad con la necesidad de estar conectados a tierra (IACS,2020, 6).
- Control inadecuado de acceso de terceros, incluyendo proveedores de servicios, contratistas y activos cibernéticos (DNV, 2023).
- Personal insuficientemente formado para gestionar una respuesta rápida y eficaz ante un ciberataque.
- Planes de contingencia inexistentes o inadecuados (DNV, 2023).

Por otro lado, sobre los sistemas típicamente vulnerables, me remito al apartado 2.3. del presente capítulo el cual se dedica a su estudio con mayor profundidad. A continuación, se citan las operaciones y sistemas que gestionan los datos, procedimientos y procesos digitales en los buques.

2.1. Documentación de sistemas IT y OT

En primer lugar, tal y como presenta DNV (2023) en el sector marítimo, al igual que en los procesos industriales, las Tecnologías de la información (en adelante, IT) son las operaciones que se encargan del uso de datos como información y, en segundo lugar, las Tecnologías operativas (en adelante, OT) son los sistemas que recopilan los datos anteriores para dirigir y analizar los procedimientos que se realizan en físico.

Tal y como plasma BIMCO et.al. (2023) para una evaluación de riesgos veraz, los sistemas IT y OT deben asumir responsabilidades de gobernanza individual dentro de un registro de activos único (p. 28). El registro debe contener el coste de valoración y mantenimiento de cada activo.

En este sentido, a pesar que únicamente sea de aplicación para los buques de nueva construcción, se ha de tener en consideración la guía que establece la Recomendación 166 de la IACS bajo el título de Recomendación de Ciberresilencia, harmonizada el 1 de abril de 2020 en tanto establece que el registro debe incluir los siguientes inventarios:

- Inventario de dispositivos de comunicación y comunicación en red.
- Inventarios de *software* (en ocasiones este inventario forma parte del sistema de registro de *software* del buque).
- Inventario de servicio de red para cada equipo.
- Mapa lógico de redes (en los que se incorporan las direcciones IP y no IP, equipos electrónicos tales como ordenadores y dispositivos y conexiones en el campo de las comunicaciones).

2.2. Sistemas típicamente vulnerables

A través del análisis de los sistemas, aplicaciones y procedimientos para averiguar los puntos débiles del sistema de ciberseguridad del buque es posible identificar las vulnerabilidades existentes y prever las posibles amenazas (ENISA, 2020).

La IMO (2023) establece que el objetivo de esta evaluación es averiguar las vulnerabilidades existentes en los sistemas de los buques por las que puedan sufrir un ciberataque. Según Soyer (2018) las diferentes vulnerabilidades se clasifican en riesgos temporales, gestión del acceso a redes e interconexiones, errores de implementación de los *softwares* y, por último, errores de procedimiento (p. 631).

Para poder realizar la propuesta de una cláusula reguladora de los ataques cibernéticos se deben estudiar los sistemas típicamente vulnerables en los buques

que, tal y como cita la IMO en el artículo 2.4 de las Directrices sobre la gestión de los riesgos cibernéticos marítimos, 2017, son los siguientes:

En primer lugar, los sistemas de gestión de carga y estiba. Es decir, los sistemas digitales que se utilizan para poder realizar el embarque, la gestión y el control de la carga. Según BIMCO et.al. (2023) el peligro añadido de estos sistemas es que se interrelacionan con diversos sistemas en tierra como puertos, estibadores, terminales marítimas y herramientas digitales para controlar los envíos disponibles para los cargadores (p.28). Los interfaces de estos sistemas hacen que las gestiones logísticas con los usuarios del puerto puedan derivar en sufrir un ataque cibernético, ya que los expone al ciberespacio.

En este aspecto, es dable comentar el grave perjuicio que podría causar cuando el *E-Bill of landing* sea sé, el conocimiento de embarque electrónico, se ponga en práctica. Podría alterar en su totalidad el contenido del mismo sin dejar huella alguna y, como es sabido, el *Bill of landing* tiene valor probatorio. Por lo que la justicia estaría a merced de los ciberdelincuentes.

Segundo, los sistemas de puentes. Hoy en día la gran mayoría están digitalizados y conectados tanto a tierra como al ciberespacio. No obstante, aquellos que aún no están conectados, se actualizan a través de medios extraíbles que han sido configurados en red. En consecuencia, siguen siendo un punto vulnerable (BIMCO et.al., 2023).

Seguidamente, los sistemas de arranque, gestión de la maquinaria y velocidad ya que, de nuevo, hoy en día están todos digitalizados (IMO, 2023). Además, está en auge la supervisión remota, lo que propicia aún más la posibilidad de ser ciberatacado ya que se generan conexiones con distintas redes.

En cuarto lugar, los sistemas de atención y gestión de pasajeros (IMO, 2023). Es decir, los procesos informáticos que se encargan de realizar el embarque y controlar el acceso. Los sistemas de atención y gestión de pasajeros son posibles víctimas de ataques cibernéticos debido a que contienen datos sensibles de los pasajeros. Además, se incluyen dentro de los sistemas mencionado, las tabletas, los escáneres de mano y las televisiones digitales. Se configuran como sistemas vulnerables ya que entre ellos envían los datos de un aparato electrónico a otro a través de la red.

En quinto lugar, uno de los sistemas más importantes a proteger son los sistemas de control de acceso. Si éstos sufren un ciberataque puede conllevar en la rotura principal del sistema de defensa del buque (BIMCO et.al., 2023).

Por consiguiente, uno de los sistemas más afectados por los ciberataques son los sistemas de datos de la navegación. Según Soyer (2018) uno de los ciberataques más repetidos por los ciberdelincuentes ha sido vulnerar y modificar los Sistemas de Posicionamiento Global, los cuales pertenecen a los sistemas de datos de la navegación. Para su estudio en profundidad, me remito al próximo apartado.

Por otro lado, controlar las redes inalámbricas conectadas a bordo del buque en beneficio de los pasajeros es complicado, en consecuencia, dichas redes públicas son un sistema crítico para la seguridad del buque, ya que, de una manera u otra, algún otro sistema del buque debe estar conectado a ellas (ENISA, 2020). Un ataque cibernético a las redes puestas a disposición de los pasajeros puede provocar un ciberataque a otros sistemas del buque.

En penúltimo lugar, al igual que las redes anteriores, las redes que proporcionan acceso a internet u otras aplicaciones son un blanco fácil para los ciberataques. En consecuencia, según DNV (2023) ningún sistema crítico para la seguridad del buque debe estar conectado a los sistemas de gestión administrativa de la tripulación.

Por último, cualquier conexión inalámbrica o vía satélite aumenta la vulnerabilidad de los buques, por tanto, los sistemas de comunicación son vulnerables a ciberataques. A título de ejemplo, las señales VSAT e incluso, las comunicaciones con las autoridades públicas pueden ser víctimas de un ataque cibernético (ENISA, 2020).

En conclusión, los equipos que gestionan estos sistemas son, por ende, cibernéticamente vulnerables. Por lo que al igual que los sistemas, deben ser revisados y evaluados. La evaluación debe basarse en preguntas sobre las premisas siguientes (DNV, 2023): autonomía del sistema y equipo, conexión directa al exterior o indirecta a través de la conexión con otros sistemas, si el sistema cuenta con medidas para mitigar el riesgo cibernético en caso de ser víctima de un ataque y, por último, cuál es el grado de dificultad de acceso al sistema.

Tras dicha valoración se debe redirigir el sistema y configurar los equipos para adoptar medidas de ciberseguridad más eficaces y así prevenir posibles ataques cibernéticos. Por tanto, la evaluación sirve para mejorar los aspectos vulnerables (DNV, 2023). Como se verá a continuación, son múltiples los casos de ciberataques en la industria marítima.

3. Ataques cibernéticos más usuales en el sector marítimo

El sector marítimo ha sido objeto de múltiples ciberataques a lo largo de los últimos años que han provocado que quedaran al descubierto deficiencias en los protocolos

de seguridad cibernética de las empresas y organizaciones del sector. Tal y como comenta Soyer (2018), con el fin de robar los cargamentos transportados redirigiendo su carga, los ciberataques a las compañías navieras suelen tener por objeto la modificación y extracción ilegal de datos.

Además, es de destacar que Cooper (2019) estima que un 15% de los ciberataques del sector son llevados a cabo ni más ni menos que entre armadores competidores, con el objetivo de obtener una ventaja comercial al provocar las pérdidas de la carga o el retraso en las mismas (p.106).

A continuación, se enumeran únicamente los ciberataques más relevantes que ha sufrido el sector marítimo, clasificándolos según la tipología del ataque. Así, se dividen entre ataques vía *ramsomware,* ataques de *phishing* y *spear phishing* y, por último, la manipulación de datos de la navegación.

3.1. Ataques cibernéticos vía ramsomware

Primero, los ataques de *ransomware,* un tipo de *malware,* es decir, de *software* malicioso*,* que se caracterizan por llevar aparejada la extorsión. A través del *ramsomware* los ciberdelincuentes roban los datos de sus víctimas y para liberarlos piden una suma de dinero considerable (Soyer, 2018, 630). A título de ejemplo, en 2018 los puertos de Barcelona y San Diego sufrieron ataques de *ramsonware* que generaron grandes demoras en las entregas de carga de esos puertos (Soyer, 2018, 630).

El ciberataque al puerto de Barcelona se produjo por una infección del *ramsomware* Ryuk. Afectó e inutilizó todos los sistemas informáticos internos. Por su parte, el ciberataque al puerto de San Diego se produjo cinco días después del ataque al puerto de Barcelona y fue a causa del mismo *ramsonware.* De nuevo, inhabilitó los sistemas informáticos internos (Molist, 2018).

El caso estrella de esta tipología de ciberataque es el ataque global del *ransomware Wanna Cry*. Afectó a empresas de todos los sectores, causando pérdidas millonarias y, el sector marítimo no fue una excepción (Subero, 2019).

Otro ejemplo es el famoso virus Petya que atacó las operaciones globales de 17 terminales portuarias de Møller-Mærsk. Las consecuencias del virus Petya fueron devastadoras para tal empresa, provocando graves demoras a sus clientes, paralizando las operaciones portuarias y afectando a más de 80 puertos (World economic forum, 2018). En tiempo récord, la empresa tuvo que modificar todo su sistema informático.

Además, Jim Hageman, presidente de Møller-Mærsk en ese momento, anunció en el Foro Económico Mundial celebrado en 2018 que el virus Petya causó pérdidas para la empresa de más de 300 millones de euros (World economic forum, 2018).

Bajo este escenario, en julio de 2018, COSCO Shipping Lines confirmó haber sido víctima de un ataque cibernético que afectó a su conexión a internet en todas sus oficinas de Estados Unidos. La empresa consiguió aislar sus redes internas de las redes globales y, por tanto, pudo frenar las consecuencias del ataque. Sin embargo, las terminales marítimas de COSCO Shipping Lines de Canadá, Sudamérica y todo Estados Unidos sufrieron grandes demoras y paralizaciones (Costa Paris, 2018).

Otro ejemplo a destacar fue el ataque al Servicio de Aduanas y Protección Fronteriza de Australia. El ciberataque se produjo en 2012, el propósito de los ciberdelincuentes era jaquear el sistema de la policía aduanera para poder abandonar la carga de aquellos contenedores que la policía estaba controlando y evitar ser detenidos (Pawelski, 2023).

Bajo esta tesitura, en el año 2019 el servidor de administración de un petrolero cerca del puerto de Naantali (Finlanda) fue jaqueado por medio de un *ransomware* que consiguió borrar los sistemas de seguridad del buque. Cuatro meses más tarde, en el mismo puerto, esa misma embarcación fue atacada cibernéticamente a través de un ordenador remoto (Erstad et al., 2021b). El propósito del ciberdelincuente era dejar el petrolero a la deriva.

En 2020 se produjo un ciberataque desastroso para el operador noruego Hurtigruten. El ataque vía *ransomware* dejó inhabilitados todos los sistemas informáticos de uno de sus cruceros durante varios días. Tanto los datos sensibles de los pasajeros como del propio crucero, fueron robados (Bøe y Jordheim, 2020).

En el mismo año, la IMO, agencia marítima de la ONU, fue víctima de un *ransomware* que inutilizó por varios días su intranet. Como es usual en los ciberataques, no se ha proporcionado demasiada información sobre la característica del virus ni los daños que ocasionó. Sin embargo, la IMO declaró que el virus era "*sofisticado*", sin más detalles (Kovacs, 2020).

3.2. Ataques cibernéticos vía phishing y spear phishing

La segunda tipología de ataques cibernéticos en el sector marítimo son los ataques de *phishing* y *spear phishing*. Estos ataques se caracterizan por realizarse a través de correos electrónicos o mensajes que transmiten virus con el objetivo de obtener información confidencial de los sistemas.

En primer lugar, cabe destacar el ciberataque a la naviera Islamic Republic of Iran Shipping Lines en 2011 ya que provocó costes y daños descomunales pues alteró en sus sistemas los datos de las tarifas, los números de carga, los lugares y la fecha de entrega de las mercancías (Erstad et al., 2021b).

Otro ejemplo a destacar es el conocido caso de MSC contra Glencore International AG (Soyer, 2018). MSC transportaba tres contenedores a Amberes bajo un conocimiento de embarque donde como cargador y persona a notificar figuraba Glencore International AG y Steinweg. Al llegar a la terminal del puerto de Amberes, MSC envió por correo electrónico los códigos de liberación a Steinweg.

