OMI 2021: *COMPLIANCE* EN CIBERSEGURIDAD PARA LA INDUSTRIA MARÍTIMA

Por: Lubign Maldonado[1]

Agosto 2020

Antecedentes

El sector marítimo es una parte vital de la economía mundial, al movilizar tanto carga como pasajeros. Los buques son cada vez más complejos y dependen del uso de tecnología y de las comunicaciones durante toda su travesía. La seguridad es una parte esencial de la actividad y fallas o inobservancias en términos de seguridad pueden dar lugar a pérdidas importantes, sean económicas o de reputación, ya que, a través de un accidente se puede hacer daño a la vida de las personas, al ambiente marino o a bienes.

En medio de este proceso de auge tecnológico, existe una necesidad y una dependencia a la actualización y el uso de nuevos sistemas. Se trata de avances que obligan a la conectividad las 24 horas del día y los 365 días del año, y se basan en sistemas que buscan la digitalización, la informatización, la integración y la automatización de los procesos, lo cual genera beneficios en eficiencia y productividad.

Esta dependencia a la tecnología resalta nuevos conceptos, equipos y prácticas, que sin duda representan un progreso en la productividad dentro de la industria marítima, pero que abren la ventana a una nueva cartera de riesgos: los riesgos cibernéticos.

Estos riesgos cibernéticos están asociados con pérdidas o daños, por fallas, uso no autorizado o uso incorrecto de sistemas de información, y aunque no son tan novedosos, estos representan

[1] Abogado de la Universidad Central de Venezuela, Realizando Trabajo Especial de Grado tanto en la Especialización en Comercio Marítimo Internacional, Mención Derecho Marítimo en la Universidad Marítima del Caribe; como en la Especialización en Derecho Económico y de la Integración en la Universidad Central de Venezuela. Consultor Jurídico de compañías del sector marítimo y Asociado Junior y Director Administrativo del Bufete BOFRAS.

peligros de gran magnitud para todos los usuarios, y mientras más se confíe en la tecnología para las comunicaciones y los procesos, más amplia será la variedad y complejidad de este tipo de riesgos.

Entonces, ¿está el sector marítimo preparado para mitigar los posibles riesgos cibernéticos? Esta pregunta se realiza en tiempo presente, basándonos en la actualidad, en la realidad del sector y no viendo la automatización y a la tecnología como algo futurista, sino como una herramienta del día a día que abre el campo de mejora para el sector marítimo mundial.

Antes de continuar, es importante realizar una aclaratoria con respecto a conceptos que pueden ser similares, pero que definen dos hechos distintos, y estos son: el riesgo, entendido como la posibilidad de que suceda un daño, futuro e incierto; y un ataque, que es un hecho doloso, que busca causar un daño.

Esto es de gran relevancia ya que, tanto la Directriz MSC-FAL.1/Circ.3 y las Directrices del sector sobre ciberseguridad a bordo de los buques, documentos a los cuales nos referiremos más adelante, no hacen una diferenciación de estos dos conceptos y los toman como iguales. En ambos documentos se habla indiscriminadamente de riesgos y ataques cibernéticos, y aunque son directrices emanadas de la Organización Marítima Internacional y de organizaciones importantes del sector marítimo, los *riesgos* y la gestión de los mismos atañe al Código Internacional de Gestión de la Seguridad (Código IGS o *ISM Code*) y los planes de protección contra *ataques* que busquen dañar la integridad del buque o instalaciones portuarias se regulan por el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP o *ISPS Code*).

Para analizar un poco la situación del sector con respecto al uso de la tecnología, encontramos un informe de la aseguradora inglesa MARSH[2], donde exponen que para 2014 la industria marítima seguía en el Siglo XX, en términos de gestión de riesgos

[2] Marsh & McLennan (Julio 2014) *The Risk of Cyber-Attack to The Maritime Sector*. Recuperado de: https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html

cibernéticos, y una prueba de ello son los ataques al puerto de Amberes[3] en 2011, donde hasta 2013, piratas informáticos tuvieron acceso al sistema del puerto logrando desviar y movilizar carga, en su mayoría drogas, y la administración del puerto, no manejaba la información, pues en su sistema todo parecía normal.

