Ciberseguridad, ciberseguros y navegación marítima

PAOLA RODAS PAREDES[1]
Prof. Ay. Dr., Departamento de Derecho Mercantil "Manuel Broseta Pont"
Universidad de Valencia
ORCID 0000-0001-5711-9035

Este trabajo busca poner de manifiesto los grandes retos que afronta la navegación marítima comercial de nuestro tiempo en el ámbito de la ciberseguridad y las posibilidades de aseguramiento de sus fallos cuando afectan al desarrollo de sus actividades empresariales habituales. En particular nuestro estudio propone, en primer término, identificar el alcance de la política general en materia de ciberseguridad, pues ello nos permitirá comprender las razones por las cuales el desarrollo regulatorio de la misma ha seguido – y sigue – el devenir actual. Seguidamente, expondremos

[1] Este trabajo se inserta en el Proyecto ADLAW (*Conducción autónoma y seguridad jurídica del transporte*, PID2021-123070NB-I00) en el que la autora es miembro del equipo de trabajo.

de manera sucinta, el contenido de la regulación en materia de estándares generales de ciberseguridad en el ámbito geográfico de la Unión Europea, y que cobrarán relevancia en nuestro sector según tendremos ocasión de poner de manifiesto en el tercer apartado de este estudio, dedicado al análisis de cuerpos normativos de diversa categoría en el sector de la navegación marítima que han empezado a buscar la manera de establecer estándares mínimos de ciberseguridad y que, por tanto, están directamente relacionados con los *incidentes*[2] de ciberseguridad que pueden dar lugar a una interrupción, retraso o pérdida de las mercancías transportadas por mar. Por último, una vez expuesto el panorama general de los ciberriesgos y las normas – de distinto rango y grado de imperatividad – que determinaran el nuevo ámbito de *ciber* diligencia del porteador marítimo, podremos prestar atención a las vigentes posibilidades del aseguramiento de su responsabilidad aludiendo, para ello, a las vías habituales de coberturas en los seguros marítimos.

I. ECOSISTEMA DE CIBERSEGURIDAD EUROPEA

Creemos oportuno iniciar nuestro trabajo haciendo una breve referencia a las políticas generales que, en materia de ciberseguridad se han desarrollado ya – y se encuentran en fase de ejecución – por las principales instituciones europeas. Es cierto que, las operaciones de la marina mercante superan el ámbito geográfico sobre el que la Unión Europea tiene una influencia normativa directa, sin embargo, creemos válida nuestra opción dada la manifiesta voluntad de la Unión de establecer criterios y principios de influencia global.

De acuerdo con los documentos oficiales procedentes de las instituciones europeas las políticas generales en ejecución en materia de ciberseguridad pueden dividirse en estrategias de objetivos generales – es el caso de los documentos que emanan de la Comisión Europea – que han sido la base política de la modificación, actualización y adopción *ex novo* de

---

[2] De acuerdo con el *Glosario de términos de ciberseguridad*, de INCIBE (disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf, accedido el 19 de julio, 2024), se define de esta manera a cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

cuerpos normativos de derecho secundario europeo en vigor o en fase de elaboración y a los que nos referiremos en el segundo apartado de este trabajo; y estrategias sectoriales que buscan una mayor concreción y adaptación de los requisitos de ciberseguridad al ámbito y/o industria a la que se dirigen, en nuestro caso, será necesario tener en cuenta aquéllas dirigidas al sector del transporte marítimo.

1. Objetivos generales

A finales del año 2020 la Comisión Europea publicó una actualización de su *Estrategia de ciberseguridad para la UE*[3] en la cual se expresa de manera fehaciente la voluntad de crear un sistema básico de protección de servicios considerados como esenciales[4] – en particular tras la crisis del COVID-19 – así como asegurar un marco de cooperación entre las cuatro ciber-comunidades europeas[5] que permita garantizar un internet global y abierto con fuertes mecanismos de salvaguarda y donde los riesgos para la seguridad y los derechos fundamentales de los ciudadanos europeos puedan contar con un adecuado nivel de protección.

Con esta finalidad, el marco de actuación normativo y económico de la Comisión ha abordado un proceso de ejecución de medidas organizado en tres puntos clave: la resiliencia cibernética y soberanía tecnológica; desarrollo de su capacidad operativa para prevenir, disuadir y responder a los retos detectados y, por último, el desarrollo de un amplio marco de cooperación para promover un ciberespacio global y abierto. (ver Fig. 1[6])

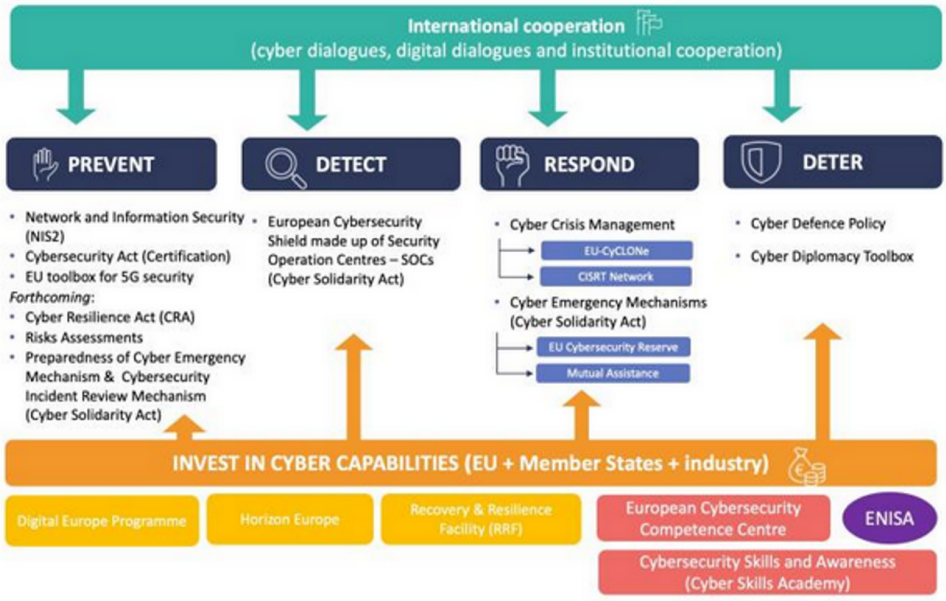
---

3 Disponible en https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, accedido el 19 de julio, 2024.

4 Comunicación de la Comisión al Parlamento Europeo, el Consejo Europeo, el Consejo Econoómico Social Europeo y el Comité de la Regiones, *Sobre la Estrategia de la UE para una Unión de la Seguridad* , COM (2020) 605 final, p. 7. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX%3A52020DC0605 accedido el 19 de julio, 2024.

5 A saber, mercado interior; fuerzas y cuerpos de seguridad, diplomacia y defensa.

6 Fuente: Comisión Europea, estrategia de ciber seguridad, https://digital-strategy.ec.europa.eu/es/policies/cybersecurity accedido el 19 de julio, 2024.