Sin embargo, Steinweg fue a la terminal dos días después de recibir el correo electrónico y 2 de los 3 contenedores ya habían sido recogidos. Los ciberdelincuentes interceptaron el correo electrónico de Steinweg y la carga fue recogida antes que llegara éste por ellos. Cabe destacar que empresas de suministro marítimo como son los almacenes sufren con frecuencia esta clase de ciberataques (Soyer, 2018).

Otro ataque cibernético de esta característica se produjo en el año 2013 en el puerto de Amberes, Bélgica en el que los ciberdelincuentes pudieron romper el sistema de seguridad y alteraron las fechas, los datos y los lugares de entrega. A pesar que el puerto contaba con una respuesta ante un ataque cibernético, los ciberdelincuentes consiguieron acceder al sistema de nuevo (Pawelski, 2023).

En el año 2020 se acusa al Gobierno Chino de robar información a través de un virus insertado en un correo electrónico sobre tecnología marítima de subcontratistas de la United States Navy y de más de 27 universidades estadounidenses (Volz, 2019).

3.3. Ataques cibernéticos vía malware para manipular datos de la navegación

Soyer (2018) establece que uno de los ataques cibernéticos más usuales en el sector es la manipulación de datos de la navegación. El propósito de los ciberdelincuentes es alterar la información que afecta a la navegabilidad del buque para mostrar información incorrecta o falsa con el fin de provocar colisiones, incomunicaciones, encallamientos o dejar el buque a la deriva.

A título de ejemplo, Sigh (2019) cita que, en el año 2012 en Irán, una plataforma localizada en el Golfo Pérsico sufrió un ataque cibernético en su sistema de comunicación y quedó incomunicada durante días.

Otro ejemplo, en el año 2016 en Corea del Sur, más de 280 buques tuvieron que volver al puerto al sufrir graves problemas en su sistema de navegación. El suceso ocurrió

en Corea del Sur y su Gobierno culpó a Corea del Norte. Sin embargo, tal y como establece Polychronis (2020) no hay pruebas que lo sustenten (p. 243).

En el año 2017 a comienzos del conflicto entre Ucrania y Rusia, Soyer (2018) establece que varios buques mercantes que navegaban en el Mar Negro fueron víctimas de un ataque cibernético que afectó a su sistema de navegación. El ataque alteró los sistemas de posicionamiento global de los buques, situándolo en tierra a pesar de estar navegando. Sin embargo, se dice que los ciberdelincuentes rusos querían atacar únicamente a los buques ucranianos. El Gobierno Ruso no ha reconocido tales ataques cibernéticos.

Meses más tarde, más de 20 buques, de nuevo en el Mar Negro, sufrieron un ataque cibernético en su sistema de posicionamiento global alterando su posición en más de 30 kilómetros. De nuevo, se cree que el ataque se realizó a manos del Gobierno Ruso (Polychronis, 2020).

De nuevo en el Mar Negro, ya entrado el año 2018, un buque sufre otro ataque cibernético en su sistema de posicionamiento global. En esta ocasión, la ubicación del buque, a pesar de estar navegando, lo situaba en tierra. El ataque cibernético duró tres días (Erstad, 2021).

También es común esta clase de ataques a plataformas petroleras. Ya en el año 2010 un ciberdelincuente jaqueó el sistema de una plataforma petrolera para provocar un siniestro en el que hubo muchos heridos. El ciberdelincuente cambió la configuración de la plataforma inclinándola hacia un lado para generar inestabilidad en el traslado de la plataforma de Corea del Sur a Brasil (Crawford, 2019).

Otro ejemplo destacable es el ataque a la plataforma petrolera Noble Regina. Este siniestro también data de una década atrás, en este caso de 2012 y, de nuevo, se produjo en el traslado de la plataforma. En este caso, la plataforma se trasladaba con el fin de terminar su proceso de construcción. El jáquer intentó escorar la plataforma ocasionando daños y pérdidas tanto a la estructura como al astillero. Más de 90 trabajadores tuvieron que necesitar asistencia médica. Caso idéntico que el ataque en las costas de África a la compañía ThetaRay en 2014 (Soyer, 2018).

4. Panorama general del mercado de seguros cibernéticos

El actual reto de los aseguradores es poder realizar una póliza que pueda amoldarse a los nuevos riesgos cibernéticos. El riesgo cibernético plantea un verdadero reto a los aseguradores ya que trastoca su protocolo de cálculo del riesgo.

Para saber que cobertura pueden ofrecer los aseguradores analizan los siniestros ocasionados por el riesgo que pretenden cubrir. Así pueden prever conductas futuras y exigir, excluir o incluir actividades en las pólizas que cubren tal riesgo. Sin embargo, este análisis no puede realizarse para un riesgo que está en constante evolución como es el riesgo cibernético. Ésta es su gran problemática (ENISA, 2020).

En primer lugar, cabe añadir que a raíz de la pandemia del COVID-19 el mundo de los seguros marítimos se trastocó (Aukera, 2020). Comenzaron a realizarse muchas más operaciones en remoto a través de sistemas sin protecciones eficaces ante posibles ataques cibernéticos (Soyer,2018). En consecuencia, los ataques cibernéticos aumentaron y los armadores y legisladores se dieron cuenta de la necesidad de un seguro que cubriese los riesgos cibernéticos (Jeremiah, 2020).

Tal y como afirma la firma israelí Naval Dome los ciberataques aumentaron hasta un 400% tras la pandemia, a partir de marzo de 2020. Naval Dome estableció que la causa principal fue un aumento de ataques vía *malware, ransomware* y correos de *phishing* que intentaron aprovecharse de las comunicaciones vía remoto (Mandra, 2020).

Por ende, la pandemia del COVID-19 fue la alarma que alertó a los altos dirigentes para que la ciberseguridad comenzara a entenderse como una preocupación. En consecuencia, las organizaciones internacionales y el legislador empezaron a dotar de importancia a los ciberataques, centrando sus esfuerzos en la creación de instrumentos legislativos para la protección de la Ciberseguridad (Maritime Executive*,* 2020).

Por su parte, tras dicha pandemia, las grandes navieras empezaron a preocuparse por cumplir con el marco normativo y actualizarse respecto las obligaciones legales que el legislador comenzó a exigirles en el campo de la ciberseguridad (Gürses, 2023).

No obstante, la tendencia de los aseguradores sigue siendo la exclusión de los ataques cibernéticos debido a la inexistencia de regulación sobre el riesgo cibernético en los seguros marítimos tradicionales. Además de la escasez de demanda que reclama obtener tal cobertura.

Según Farrar (2019) esto genera que el desconocimiento sobre el funcionamiento de una póliza que cubra el riesgo cibernético perdure. Además, genera que aumente el desconocimiento de los asegurados para entender qué riesgos estarían cubiertos ante una cláusula que cubriese una tipología en concreto de riesgo cibernético.

En este sentido, Deloitte (2018) establece que ésta gran incertidumbre por los usuarios que buscan ser asegurados ante riesgos cibernéticos puede provocar que no quieran participar en el mercado de tales seguros.

Partimos de la premisa comentada a lo largo de todo el presente trabajo, el seguro marítimo no ha sabido actualizarse a la era de la digitalización. Sin embargo, tal y como establece Jao (2023) para poder dar un impulso al comercio internacional y poder gestionar el riesgo cibernético, en otros sectores los expertos empiezan a basarse en el *blockchain*.

No obstante, los siniestros causados por ataques cibernéticos en el sector marítimo siguen siendo confusos para las aseguradoras a pesar que se pueden establecer tres tipologías usuales de los mismos, como se ha comentado en el presente TFM. En consecuencia, los aseguradores aún no han elaborado una lista con los siniestros más usuales del sector. Por ende, no han elaborado aún una cláusula estándar que cubra el ataque cibernético.

Farrar (2019) comenta que las aseguradoras aún no han obtenido el consenso ni en que rama se clasificarían dichos ataques cibernéticos, en el de mercados marítimos o en el cibernético.

Además, Soyer (2018) presenta que es una preocupación para las aseguradoras la incorporación del riesgo cibernético en sus pólizas ya que puede alcanzar un coste considerablemente elevado debido a que los sistemas informáticos están interconectados y es factible que puedan llegar a una escala masiva (p.631).

Como es sabido, un ciberdelincuente puede estar en cualquier parte del mundo mientras realiza el ciberataque. En consecuencia, plantea un problema a las aseguradoras para cuantificar el riesgo con límites geográficos.

De todo lo anterior expuesto, puede entenderse que una gran parte del problema de las aseguradoras al cubrir el riesgo cibernético es la capacidad de las reaseguradoras para asumir tales riesgos. Así, Inga Beale, consejera delegada de Lloyd’s en Londres finalizó la conferencia celebrada en Paris en 2018 con la conclusión de que el seguro de riesgo cibernético podría llegar a ser seis veces más caro que el seguro de mercancías y tres veces más caro que el seguro de responsabilidad civil (Organisation for Economic Co-operation and Development [OECD], 2018).

II. EL CONTRATO DE SEGURO MARÍTIMO

1. Características del contrato

En primer lugar, se realiza entre dos empresarios marítimos y, por tanto, entre dos partes fuertes. Las contraprestaciones se presumen equilibradas excepto en casos de embarcaciones civiles que sustentan la condición de consumidor, pero que tales no son objeto del presente trabajo.

La Ley 14/2014, de 24 de julio, de Navegación Marítima (en adelante, LNM) dedica el Título VIII en exclusiva al contrato de seguro marítimo. Por tanto, es preceptivo preguntar, ¿Por qué el seguro marítimo tiene una especial regulación? El artículo 406 LNM nos resuelve esta cuestión al establecer que la cobertura del riesgo marítimo reside en los riesgos que puedan originarse durante la navegación marítima.

Es dable citar que, como es usual en la práctica del seguro y tal y como dice Pulido Beginés (2015) el seguro marítimo está compuesto por condiciones particulares que prevalecen sobre las generales en tanto el principio *lex especialis derogat lex generalis*.

Es preceptivo comentar que las condiciones generales están compuestas tanto por las realizadas por los aseguradores españoles como por las *Institute Cargo Clauses* elaboradas por el Instituto de Aseguradores de Londres (Pulido Beginés, 2015), temática estudiada con mayor profundidad en el apartado 3 del presente capítulo, al cual me remito.

Por tanto, el seguro marítimo es aquel contrato con el propósito de indemnizar unos daños sufridos durante la navegación marítima por parte de un sujeto que ocupa la posición jurídica de asegurado. Para que el daño soportado se indemnice debe estar cubierto por la póliza de seguro celebrada entre los firmantes por lo que no puede ser una situación excluida. Además, esta obligación por parte del asegurador a realizar la indemnización al asegurado se produce siempre a cambio de haber pagado la prima pactada (Arroyo Martínez, 2014).

Así se puede llegar a la conclusión que dentro de la definición del contrato de seguro marítimo caben los daños sufridos no solo durante la navegación sino también todos los daños ocasionados con posterioridad al siniestro. Dicho de otra manera, el contrato de seguro cubre aquellos buques que se hallen en los puertos o que aún no estén finalizados y se hallen en construcción dentro de un astillero (Pulido Beginés, 2015). A continuación, se analizan las características propias del contrato de seguro marítimo.

Primero, el contrato de seguro marítimo tiene una naturaleza sinalagmática ya que tal y como establece Arroyo Martínez (2014) las partes se comprometen recíprocamente a cumplir con lo pactado en el contrato. En consecuencia, el asegurador solo procederá a indemnizar en el caso que el daño ocasionado en un siniestro sea consecuencia de un riesgo cubierto por el contrato de seguro marítimo.

En segundo lugar, el contrato de seguro marítimo es dispositivo ya que el artículo 407.2 LNM establece que no necesita de forma escrita para su validez. Sin embargo, con base al artículo 421 LNM esta forma escrita opera únicamente *ad probationem* no *ad solemnitatem* (Pulido Beginés, 2015), en consecuencia, los artículos mencionados establecen que el asegurador debe entregar un certificado provisional de la póliza, pero cualquier comprobante de pago se considera pago en concepto de primas y, en consecuencia, prueba de la celebración del contrato.

Bajo esta tesitura, la LNM proclama el carácter dispositivo del contrato de seguro marítimo (Pulido Beginés, 2015). Sin embargo, en virtud del artículo 470.1 LNM prima la voluntad de las partes en tanto pueden excluir e incorporar los riesgos cubiertos. En consecuencia, contrasta con el carácter imperativo que plasma la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (en adelante, LCS) (Sánchez Calero, 2010).

Tal y como establece Pulido Beginés (2015) la tercera característica del contrato reside en su carácter bilateral o plurilateral. En el contexto del seguro marítimo es usual encontrar como partes involucradas no solo al asegurador y al asegurado, sino también un tercero beneficiario, quién recibiría la indemnización en caso que suceda el riesgo cubierto.

La cuarta cualidad del contrato de seguro marítimo es su naturaleza onerosa regulada por el artículo 429 LNM en tanto establece que el asegurador se compromete a indemnizar el siniestro en las condiciones pactadas en el contrato y siempre que se haya realizado el pago de la prima establecida.

En relación con la anterior característica cabe mencionar la aleatoriedad del contrato que nos ocupa pues es la característica estrella de todo contrato de seguro. Según Salinas Adelantado (2015) la aleatoriedad es la posibilidad que el riesgo asegurado no ocurra jamás y, sin embargo, la parte asegurada tiene la obligación de pagar la prima siempre (art. 425 LNM).