Igualmente, la compañía A.P Moller-Maersk, reportó en 2017, una brecha en sus sistemas informáticos, que generaron pérdidas de entre 250 y 300 millones de dólares, pudiendo recuperar el control total de sus operaciones pasado un mes del ataque, que afectó todas sus operaciones en buques portacontenedores, tanqueros, plataformas costa afuera y sus oficinas a nivel mundial.

Estos, como nos referimos anteriormente, fueron ejemplos de ataques cibernéticos, al ser actos dolosos, utilizando herramientas tecnológicas y dirigidas intencionalmente a causar un daño; igualmente estos hechos nos ubican en las debilidades de la industria en cuestión de protección, pero intrínsecamente no son vinculados con los accidentes cibernéticos o a la gestión de seguridad. Un estudio publicado en la Facultad de Estudios Marítimos de la Universidad de Rijeka, Croacia[4], analizó accidentes publicados por la MIAB (Subdivisión de Investigación de Accidentes Marinos del Reino Unido) desde el año 2012 al 2014, y el 33% de los accidentes analizados tenían como causa la tecnología, producidos por un diseño inadecuado de los equipos, poco conocimiento de los sistemas de los buques, exceso de confianza en sistemas computarizados y falta de medidas preventivas o familiarización; todos estos riesgos pudieron cubrirse a través de medidas preventivas impulsadas por la Compañía operadora del buque, a través de un Sistema de Gestión de la Seguridad, que cubriese la gestión de riesgos cibernéticos.

En este orden de ideas, es importante resaltar la labor continua de la Organización Marítima Internacional, impulsando cambios y desarrollando las directrices y normativas de los convenios

[3] Idem

[4] Bielić, T. Hasanspahić, N. Čulin, J. (2017) *Preventing marine accidents caused by technology-induced human error. Scientific Journal of Maritime Research* 31. pp 33-37. *Faculty of Maritime Studies Rijeka.*

internacionales ampliamente aceptados en el sector, tocando desde temas ambientales hasta temas de seguridad, que pueden afectar en pequeña o gran escala el negocio marítimo, pero cambios que buscan la mejora continua en los procesos de los sujetos involucrados en el negocio naviero y en última instancia, buscan cumplir con los objetivos de la Organización, es decir, una navegación segura, protegida y eficiente en mares limpios.

Como ejemplo de estos cambios y en respuesta a la realidad del sector en cuestión de tecnología, el Comité de Seguridad Marítima (MSC), aprobó las Directrices del MSC-FAL.1/Circ.3 sobre la gestión de los riesgos cibernéticos marítimos y la Resolución MSC.428 (98) sobre la Gestión de los Riesgos Cibernéticos Marítimos en los Sistemas de Gestión de la Seguridad.[5]

Sistemas de Gestión de la Seguridad y el Código Internacional de la Gestión de la Seguridad

Los Sistemas de Gestión de la Seguridad vienen regulados en el Código Internacional de Gestión de la Seguridad (Código IGS), y la Resolución MSC.428 (98) afirma que todo Sistema de Gestión de la Seguridad debe tomar en cuenta un apartado a los riesgos cibernéticos, incluyendo a estos, como un punto a ser evaluado en las revisiones anuales realizadas por las Administraciones.

Ahora, los riesgos cibernéticos no representan algo nuevo, estos existen y pueden evaluarse desde el uso personal o comercial de cualquier computador, pero para el sector marítimo representan una nueva realidad, y la Organización Marítima Mundial, a través del Comité de Seguridad Marítima (MSC) toma las "Directrices del sector sobre ciberseguridad a bordo de los buques" documento impulsado por organizaciones como BIMCO, CLIA, ICS, INTERCARGO e INTERTANKO como antecedente directo para la MSC-FAL.1/Circ.3 y la Resolución MSC.428 (98), antes mencionadas.

[5] Esta Resolución hace referencia a la Gestión de Riesgos Cibernéticos y correctamente lo vincula al Código IGS, y es a este Código y su contenido al que nos referiremos. Consideramos que la protección frente ataques y lo relativo a los mismos, debería ser abordada por los planes de protección y siguiendo lo especificado en el Código PBIP.