Con la finalidad de alcanzar este alto nivel de ciberseguridad básica necesaria, la Comisión ha visto necesario actualizar las normas de ciberseguridad de la UE introducidas en 2016 con la Directiva *NIS*[7] que vino a desarrollar, por primera vez, un marco general de cooperación entre entidades estatales sobre seguridad de las redes y sistemas de información. Así en diciembre de 2022 aprobó la Directiva *NIS2*[8]que, entre otras novedades, ha introducido importantes competencias en el mandato de la Agencia Europea para la Ciberseguridad (*European Union Agency for Cybersecurity, ENISA*) de manera que en la actualidad este organismo deberá desarrollar y mantener un registro europeo de vulnerabilidades; hacerse cargo de la Secretaría de la Red Europea de Organizaciones de Enlace en Crisis Cibernéticas (CyCLONe); publicación de un informe anual sobre el estado de la ciberseguridad en la UE; apoyo en la organización de revisiones de la normativa vigente en materia de ciberseguridad y ciber resiliencia entre pares entre los Estados miembros; asunción de la creación y mantenimiento de un registro para entidades que brindan servicios transfronterizos (proveedores de servicios DNS, registros de nombres de TLD, entidades

7 *Vid. infra* Directiva UE 2016/1148.

8 *Vid. infra* Directiva UE 2022/2555.

que brindan servicios de registro de nombres de dominio, proveedores de servicios de computación en la nube, proveedores de servicios de centros de datos, etc.); todo ello con el fin de dar cabida a la implantación y consecución de los objetivos marcados en la estrategia de ciberseguridad.

La expresión normativa del desarrollo de esta estrategia será abordada en el siguiente apartado de este trabajo, razón por la que solamente queda hacer referencia a otro elemento del mandato de ENISA: el desarrollo del marco de certificación de ciberseguridad de la UE. Esta herramienta busca establecer un sistema conjunto de reglas, requisitos técnicos, estándares y procedimientos sobre la evaluación de las propiedades de seguridad de un producto o servicio específico basado en TIC que hayan alcanzado una certificación de acuerdo con el esquema europeo. Está previsto que este marco permita discernir entre categorías de productos y servicios cubiertos; requisitos de ciberseguridad (estándares o especificaciones técnicas); el tipo de evaluación o autoevaluación realizada y el nivel de seguridad previsto[9]. El certificado resultante será reconocido en todos los Estados miembros de la UE, lo que facilitará a las empresas el comercio transfronterizo y a los compradores y usuarios la comprensión de las características de seguridad del producto o servicio contratado.

Se ha planificado que el primer esquema europeo de ciberseguridad adoptado esté basado en el estándar internacional *common criteria*[10] que busca garantizar que la política general de seguridad respete los valores comunes europeos garantizando, a su vez la aplicación de los principios de necesidad, proporcionalidad y legalidad, que den lugar a la implantación de una cultura de ciberseguridad a través del diseño – sin dejar atrás la protección de datos[11]–que fomente la cooperación entre las autoridades

---

9 De acuerdo con la Comisión, los niveles de seguridad se utilizan para informar a los usuarios sobre el riesgo de ciberseguridad de un producto y pueden ser básicos, sustanciales y/o altos. Son proporcionales al nivel de riesgo asociado con el uso previsto del producto, servicio o proceso, en términos de probabilidad e impacto de un accidente. Un nivel de seguridad alto significaría que el producto certificado pasó las pruebas de seguridad más estrictas.

10 Vid. texto de la Propuesta de Reglamento de implementación de la Comisión sobre la adopción de un esquema de certificación de ciberseguridad europea basado en Common Criteria (EUCC) publicado el 31 de enero de 2024, disponible en https://ec.europa.eu/newsroom/dae/redirection/document/101749 accedido el 19 de julio, 2024.

11 Comunicación sobre la protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos [COM(2020) 264].

pertinentes de manera que se establezca una unidad informática conjunta a cargo de la cooperación operativa estructurada y coordinada entre los distintos actores del ecosistema europeo de ciberseguridad[12]. Una vez en marcha, este sistema de certificación podrá utilizarse como indicador del cumplimiento del deber de cuidado del empresario que actúe o utilice determinados servicios digitales.

Por último, esta estrategia permitirá fomentar la sensibilización de la población general en materia de cuestiones de seguridad de las comunicaciones, así como la adquisición de las capacidades necesarias para hacer frente a las amenazas potenciales. En este sentido, será necesario fomentar la adquisición de un conocimiento básico de las amenazas para la seguridad y de la manera de combatirlas para conseguir un impacto real en el grado de resiliencia del público, así como su concienciación sobre los riesgos de la ciberdelincuencia y la necesidad de protegerse ante ellos, pueden añadirse a la protección de los proveedores de servicios frente a los ciberataques[13].

2. Estrategias sectoriales

En el ámbito del sistema *Eurojust*, es necesario hacer referencia a la plataforma EMPACT[14] que ha incluido entre sus prioridades el cibercrimen como elemento independiente de otras actividades delictivas[15]. Por este motivo se han creado una serie de instrumentos y estrategias sectoriales específicos de la UE para seguir desarrollando la cooperación policial

---

12 Adicionalmente a ENISA, será necesario tener en cuenta la actuación de los Centros de intercambio y análisis de información (*Information Sharing and Analysis Centres, ISACs*); el Centro Conjunto de Investigación (*Joint Research Center, JRC*) de la Comisión, a cargo de desarrollar la taxonomía de ciberseguridad, los Equipos de Respuesta de Emergencia a Incidentes de Seguridad Informática (*Computer Security Incident Response Teams, CSIRTs*), la Organización Europea de Ciberseguridad, (*European Cybersecurity Organisation, ECSO*) y la plataforma *Women4Cyber*, puesta en marcha por la Comisión para permitir la visualización de este grupo poco representado.

13 Vid. Agenda de Capacidades Europea para la competitividad sostenible, la equidad social y la resiliencia [COM(202) 274 final].

14 Plataforma multidiciplinar europea contra las amenazas delictivas (European Multidisciplinary Platform Against Criminal Threats) EMPACT.

15 https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/operational-cooperation_en

operativa entre los Estados miembros. Uno de sus principales instrumentos es el Sistema de Información de Schengen, utilizado para intercambiar datos sobre personas buscadas y desaparecidas en tiempo real. A pesar de los éxitos, es necesario tener en cuenta que la mayor parte del entramado legal de la UE que sustenta la cooperación policial operativa fue puesta en marcha hace ya 30 años a través de una compleja red de acuerdos bilaterales entre Estados miembros cuestión que, dado el desarrollo de la técnica y la interconectividad de las actuaciones maliciosas en la red, ocasiona limitaciones de actuación al organismo.

En el caso del sector financiero, será necesario tener en cuenta el *Reglamento DORA*[16] cuyo objetivo principal busca establecer normas uniformes relativas a la seguridad de las redes y los sistemas de información de las entidades financieras – banca, bolsa y seguros – de manera que éstas[17] tengan la obligación de tomar las medidas necesarias[18] para hacer frente, responder y recuperarse de cualquier *incidente de seguridad*.

En relación al tema de nuestro interés, el Plan de Acción de la Estrategia de Seguridad Marítima de la UE, que dio lugar a importantes logros con la cooperación en las tareas de guardacostas entre las agencias europeas pertinentes, ha dado lugar a una Comunicación conjunta del Parlamento

---

16 Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 y (UE) 2016/1011 (Texto pertinente a efectos del EEE), DO L 333 de 27.12.2022, p. 1/79.

17 El ámbito objetivo del Reglamento señala como elementos de protección no solamente a los actores principales ya mencionados sino que también incluye a todas las entidades de crédito, de pago, de dinero electrónico y de pensiones de jubilación; los proveedores de servicios de información sobre cuentas, criptoactivos, notificación de datos, financiación participativa y terceros de TIC; las empresas de inversión, fondos de inversión alternativos, sociedades gestoras, agencias de calificación crediticia y administradores de índices de referencia esenciales; registros de operaciones y titulizaciones, depositarios centrales de valores, contrapartes centrales y centros de negociación; así como a todas las entidades de seguros y reaseguros y sus intermediarios.