En este sentido, a la luz del artículo 422.2 LNM que el asegurador solo proceda a pagar en el caso de que el siniestro se produzca a causa de un riesgo cubierto en el contrato, no significa que el asegurador incumpla con su obligación pactada en el contrato, sino todo lo contrario, su obligación es cubrir la posibilidad que suceda un

siniestro a causa del riesgo cubierto en el contrato. Por tanto, no quiere decir que deba suceder el siniestro para que el asegurador cumpla con sus obligaciones, ya está cumpliendo con ellas al proteger el riesgo y únicamente pagará en caso que suceda (art. 422.2 LNM).

La sexta particularidad del contrato de seguro marítimo radica en su carácter de tracto sucesivo ya que las obligaciones únicamente perduran durante el período pactado en la póliza. El asegurado tiene la obligación de pagar la prima, pero el asegurador solo indemnizará en el caso de que ocurra un siniestro cubierto dentro de la horquilla de tiempo pactado (Arroyo Martínez, 2014).

En séptimo lugar es dable hablar de la presunción que emana de cualquier contrato, la buena fe superlativa. En puridad la buena fe superlativa es el compromiso de actuar conforme las obligaciones pactadas en el contrato (Pulido Beginés, 2015). Además, la LNM en su artículo 422 estipula la obligación de realizar una declaración del estado del bien asegurado por parte de la parte asegurada. Si no se cumple con tal obligación, la LNM en calidad de ley dispositiva provoca la anulación del contrato y, si el riesgo se ha producido, exime de la obligación de la Aseguradora a indemnizar el siniestro.

La LNM en su artículo 423 establece la obligación del tomador del seguro de comentar durante el periodo de vigencia del contrato, las circunstancias conocidas o que debiera razonablemente conocer y que puedan agravar el riesgo.

El siguiente elemento, producto de la dinámica del sector, es la pluralidad heterogenia de riesgos. Así la LNM plasma unos riesgos sobre los que directamente excluye o incluye de la cobertura. No obstante, prima la voluntad de las partes.

Por último, con base al artículo 409 LNM es dable señalar la pluralidad de intereses. Así el precepto citado regula los seguros marítimos existentes, para su estudio me remito al apartado 2.3. del presente capítulo. Sin embargo, resulta necesario recalcar que la LNM no se pronuncia sobre el Ciberseguro.

2. Elementos del contrato de seguro marítimo

2.1. Elementos subjetivos

Los elementos subjetivos o personales esenciales en el seguro marítimo son el asegurador, el asegurado y el tomador. No obstante, cabe decir que como en las otras tipologías de seguros, puede recaer sobre la misma persona la posición jurídica de asegurado y tomador.

De forma breve tal y como establece Rodríguez Carrión (2003) se puede definir al asegurador como la persona que se obliga a asumir la pérdida del asegurado a cambio de una prima. Únicamente se obliga a cubrir el riesgo que quepa en las condiciones pactadas entre las partes.

Por tanto, en virtud del artículo 429 punto 1 LNM y después de haber sido acreditado el daño y sus causas, la obligación que caracteriza al asegurador es la de indemnizar el riesgo cubierto por el contrato de seguro marítimo.

Como consecuencia de los grandes riesgos y complejidad asociadas a las operaciones logísticas del sector, es habitual que los aseguradores participen conjuntamente en la cobertura de un mismo riesgo. No podemos hablar de coaseguros sin mencionar a Lloyd's líder en coaseguros marítimos a nivel mundial y dueños de la mayor red de comerciantes marítimos, entre ellos, las Sociedades de Seguros (Soyer, 2018).

Tal y como establece Fuestes Carsi (1946) Lloyd's nació precisamente de la necesidad que surgió en los aseguradores ingleses de crear una corporación para poder dar respuesta a los múltiples comerciantes marítimos que requerían de una cobertura para protegerse ante la inmensidad de riesgos existentes. Además de aumentar sus primas generando más ganancias.

Por tanto, el coaseguro tiene como finalidad segmentar la obligación del asegurador y, por consiguiente, ramificar el riesgo. Por su parte, es evidente que beneficia al asegurado pues así puede obtener una cobertura más completa del riesgo.

Según Arroyo Martínez (2014) el tomador es quién contrata el seguro y, como ha sido comentado anteriormente, puede ser una persona distinta al asegurado. En este caso, el tomador contrata un seguro en nombre de la persona asegurada. Por su parte, el asegurado es quién recibe la indemnización en caso que tenga lugar el riesgo cubierto por la póliza.

2.2. Elementos objetivos o reales

El elemento objetivo principal del contrato de seguro marítimo es el interés del seguro definido en virtud de la Sentencia de la Audiencia Provincial de Islas Baleares (154/2016) (Sala de lo civil, sección 5ª), de 6 de junio de 2016, como el vínculo que mantiene una persona con una cosa asegurada por un contrato de seguro para el caso que tenga lugar un siniestro ocasionado por un riesgo en particular.

Además, dicho vínculo debe estar ligado de alguna manera a la navegación para que se cumplan los requisitos del interés asegurable en el contrato de seguro marítimo. Por tanto, el interés debe ser legítimo y el riesgo debe encontrarse en la navegación (art. 408.1 LNM).

Los seguros marítimos se realizan con pólizas estimadas, es decir, el valor del interés se tiene en cuenta para calcular la indemnización. Por tanto, es distinto al seguro de daños convencional donde la suma asegurada es igual al valor del interés.

La póliza estimada debe ser expresamente aceptada ya que, y a pesar del tenor literal del artículo 414 LNM, es requisito indispensable para la póliza la aceptación expresa del asegurador. Tal y como establece Girgado (2017) el propósito de esta póliza es liberar al asegurado de la obligación de tasar el valor de la cosa asegurada justo antes de que tenga lugar el siniestro.

Por otro lado, en tanto al concepto de valor asegurado, éste está intrínsecamente conectado con el valor asegurable. Así, tomando las palabras de Ruiz Soroa, Arranz de Diego y Zabaleta Sarasua (1993) el valor asegurado es la cantidad máxima que el asegurador se obliga a cubrir (p. 51). Por su parte, tal y como define Pulido Beginés (2015) la suma asegurada es la cifra en que el interés asegurable es garantizado por la póliza de seguro. El valor asegurable mantiene una forma objetiva en virtud de la relación entre la cosa asegurada y el asegurador (Ruiz Soroa et al, 1993).

Por su parte, el valor asegurable es la cifra plasmada en el contrato de seguro y, por ende, expresa la cifra máxima que puede alcanzar la posible indemnización en caso que se materialice el daño asegurado (Pulido Beginés, 2015).

Además, el importe del valor asegurable siempre debe ser inferior al valor asegurado ya que si fuera superior el asegurado obtendría un enriquecimiento injusto (art. 26 LCS). Dicha premisa responde a la lógica del contrato de seguro que no es menos que la restauración de la situación inicial del asegurado en caso de sufrir un daño.

Por otra parte, es indispensable para que pueda celebrarse un contrato de seguro que el riesgo asegurado exista y no haya tenido lugar el siniestro (art. 4 LCS) o sino será nulo (Sánchez Calero, 2010). Además, debe ser probado que el daño se produjo a causa de un riesgo de mar (art. 418 LNM).

De esta forma es imprescindible citar el artículo 417 y siguientes de la LNM. La LNM recoge bastantes riesgos excluidos y cubiertos del contrato de seguro marítimo.

En primer lugar y de forma breve, el artículo 417 establece que la aseguradora tiene la obligación de indemnizar al asegurado por los riesgos de la navegación cubiertos por el contrato de seguro marítimo.

Así, el artículo 418 LNM excluye algunos riesgos tales como la guerra, la detención ordenada por una autoridad pública, el terrorismo, la piratería, las huelgas y, por último, las explosiones radioactivas, entre otros.

Prosiguiendo con la lectura de la LNM, el artículo 419 presupone aquellas situaciones en que el asegurado presuntamente interviene con dolo, culpa o negligencia. En los casos en que intervenga dolo, la ley contempla la prohibición de responder por parte del asegurador, sin ser posible pacto en contrario.

Por su parte, el articulo 420 LNM establece que la cobertura del seguro excluye las circunstancias en que el daño se debe a un defecto inherente del objeto asegurado, sea sé, vicio propio. Como pequeña conclusión, es importante citar que nada se dice del riesgo cibernético.

3. Elementos formales

En primer lugar, es importante destacar que las pólizas pueden realizarse a la orden, nominativas y al portador, valoradas o no valoradas y su vigencia depende mucho del trayecto (Pulido Beginés, 2015).

En la práctica del sector es usual la utilización de cláusulas inglesas que excluyen riesgos en los seguros concertados bajo las leyes españolas; es pacífica la jurisprudencia que admite tales cláusulas extranjeras. A título de ejemplo, la Sentencia de la Audiencia Provincial de Pontevedra 250/2020 (Sala de lo civil, sección 1), de 26 mayo de 2020 (recurso 79/2020) y la Sentencia de la Audiencia Provincial Valencia 310/2022 (sala de lo civil, sección 9ª) de 5 de abril de 2022 (recurso 1531/2021).

De hecho, es dable citar la Sentencia de la Audiencia Provincial de Pontevedra 250/2020 (Sala de lo civil, sección 1), de 26 mayo de 2020 (recurso 79/2020) en tanto establece que las cláusulas inglesas integradas en el póliza deben ser interpretadas tal y como son aplicadas en Inglaterra.

Por otro lado, hay que señalar que en el mundo marítimo el seguro adquiere una relevancia especial. En este sentido es crucial comprender las diferentes modalidades de pólizas de seguro marítimo. En función del interés asegurado y la duración de la cobertura podemos clasificar las pólizas en dos ramas.

En primer lugar, en función la duración (art. 439 LNM) las pólizas se clasifican por tiempo o por viaje. En este sentido es importante destacar que en el plano internacional no existe óbice para combinar ambas en una misma póliza, así lo recoge la sección 25 de la *Marine Insurance Act*. No obstante, en el plano práctico es usual encontrarse con una tradición asentada donde el seguro que cubre el buque sea por tiempo determinado y el de mercancías, por viaje.

Entonces, ¿cuál es el criterio que las diferencia? La repuesta a esta pregunta viene recogida por la LNM en su artículo 440 y siguientes. En primer lugar, se entiende como póliza por viaje en el caso que el viaje se realice con carga, aquella en que la responsabilidad del asegurador empieza cuando se recibe la carga a bordo y finaliza tras la descarga. Además, el artículo 440 LNM *in fine* añade que la responsabilidad de la aseguradora termina, en cualquier circunstancia, al transcurrir 15 días desde la llegada al puerto de destino. No obstante, cuando el buque viaje en lastre, la responsabilidad del asegurador comienza desde que se eleva el ancla hasta que se amarra en destino (Pulido Beginés, 2015).

Por otro lado, la cobertura de la póliza por tiempo se extiende durante una horquilla de tiempo específica y, en consecuencia, sin importar la cantidad de viajes que se realicen durante su vigencia.

Así, el artículo 441 LNM que la responsabilidad del asegurador empieza a partir del día siguiente a la fecha de celebración del contrato de seguro y finaliza el día completo pactado como su fin. Como en la clasificación anterior, la LNM recoge en el artículo 442 *in fine* una excepción a la norma general en tanto si el buque está en situación de peligro o en un puerto de refugio y dicha situación es notificada al asegurador, se prorroga el seguro hasta que el buque llegue a destino. Así es importante recalcar que la prórroga es onerosa, en tanto el asegurado deberá asumir la proporción del aumento de prima que corresponda.

Como ha sido comentado, existe la posibilidad de realizar una póliza mixta que combine la póliza por viaje y por tiempo. Esto ocurre cuando se asegura el objeto de interés para un viaje específico y, además, se extiende la protección durante un período determinado posterior al mismo.

4. Liquidación del siniestro

El artículo 433 LNM regula que el asegurado puede escoger cómo realizar la liquidación del siniestro entre dos acciones, la acción de abandono o la de avería. Sin embargo, el artículo 449 LNM establece que la acción de abandono solo se admite en

los casos contemplados en el precepto citado relativo al seguro de buques y relativo al seguro de mercancía (art. 461 LNM).

Según lo estipulado en el artículo 435 LNM la acción de abandono tiene su naturaleza en la transmisión de la propiedad del objeto asegurado al asegurador. En consecuencia, únicamente puede realizar esta acción el asegurado propietario del bien (art. 373 LNM).

Por otro lado, el artículo 435.2 LNM recoge la presunción de la aceptación del asegurador si no manifiesta en el plazo de un mes ninguna intención de rechazar de forma expresa el abandono. Por su parte, el asegurador desde la acreditación del asegurado del daño tiene el mismo plazo para manifestar su intención de aceptar o no el abandono. Desde su elección, el asegurador puede proceder a la liquidación del siniestro en el plazo establecido en contrato de seguro y, en virtud del artículo 437 LNM, deberá abonar la indemnización al asegurador en el plazo máximo de 15 días.

Por otro lado, no es pacífica la jurisprudencia sobre la aplicación del interés punitivo del artículo 20 LCS en el seguro marítimo, no obstante, conforme lo establecido por la LNM en su artículo 435 y jurisprudencia tal y como plasma la Sentencia del Tribunal Supremo 43/2009 (Sala Civil, sección 1a), de 5 de febrero 2009 (recurso 2352/2003) la demora en el pago de la indemnización obliga al asegurador a indemnizar el interés legal.

Es necesario comentar, aunque de forma breve, que en virtud del artículo 438 LNM la prescripción para el ejercicio de acciones nacidas en el contrato de seguro marítimo tiene un plazo de dos años.