El Código Internacional de Gestión de la Seguridad, adoptado en su forma obligatoria en 1993 por la resolución A.741 (18) y en vigor desde el 1 de julio de 1998, desarrolla el Capítulo IX del Convenio internacional para la seguridad de la vida humana en el mar (SOLAS); tiene como objetivo general garantizar la seguridad marítima y de esta manera evitar lesiones personales, pérdidas de vida humana, daños al medio ambiente y/o daños a los bienes que son transportados por el mar"[6].

Y para ello, a través de los Sistemas de Gestión de Seguridad, las compañías navieras deberán:

1. Establecer prácticas de seguridad en las operaciones del buque.
2. Evaluar riesgos para sus buques, personal, medio ambiente y tomar las medidas oportunas.
3. Mejorar los conocimientos de todo su personal sobre la gestión de la seguridad[7].

Además, estos Sistemas deben garantizar el cumplimiento de la normativa vigente, sean códigos, directrices y/o normas recomendadas por la OMI, Estados Bandera, Sociedades de Clasificación y demás organizaciones.

Cumplidos estos requisitos, se otorga un Documento de Cumplimiento (DOC) a la compañía y un Certificado de Gestión de la Seguridad a cada buque, que certifica por parte de la Administración que el Sistema de Gestión de la Seguridad cumple con los parámetros establecidos en el Código IGS y que está correctamente implementado en las operaciones del buque.

Haciendo un análisis, podemos afirmar que aun sin la resolución MSC.428 (98), las compañías que usan tecnología en sus oficinas o buques, estaban en la obligación de adelantar un análisis de riesgo cibernético, que permitiese garantizar la disponibilidad de la información necesaria para la operación de los buques en caso de accidentes relativos al uso de estas tecnologías; pero la propia Organización Marítima Internacional en el preámbulo de la Resolución reconoce que el riesgo

[6] Organización Marítima Internacional (2014) 1.2 Objetivos. Código Internacional de Gestión de la Seguridad y directrices para su implantación, Edición Electrónica. Londres.

[7] *Idem.*

cibernético no está inmerso en la cultura de seguridad del sector; y mediante estas directrices busca ampliar la conciencia y así proteger al sector marítimo de dichos riesgos.

Esta resolución, alienta a que los riesgos cibernéticos se aborden adecuadamente en los Sistema de Gestión de la Seguridad de las Compañías, a más tardar en la primera verificación anual del DOC después del 1 de enero de 2021.

Esta Resolución se emite basándose en el Código IGS, y la Organización Marítima Internacional, no hace mención del Código Internacional para la Protección de Buques e Instalaciones Portuarias.

Debemos hacer énfasis en la posibilidad de hacer daños materiales importantes a buques o a puertos a través de un ataque cibernético. Por ello creemos que desde un punto de vista de protección se hace necesario realizar nuevas evaluaciones de protección que consideren los riesgos cibernéticos e incluir estos en los distintos Planes de Protección de los Buques y Puertos, pues un ataque puede interferir en la navegación, revelar información valiosa sobre la carga, y demás consecuencias que pueden afectar la integridad del buque, puerto y las personas involucradas en la operación; y esta protección, aun cuando está contemplada en el Convenio SOLAS, se desarrolla propiamente en el Código PBIP, por lo que la Resolución MSC.428 (98) al solo hacer mención a los Sistemas de Gestión de Seguridad, alienta a la evaluación de los riesgos cibernéticos y no a los ataques.

<u>Cumplimiento de la Resolución MSC.428 (98)</u>

La correcta gestión de los Riesgos cibernéticos, requiere velar por varios estándares impuestos, bien sea por las propias compañías, por organizaciones privadas (INTERTANKO, OCIFM, por nombrar algunas), administraciones u Organizaciones Internacionales. Aun cuando estos requisitos de cumplimiento varían, estos implican la utilización de una serie de procesos, procedimientos y organización enfocados a proteger la integridad y tecnologías organizativas específicas para salvaguardar los datos.