18 A grandes rasgos clasificados en obligaciones de gestión de riesgos – directos y derivados de terceros – relacionados con las TIC; obligaciones de gestión, clasificación e informes relacionados con las TIC; obligatoriedad de realizar pruebas de resiliencia operativa digital; posibilidad de establecer acuerdos de intercambio de información entre entidades; y aplicar el marco de supervisión de proveedores terceros esenciales de servicios de TIC.

Europeo y del Consejo sobre la estrategia ampliada europea de Seguridad Marítima para amenazas marítimas en evolución[19] que ha venido a incluir la ciberseguridad marítima como un elemento específico de la misma.

En particular, la Directiva UE 2022/2557 relativa a la resiliencia de las entidades críticas[20] que busca la reducción de las vulnerabilidades cibernéticas y el aumento de su resiliencia ha incluido a todos los medios de transporte entre los sectores objeto de su regulación[21].

De acuerdo con los deberes dimanantes del texto legal, cada estado miembro, deberá adoptar una estrategia nacional que incluya evaluaciones periódicas de los riesgos; tener en cuenta los resultados de éstas; identificar las entidades que prestan servicios esenciales a la sociedad, la economía, la salud pública, la seguridad o al medio ambiente; apoyar a las entidades críticas identificadas en la mejora de su resiliencia; garantizar que las autoridades nacionales tengan las competencias, los recursos y los medios necesarios para llevar a cabo sus tareas de supervisión, incluida la competencia sancionadora por incumplimientos; así como especificar las condiciones en las que una entidad crítica puede presentar solicitudes de verificación de antecedentes del personal que desempeña funciones sensibles. Por su parte, las entidades críticas deberán llevar a cabo evaluaciones de riesgos propias con el fin de identificar aquéllos que podrían afectar a su capacidad para prestar servicios esenciales; adoptar medidas técnicas, de

---

19 "An enhanced EU Maritime Security Strategy for evolving maritime threats", JOIN (2023) 8 final https://oceans-and-fisheries.ec.europa.eu/document/download/7274a9ab-ad29-4dae-83fb-c849d1ca188b_es?filename=join-2023-8_es.pdf, accedido el 19 de julio, 2024.

20 Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (Texto pertinente a efectos del EEE), DO L 333 de 27.12.2022, p. 164/198.

21 Están incluidos entre otros, el sector de la energía; transportes; la banca (también sujeta al Reglamento (UE) 2022/2554); la infraestructura de los mercados financieros; la salud; los proveedores y distribuidores de agua potable; la eliminación y el tratamiento de aguas residuales; las infraestructuras digitales, incluidos los servicios de comunicaciones electrónicas y los centros de datos, (también sujetos a la Directiva (UE) 2022/2555); entidades de la administración pública a nivel del Gobierno central, excepción de la seguridad nacional, la seguridad pública, la defensa y las fuerzas del orden; los operadores espaciales de infraestructuras terrestres; y las empresas alimentarias que se dedican exclusivamente a la logística y a la distribución al por mayor, así como a la producción y transformación industriales a gran escala.

seguridad y organizativas para mejorar su resiliencia; y notificar incidentes perturbadores significativos a las autoridades nacionales.

En suma, al menos desde el punto de vista de la planificación general, y también sectorial, podemos señalar que existe un importante avance en la voluntad de elevar el marco de actuación y concienciación de la necesidad de adoptar medidas efectivas de ciberseguridad. Con todo, el acelerado ritmo del avance de la integración – y por tanto interdependencia – global de los sistemas operacionales generales y del transporte marítimo exigen, a nuestro entender, una mayor celeridad tanto en la implantación de los sistemas de certificación, como de las políticas de prevención y concienciación, como mínimo entre proveedores de productos y servicios en el mercado interior.

II. DESARROLLO NORMATIVO DEL MARCO GENERAL EUROPEO DE CIBERSEGURIDAD

1. Reglamento UE 2019/881 de ciberseguridad[22]

Tal y como hemos adelantado, el *Reglamento de ciberseguridad* tiene como principal objetivo la consolidación de ENISA como agencia permanente europea con el mandato de alcanzar un elevado nivel común de ciberseguridad para toda la UE; apoyar a las autoridades nacionales e instituciones, órganos, oficinas y organismos europeos para mejorar su ciberseguridad; servir como punto de referencia de asesoramiento científico y técnico y de conocimientos sobre ciberseguridad para las instituciones, órganos, oficinas y organismos europeos; así como contribuir, a través de políticas e iniciativas conjuntas, a la reducción de la fragmentación del mercado interior.

Como elementos adicionales, este Reglamento estableció un *Grupo de partes interesadas* sobre certificación de ciberseguridad que deberá asesorar a la Comisión sobre asuntos estratégicos relativos al ya mencionado *marco de certificación de ciberseguridad UE*, además de otro *Grupo Europeo*

---

[22] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) no 526/2013 («Reglamento sobre la Ciberseguridad»), DO L 151 de 7.6.2019, p. 15/69.

de Certificación de Ciberseguridad, compuesto por representantes nacionales, también encargado de asistir a la Comisión en su labor, con la misión de garantizar la coherencia en la ejecución y aplicación del Reglamento UE 2019/881, y a ENISA en la preparación de posibles esquemas de certificación de ciberseguridad.

De momento, bajo este marco normativo, todos los esquemas de certificación de ciberseguridad serán *voluntarios* y deberán tener como objetivo la consecución de objetivos de seguridad de los datos y operatividad, como ser la protección de datos almacenados, transmitidos o procesados; categorizar el nivel de seguridad de los productos, servicios y procesos de TIC como «básico», «sustancial» o «elevado»; permitir la *autoevaluación de conformidad* a fabricantes y proveedores de productos, servicios y procesos TIC de bajo riesgo[23].

2. Directiva (UE) 2016/1148 sobre ciberseguridad de las redes y sistemas de información[24] [NIS1]

Precursora del marco vigente sobre seguridad de las redes, la Directiva *NIS1* fue la primera en establecer la obligación, por parte de los Estados miembro, de crear equipos de respuesta a incidentes de seguridad informática (CSIRTs)[25], así como la designación de las autoridades competentes en cada Estado Miembro para evaluar las políticas de ciberseguridad y seguridad de los operadores de servicios esenciales en cada Estado Miembro; supervisar a los proveedores de servicios digitales; informar al público

---

23 Normas más concretas han sido desarrolladas en el Reglamento de ejecución (UE) 2024/482 de 31 de enero, 2024 [DO L, 2024/482, 7.2.2024] cuya entrada en vigor se ha previsto para el 27 de febrero de 2025.

24 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, DO L 194 de 19.7.2016, p. 1/30.

25 Estableciendo como funciones principales de éstos el de servir de plataformas de intercambio de información con otros CSIRT tanto sobre servicios como en relación con incidentes de ciberseguridad; prestar apoyo a los países de la UE a la hora de abordar los incidentes transfronterizos; debatir y consensuar una respuesta coordinada a un incidente identificado por un país de la UE; coordinar la respuesta a riesgos e incidentes que afecten a más de un país de la UE; informar al grupo de cooperación sobre sus actividades y solicitarle directrices; discutir sobre la experiencia adquirida a partir de los ejercicios relativos a la ciberseguridad.