5. Tipología del contrato de seguro marítimo

Una vez presentado el contrato de seguro marítimo en general, necesariamente, aunque de forma breve, se explicarán los tres seguros marítimos tradicionales más relevantes del sector. Es decir, el seguro de buques, el seguro de mercancías y por último, el seguro de responsabilidad civil.

5.1. Seguro de buques

Regulado en los artículos 439 al 451 LNM tal y como establece Salinas Adelantado (2015), el seguro de buques tiene carácter rotativo ya que se reconstruye de forma automática una vez pagada la indemnización en caso que ocurra un siniestro. Otra particularidad a destacar sobre esta tipología de seguro marítimo es que la

seaworthiness o mantenimiento de la navegabilidad del buque, pesa sobre el asegurado (art. 444 LNM).

Es dable destacar que Pulido Beginés (2015) comenta que el contrato de seguro de buques suele contener las anglosajonas clausulas *Institute Time Clauses Hull* con el fin de cubrir el riesgo que la navegación puede ocasionar al propio transporte.

A la luz del artículo 439 LNM, esta clase de seguro tiene dos tipologías, por viaje o por tiempo. La cobertura del seguro de buque por tiempo comienza desde que se recibe la carga a bordo hasta que se descarga la mercancía del buque (art. 440.1 LNM). Por otro lado, en virtud del art. 441 LNM la tipología por tiempo comienza a las doce de la noche del día siguiente a la celebración del contrato y finaliza a las doce de la noche del último día.

5.2. Seguro de mercancías

La LNM regula en los artículos 453 a 462 esta tipología de seguro marítimo como aquella que cubre los daños que puedan padecer las mercancías transportadas. De nuevo, en el tráfico es común la aplicación de las *Institute Cargo Clauses*. Estas cláusulas sustentan tres categorías, A, B y C según la extensión de cobertura del riesgo (Soyer, 2018).

En este sentido, el artículo 455 LNM establece que el interés se asegura para un viaje y la cobertura comienza cuando las mercancías dejan el puerto de origen para ser embarcadas y termina al llegar a tierra del puerto de destino.

5.3. Seguro de responsabilidad civil

El seguro marítimo de responsabilidad civil por antonomasia es el que cubre los clubes de protección e indemnización o también llamados P&I Clubs (en adelante, P&I).

Tal y como plasma Sierra Noguero (2016), el límite que se considera dentro de la cobertura es el límite de la suma asegurada durante la vigencia del contrato de seguro marítimo, como así lo delimita el artículo 466 LNM y tal y como presenta Sánchez Calero (2010) ocurre lo mismo para los seguros regulados bajo la LCS por su artículo 37.

En este sentido, Pulido (2015) establece que, y cito, textualmente, "*la obligación de indemnización existe para el asegurador desde el momento en que surge la responsabilidad del asegurado ante el tercer perjudicado*" (p.499).

Hay que destacar como principio imperativo de esta tipología de contrato de seguro marítimo, que el perjudicado tiene acción directa contra el asegurador de responsabilidad civil para exigir que cumpla con sus obligaciones, sin que pueda pactarse lo contrario (art. 465 LNM).

III. PROBLEMAS JURÍDICOS DEL SEGURO DE RIESGO CIBERNÉTICO

1. Cobertura del riesgo cibernético

Soyer (2018) comienza señalando que es frecuente que en los seguros marítimos se incluya la cláusula CL380, una cláusula muy amplia que excluye los riesgos cibernéticos.

Además, tal y como establece Soyer (2018) no existe una cobertura estándar de riesgo cibernético en el mercado de los seguros marítimos. Tal y como establecen Eling y Hendrik (2015), la cobertura del riesgo cibernético que podría obtenerse en los seguros marítimos sería la enfocada a cubrir las pérdidas que deriven de la interrupción de la actividad, la ciberextorsión, los gastos de gestión de crisis, los daños materiales, las multas y sanciones o las pérdidas de datos. A continuación, se comenta cada una de ellas para entender cuál sería su cobertura en el sector marítimo.

En tanto a la interrupción de la actividad ésta se refiere a la cobertura de un ciberataque que provoque el cierre de los sistemas el cual podría acarrear importantes pérdidas financieras. Tal y como establece Soyer (2018), en otros sectores suele requiere que el siniestro sea consecuencia del acceso no autorizado en la red, recepción de un virus o interrupción de las operaciones comerciales que generen la pérdida de datos sensibles.

De nuevo, Soyer (2018) establece que el valor del lucro cesante en las pólizas que cubren el riesgo cibernético debe calcularse por referencia al beneficio neto más los costes fijos continuados.

Por otro lado, en tanto a la ciberextorsión Soyer (2018) predice que se crearán pólizas y cláusulas que indemnicen al asegurado cuando pague un rescate en respuesta a la amenaza de inutilizar sus sistemas. Sin embargo, aún no existen.

Respecto los gastos de gestión de crisis, las coberturas que cubren los riesgos cibernéticos en otros sectores suelen indemnizar al asegurado por los gastos de notificación, asistencia y relaciones públicas (ABI, 2023).

Sobre los daños materiales como la recuperación y reparación de datos, cabe decir que los contratos de seguro en otros sectores cubren los daños personales y los daños en activos digitales al mismo tiempo (IBM, 2020).

Por su parte, respecto la pérdida de datos en estas pólizas en el seguro marítimo se incluiría la cobertura de cualquier pago de responsabilidad a terceros cuyos datos

hayan sido dañados o perdidos por el asegurado como resultado de una violación de datos, siempre que el asegurador haya respaldado la acción (ABI, 2023).

En penúltimo lugar, tal y como menciona Sighn (2019), la mayoría de pólizas o cláusulas que cubren el riesgo cibernético cubren las multas y las sanciones en la medida que lo admita la legislación aplicable, así que es oportuno entender que las pólizas que cubran los riesgos cibernéticos en el sector marítimo también cubran dichas sanciones.

Por último, en tanto a la pérdida de propiedad intelectual o impacto de la reputación, los seguros que cubren en riesgo cibernético suelen ampliar la cobertura a las responsabilidades informáticas de cada empresa.

Por su parte, en cuanto al alcance de la cobertura, es dable citar que al tratarse de un producto tan nuevo no existe jurisprudencia que nos pueda orientar en la interpretación de las pólizas y, sobre todo, en atención a los términos técnicos que se emplean en ellas, tales como, por ejemplo, “fallo electrónico” o “código malicioso”.

Sin embargo, Kumar (1949) estableció que cualquier contrato de seguro que entre en conflicto por la definición de una palabra incluida en él, se presume que prevalece la definición técnica. No obstante, De Maurier (1967) sostuvo que en el caso que los significados ordinarios y los significados técnicos difieran, los tribunales no pueden dictaminar un significado técnico a las palabras.

De Maurier (1967) se basa en proteger al asegurado sin conocimiento sobre la materia (en el caso que nos ocupa serían las compañías navieras) ya que no puede entenderse que estén familiarizadas con tales tecnicismos (en este contexto, tecnicismos sobre ciberseguridad). Sin embargo, no es la doctrina mayor respaldada.

Otra problemática que presenta la cobertura de un riesgo cibernético en el sector marítimo es que en las otras industrias en las que ya se está aplicando el seguro suele acompañarse con una cláusula de exclusión para el caso que el siniestro sea debido a un acto de terrorismo. Esto supondría un grave perjuicio para las compañías navieras ya que, como hemos comentado a lo largo del presente trabajo, existen informes que parecen sugerir que muchos ciberataques sean motivados políticamente (VMware security, 2023).

Por su parte, Soyer (2018) comenta otra problemática en tanto que como la cobertura del riesgo cibernético está aún en fase de desarrollo, es posible que el asegurado contrate una póliza de riesgo cibernético para un riesgo que ya está cubierto por un producto de seguro distinto. Si ambas pólizas responden al mismo siniestro, se trataría de un caso de doble seguro y esto no supone necesariamente una ventaja monetaria

para el asegurado incluso, nos encontraríamos ante una situación en la que el asegurado estaría pagando una prima adicional por la póliza de un seguro marítimo que cubra el riesgo cibernético en la que su siniestro ya estaría cubierto por una póliza tradicional.

A título de ejemplo, imaginemos una grúa en una terminal de un puerto y debido a un ataque cibernético, cae y, además, daña a dos trabajadores. El seguro de responsabilidad civil de la terminal probablemente cubra esa caída, pero, además, puede ser que también esté cubierto por la póliza que cubre el ciberseguro, salvando que tuviera alguna excepción que afectase al caso que nos ocupa.

Otra problemática es la cobertura no afirmativa la cual explicaremos a continuación.

1.1. Cobertura cibernética silenciosa (no afirmativa).

Cuando una póliza marítima tradicional no excluye directamente o no menciona las pérdidas relacionadas con el ciberespacio es posible que la misma llegue a cubrir las pérdidas ocasionadas con un riesgo cibernético si se considera que la causa próxima que originó el siniestro es un riesgo cubierto por la póliza. Tal y como establece Soyer (2018) y cito textualmente, este supuesto es conocido por los expertos como “póliza silenciosa” o “póliza no afirmativa” (p. 637).

Parecido al caso de Amberes de MSC que se ha comentado con anterioridad, por ejemplo, imaginemos que un envío de ordenadores portátiles asegurados con unas *Institute Cargo Clauses* (ICC) 2009 (A) se transportan de China a Valencia. En un puerto de transbordo, el jáquer consigue romper el sistema de seguridad del sistema de posicionamiento global de los contenedores y cambia los datos para enviarlos a Reino Unido.

En este supuesto y al tratarse de unas ICC(A) probablemente el asegurado reciba su indemnización porque no habrá exclusión que lo impida ya que las exclusiones en estas cláusulas excluyen pérdidas atribuibles a la naturaleza de la carga (cláusulas 4 a 7 de las ICC (A) 2009).

Sin embargo, en el supuesto de una póliza de cobertura cibernética silenciosa, el asegurado no obtendrá indemnización si el riesgo cibernético desencadena la aplicación de una de las exclusiones de la póliza.

Sin embargo, en el contexto de una póliza de cobertura cibernética silenciosa el asegurado jamás quedará cubierto si a través del riesgo regulado en el contrato de seguro marítimo provoca la aplicación de una exclusión.

A título de ejemplo y tomando por base la sentencia que surgió tras el conflicto de MSC *Mediterranean Shiping Co SA* contra *Glencore International SA* (caso comentado en el apartado 3 del Capítulo I al cual me remito para su explicación) cuando el tenedor legítimo del conocimiento de embarque no pudo recoger las mercancías, demandó al transportista (Hill Dickinson, 2017).

El litigio se resolvió en Reino Unido, donde el juez de primera instancia y el de apelación dictaron sentencia estimatoria al demandante, el titular legítimo de las mercancías, ya que la entrega debió ser efectiva (Martin, 2020). En consecuencia, el transportista tuvo que responder por el incumplimiento del contrato que consistió en una vulneración de datos.

En principio el transportista queda cubierto por los P&I en tanto a su responsabilidad frente a terceros, sin embargo, no quedó cubierto por la cobertura P&I puesto que éstos excluyen la responsabilidad por la entrega sin la presentación de un conocimiento de embarque. Es una de las exclusiones fundamentales de responsabilidad por pérdida o daño de la carga (Soyer, 2018). Por lo que en este caso el transportista no podría recuperar de su asegurador la responsabilidad de su incumplimiento por tratar de un riesgo cibernético.

Si bien es cierto que, a causa de la LMA5403, estudiada en el siguiente apartado al cual me remito, Lloyd's ha excluido la cobertura silenciosa en todas las situaciones que contempla la cláusula CL380 (International Union of Marine Insurance [IUMI], 2019).

2. Ciberexclusiones

Es común en el tráfico de los seguros marítimos tradicionales incorporar la Cláusula CL380 del *Institute Cargo Clauses* la cual excluye directamente las pérdidas ocasionadas por un ataque cibernético. Dicha cláusula es la pionera de las cláusulas que excluyen el riesgo cibernético. Sin embargo, como se expone en el presente apartado, ha sido suplida por cláusulas más novedosas. Sin embargo, sigue en aplicación y es la más utilizada a día de hoy.

En este sentido, la CL380 estándar sería aquella que excluye del seguro en el que está incluida, los daños, gastos y responsabilidades que de forma directa o indirecta hayan sido causados a través de cualquier aparato digital, sistema, virus, *ramsomware* o programa con la intención de causar daño a la persona destinataria del ataque.

La cláusula es bastante amplia ya que tal y como establece Soyer (2018), el redactor de la cláusula quiso descartar la aplicación de la causa próxima. La doctrina de la

causa próxima es la próxima en eficacia, la que desencadenó el siniestro. Es en otras palabras la causa directa o indirectamente que ha contribuido al daño. En consecuencia, la causa indirecta necesita únicamente una relación de cadena de causalidad, por ende, excluir su aplicación es la forma más completa de exclusión posible.

Así, y cito textualmente a Soyer (2018), cualquier conexión causal entre el siniestro y el funcionamiento de un sistema informático, código malicioso o cualquier sistema electrónico con el propósito de influir en el daño quedaría dentro de la exclusión.

A título de ejemplo, en caso que se utilice un móvil inteligente para las comunicaciones entre los miembros de una organización delictiva que, por ejemplo, detiene un camión para robar la carga que transportan, consistiría en un supuesto de exclusión por la CL380.