La Organización Marítima Internacional sugiere y hace mención de tres documentos de gran importancia para el cumplimiento e implementación de la Gestión de Riesgos cibernéticos, los

cuales son: La Guía o Directrices del sector sobre ciberseguridad a bordo de los buques, elaboradas por BIMCO, CLIA, ICS, INTERCARGO e INTERTANKO; la Norma ISO/IEC 27001 sobre el Manejo y la Seguridad de la Información, publicada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI); y el Marco de mejora de la ciberseguridad de las infraestructuras críticas del Instituto Nacional de Normas y Tecnologías (NIST) (Marco NIST) de los Estados Unidos, esta última publicada en el año 2014 y es una guía básica que permite a organizaciones de cualquier tamaño implementar procesos para el seguimiento y control de los riesgos cibernéticos, basada en 5 puntos de importancia para esta gestión, siendo estos 5 puntos:

- Identificación
- Protección
- Detección
- Respuesta
- Recuperación

Por supuesto, cada situación es particular y en el caso del cumplimiento, más aun, dependerá de las normas aplicables al buque y la compañía, ya que para la Resolución MSC 248 (98) con la aplicación de las políticas establecidas en el Marco NIST se estaría en pleno cumplimiento de la misma, pero como se mencionó, dependerá de las normas aplicables a la Compañía y al Buque; las leyes del pabellón, normas internacionales o reglamentos privados, que pueden regular de manera más estricta la gestión de riesgos cibernéticos.

Aunque exista una conciencia colectiva a la protección de datos, a la integridad de los mismos en cuanto al uso de las tecnologías, se diferencia de aplicar los estándares de ciberseguridad, siendo que, para la mitigación de riesgos se manejan conceptos nuevos, que tal vez, para quienes desempeñan roles operacionales, no se venían manejando en lo absoluto y métodos de implementación que pueden cambiar los procesos de las compañías.

Sin duda, la OMI al hacer referencia a los 3 documentos que mencionamos, ofrece un esquema que ayudará a las Compañías a la correcta implementación de un plan de ciberseguridad dentro de sus Sistemas de Gestión de la Calidad.

Sanciones en caso de incumplimiento

La Resolución 428 (98) deja claro que los riesgos cibernéticos deben abordarse a partir del 1° de enero del 2021, y que las verificaciones realizadas por las Administraciones deben tomar en cuenta este punto para la renovación de los certificados y documentos correspondientes relativos a los Sistemas de Gestión de la Seguridad de las Compañías y de los buques que operan en su territorio.

En caso de que la Administración a partir de esta fecha, en la revisión anual realizada a una Compañía naviera, verifique que el Sistema de Gestión no incluye la gestión de riesgos cibernéticos, podrá suspender de manera temporal o indefinida el Documento de Cumplimiento de la Compañía y, por ende, el Certificado de Gestión de la Seguridad del Buque hasta que incluyan los nuevos riesgos, lo que conlleva a la suspensión de la actividad comercial de la compañía y el buque. Esto, basado en la Parte B del Código IGS, relativo a la Certificación y Verificación [8] de igual forma, las sanciones podrán ser más estrictas a las establecidas en el Código, dependiendo de la norma aplicable.

Aplicabilidad en Venezuela

Venezuela es Estado parte del Convenio Internacional para la Seguridad de la Vida Humana en el Mar[9] [10], por lo tanto, mediante el Anexo IX del mismo es aplicable el Código Internacional de la Gestión de la Seguridad a toda Compañía que sea propietaria u opere un buque dentro del territorio nacional.

De esta manera, nuestro país es un Estado más a los que la Resolución MSC.428 (98) alienta a garantizar que los riesgos cibernéticos estén siendo abordados de la manera correcta por los Sistemas de Gestión de Seguridad, y que siguiendo las medidas de esta Resolución, desde el 1° de enero del año 2021, toda compañía que opere o explote buques dentro del territorio

[8] Organización Marítima Internacional (2014) Certificación y Verificación. Código Internacional de Gestión de la Seguridad y directrices para su implantación, Edición Electrónica. Londres.

[9] Ley Aprobatoria de la Convención Internacional De La Seguridad De La Vida Humana En El Mar 1974. Gaceta Oficial de la República de Venezuela N° 1.248 Extraordinario. 8 de noviembre 1968.

[10] Ley Aprobatoria del Protocolo 1988 SOLAS relativo al Convenio Internacional para la Seguridad Vida Humana en el Mar 1974. Gaceta Oficial de la República de Venezuela N° 5.187 Extraordinario. 5 de diciembre 1997.

nacional tendrá, obligatoriamente, que incluir los Riesgos cibernéticos dentro de su Sistema de Gestión de la Seguridad para la renovación de su documentación y certificados correspondientes.