– según necesidad– para evitar un incidente o gestionar uno ya producido, respetando la confidencialidad.

Otro de los elementos principales introducidos en el sistema general de ciberseguridad europeo a través de la NIS1, fue la obligación de determinar – por parte de cada Estado Miembro – los operadores de servicios esenciales en sectores fundamentales[26] – energía, transporte, sistema financiero, salud, agua e infraestructura digital – en los que un ciberataque podría perturbar un servicio esencial.

En relación con el cumplimiento de estos deberes, la norma establece el ámbito de supervisión de las autoridades nacionales competentes, reconociéndoles competencia, entre otras, para recibir la notificación obligatoria, por parte de los operadores de servicios esenciales y sus proveedores de servicios digitales[27], de cuantos *incidentes* afecten la seguridad de las redes y sistemas de información utilizados para la prestación de los servicios esenciales.

En cuanto a su proceso de adaptación a nuestro ordenamiento jurídico, es necesario señalar que esta norma fue transpuesta a través del RD-Ley 12/2018 de 7 de septiembre, de seguridad de las redes y sistema de información[28] que tuvo el acierto de *ampliar* el ámbito subjetivo de aplicación, incluyendo en este a todos los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, opción de política legislativa que permitirá, a los operadores españoles, una transición mucho más tranquila hacia la correcta implementación de NIS2.

---

26 Según el art. 5 de NIS1, los criterios para la identificación de operadores de servicios esenciales se basaban en incluir como tales a las entidades que presten un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; aquellas que para prestar sus servicios dependan de las redes y sistemas de información, y aquéllas que si llegaran a sufrir un *incidente*, este tendría efectos perturbadores significativos en la prestación de los servicios prestados.

27 Art. 14.3 y 16, Directiva 2016/1148.

28 BOE núm. 218, de 08/09/2018.

3. Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión[29] [NIS2]

Tal y como hemos adelantado en el primer apartado de este estudio, la NIS2 marcará un punto de inflexión en el establecimiento de un marco regulador común de ciberseguridad europeo. Con esta finalidad el sistema introduce la obligatoriedad de introducción, en los EM, de medidas concretas de gestión de riesgo de ciberseguridad, así como la creación de una red de cooperación, comunicación y notificación de riesgos en sectores críticos.

En relación con el ámbito objetivo, NIS2 extiende su aplicación a otros sectores anteriormente no incluidos[30], creando la obligación de los EM de establecer una lista de entidades esenciales e importantes, que también incluya a las entidades que presten servicios de registro de nombres de dominio, con obligación de revisar y, en su caso, actualizar esa lista periódicamente, y como mínimo cada dos años a partir del 17 de abril de 2025[31].

Por tanto, otra de las novedades de NIS2 respecto al sistema anterior es que el criterio de clasificación ya no se basa en la producción u ofrecimiento de servicios digitales, sino en la *posibilidad de afectación* a la sociedad, economía o determinados sectores o tipos de servicios, independientemente

---

29 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) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE), DO L 333 de 27/12/2022, p. 80/152.

30 De acuerdo con el Anexo II, servicios postales y de mensajería, gestión de residuos; fabricación, producción y distribución de sustancias y mezclas químicas; producción, transformación y distribución de alimentos; fabricación de productos sanitarios, informáticos, electrónicos y ópticos, de determinados tipos de material eléctrico y maquinaria, y de vehículos de motor y otro material de transporte; los proveedores de servicios digitales de mercados en línea, de motores de búsqueda y redes sociales; y organismos de investigación.

31 *Vid.* las *directrices [DO C 328 de 18.9.2023, p. 2/10*] publicadas por la Comisión Europea sobre la aplicación del Art. 4.1 y 4.2 de la Directiva UE 2022/2555 relativas a su aplicación y los actos jurídicos de la UE actuales y futuros, específicos del sector, que abordan medidas de gestión del riesgo de ciberseguridad o requisitos de información sobre incidentes.

del *tamaño* de la empresa[32], así se consideran entidades esenciales todas las grandes empresas de los sectores de alta criticidad del anexo I; independientemente de su tamaño, se considerarán como tales a los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y los proveedores de servicios de DNS así como las entidades identificadas como críticas con arreglo a la Directiva (UE) 2022/2557, y aquellas identificadas por un EM como operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 o el derecho nacional. Por su parte NIS2 considera como entidad importante todas aquellas de uno de los tipos mencionados en los anexos I o II que no puedan considerarse entidades esenciales, atribuyéndose potestad a cada EM para identificar a una entidad, independientemente de su tamaño, como esencial o importante[33]

En cuanto a la notificación de incidentes, NIS2 modifica los procedimientos a realizar de manera que según el caso, la entidad afectada deberá realizar una primera notificación – al CSIRT o autoridad competente designada por el EM – de *alerta temprana* dentro de las 24h desde que tenga conocimiento del mismo; realizará otra que incluirá una evaluación inicial de la gravedad o impacto del incidente, antes de las 72h de su inicio – con indicación de los Indicadores de compromiso, IoT, si fuera el caso – a continuación la autoridad competente o CSIRT podrá solicitar un informe intermedio; mientras que, a más tardar un mes después de la presentación

---

[32] El Anexo I de la norma señala con detalle los *sectores de alta criticidad*, que ha ampliado su aplicación a nuevos subsectores, a modo ilustrativo, en el caso del sector energético al almacenamiento y transporte de hidrógeno, sistemas urbanos de calefacción y refrigeración, mientras que en el sector de infraestructuras digitales se ha incluido a proveedores de redes de servicios de computación en la nube, proveedores de distribución de contenidos, prestadores de servicios de confianza, proveedores de servicios de centro de datos y proveedores de redes públicas de comunicaciones electrónicas, así como servicios de comunicaciones electrónicas disponibles para el público.

[33] Si ésta es única proveedora de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas; si la perturbación del servicio prestado por la entidad puede tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública; si una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo; o si la entidad es crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en ese Estado miembro.

inicial, la entidad deberá presentar un *informe final*[34], a menos que el incidente siga en curso, en cuyo caso a la fecha deberá presentarse un informe de situación y el informe final al mes de haberse gestionado el incidente.

En relación con las competencias de supervisión, NIS2 establece un marco más exigente a las entidades esenciales con medidas tanto preventivas como reactivas[35] mientras que en el caso de las entidades importantes la mayor parte serán post-incidente[36], además de reconocerle potestad sancionadora por incumplimientos, que incluye medidas de diversa índole entre las que se encuentran multas pecuniarias de diverso rango según se trate de una entidad esencial o importante.

4. Propuestas de Reglamentos UE

4.1 Propuesta de Reglamento UE relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales [Reglamento de ciberresiliencia][37]

Dentro del esquema de desarrollo normativo del nuevo marco básico de ciberseguridad europeo, esta propuesta de Reglamento – autodenominada *Ley de ciberresiliencia* – centra su atención en el *IoT, internet of things*, con previsiones normativas para productos: control de introducción en el mercado europeo de productos con elementos digitales; regulación de los requisitos esenciales para el diseño, desarrollo y fabricación

---

34 El contenido mínimo del mismo deberá contener: una descripción detallada del incidente, incluyendo su gravedad e impacto; el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente; las medidas paliativas aplicadas y en curso y; cuando proceda, las repercusiones transfronterizas del incidente.