En este sentido, se debe responder a la pregunta de si en caso que un tercero envíe un *malware* de forma aleatoria y afecte a un buque, si es posible que los aseguradores excluyan su cobertura en virtud de la cláusula CL380. Como no existe jurisprudencia española, en virtud de la Sentencia del caso Tektrol en la corte de apelación de Reino Unido, *Tektrol Ltd v International Insurance Company of Hanover Ltd and Another,* se entiende que al redactar "personas malintencionadas" y a la luz de una interpretación restrictiva, no cabría dentro de la exclusión (Soyer, 2018).

Si un tercero crea un *malware* sin un destinatario claro, no sabe quién sufrirá el daño y, en consecuencia, la sentencia establece que la cláusula CL380 descarta el sistema o instrumento informático que una persona utilice con la intención de infligir daño a una persona directamente, por lo que en caso que no sea así, no quedaría (Soyer, 2018).

Sin embargo, en los seguros de casco y maquinaría existen una variación de la CL380 que se llama "CL380 *Hull amended*", esta cláusula rechaza la cobertura cuando los programas informáticos o sistemas relacionados sean directa o indirectamente la causa de la pérdida física emergente (*Mitsui Sumitomo Insurance* [MS&AD], 2022).

Como ha sido comentado con anterioridad, la CL380 ha estado incluida en múltiples contratos hasta 2019 y, a pesar de seguir siendo la más utilizada, han surgido nuevas cláusulas que intentan excluir el riesgo con mayor rigor (Pawelski, 2023).

En este sentido, actualmente esta cláusula es incluida en múltiples ocasiones junto la cláusula LMA5403. Ésta última establece que la cláusula de exclusión se active cuando el asegurador está dispuesto a cubrir un riesgo pero que, al ser ocasionado

por un sistema informático o virus, ese riesgo presuntamente cubierto deja de estarlo. Así, la LMA5403 (2019) se basa en las siguientes características.

Se compone de tres apartados. El primer apartado hace referencia a la exclusión de los daños, pérdidas y responsabilidades que hayan sido causados de forma directa o indirecta por un medio electrónico o digital para infligir daño. Cita como ejemplo los ordenadores, *malwares*, programas, sistemas informáticos y virus. Además, finaliza añadiendo una puerta para que cualquier medio digital quede excluido, ya que termina poniendo y, cito textualmente, "*o cualquier otro sistema electrónico".*

Por su parte, el apartado segundo de la cláusula establece que la misma está sujeta a las características reguladas en la póliza a la que pertenece. Por tanto, se sujeta a todos límites y exclusiones de la póliza. Es importante destacar de este apartado que la LMA5403 cita que la indemnización al asegurado no será excluida si el ataque cibernético no se produjo como medio por infligir daño.

Finalmente, el tercer apartado se vincula con el primero y establece que cuando la cláusula LMA5403 se endose a una póliza que cubra los riesgos de guerra, terrorismo, rebelión o daños por una persona que actúe por motivos políticos, entre otros, el primer apartado de la cláusula no se podrá utilizar para excluir pérdidas que de otra forma si estarían cubiertas y sean consecuencia de ataques cibernéticos vía ordenadores, *malwares,* sistemas informáticos, programas y virus o cualquier otro sistema digital para ayudar al lanzamiento de un misil o de cualquier arma.

La LMA5403 es un endoso a la cláusula que excluye el riesgo cibernético, sobre todo se utiliza para los seguros de cascos. A modo de resumen, Howden (2020) establece que la LMA5403 excluye las pérdidas cibernéticas maliciosas y genera que la amplia interpretación de la cobertura silenciosa no tenga lugar. Así, la cobertura silenciosa ya no está permitida en Lloyd's cuando se use la CL380 junto con la LMA5403 ya que, y cito textualmente parte de la LMA5403, "*una póliza puede ofrecer cobertura silenciosa si a) no se utiliza la CL380 o b) para riesgo cibernético no malicioso, aunque se utilice la CL380"* (IUMI, 2019).

Sin embargo, la cláusula se refiere a "*cualquier ordenador contribuyente a la pérdida"* por lo que sigue siendo una exclusión amplia y, en consecuencia, sin necesidad de causalidad directa.

Así las cosas, como la CL380 no es clara, el Lloyd's de Londres ha iniciado la elaboración de una nueva cláusula excluyente del riesgo cibernético que suple la CL380 (IUMI, 2019), la LMA5402, y se caracteriza por las notas que prosiguen.

En primer lugar, la cláusula comienza citando que, en caso de conflicto, la misma prevalece sobre cualquier otra cláusula del seguro al que pertenece. Su único apartado regula que en ningún caso el seguro al que pertenece cubre pérdidas, responsabilidades, gastos o daños que sean causados de forma directa o indirecta derivados de, en primer lugar, el error en el funcionamiento normal de un aparato electrónico o sistema informático y, en segundo lugar, el fallo o mal funcionamiento de cualquier sistema informático, programa o aparto electrónico como medio para infligir daños al destinatario de tal ataque cibernético a través de un virus, *malware,* proceso electrónico u otro sistema (LMA5402, 2019).

La cláusula LMA5402 se ha redactado para un uso general en todas las categorías de seguros marítimos. En este sentido, su novedosa introducción establece la excusión de las pérdidas cibernéticas, ya sean maliciosas o no. De nuevo, su exclusión es muy amplia y el lenguaje sigue sin ser restrictivo (Soyer, 2018).

3. Intentos legislativos para regular las cuestiones legales de seguridad cibernética marítima

La disyuntiva entre la seguridad y la solvencia en un sector tan complejo como es el marítimo es complicado ya que la transmisión de datos entre entes, empresas y organizaciones es constante y e gran masa. Cabe señalar que las organizaciones marítimas también generan, almacenan, transmiten y gestionan datos y sistemas de seguridad que protegen el comercio marítimo internacional (Singh, 2019).

Esta compleja estructura formada tanto por organizaciones públicas como privadas con sus sistemas conectados en red entre sí, es, en puridad, un gran peligro cibernético. Un sistema de seguridad de una empresa que no sea cibernéticamente eficaz puede causar problemas que pueden afectar incluso a la seguridad nacional (Howden, 2020). Un eslabón débil en la cadena de seguridad es una pieza del engranaje que se rompe y provoca el fallo de toda la cadena.

Los primeros en atender la problemática legislativa de la Ciberseguridad en el ámbito marítimo fue Estados Unidos en 2020 bajo el título *"Guidelines for addressing cyber risks at maritime transportation security act (mtsa) regulated facilities"*

En el mismo año, el Consejo Nacional de Seguridad Marítima de España publicó una Guía Legal de Buenas prácticas para puertos bajo el título "*Guía de buenas prácticas para la gestión de riesgos de ciberseguridad en buques e instalaciones portuarias".* Esta guía legal es realmente completa y aconseja a agentes que intervienen en múltiples actividades del sector, como quienes se dedican a la gestión financiera y

operativa del puerto, los acuerdos contractuales con terceros, explotación de los sistemas portuarios y su diseño, incluidos los programas informáticos de ciberseguridad y la gestión de tareas de protección como la respuesta ante incidentes. En consecuencia, sirve de orientación para los criterios cibernéticos a seguir para la seguridad de los buques.

Por su parte, tal y como se ha comentado desde el inicio del presente trabajo; según la ENISA (2020) el comercio mundial está determinado por el comercio marítimo. A medida que el sector sufre una transformación digital con la convergencia entre TI y OT, el perfil del riesgo cibernético cambia. Por ende, junto con los múltiples ciberataques, este cambio presenta la necesidad de abordar con precisión la ciberseguridad marítima.

En Europa también cabe destacar que en la segunda conferencia de Ciberseguridad Marítima celebrada el año pasado, en la ENISA, se exploraron las ciberamenazas que está sufriendo el sector y los retos a los que se deberá enfrentar (Drougkas y De Sousa Figueiredo, 2020).

Se dejó constancia de la problemática creciente que surge en los buques marítimos autónomos respecto de los tradicionales, el riesgo cambia y en los automáticos atacan directamente a la ingeniería social y aspectos en la red.

Se hizo especial hincapié en los ataques a la cadena de suministros y en los múltiples espacios de ciberseguridad existentes ya que un incidente en la cadena de suministro podría generar un efecto en cascada en todos los puertos europeos con efectos desastroso para la los buques y la economía global.

Drougkas y De Sousa Figueiredo (2020) declararon que la ciberseguridad es un tema necesario a tratar y que se dedicará durante los próximos años a su estudio con el objetivo de mejorar las políticas existentes. Centrándose en la necesidad de concienciar, por parte de los Estados miembros y de la Comisión Europea, a los entes intervinientes en el sector y en el intercambio de información sobre métodos para gestionar la ciberseguridad marítima.

4. Intentos legislativos para abordar las cuestiones legales del riesgo cibernético

A pesar que muchas de ellas han sido comentadas con anterioridad durante el presente trabajo, cabe agrupar las iniciativas surgidas por parte de las agencias internacionales con el fin de procurar una mejor gestión del riesgo cibernético y estudiar en profundidad sus regulaciones.

En primer lugar, la IMO ha realizado dos resoluciones sobre la temática del riesgo cibernético. En primer lugar, la Resolución MSC.428(98) Gestión del riesgo cibernético marítimo en los sistemas de gestión de la seguridad, de fecha 16 junio de 2017, la cual anima a las Administraciones de los Estados parte a garantizar que los riesgos cibernéticos se protejan de forma adecuada los sistemas de seguridad de los buques.

En segundo lugar, las Directrices sobre la gestión de los riesgos cibernéticos marítimos, de 5 julio 2017, la cuales recomiendan ciertos elementos y procesos para gestionar de forma eficaz el riesgo cibernético marítimo. En ella se establece que la mejor gestión del riesgo cibernético se realiza partiendo de cinco premisas básicas: identificar, proteger, detectar, responder y recuperar.

Por su lado, BIMCO ha elaborado una cláusula de Ciberseguridad estándar para su inclusión en contratos. La cláusula se publica en BIMCO 2019 bajo el nombre "*Cyber Security clause"*. Constituye un paso adelante ante la posible regulación de una cláusula estándar de obligaciones recíprocas de ciberseguridad. Esta cláusula exige a las partes mantener un nivel de ciberseguridad "adecuado" a sus negocios y "esfuerzos razonables" con el fin de garantizar que sus subcontratistas hagan lo mismo. Sin embargo, en la práctica aún no se aplica de forma usual.

Contiene la obligación de notificar el incidente en menos de 12 horas y exige tomar medidas "razonables" para mitigar y resolver el incidente. No obstante, la cláusula ni aborda el fraude de pagos ni contiene disposiciones de fuerza mayor por lo que las partes no están exentas del cumplimiento del resto de obligaciones establecidas en el contrato.

Por otro lado, la cláusula establece que, en caso de incumplimiento por negligencia grave o dolo, el límite aconsejable y subsidiario por daños y perjuicios es de 100.000 dólares.

La presente cláusula se estudia en profundidad en el capítulo IV primer punto del presente trabajo, al cual me remito para la explicación de sus problemáticas y con el fin de poder acomodarla para su introducción en una póliza de seguro. Todo ello con el propósito de poder realizar una cláusula que cubra los ciberataques, siendo, por tanto, necesaria una cláusula que exija ciertos criterios mínimos de Ciberseguridad.

Así, tal y como se ha plasmado a lo largo del presente trabajo, la cláusula citada es la única existente que plantea obligaciones recíprocas de ciberseguridad. Sin embargo, a pesar de ser un gran avance no es aceptada por el tráfico del sector (Howden, 2020). La primera deficiencia que presenta es su propósito. Como plasma la misma, la intención de su creación es sensibilizar a propietarios, fletadores y agentes sobre los

riesgos cibernéticos. A pesar de ello, no se ha logrado pues no está siendo de aplicación.

En este sentido, su segundo propósito radica sobre la premisa de proporcionar un mecanismo para garantizar que las partes del contrato dispongan de sistemas que contribuyan a minimizar el riesgo a que se produzca un incidente y, en caso que se lleve a cabo, mitigar sus efectos (BIMCO et. al, 2019). Su alcance ha sido motivador, pero ciertamente, escaso.

Por su parte, el lenguaje utilizado en la cláusula es amplio y fácil de ser cuestionado ante los juzgados. Palabras tales como "*esfuerzos razonables", "razonablemente posible"* o *"tomar medidas razonables".*

Sin embargo, teniendo en cuenta que es pionera en su campo, es oportuno destacar que consolida un gran paso ante una regulación y conciencia mayor sobre el riesgo cibernético. Además, la cláusula comienza con una definición de los términos técnicos que pueden ser desconocidos para una de las partes.

Sin embargo, las definiciones son escasas y no propiamente técnicas. Hecho que puede derivar en controversias, tal y como ocurre con la C380 (De Maurier, 1967) por no tener definiciones claras y discrepar con su significado técnico. Además, únicamente se definen las siguientes palabras: "incidente de ciberseguridad", "ciberseguridad" y "entorno digital".

En consecuencia, para poder amoldar la cláusula para su posible incorporación en una póliza de seguro es preciso comenzar señalando que las pólizas de seguro cibernético en cualquier sector se describen como costosas y aún están lejos de tener un precio justo (Biener, Eling y Hendrick, 2015, 17). Esto es debido a la novedad del producto, el reducido número de participantes, la escasez de datos y la costosa verificación del estado y evaluación previa del riesgo.

Por otra parte, con el propósito de establecer unas normas básicas para la gestión del riesgo cibernético marítimo y establecer un proceso para operar, revisar y mejorar el Sistema de Gestión de la Seguridad la Información (en adelante, SGSI), tanto a bordo como en tierra, las normas ISO27000 se dirigen a armadores y partes interesadas del negocio marítimo. La certificación que han creado es para poder probar un SGSI óptimo y actualizado (Howden, 2020).