35 Inspecciones *in situ* y a distancia incluidas aleatorias; auditorías de seguridad periódicas y específicas; auditorías *ad hoc* (tras un incidente); análisis de seguridad; solicitudes de información necesaria para evaluar las medidas de gestión de riesgos adoptadas; solicitudes de acceso a datos e información para supervisión; solicitudes de acreditación de la aplicación de las políticas de ciberseguridad.

36 Inspecciones in situ; auditorías específicas; solicitud de información para evaluar las medidas de gestión de riesgo adoptadas, etc.

37 La más reciente versión del texto en tramitación parlamentaria data del 12 de marzo, 2024, disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_ES.pdf, accedido el 19 de julio, 2024.

de productos con elementos digitales; procedimientos de garantías de ciberseguridad, procesos de gestión de vulnerabilidades conocidas por los fabricantes de productos con elementos digitales; y normas relativas a vigilancia del mercado.

La norma propuesta clasificará a estos productos según categorías de relevancia: productos con elementos digitales (Anexo I de la Propuesta), productos importantes con elementos digitales (Anexo III de la propuesta, sujeto a los procedimientos de evaluación de la conformidad del art. 32 del mismo texto) y productos críticos con elementos digitales (Anexo IV, con obligación de obtener un certificado europeo de ciberseguridad con un nivel de garantía al menos «sustancial» en el marco de un esquema europeo de certificación de la ciberseguridad adoptado con arreglo al Reglamento (UE) 2019/881 para demostrar su conformidad con los requisitos esenciales establecidos en el anexo I del mismo texto legal). Los productos importantes, a su vez, estarán divididos según su potencial nivel de riesgo de ciberseguridad (clases I y II). Mientras que serán clasificados como productos *críticos* aquellos de los que presenten una dependencia crítica las entidades esenciales señaladas en el Art. 3 Directiva UE 2022/2555 y, aquellos cuyos incidentes y vulnerabilidades aprovechadas puedan dar lugar a perturbaciones graves en las cadenas de suministro críticas en todo el mercado interior.

En todo caso, la norma propone crear un marco de seguridad general de productos aplicable a todos los productos con elementos digitales cuando dichos productos no estén sujetos a requisitos de seguridad específicos establecidos en otra legislación de armonización de la Unión tal como se define en el art. 3.27, del Reglamento (UE) 2023/988. También se prevén normas específicas para los productos con elementos digitales clasificados como sistemas de IA de *alto riesgo* por el art. 6 del Reglamento de *inteligencia artificial*[38]. Otro elemento recientemente añadido al ámbito de la responsabilidad del fabricante es que éste deberá asumirla cuando integre, en sus productos, componentes procedentes de terceros y componentes de

---

[38] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DO L, 2024/1689, 12.7.2024.

programas informáticos libres y de código abierto que no se hayan comercializado en el transcurso de una actividad comercial[39].

El texto más recientemente aprobado, también ha introducido, al efecto de instrumentar las diversas notificaciones de vulnerabilidades, la creación de una plataforma única de notificación a cargo de ENISA[40].

A lo largo del texto, la norma también establece procedimientos y obligaciones de comunicación claras, respecto de los fabricantes, en relación con los períodos de soporte de los productos con elementos digitales que hubieran puesto en circulación en la Unión. Otro aspecto que permea la regulación aquí comentada es la repetida autorización a la Comisión para aprobar Reglamentos de ejecución – en diversos apartados – que permitan actualizar o dar mayor contenido a los aspectos técnicos necesarios para dotar de efectividad a las medidas generales dimanantes de la Propuesta.

4.2 Propuesta de Reglamento UE sobre ciber solidaridad[41]

Llamado a reforzar los mecanismos de colaboración y cooperación entre los distintos actores, supervisores y, en general, instituciones de diverso rango en el ámbito de la aplicación del marco general de ciberseguridad descrito en los puntos anteriores, esta Propuesta de Reglamento busca establecer un *hub* de ciber datos transfronterizos, *cross-border cyber hub*, que permita el intercambio de inteligencia de ciber amenazas entre los diversos actores – CERTs, CSIRTs, ISACs, operadores de infraestructuras críticas – y supervisores.

---

39 En el caso de programas informáticos de código abierto, la Propuesta prevé obligaciones de diligencia de sus administradores, quienes deberán documentar la adopción de una política de ciberseguridad que fomente el desarrollo de un producto con elementos digitales seguros y una gestión eficaz de sus vulnerabilidades, obligaciones de cooperación con las autoridades de vigilancia del mercado y un Esqueda de certificación de seguridad específico para este tipo de programas (*Vid.* art. 24 y 25 de la Propuesta).

40 Art. 16 de la Propuesta.

41 *Cyber solidarity Act,* Proposal for a Regulation EU laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, disponible en https://data.consilium.europa.eu/doc/document/ST-8047-2024-INIT/EN/pdf, accedido el 19 de julio, 2024.

En general el Reglamento propone vías de adopción de procedimientos de cooperación entre los participantes de estos *hubs*[42], con previsión de participación de estos actores en el sistema europeo de alertas de ciberseguridad[43], siendo este último, el elemento esencial que instrumentará la consecución de los objetivos de cooperación ya señalados[44], además del establecimiento de un mecanismo de emergencias de ciberseguridad[45], y un mecanismo pan-europeo de revisión de incidentes de ciberseguridad[46] .

Con todo, el texto propuesto se encuentra en las primeras fases de su tramitación parlamentaria. A pesar del interés que, sin duda, despierta la regulación del marco de cooperación de estos actores y organismos, no es menos destacable que no podemos dar por concluidas las reformas a introducirse en el mismo, tanto en relación con los mecanismos de cooperación previstos, como con las competencias a éstos o la previsión de la creación de una Reserva Europea de Ciberseguridad[47].

III. CIBERSEGURIDAD DE LA NAVEGACIÓN MARÍTIMA

El panorama regulatorio hasta ahora descrito conoce, como sabemos, especialidades normativas y técnicas aplicables al transporte marítimo[48].

---

42 En directa relación con la obligación de los CSIRTs de establecer redes que promuevan una rápida y efectiva cooperación operacional entre los EM, según la Directiva EU 2022/2555.

43 Art. 3 de la Propuesta.

44 De acuerdo con el *Programa Europa Digital*, el Escudo Europeo de Ciberseguridad integrará todos los centros de operaciones de seguridad nacionales y transfronterizos con el objetivo de analizar, detectar y compartir advertencias sobre ciberamenazas, *Vid.,* https://digital-strategy.ec.europa.eu/en/library/eu-cyber-solidarity-act-factsheet.

45 Art. 9 de la Propuesta.

46 Art. 18 de la Propuesta.

47 Art. 12 de la Propuesta.

48 De acuerdo con JUAN Y MATEU, F., "El transporte marítimo y la ciberseguridad", *RDM* 323, 2022, p. R.R-3.2, la conectividad y accesibilidad de los sistemas de comunicación e información de la industria marítima ha sobrepasado ya el simple recurso a sistemas de tecnologías de la información (IT, por sus siglas en inglés) para el almacenamiento, tratamiento y transmisión de datos, habiendo sido incorporado a los sistemas y tecnologías operacionales (OT), encargadas de controlar la propulsión y navegación de la embarcación.

Es conocido que, desde hace un par de décadas la *e-navegación*[49] es una tendencia que ha permitido – y permite – no solo un considerable ahorro de costes operativos a las empresas de transporte marítimo, sino que también permite el acceso y uso de una serie de avances tecnológicos que han redundado en una navegación más planificable y previsible[50].