Bajo esta tesitura es dable destacar que los P&I realizan análisis de carencias en el seguro marítimo frente a la posible cobertura de riesgos cibernéticos en atención a cada asegurado en particular, no de forma estándar (Soyer, 2018).

IV. PROPUESTA INNOVADORA DE UNA CLÁUSULA ESTÁNDAR QUE CUBRA EL RIESGO CIBERNÉTICO

1. Cláusula previa sobre exigencias de Ciberseguridad

Las premisas básicas para que un seguro sea eficiente y eficaz son el conocimiento del riesgo, su evaluación e impacto en el sector. En consecuencia, no es posible realizar una cláusula innovadora que cubra el riesgo cibernético sin adecuar una cláusula sobre ciberseguridad a las necesidades actuales del sector.

En este sentido, a continuación, se propone una cláusula estándar que ordene una correcta Ciberseguridad, tomando como base la Cláusula de Ciberseguridad creada por BIMCO 2019 "*Cyber Security clause".* La cláusula anterior se amplia y se amolda para su posible incorporación a una póliza de seguro.

En consecuencia:

Cláusula de Ciberseguridad CL2 – 2023/ESP/TFMUAO

En primer lugar, los términos descritos a continuación se entenderán en la presente cláusula como:

La **"Ciberseguridad"** se refiere a la práctica de proteger recursos tecnológicos, sistemas, redes y datos digitales de posibles ciberataques mediante sistemas de ciberseguridad (Lyons, 2020). Su objetivo es garantizar la confidencialidad e integridad de la información en espacios digitales (IBM, 2020).

Los **"Sistemas de Ciberseguridad"** son el conjunto de recursos tecnológicos, métodos y regulaciones diseñados para identificar, prevenir, mitigar y responder ante ciberataques. Estos sistemas comprenden *firewalls*, detección de intrusos y gestión de vulnerabilidades. Su objetivo es salvaguardar los recursos tecnológicos de posibles intrusiones (IBM, 2020). En consecuencia, están programados para mantener a salvo la ciberseguridad de los recursos tecnológicos de la empresa.

Los "**Recursos tecnológicos**" tangibles son los dispositivos electrónicos tales como ordenadores, móviles inteligentes, servidores*, pdas,* tabletas e intangibles o transversales son los sistemas digitales tales como *softwares*, redes de comunicación, servicios en línea y aplicaciones (Lyons, 2020).

Los **"Ciberataques"** son un intento malicioso y no autorizado que consigue quebrantar un espacio digital y generar la pérdida, destrucción, robo o alteración de

activos, datos o información no deseados. Los ciberataques pueden producirse vía *ransomware*, *malware,* o *phishing* y *spear phishiing* (Daniel Mija, 2021).

El **"Espacio digital"** es el conjunto de sistemas electrónicos conectados a un entorno digital o red, ya sea pública o privada, en la que se realizan operaciones, intercambio de datos y transacciones. Ergo también se incluyen recursos tecnológicos y la información guardada en ellos (IBM, 2020).

a. El incumplimiento de la presente cláusula dejará sin efectos la Cláusula de Cobertura de Ciberataque CL1 – 2023ESP/UAOTFM. Por consiguiente, el asegurado perderá todo derecho a indemnización bajo esa cláusula.
b. La parte asegurada debe cumplir las siguientes obligaciones:
    i. Contar con sistemas de ciberseguridad adecuados, actualizados y eficaces con el fin que su ciberseguridad no se vea comprometida y sea técnicamente difícil de quebrantar (Singh, 2019). Haciendo hincapié en la ciberseguridad de los sistemas que prosiguen;
        1. Sistemas de gestión de carga y estiba.
        2. Sistemas de puente.
        3. Sistemas de arranque y gestión de la maquinaria y control de la velocidad.
        4. Sistema de atención y gestión de pasajeros.
        5. Sistemas de control de acceso de Redes públicas orientadas a pasajeros.
        6. Sistemas de comunicación.
        7. Sistemas administrativos y de bienestar de la tripulación.
        8. Sistemas de datos de la navegación.
    ii. Contar con protocolos de respuesta actualizados, eficaces y eficientes ante la producción de un ciberataque (Daniel Mija, 2021).
    iii. Realizar cada trimestre verificaciones e inventario de sus sistemas de ciberseguridad y guardar su registro favorable durante 3 años.
        1. Inventario de dispositivos de comunicación y comunicación en red.
        2. Inventarios de software.
        3. Inventario de servicio de red para cada equipo.
        4. Mapa lógico de redes.
c. La parte asegurada requerirá a terceros que presten servicios en su nombre, en relación con el presente contrato, documentación que acredite el cumplimiento de la subcláusula b. i y iii.

d. Desde que la parte asegurada tenga conocimiento de un ciberataque que pueda afectar a la ciberseguridad de cualquiera de las demás partes, debe notificarlo de forma inmediata (Gürses, 2023).
    i. Ante un ciberataque, la parte asegurada debe:
        1. Aplicar el protocolo de respuesta de forma inmediata para mitigar y/o resolver el ciberataque; y
        2. Tan pronto como sea posible, pero a más tardar 12 horas después de la primera notificación, proporcionar a la otra parte un informe sobre que vía es la más segura para comunicarse con ella y toda información relativa al ciberataque que tenga en sus manos con el fin de mitigar y/o prevenir cualquier efecto del incidente. Obligatoriamente debe constar la situación en la que se encuentran, como les ha afectado y como tratan de mitigarlo. A ser posible el presunto origen del ciberataque y como pretenden resolverlo.
    ii. Cada Parte debe compartir con la otra parte cualquier información que disponga posteriormente y pueda ayudar a la otra parte a mitigar y/o prevenir los efectos del ciberataque (Howden, 2020).

2. Cláusula de cobertura del riesgo cibernético en el contrato de seguro marítimo

Tras todo el estudio realizado y la elaboración de una cláusula estándar eficaz de ciberseguridad, a continuación, se presenta la propuesta de una cláusula estándar que cubra el ciberataque**.** Para evitar reiteraciones es dable añadir que la definición de la terminología presentada en la cláusula anterior será aplicable a la presente, más las nuevas necesarias aplicadas únicamente a la presente cláusula.

Sobre las posibles cuestiones que se puedan suscitar dentro de la misma, su definición e interpretación corresponderá a lo contemplado en el presente trabajo.

En consecuencia:

Cláusula de Cobertura de Ciberataque - CL1 – 2023/ESP/TFMUAO

En primer lugar, los términos descritos a continuación se entenderán en la presente cláusulas como:

La “**Doctrina de causa próxima**” corresponde a cualquier conexión causal entre el siniestro y el funcionamiento de un ordenador, sistema informativo, virus, código malicioso o cualquier proceso o sistema electrónico con el propósito de influir un daño quedaría cubierto (Soyer, 2018). La causa indirecta necesita únicamente una relación

de cadena de causalidad. En consecuencia, debe entenderse como causa del siniestro cibernética la causa que directa o indirectamente haya contribuido al daño (Soyer, 2018).

a. Sujeto únicamente al contenido de esta cláusula y la Cláusula de Ciberseguridad CL2 – 2023/ESP/TFMUAO, el presente contrato cubrirá las pérdidas, daños, responsabilidades o gastos causados directamente por o a los que se haya contribuido o que se deriven del uso o funcionamiento como medio para infligir daños, de forma malintencionada o no, a través de cualquier ordenador, sistema informático, *software*, programa informático o proceso o cualquier sistema electrónico.

   A continuación, se recoge una lista que incluye las pérdidas, daños, responsabilidad o gastos derivados de:

   i. Interrupción de la actividad (Soyer,2018).
   ii. Ciberextorsión y fraude de pagos (Soyer,2018).

      Únicamente sí:

      1. El asegurado haya respaldado la decisión (ABI, 2023) y;
      2. El asegurador haya respaldado la decisión (ABI, 2023).

      Sin embargo,

      1. Si en virtud de su protocolo de respuesta ante un ciberataque el asegurado realiza el pago y sufre otro ciberataque habiendo adoptado las medidas de prevención adecuadas según su protocolo de respuesta, la responsabilidad queda cubierta hasta un límite de ….. (o, si se deja en blanco, 500.000€).

   iii. Gastos en gestión de crisis (incluida notificación, asistencia y relaciones públicas).
   iv. Daños materiales como la recuperación de datos (IBM, 2020).
   v. Responsabilidad ante terceros cuyos datos han sido dañados o violados como resultado de un ciberataque al asegurado.
   vi. Terrorismo, guerra civil, revolución, rebelión, disturbios civiles, acto hostil o beligerante (Soyer, 2018, 640).
   vii. La interpretación de la presente cláusula está sujeta a la Doctrina de la causa próxima. (Soyer, 2018, 641).

b. La presente cláusula prohíbe la cláusula silenciosa y la doble cobertura del riesgo, en consecuencia:

   i. La presente cláusula es la única que regula la cobertura de un riesgo cibernético.

ii. La presente póliza no cubre situaciones cibernéticas más allá de las plasmadas en la presente póliza.

c. Respecto al cálculo de la indemnización, el valor del lucro cesante en las pólizas cibernéticas se calcula por referencia al beneficio neto más los costes fijos continuados (Soyer, 2018). El límite de la indemnización será de ……. (o, si se deja en blanco, 1.000.000€).

Así queda plasmado el primer intento por realizar una cláusula que cubra el riesgo cibernético en atención a los criterios de los aseguradores y las necesidades actuales del sector.

V. CONCLUSIONES

La tecnología está presente en todos los sectores, incluido el marítimo. Sin embargo, está constituido por una industria basada en hábitos analógicos, el seguro marítimo. Así se ha comprobado tras un estudio exhaustivo del seguro marítimo tradicional regulado en la LNM y en las influencias anglosajonas aceptadas por el sector ya que nada se dice sobre los riesgos tecnológicos. Además, pocos son los estudios realizados sobre el riesgo cibernético y su aplicación.

Debido a ello, después de realizar un estudio sobre la regulación del seguro marítimo, poco nos esclarece sobre la temática que nos ocupa; ni nuestra doctrina nos ayuda a entender como proseguir ante un riesgo cibernético en la industria marítima. Sin embargo, era necesario estudiar la institución del seguro marítimo con el propósito de comprobar si se hacía mención de alguna manera en su articulado al riesgo cibernético. Además de estudiar las tipologías existentes de seguro marítimo para prestar mayor atención a otros aspectos, elementos o requisitos del seguro.

En consecuencia, tras analizar la institución del seguro marítimo en atención al riesgo cibernético es importante destacar, en primer lugar, la falta de jurisprudencia, legislación y práctica existente sobre la temática, ya no solo a nivel estatal sino también como se ha podido comprobar, a nivel internacional. Lo que demuestra de forma palpable una falta de interés por el estudio del riesgo cibernético.

Primero, comenzando por el hecho que la industria marítima constituye una pieza clave para con el bienestar económico de la población global en atención a su economía y transporte de personas, medicamentos y alimentos de primera necesidad y, tal y como afirma UNCTAD (2021) está sufriendo un crecimiento notorio los últimos años y se configura como un sector clave para el progreso de la economía mundial. Por ende, es indispensable que la industria marítima opere con normalidad.

De esta forma, ha sido vital para el progreso del trabajo estudiar los requisitos o problemas legales que se encontraban los aseguradores ante la posible cobertura de un riesgo cibernético, partiendo de la práctica existente en otros sectores, debido a que no hay constancia sobre prácticas en el marítimo.

Por otro lado, el riesgo cibernético ha sido objeto de controversia en múltiples reuniones de profesionales marítimos a nivel internacional en la que tal y como nos plasma Farrar (2019) se han cuestionado las problemáticas legales para la adecuación de los seguros tradicionales a los riesgos cibernéticos.

Desgraciadamente, tal y como nos presenta Crawford (2019) los riesgos cibernéticos crecen de forma rápida mientras que, debido a los lentos intentos de actualización, las

protecciones cibernéticas en el sector marítimo quedan obsoletas. Lo que genera que los ciberdelincuentes aprovechen dichas vulnerabilidades para atacar con más asiduidad.

Son múltiples los ataques que ya ha sufrido la industria marítima y que, cada vez más, empiezan a sufrir tanto puertos como buques, plataformas petrolíferas, entre otros usuarios del sector (TransNav, 2021). No se salva nadie ante los ciberataques y el sector marítimo ha quedado probado que no es una excepción. A título de ejemplo es dable recordar que Kovacs (2020) nos cita que incluso la IMO, agencia marítima de la ONU, ha sido víctima de un ciberataque.

Bajo la tesitura de los ciberataques, son tres las tipologías de ataque usuales llevadas a cabo por los ciberdelincuentes, escogidas conforme la vulnerabilidad que presenta cada usuario del sector. Con independencia que sean entidades del sector púbico o del sector privado.

Además, se ha comprobado que los daños pueden llegar a ser desastrosos, tanto para la entidad que sufre el ciberataque como para la economía mundial por la relevancia que sustenta la industria marítima.

En consecuencia, tras el aumento de ciberataques en la industria marítima por la pandemia del Covid-19, las organizaciones internacionales han empezado a preocuparse por la ciberseguridad y los efectos que puede generar la falta de aseguramiento ante tales riesgos. Sin embargo, como se ha plasmado, se preocupan más por la vertiente de ciberseguridad y no generan incentivos para que los aseguradores se propongan asegurar un riesgo que es contrario a su forma de actuación.

Por ende, se llega a la conclusión que el riesgo cibernético, a pesar de ser palpablemente un riesgo existente en la industria marítima, no está en la posición de importancia que debería estar frente a las organizaciones internacionales, Estados y grandes compañías.

Además, la LNM no dice nada sobre el riesgo cibernético ni los seguros que cubren los ciberataques. A través de una óptica internacional únicamente se encuentra una cláusula, pero con obligaciones reciprocas de ciberseguridad entre las partes de un contrato. En consecuencia, no existe ninguna cláusula estándar que cubra el riesgo cibernético para poder ser incorporada en un seguro marítimo.

Soyer (2018) plasma el porqué de la no existencia de esta cláusula a pesar de su notoria importancia. Los ciberataques se actualizan, mejoran, cambian, se ocultan… de tal forma que no pueden ser estudiados ni previsibles para poder realizar una

cláusula que lo cubra. Sin embargo, existen seguros que cubren el riesgo cibernético en otros sectores.

Reiterar que no existen referencias legales sobre los ciberseguros en el sector marítimo español y muy poco a nivel internacional. En tanto a la jurisprudencia únicamente existe una sentencia de un tribunal inglés sobre la interpretación de la cláusula de exclusión del riesgo cibernético. Su razón se sustenta en que no hay seguros que cubran los ciberataques en el mundo marítimo.

Sin embargo, tal y como dice Soyer (2018) y la Comisión Europea (2023), los ataques cibernéticos van a seguir creciendo exponencialmente. En este sentido, es posible afirmar que el riesgo cibernético es el gran excluido de los seguros marítimos a pesar que sea inminentemente necesario. Incluso se puede llegar a afirmar que el riesgo cibernético es el gran olvidado de Derecho Marítimo ya que, a pesar de ser el gran peligro de nuestra era tecnológica, el legislador no responde de forma eficaz ante las problemáticas existentes.

Quienes se han movilizado son los aseguradores para excluir los riesgos cibernéticos en sus pólizas de seguros. Ya que no hay presión por parte de los profesionales del sector ni de los Estados ni organizaciones internacionales para que cubran este riesgo aunque sean múltiples las vulnerabilidades cibernéticas existentes en un buque.

En plena era de la tecnología en la que todos los sectores se ven afectados por los ciberataques, el sector marítimo no es una excepción y la cantidad de ciberataques en las próximas décadas aumentará de forma exponencial. No es posible que un sector que afecta en tal escala a la economía mundial, no se proteja ante el riesgo de nuestra generación, de nuestra era tecnológica. Los daños que puede provocar un ciberataque ya no solo pueden abarcar a una empresa sino a la economía global.

Bajo esta tesitura, la elaboración de un clausulado estándar que cubra el riesgo cibernético en los seguros marítimos es sencillamente elemental. Una tarea compleja ante la falta de doctrina, regulación y práctica sobre la materia, pero al mismo tiempo necesaria. Con el propósito de crear una base para su aplicación práctica, tras el estudio realizado en este TFM es imprescindible la movilización del sector por implementar una cláusula que pueda cubrir este riesgo.

En consecuencia, la cláusula elaborada da respuesta a la necesidad que presenta el sector marítimo. Por ende, tomando por base las cláusulas que cubren los ciberataques en otros sectores y las problemáticas estudiadas en el sector marítimo, se da solución a la cobertura de un riesgo cibernético en este sector.

Así, la cláusula debía cubrir los riesgos cibernéticos esenciales que cubren las pólizas de seguros cibernéticos en otros sectores para que fuese eficaz, útil y que los aseguradores quisieran aplicarla y, al mismo tiempo, cubriese las necesidades reales de los clientes. Por ello, se incluyen tanto la ciberextorsión, como los gastos de gestión de crisis, daños materiales como la recuperación de datos, pérdida de datos con la inclusión del pago a terceros por la vulneración de sus datos y, por último, las multas y sanciones.

La razón de ser de la cláusula es la incorporación de la misma en una póliza de seguro marítimo. Al mismo tiempo, modernizar la industria vetusta que configura el seguro marítimo dejando los hábitos analógicos a un lado y actualizarla a las necesidades reales de la era tecnológica. Marcar un punto y aparte en el desconocimiento del riesgo cibernético en las pólizas de los seguros marítimos e incorporar dicha cláusula en los seguros marítimos españoles. Su propósito era marcar el cambio, un acercamiento a su regulación, un acercamiento a la protección de este riesgo que está agonizando al sector.

Como se ha presentado, no existe ninguna otra cláusula en pólizas y es escasa la jurisprudencia y doctrina sobre la materia. Por ello, con el fin de evitar una interpretación equivocada de los tecnicismos y palabras incorporadas en la cláusula, primero, propio de los seguros americanos, se elabora un listado con la definición de aquellas palabras que pueden llegar a controversia por la falta de conocimiento del asegurado sobre esta temática, así como un resguardo para los aseguradores. Las definiciones se fundamentan en la definición técnica de la palabra.

Sin embargo, es evidente que por la problemática que significa para los aseguradores cubrir un riesgo tan cambiante como es el ciberriesgo, era necesaria además una cláusula con obligaciones cibernéticas a cumplir por asegurado con el fin de proteger a los aseguradores de un asegurado vulnerable a los ciberataques. Por tanto, como cláusula adscrita a la cláusula que cubre los ciberataques era necesario elaborar, además, una cláusula con exigencias cibernéticas para que la cláusula del riesgo cibernético cubra o no el siniestro.

La cláusula que regula criterios de ciberseguridad se fundamenta en la exigencia de unos requisitos básicos de protección cibernética de aquellos sistemas, estudiados en el presente trabajo, que se configuran como vulnerables ante posibles ciberataques. Además de exigir los inventarios de ciberseguridad que plasma la Recomendación 166 de la IACS bajo el título de Recomendación de Ciberresilencia, harmonizada el 1 de abril de 2020.

Así, se puede llegar a la conclusión de que, a pesar de los intentos de las organizaciones internacionales por elaborar directrices de buenas prácticas en atención a la ciberseguridad, si los profesionales del sector no se percatan de la importancia del riesgo cibernético y no toman medidas de ciberseguridad eficaces, los aseguradores no serán quienes quieran dar el paso por protegerles ante un riesgo que prefieren no proteger.

En consecuencia, urge concienciar a los usuarios del sector marítimo, a la doctrina, a los aseguradores, a los profesionales, a las organizaciones internacionales y a los Estados para con el interés por el riesgo cibernético, su cobertura, su problemática y su necesidad de regulación sistemática.

No es por tanto un problema únicamente para con el sector sino de los Estados y organizaciones. Un ciberataque en el sector marítimo podría desestructurar la economía mundial. En consecuencia, es esencial tanto una mayor eficacia cibernética ante ciberataques como una regulación del riesgo cibernético.

Como se ha dejado claro en la introducción, el presente trabajo no pretendía elaborar una guía de buenas prácticas técnica para que un buque pueda ser ciberasegurado pues escapa de lo que sería el ámbito legal. Sin embargo, necesariamente para poder realizar la cláusula era preceptivo tanto el estudio de las vulnerabilidades como presentar aquellos aspectos técnicos esenciales que quedarían cubiertos y así poder elaborar una cláusula previa de ciberseguridad.

Por tanto, una cláusula incorporada dentro de un seguro marítimo que cubra el riesgo cibernético en los buques no es el futuro, sino el presente inmediato. Nada más lejos de la realidad pues ya existen seguros en otros sectores que cubren el riesgo mencionado y, de facto, no es descabellado reclamar que también exista uno en la industria marítima.

Sin embargo, para ello es necesario que el sector marítimo se movilice, reclame un seguro que cubra el riesgo descrito y exija una protección eficaz y eficiente frente al mismo, en el que ambas partes estén satisfechas. A partir de la pandemia del Covid-19 las organizaciones Internacionales han empezado a cuestionarse la problemática del riesgo cibernético, pero espero que no sea necesaria otra pandemia a nivel mundial para que los altos dirigentes del sector público y privado se percaten que es un riesgo real que está a la orden del día y que debe ser paliado cuanto antes mejor.

Con el fin de ayudar a los aseguradores y profesionales, es indispensable que los teóricos y el legislador realicen una regulación eficaz ya no solo a nivel estatal sino también de forma internacional. Los ciberataques a nivel global constituyen una de las

mayores preocupaciones de todos los profesionales y el marítimo no puede ser una excepción debido a que ha sido víctima de ciberataques alarmantes y las pérdidas pueden ser descomunales.

Para finalizar, la cláusula propuesta constituye una aproximación a la regulación de este riesgo olvidado por el sector y un paso adelante para su protección. De este modo, ha quedado probado que era necesaria una cláusula estándar que cubra el riesgo cibernético y ésta sería una propuesta general eficaz. No se entiende como aún no existe una cobertura de un riesgo que está sembrando el pánico en toda la industria y que ha afectado incluso a las mayores empresas del sector.

Así la cláusula elaborada está preparada para su aplicación dentro de cualquier seguro marítimo tradicional para que el riesgo cibernético tenga protección y en general el sector marítimo pueda estar ciberasegurado. Sin embargo, debido a la constante evolución que presentan los riesgos cibernéticos la misma puede ser objeto de ulteriores modificaciones con el fin de prestar mejores servicios a los profesionales del sector.

Es necesario prestar atención al riesgo cibernético e intentar combatirlo a través de todos sus ámbitos. Esa lucha solo puede comenzar por un seguro que proteja al asegurado ante los riesgos cibernéticos.

VI. BIBLIOGRAFÍA

1. Doctrina

Arroyo Martínez, I. (2014). *Compendio de derecho marítimo (Ley 14/2014, de navegación marítima*. (ed. 8) Madrid: Editorial Tecnos.

Biener C., Eling, M., y Hendrick, J. (2015). *Insurability of Cyber Risk: An Empirical Analysis.* En *Working papers on risk management and insurance no. 151* (pp. 131- 159). Suecia: Hato Schmeiser.

Drougkas A. y De Sousa Figueiredo, R. (14-15 de octubre de 2020). *Preparing maritime for emerging cybersecurity challenges.* Conferencia de European Union Agency for Cybersecurity, Lisboa, Portugal.

Erstad, E., Ostnes, R., & Lund, M. S. (2021). An operational approach to maritime cyber resilience. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(1), 27-34. https://doi.org/10.12716/1001.15.01.01

Erstad, E., Hopcraft, R., Palbar, J. D., & Tam, K. (2023). CERP: a maritime Cyber risk decision making tool. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *17*(2), 269-279. https://doi.org/10.12716/1001.17.02.02

Fotinopoulou Basurko, O (2017). *New Trends in Maritime Law*. Pamplona: Aranzadi.

Fuentes Carsi, F. (1946). La Corporación «Lloyd's» en el Seguro Marítimo Español. *Revista critica de derecho inmobiliario* (v.213), pp. 85 – 93.

Girgado (2017). En torno al alcance de la fijación convencional del valor del interés asegurado en los seguros de cascos. Comentario a la SAP Islas Baleares de 6 de junio de 2016. *Revista de Derecho del Transporte*, (v.19), pp. 434 - 441.

Gürses, O. (2023) *Marine Insurance Law.*(ed.3). Londres: Routledge.

Jao, J., y Chuah, J. (2023). Cyber and AI security challenges for LNG maritime transport and terminals—Responses in law and standards. *The Journal of World Energy Law & Business*, *16*(4), 354-366. https://doi.org/10.1093/jwelb/jwad014

Kumar (1949). Life Insurancee Corporation of India. *Lloyd's* (174), pp. 140 a 156.

Otto.L. (2021): *Global Challenges in Maritime Security* An IntroductionAdvanced Sciences and Technologies for Security Applications. Londres: *Springer International publishing.*

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

Rodriguez Carríon, J (2003). *Los Seguros Marítimos y aéreos* (v.1). Madrid: Marcial Pons*.*

Ruiz Soroa, Arranz de Diego y Zabaleta Sarasua (1993). *Manual de Derecho del Seguro Marítimo.* Vitoria: Escuela de Administración Marítima.

Salinas Adelantado (2015). *El seguro de buques en la Ley de Navegación Marítima.* En *Asociación Española de Derecho Marítimo, Comentarios a la Ley de Navegación* Marítima (pp. 337-296), Madrid: Dykinson.

Sánchez Calero (2010). *Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, de 8 de octubre, y a sus modificaciones*. Pamplona: Aranzadi.

Sierra Noguero (2016). *El Seguro de Responsabilidad Civil derivada de la navegación de buques.* Madrid: Fundación Mapfre.

Singh, H. (2019) *Cyber Security in Maritime Industry*: The exposures, Risks, Preventions and Legal Scenarios (Tesis doctoral, *University of Oslo,* 2020,1,56).

Soyer, B. (2018). *Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems.* En *Maritime Law In Motion*(1) (1) (pp. 627-642) Londres :Springer Cham.