No obstante, la perenne interconectividad de sistemas IT y OT, unido a una serie de decisiones técnicas de implantación global que limitan la capacidad de adoptar medidas efectivas de ciberseguridad[51] han puesto de manifiesto la urgente necesidad de prever nuevos parámetros y protocolos efectivos de ciberseguridad, que solo serán efectivos con un cambio en la cultura empresarial y laboral de la navegación marítima[52].

Al margen de la normativa europea en vigor y prospectiva, en el caso de la industria marítima en general, por sus características de internacionalidad, veremos cómo, a diferencia del apartado anterior, los textos de referencia – incluso aquéllos preparados por instituciones supervisoras y con competencias coercitivas – son de carácter mayoritariamente potestativos o que van dirigidas a los Estados en los que se realiza el transporte marítimo, cuando no son, directamente *derecho blando* emanado de asociaciones profesionales de la navegación. No olvidamos que, en el transporte marítimo internacional, éstas últimas han sido las herramientas más efectivas y eficientes de modificación de políticas generales de actuación o regulación de la introducción e incorporación de los avances de la técnica. Sin embargo, creemos que fruto del acelerado ritmo de evolución de los riesgos

---

49 Así definida por la OMI en el documento *Estrategia para el desarrollo y la implantación de la navegación electrónica*, MSC 85/26/Add.1, Anexo 20, Organización Marítima Internacional, Londres, 2008.

50 En detalle, LÓPEZ VARELA, P.; SALGADO DON, A., PÉREZ CANOSA, J. M., "Análisis crítico de la navegación-e: situación actual y perspectivas de futuro" en AAVV, *Derecho marítmo, las nuevas tecnologías y los retos del progreso*, Aranzadi, Cizur Menor, 2021, edición digital.

51 A modo ilustrativo, bástenos señalar la ausencia de sistemas de encriptación o autenticación de las señales del *Global Positioning System, GPS*, que permite su manipulación, bloqueo o sustitución con alarmante facilidad, JUAN Y MATEU, F., "El transporte marítimo y la ciberseguridad", p. R.R-3.2.

52 Ampliamente comentado ha sido el caso de *NotPetya*, código malicioso que ingreso en el sistema de la naviera MAERSK a través de un solo ordenador en el puerto ucraniano de Odessa, *vid.,* WILSON, B., "Maritime Cyber Security" en Cambridge University Press, Cambridge, 2022, p. 158.

cibernéticos, esta vía no parece que vaya a ser suficiente para mantener un nivel mínimamente adecuado de ciberseguridad.

1. Políticas de protección desde el sector marítimo

La concienciación en materia de medidas de ciberseguridad en este ámbito ha resultado en la adopción de guías de buenas prácticas que, tanto desde las organizaciones internacionales – Organización Marítima Internacional – como desde la Autoridad Europea para la Seguridad Marítima han comenzado a buscar la adopción de medidas concretas que generen un nivel mínimo de protección.

1.1 IMO Guidelines[53]

Publicado en 2017, el prolijo texto redactado por la organización se autodenomina "recomendaciones para la administración de ciberriesgos marítimos para salvaguardar el transporte marítimo de ciber amenazas y vulnerabilidades presentes y emergentes".

A continuación, se realiza una enumeración del tipo de sistemas que, a primera vista, serían vulnerables para proseguir con una referencia al tipo de organización a las que va dirigida la guía, cuestión que pone de manifiesto la principal dificultad que encontrarán la mayor parte de textos de similar naturaleza: la falta de mecanismos de coercibilidad o vigilancia del cumplimiento de su contenido.

El tercer punto abordado por la IMO comienza con una definición de la actividad que propugna acometer; la administración de los ciberriesgos a través de acciones llamadas a aceptar la existencia de los mismos, evitarlos, transferir o mitigar su aparición a niveles aceptables a través de acciones que tengan en cuenta los costes y beneficios para con todos los interesados. A pesar de que la guía también hace referencia a los cinco elementos generalmente aceptados que integran las estrategias habituales de gestión de

---

53 IMO, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3 de 5 de julio, 2017, disponible en https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf, accedido el 19 de julio, 2024.

los ciberriesgos[54], el texto es tan exiguo que, sin duda cualquier elemento general puede, podría, clasificarse como una respuesta mínima adecuada según estos principios[55].

También es importante señalar la referencia no exhaustiva, como marco adicional de referencia, que el texto realiza respecto de la Guía de ciber seguridad a bordo de barcos, publicada por BIMCO[56]; el estándar ISO/IEC 27001 sobre tecnologías de la información y el Marco de mejora de la ciberseguridad de infraestructuras críticas, publicado por el Instituto nacional de estándares y tecnología de los Estados Unidos (NIST *cybersecurity framework*[57]).

1.2 Política de transporte marítimo de la EMSA

En el caso de la Agencia Europea de Seguridad Marítima, EMSA, es conocida la recientemente publicada guía sobre la forma de afrontar la ciberseguridad a bordo de las embarcaciones durante auditorías, controles, verificaciones e inspecciones[58].

Al igual que en el caso anterior, el documento, de escasa extensión y contenido técnico, señala en sus inicios su carácter dispositivo, con una particularidad: establece que esta cualidad se ha establecido así por buscar concordancia con las normas marítimas europeas en materia de medidas y mecanismos de seguridad vigentes. Así pues, a nuestro entender, es posible que, una vez adoptado el Reglamento de ciber resiliencia[59], el texto de la EMSA adquiera una cualidad distinta y deba ser modificado. De momento

---

54 Identificación, protección, detección, respuesta y recuperación.

55 Al respecto, WILSON B. Maritime Cyber Security en KRASKA J, PARK Y-K, eds. *Emerging Technology and the Law of the Sea.* Cambridge University Press; 2022, p. 169, pone de manifiesto uno de los grandes problemas de este tipo de textos potestativos y es que los grandes actores del transporte marítimo – en este caso concreto WILSON se refiere a China – pueden preferir eliminar contenido regulatorio de valor jurídico a estos textos con la finalidad de mantener el control y competencias de supervisión en sus legislaciones nacionales.

56 Versión 2020 en https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf, accedido el 19 de julio, 2024.

57 Disponible en https://doi.org/10.6028/NIST.CSWP.04162018, accedido el 19 de julio, 2024.

58 Disponible en https://emsa.europa.eu/component/flexicontent/download/7660/5074/23.html, accedido el 19 de julio, 2024.

59 *Vid. supra* II.4.1

la mayor parte del contenido material de la guía en cuanto al contenido del *análisis de seguridad de la embarcación*, y el *Plan de seguridad de la embarcación* encuentran contenido directo con las directrices fijadas en el Reglamento (CE) 725/2004[60].

Otro aspecto que juega a favor de la brevedad del texto es su vocación de documento de coordinación entre otros textos con escaso rango normativo coercitivo por la institución, pero de extendida validación en su uso práctico[61]. A pesar de ello, es necesario tener en cuenta que estas referencias cruzadas se centran en regulación general basada en consecuencias – daños – *físicos* a las personas o las cosas y no así a situaciones de daños o peligros en los sistemas IT y OT de la navegación[62] .

Por último, no esta de más señalar que muchos aspectos de la regulación aquí referida han sido desarrollados en primer término con la finalidad de proporcionar un marco regulatorio que incentive el desarrollo tecnológico, en particular en el caso de la *automatización* del transporte marítimo, con políticas abiertamente favorables a la introducción de buques autónomos. Razón por la cual también será necesario, tomar en cuenta la regulación europea en materia de usos civiles de inteligencia artificial[63].

---

60 Reglamento (CE) n° 725/2004 del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y las instalaciones portuarias, DO L 129 de 29.4.2004, p. 6/91.

61 Es el caso del Código ISM, IMO Res. A.741(18), International Management Code for the Safe Operation of Ships and for Pollution Prevention, annex (Nov. 17, 1993).

62 Este aspecto también ha sido comentado por WILSON B. "Maritime Cyber Security", cit., p. 173.

63 En este sentido, en relación con el transporte en todas sus modalidades, SIERRA NOGUERO, E., "Towards a European Law on cooperative, connected and automated mobility (CCAM)", *CEUR Workshop Proceedings,* 2022, p. 80, NUÑEZ ZORRILLA, M. C. "Hacia un marco legal europeo uniforme en la prevención de los riesgos y la responsabilidad civil en el ámbito de la conducción automatizada inteligente" *CDT* vol. 15, 2023, p. 695; en el caso del transporte marítimo, RODAS PAREDES, P., "La responsabilidad del empresario marítimo de buques autónomos" en PETIT LAVALL, M. V.; PUETZ, A., (dirs.) *El transporte ante el desarrollo tecnológico y la globalización* Colex, Madrid, 2023, p. 745.

2. Otras propuestas normativas

2.1. Geneva Association's Hostile Cyber Activity

A pesar de tratarse de una asociación internacional de aseguradores *terrestres*, creemos relevante tomar en cuenta el trabajo realizado por la *Geneva Association* en tanto que este organismo lleva bastante tiempo analizado las maneras de generar una *definición legal* de ciber amenazas y ciber riesgos que pueda servir como base actuarial para la industria aseguradora.

Por ello, en el caso de la ciberseguridad, es destacable señalar el particular cuidado con el que esta asociación ha marcado el camino en la materialización de un concepto de ciber riesgo que, de momento apuesta por la diferenciación en la *actividad* en el ciberespacio, de manera que el riesgo este ligado a una actividad *hostil* en la que será esencial – en particular para los *grandes riesgos*, como es el caso de la navegación marítima – determinar si la actividad hostil así definida estaría sujeta a actividades contra la defensa y seguridad de un Estado, en cuyo caso, las habituales *exclusiones de guerra* serían aplicables[64].

2.2. La guía sobre ciberseguridad a bordo de embarcaciones, de BIMCO

Ya en su cuarta versión, sin duda son el texto de referencia en el sector de la navegación marítima comercial. El texto incluye apartados dedicados a la visión de conjunto sobre la ciberseguridad y la gestión del ciberriesgo en el ámbito marítimo; la identificación de amenazas; identificación de vulnerabilidades; valoración de la probabilidad de que se produzca un ciberincidente, que a su vez depende de cuáles sean las amenazas y vulnerabilidades; valoración del impacto (efectos) que el ciberincidente puede producir; valoración del riesgo, que a su vez depende de la probabilidad y el impacto del ciberincidente; el desarrollo de medidas de protección; el desarrollo de medidas de detección; el establecimiento de planes de contingencia; y la respuesta y recuperación tras un ciberincidente.

---

64 *Vid.* CARTER, R., PAIN, D., ENOIZI, J., *Insuring Hostile Cyber Activity: in search of sustainable solutions*, Geneva Association Publishing, Ginebra, 2023, p. 13, disponible en https://www.genevaassociation.org/sites/default/files/cybersolutions_web.pdf, accedido el 19 de julio, 2024.

Al igual que con los textos de EMSA, el documento señala su calidad de texto de aplicación voluntaria, habiendo sido desarrollado a la par con otros textos de asociaciones profesionales con contenido similar[65] y que, al igual que el texto de BIMCO, busca incentivar el desarrollo y adopción de medas efectivas de protección en este ámbito.

2.3. La posición de la International Association of Classification Societies (IACS) sobre sistemas ciber

Especial referencia entre este tipo de textos merece, sin duda, el *Position Paper* de la IACS, que en 2020 ya había publicado una "recomendación sobre ciber resiliencia[66] con el objetivo de promocionar la adopción de directrices a ser implantadas desde el diseño y construcción de buques, de manera que éstos no solo sean ciber resilientes, sino que puedan mantener esta cualidad a lo largo de su vida útil. Este texto inicial asumía como principio fundamental la promoción de la prevención de incidentes y eventos de ciberseguridad. Buscaba, a su vez, incentivar el cumplimiento de la Resolución MSC.428(98) de 16 de junio de 2017 sobre la Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad.

En relación con su contenido, a diferencia de otros textos ya comentados en este trabajo, incluía una exhaustiva definición y descripción del ámbito de aplicación, tablas de ayuda a las referencias cruzadas de otras guías y estándares, amplia descripción de los detalles y requisitos técnicos que deberían cumplirse, así como un detallado procedimiento de verificación y prueba de su cumplimiento, además de una serie de anexos que ponen el texto en relación con otras guías y estándares, así como mayores detalles de los elementos operacionales que deben ser cumplidos y que forman parte de los procedimientos descritos en el texto principal.

Con este contenido, sin duda el *Position Paper* como documento sintetizador cumple la función de establecer el marco general aplicable desde este punto álgido de la industria naviera. Tal y como puede comprenderse, el valor práctico y su capacidad de influencia en el sector de ambos textos es,

---

65 Vid., la guía desarrollada por la *Nippon Kaji Kyokai* (ClassNK, Guidelines for designing Cyber Security Onboard Ships, 2nd ed. 2020), sociedad de clasificación japonesa.

66 IACS, Recommendation No. 166 on Cyber Resilience, 2020.

sin duda muy apreciable dada la posibilidad de ampliación de las líneas de negocio de estas empresas y su altísimo conocimiento técnico operacional[67].

IV. EL CIBERRIESGO Y SU ASEGURAMIENTO EN EL TRANSPORTE MARÍTIMO

Tanto el marco jurídico general y sectorial descrito hasta ahora, como el desarrollo incontestable de la permanente conectividad y las dependencias que ésta crea han incidido en todas las modalidades de transporte y, por tanto, también en el transporte marítimo, en el creciente interés de implantación de seguros que cubran, en alguna medida, los daños directos o responsabilidad extracontractual causados por el riesgo residual asociado al uso de los sistemas de información de los propietarios de activos. También denominados *ciber seguros*.

A pesar de la gran cantidad de avances que han tenido lugar en los últimos años, en el mercado de seguros de grandes riesgos los ciber seguros aún no han tenido una tasa de implantación importante. Si bien algunas regiones han logrado avances sobre la base de una legislación de apoyo, se ha constatado que, en comparación con otros sectores de seguros de daños, el estado de los ciber seguros se encuentra en una etapa menos madura[68].

A nuestro entender, el principal problema al que se enfrenta la industria aseguradora del transporte marítimo pasa por la determinación del contenido del riesgo cubierto dada la naturaleza progresiva del tipo de daños que pueden derivarse de los riesgos cibernéticos. En este último apartado del trabajo, nuestra labor se centrará, por tanto, en establecer la

---

67 También en este sentido JUAN Y MATEU, F., "El transporte marítimo y la ciberseguridad", cit., p. R.R-3.19, quien cita los nuevos servicios ofrecidos por este sector de la industria como ser la comprobación de la robustez de los sistemas (*penetrating tests*); formación del personal de abordo (presencial u *on line* para las dotaciones); el grado de preparación para el cumplimiento del estándar ISO/IEC 27001, la verificación de cumplimiento del mismo; o la evaluación del cumplimiento de la Directrices BIMCO.