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2011). A survey of cyber crimes. *Security and Communication Networks*, *5*(4), 422-437. https://doi.org/10.1002/sec.331

2. Referencias bibliográficas web

ABI (2023). *What does cyber insurance cover?.* Recuperado en fecha 4 de junio de 2023, desde https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/#:~:text=Cyber%20insurance%20covers%20the%20losses,arising%20from%20a%20cyber%20event

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners [INTERCARGO], InterManager, International Association of Independent Tanker Owners [INTERTANKO], International Chamber of Shipping [ICS], International Union of Marine Insurance [IUMI], Oil Companies International Marine Forum [OCIMF], Superyacht Builders Association [Sybass] y World Shipping Council [WSC](2023). *The Guidelines on Cyber Security onboard Ships - Version 4.* Recuperado en fecha 2 de abril de 2023, desde https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Bøe, E. y Jordheim, H. (2020). *Politiet etterforsker dataangrepet mot Hurtigruten.* Recuperado en fecha 2 de abril de 2023, desde https://e24.no/hav-og-sjoemat/i/7KPeEK/politiet-etterforsker-dataangrepet-mot-hurtigruten

Castro Pereira, A. (2022). *La gestión de los riesgos cibernéticos en los sistemas de seguridad en buques y empresas navieras.* Recuperado en fecha 4 de abril de 20023, desde https://armada.defensa.gob.es/archivo/rgm/2022/03/rgmmar2022cap03.pdf

Costas Paris (2018) *China's Cosco Shipping Hit by Cyberattack in U.S. The Wall Street Journal.* Recuperado en fecha 2 de abril de 2023, desde https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557

Court of Appeal (Civil Division)(2005). *Tektrol Ltd v International Insurance Company of Hanover Ltd.* Recuperado en fecha 3 de mayo de 2023, desde https://vlex.co.uk/vid/tektrol-ltd-v-international-793545037

Crawford, J. (2019) *Ciberataque al transporte marítimo ¿amenaza real o ciencia ficción?* Recuperado en fecha 23 de abril de 2023, desde https://revistamarina.cl/es/articulo/ciberataque-al-transporte-maritimo-amenaza-real-o-ciencia-ficcion

CSO Alliance (2023). *Maritime Cyber Alliance.* Recuperado en fecha 4 de abril de 2023, desde https://maritimecyberalliance.com/

Daniel Mija, K. (2021). *Riesgo Cibernético Marítimo*. Recuperado en fecha 23 de abril de 2023, desde https://marineandnavalengineering.com/articulos/riesgo-cibernetico-maritimo/

DataPolis (2009). *Institute Time Clauses – Hulls (1.10.83)*. Recuperado en fecha 3 de diciembre de 2023, desde https://datapolis.id/wp-content/uploads/2018/07/Institute-Time-Clauses-%E2%80%93-Hulls-Disbursements-and-Increased-Value-%E2%80%93-1-10-83-%E2%80%93-Cl.-290.pdf

Det Norske Veritas group [DNV] (2023). *Ciber priority 2023*. Recuperado en fecha 3 de abril de 2023, desde https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html?utm_source=google&utm_medium=cpc&utm_campaign=Maritime-Energy-EU-Pmax&gad=1&gclid=Cj0KCQjwrfymBhCTARIsADXTablDgvwoSSqdNWKcu3zCYvjbFtkEs4wo4RMw32oZESZ5uGTHq28ykE0aAiPHEALw_wcB

Farrar, B. (2019). *Cybersecurity: The new Enigma* [Archivo PDF]. Recuperado en fecha 1 de enero de 2023, desde https://www.sunymaritime.edu/sites/default/files/2019-12/Panel3_BF.pdf

Hill Dickinson (2017). MSC Mediterranean Shipping Company S.A. -v- Glencore International AG [2017] EWCA Civ 365. Recuperado en fecha 2 de enero de 2023, desde https://www.hilldickinson.com/insights/articles/msc-mediterranean-shipping-company-sa-v-glencore-international-ag-2017-ewca-civ

Howden (2020). *Marine Cyber riesk insurance*. Recuperado en fecha 4 de junio de 2023, desde https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden

IACS (2020). *Recommendation 166 on Ciber Resilience.* Recuperado en fecha 2 de marzo de 2023, desde https://iacs.org.uk/news/iacs-launches-single-standalone-recommendation-on-cyber-resilience/https://www.mundomaritimo.cl/noticias/ics-abordo-los-desafios-e-implicancias-de-la-ciberseguridad-en-el-transporte-maritimo-mundial

IBM (2020). *What is cybersecurty?.* Recuperado en 2 de junio de 2023, desde https://www.ibm.com/topics/cybersecurity

If- insurance (2009). *Institute of Cargo Clauses 2009*. Recuperado en fecha 3 de diciembre de 2023, desde https://www.if-insurance.com/globalassets/industrial/files/marine-cargo/institute-clauses/institute-cargo-clauses-a-2009.pdf

If- Insurance (2019). *Marine Cyber Endorsement- LMA5403.* Recuperado en fecha 1 de abril de 2023, desde https://www.if-insurance.com/globalassets/industrial/files/marine-cargo/institute-clauses/marine-cyber-endorsement-lma-5403.pdf

Instituto Nacional de Normas y Tecnologías [NIST] (2018) *Marco de mejora de la ciberseguridad de las infraestructuras críticas* Recuperado en fecha 3 de abril de 2023, desde https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

International Maritime Organization [IMO](1993). *Código internacional de gestion de la seguridad operacional del buque y la prevencion de la contaminacion (codigo internacional de gestion de la seguridad cgs). resolucion a.741(18), adoptada el 4 de noviembre de 1993, por la conferencia de los gobiernos contratantes del convenio internacional para la seguridad de la vida humana en el mar 1974.* Recuperado en fecha 3 de abril de 2023, desde https://www.mitma.es/recursos_mfom/pdf/FD0AEFA6-E601-4470-B6EEA41E8393DDEC/121763/CODIGOIGS.pdf

International Maritime Organization [IMO] (2017). *Directrices sobre la gestión de los riesgos cibernéticos marítimos, de 5 julio 2017.* Recuperado en fecha 3 de abril de 2023, desde https://wwwcdn.imo.org/localresources/es/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20%20Directrices%20Sobre%20La%20Gesti%C3%B3n%20De%20Los%20Riesgos%20Cibern%C3%A9ticos%20Mar%C3%ADtimos%20(Secretar%C3%ADa)%20(1).pdf

International Maritime Organization [IMO] (2017). *Revised 2017 compliance procedures and mechanisms pursuant to article 11 of the 1996 protocol to the london convention 1972 (Adopted in 2007: LC 29/17, annex 7).* Recuperado en fecha 30 de marzo de 2023, desde https://wwwcdn.imo.org/localresources/en/OurWork/Environment/Documents/Revised%202017%20CPM.pdf

INCIBE (2019). *Estándares de Seguridad en el Mar.* Recuperado en fecha 4 de abril de 2023, desde Estandares Ciberseguridad El Mar | INCIBE-CERT | INCIBE

IUMI (2019) *Cyber Risck- Cargo: new solutions?* [Archivo PDF] Recuperado en 10 de junio 2023, desde https://iumi.com/uploads/Webinar/IUMI_cyber_webinar_20.01.20.pdf

Jeremiah, U. (2020). *Maritime cyber attacks increase by 900% in three years*. Recuperado en fecha 3 de abril de 2023, desde https://www.vanguardngr.com/2020/07/maritime-cyber-attacks-increase-by-900-in-three-years/

Kovacs, E. (2020). *UN Maritime Agency Hit by 'Sophisticated Cyberattack.* Recuperado en fecha 4 de diciembre 2022, desde UN Maritime Agency Hit by 'Sophisticated Cyberattack' - SecurityWeek

Legislation.org.uk (1906). *UK Public General Acts*: *Marine Insurance Act 1906*. Recuperado en fecha 2 de marzo de 2023, desde https://www.legislation.gov.uk/ukpga/Edw7/6/41/part/1

Mandra, J. (2020). *Naval Dome: 400% increase in attempted hacks since February 2020.* Recuperado en fecha 2 de abril de 2023, desde https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/

Maritime Executive (2020). *Maritime Cyberattacks Up by 400 Percent*. Recuperado en fecha 4 de julio de 2023, desde https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent

Marsh (2014) *Cyber gap insurance cyber risk: filling the coverage gap.* Recuperado en fecha 3 de julio de 2023, desde file:///C:/Users/YOLI/Downloads/Cyber%20Gap%20Insurance%20Cyber%20Risk%20Filling%20the%20Coverage%20Gap-07-2014%20(11).pdf

Martin, G. (2020). *Commodity chain digitalisation pushed along Covid-19*. Recuperado en fecha 2 de marzo de 2023, desde https://www.txfnews.com/articles/6990/commodity-supply-chain-digitisation-pushed-along-by-covid-19

Mitsui Sumitomo Insurance [MS & AD] (2022). *Hull Insurance Clause Book 2022* [Archivo PDF]. Recuperado en fecha 23 de enero de 2023, desde https://www.ms-ins.com/marine_navi/hull/info/clause/pdf/HullInsuranceClauseBook_2022.pdf

Møller – Mærsk (2017) *Cyber Attack Update - A.P. Møller - Mærsk A/S*. Recuperado en fecha 3 de abril de 2023, desde https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Molist, M. (2018) *Puerto de BCN, Maersk... Una oleada de ciberataques 'estratégicos' golpea Cataluña.* Recuperado en fecha 3 de julio de 2023, desde https://www.elconfidencial.com/tecnologia/2018-10-02/puerto-barcelona-maersk-ransomware-ciberataques_1623718/

National Cyber Securty Center [NCSC] (2023). *Small business Guide: Cyber Security*. [Archivo PDF]. Recuperado en fecha 2 de mayo de 2023, desde https://www.ncsc.gov.uk/collection/small-business-guide

Organisation for Economic Co-operation and Development [OECD] (2018). *Conference on unleashing the potential of the cyber insurance market.* Recuperado en fecha 3 de enero de 2023, desde https://www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm

Aukera. (2020). *Crecen los ciberataques en la industria marítima*. Recuperado en fecha 34 de abril de 2023, desde https://prosertek.com/es/blog/ciberataques-en-la-industria-maritima/#:~:text=Los%20ciberataques%20han%20aumentado%20hasta,en%20estos%20tiempos%20de%20pandemia.%20Crecen%20los%20ciberataques%20en%20la%20industria%20mar%C3%ADtima%20-%20Prosertek

Subero, D. (2019). Modalidades de ataques de ciberseguridad en Latinoamérica. *Organización de los Estados Americanos* [Archivo PDF] Recuperado en fecha 3 de abril de 2023, desde https://portalcip.org/wp-content/uploads/2019/11/3-Diego-dsubero-Maritime_CIP_v2_compressed-1.pdf

United Nations Conference on Trade and Development [UNCTAD] (2021). *Conferencia de las naciones unidas sobre comercio y desarrollo: Informe sobre transporte marítimo* [Archivo PDF]. Recuperado en fecha 3 de marzo de 2023, desde https://unctad.org/system/files/official-document/rmt2021summary_es.pdf

VMware security (2023). *Seguridad de VMware.* Recuperado en fecha 5 de enero de 2023, desde https://www.vmware.com/es/security.html

Volz. D (2019): *Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets.* Recuperado en fecha 4 de junio de 2023, desde

https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

World Economic Forum (2018). *Securing a Common Future in Cyberspace.* Recuperado en fecha 3 de abril de 2023, desde (177) Securing a Common Future in Cyberspace - YouTube

3. Listado legislativo

Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio. (DOUE [en línea] núm. 333, de 27 de diciembre de 2009, páginas 1 a 333) <https://www.boe.es/doue/2009/335/L00001-00155.pdf >.[Consulta: 1 de enero de 2023].

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). (DOUE [en línea] núm. 333, de 27 de diciembre de 2022, páginas 80 a 152) < https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:2022:277:TOC >. [Consulta: 1 de enero de 2023]

Instrumento de Ratificación de 16 de noviembre de 1981, del Protocolo de 21 de diciembre de 1979, que modifica el Convenio Internacional para la unificación de ciertas reglas en materia de conocimientos de embarque de 25 de agosto de 1924 («Gaceta de Madrid» de 31 de julio de 1930), enmendado por el Protocolo de 23 de febrero de 1968 (BOE [En línea] núm. 36, de 11 de febrero de 1984, páginas 3674 a 3677) < https://www.boe.es/diario_boe/txt.php?id=BOE-A-1984-3645 > [Consulta: 2 de enero de 2023]

Ley 50/1980, de 8 de octubre, de Contrato de Seguro (BOE [en línea] núm. 250, de 17/10/1980) <https://www.boe.es/buscar/act.php?id=BOE-A-1980-22501>[Consulta: 21 de febrero de 2023].

Ley 14/2014, de 24 de julio, de Navegación Marítima (BOE [en línea] núm. 180, de 25/07/2014) <https://www.boe.es/buscar/act.php?id=BOE-A-2014-7877> [Consulta: 2 de febrero de 2023].

Ley 20/2015, de 14 de julio, de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras (BOE [en línea] núm. 168, de 15/07/2015).

<https://www.boe.es/buscar/act.php?id=BOE-A-2015-7897> [Consulta: 21 de febrero de 2023].

Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados (BOE [en línea] núm. 267, de 05/11/2004 5). < https://www.boe.es/buscar/act.php?id=BOE-A-2004-18908 >[Consulta: 1 de enero de 2023].

4. Listado jurisprudencial

Sentencia del Tribunal Supremo 43/2009 (Sala Civil, sección 1a), de 5 de febrero 2009 (recurso 2352/2003).

Sentencia de la Audiencia Provincial de Islas Baleares (154/2016) (Sala de lo civil, sección 5ª), de 6 de junio de 2016 (recurso 1348/2015).

Sentencia de la Audiencia Provincial de Pontevedra 250/2020 (Sala de lo civil, sección 1), de 26 mayo de 2020 (recurso 79/2020).

Sentencia de la Audiencia Provincial Valencia 310/2022 (sala de lo civil, sección 9ª) de 5 de abril de 2022 (recurso 1531/2021).