68 En nuestro ámbito geográfico de referencia, ENISA destaca esta ausencia de desarrollo del mercado asegurador en la cobertura de los riesgos a los que se enfrentan los operadores de servicios esenciales, ENISA, *Demand side of cyber incsurance in the EU,* 2023 p. 5, disponible en https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu, accedido el 19 de julio, 2024.

conexión entre la operativa habitual de los seguros marítimos con los riesgos asociados al uso de tecnologías de la comunicación e información para concluir con la referencia a la situación actual de la práctica aseguradora.

1. La delimitación del riesgo

Tal y como hemos podido manifestar en los primeros apartados de este estudio, los riesgos asociados a la digitalización, en todos sus ámbitos, han aumentado su alcance paralelamente a la expansión del progreso tecnológico.

1.1. El problema de la individualización del riesgo

En el caso de los seguros marítimos, será necesario tener en cuenta el marco normativo internacional vigente a la hora de determinar la responsabilidad de los operadores de la navegación. Tomando en cuenta el grado de dependencia tecnológica que representa la ciber seguridad, a nuestro entender la atención prestada a la misma incide, y por tanto debe formar parte del *deber de navegabilidad* del buque en tanto que su deterioro por faltas de ciber seguridad afecta directamente al manejo *físico* del buque y al manejo operacional del mismo abordo[69]. Si tomamos en cuenta que se alude a la innavegabilidad cuando éste presenta deficiencias que afectan a su seguridad, podemos comprender la naturaleza de este nuevo riesgo[70] creemos que este debe ser el punto de partida desde el que se construya el ámbito de la responsabilidad del empresario de la navegación marítima[71].

---

69 Tal y como señalaba entre otros BENETT, H., *The Law of Marine Insurance*, 2nd. Ed., Londres, 2006, p. 566, la navegabilidad comprende tres aspectos esenciales: el estado físico del buque y todo su equipamiento a bordo, la profesionalidad y número del personal abordo, y el cumplimiento de todos los deberes de documentación.

70 También en este sentido, JUAN Y MATEU, F., "El transporte marítimo y la ciberseguridad", cit., p. R.R-3.19, KAO, B., "Cybersecurity in the shipping industry and the English Marine Insurance Law", *Tulane MAritime Law Journal*, vol. 45, 2021, p. 493.

71 Así, deberá tenerse en cuenta el contenido de las *Reglas de la Haya-Visby* respecto a la navegabilidad.

1.2. El problema de la determinación del alcance de la cobertura

Sin duda en la consideración de los daños contractuales y extracontractuales por falta de políticas efectivas de ciber seguridad, será necesario establecer el ámbito de cobertura directa al empresario y su actividad – pérdida o inutilización temporal o continuada del buque, su equipación o elementos operacionales – así como también, al igual que ocurre en seguros terrestres con los seguros de paralización del negocio, si existe cobertura para la empresa marítima como tal.

2. El status questionis de la práctica

2.1. Las cláusulas de la IUA

De momento, tanto en el caso de pólizas con referencia a las Cláusulas A, B o C, de las *cargo clauses*, como en el caso de las *hull clauses*, la falta de navegabilidad constituye una exclusión directa de cobertura:

In no case shall this insurance cover loss damage or expense arising from unseaworthiness of vessel or craft or unfitness of vessel or craft for the safe carriage of the subject-matter insured, where the Assured are privy to such unseaworthiness or unfitness, at the time the subject-matter insured is loaded therein.

A mayor abundamiento, en el caso de las "garantías implícitas" del asegurador usuario de las ICC, el párrafo 5.3 también las excluye de cobertura: *The Insurers waive any breach of the implied warranties of seaworthiness of the ship and fitness of the ship to carry the subject-matter insured to destination.*

2.2. Los formularios BIMCO

En el caso de los formularios BIMCO relativos a la navegabilidad, si tomamos en cuenta el cumplimiento de medidas de ciberseguridad como parte de la navegabilidad y, dado que esta asociación tiene, como ya hemos expuesto, una Guía de ciber seguridad, sí puede esperarse que la adscripción de estas medidas al deber de navegabilidad sea aceptada como tal.

En este sentido, en el caso de los formularios BIMCO, se ha propuesto integrar el cumplimiento de la guía de ciber seguridad como parte de los deberes de documentación que integran la navegabilidad[72] cuestión que,

---

[72] KAO, B., "Cybersecurity in the shipping industry…" cit., p. 502.

a nuestro entender, redundaría en una mayor efectivad de las medidas propugnadas por la asociación.

V. CONCLUSIONES

La normativa europea en materia de ciberseguridad ha tomado un acelerado ritmo de desarrollo, sin duda con el objetivo de alcanzar un nivel adecuado de implantación de medidas de ciberseguridad en el territorio y actividades digitales de ámbito europeo.

Sin embargo, tal y como queda demostrado del análisis de los sectores en los que se implementa de manera más categórica, en el ámbito de la navegación marítima no hay previsión de adoptar un texto o reglas, en materia de medidas mínimas de ciberseguridad, que sean imperativas. Queda por ver la efectividad auténtica que, tanto la *Ley de ciber resiliencia* como la *Ley de ciber solidaridad* tendrán, si ambos textos europeos llegan a adoptarse.

En el caso de la NIS2, la posibilidad de una rápida implementación de su contenido, dado su carácter imperativo, puede dar lugar a un necesario cambio, o mejor, evolución en la cultura empresarial, en este caso del sector marítimo, y del transporte en general, que facilitará una rápida adaptación a los niveles de previsión, detección, respuesta y freno a los incidentes y eventos de ciberseguridad en este sector.

A pesar de lo anterior, la narración sucinta de las políticas, guías y códigos de buenas prácticas que diversos actores del sector marítimo han puesto en marcha con la finalidad de adaptar su modelo de negocio a la digitalización de los procesos operativos de la industria deja claro que éstas no solo son heterogéneas en su contenido técnico, sino también en la imperatividad de sus mandatos, razón que pone de manifiesto el escaso valor jurídico de las mismas.

Los textos redactados por asociaciones profesionales del sector buscan incentivar el desarrollo de procedimientos operacionales estándar en la industria marítima. Sin embargo, a nuestro entender, la falta de coercibilidad de las instituciones que ha empezado a preparar, publicar y actualizar estos documentos no permite vislumbrar una pronta adopción de medidas mínimas y uniformes en favor de la ciberseguridad.

El brevísimo repaso a la situación jurídica de la construcción de seguros del transporte marítimo que cubran este tipo creciente de daños está aún en incipiente desarrollo, a pesar del rápido incremento de los riesgos asociados a la ciberseguridad.

CONDUCCIÓN AUTÓNOMA Y SEGURIDAD JURÍDICA DEL TRANSPORTE DESDE LA PERSPECTIVA EUROPEA E INTERNACIONAL

Director:
Eliseo Sierra Noguero

tirant lo blanch
Valencia, 2025

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email: tlb@tirant.com
www.tirant.com
Librería virtual: www.tirant.es
DEPÓSITO LEGAL: V-1238-2025
ISBN: 978-84-1095-453-3

Si tiene alguna queja o sugerencia, envíenos un mail a: *atencioncliente@tirant.com*. En caso de no ser atendida su sugerencia, por favor, lea en *www.tirant.net/index.php/empresa/politicas-de-empresa* nuestro procedimiento de quejas.

Responsabilidad Social Corporativa: *http://www.tirant.net/Docs/RSCTirant.pdf*