Por su parte, en la Ley de Marinas y Actividades Conexas[11], en su artículo 23 establece que todo buque inscrito en el Registro Naval Venezolano, de arqueo bruto mayor a 150 UAB deberá poseer, entre otros, un Certificado Internacional de Gestión de la Seguridad; es así como, en Venezuela se amplía el alcance de lo establecido en el Código IGS, que exige este certificado a buques con un mínimo de 500 UAB. Por tanto, nuestra legislación es más estricta y busca aplicar estándares de seguridad a muchos más buques dentro del territorio nacional.

En caso de inscripción o renovación de una Compañía naviera en Venezuela ante el Instituto Nacional de los Espacios Acuáticos y ante el Registro Naval Venezolano, el Sistema de Gestión de Seguridad deberá incluir la gestión de riesgos cibernéticos para que sea emitido el Documento de Cumplimiento que valide la correcta implementación del sistema.

Igualmente, como se mencionó *supra*, el no cumplimiento acarrearía la suspensión temporal o definitiva de los certificados; y en Venezuela, al no contar con los certificados correspondientes, la Ley de Marinas y Actividades Conexas establece, en su artículo 40, el deber de no autorizar el zarpe del buque por parte del Capitán de Puerto, por incumplimiento legal de normativas de seguridad; y a su vez, en los artículos 287 y siguientes, encontramos sanciones de carácter administrativo, a compañías que operen sin los certificados correspondientes.

Conclusiones

Cuando nos referimos a riesgos cibernéticos no estamos hablando de un futuro lejano o cercano, sino de una realidad que afecta y seguirá afectando al sector marítimo, como consecuencia de que cada día se crean y se utilizan más soluciones tecnológicas dentro de los buques o en compañías para facilitar y automatizar los procesos, y todo indica que la tecnología es el camino que, más

[11] Decreto con Rango, Valor y Fuerza de Ley de Marinas y Actividades Conexas. Gaceta Oficial de la República Bolivariana de Venezuela. N° 6.153 Extraordinario del 18 de noviembre de 2014.

pronto que tarde, llevará a puerto seguro a los buques y sus cargas de manera autónoma.

Viendo esto, la Organización Marítima Internacional tomó medidas de carácter normativo, que hacen imperativo a las Administraciones incluir en los Sistemas de Gestión de Seguridad los riesgos cibernéticos que pueden afectar la integridad de los humanos, el medio ambiente y bienes.

Es importante a su vez, aclarar la diferencia entre riesgo y ataque, pues los primeros se refieren a la prevención de accidentes (*safety*) dentro de los Sistemas de Gestión de Seguridad, regulados por el Código Internacional de Gestión de la Seguridad; y los segundos aluden a la protección frente ataques (*security*) llevados en los Planes de Protección y regulados por el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias.

Las medidas para la implementación de la gestión de riesgos cibernéticos tomadas por la OMI, son lo bastante amplias para asegurar un cumplimiento por parte de Armadores y Operadores de buques dentro del sector marítimo, sin dejar de ser de carácter obligatorio desde el próximo año, garantizando así un cumplimiento general en aras de cambiar la cultura de seguridad referente al uso de las tecnologías y cumplir con los objetivos, tanto del Código IGS, como de la Organización Marítima Internacional.

En caso de incumplimiento por parte de la Compañía operadora, dependerá de la normativa aplicable, tanto en el Estado del Pabellón como en el Estado Rector del Puerto; pero siguiendo lo establecido en el Código Internacional, tanto la compañía como el buque, perderían temporal o indefinidamente los documentos y certificados que garantizan el cumplimiento de la normativa de seguridad, lo que detendría sus operaciones hasta que se subsane el incumplimiento.

En el caso venezolano, vemos que no somos la excepción de la Resolución, por lo tanto, toda compañía que opere o explote buques dentro de nuestro territorio deberá incluir en su Sistema de Gestión, los riesgos cibernéticos y recae en la Autoridad Acuática Venezolana (INEA), de acuerdo a lo establecido en el Artículo 74 de la Ley Orgánica de los Espacios Acuáticos en sus numerales

3°, 9° y 13°[12], la obligación de velar por el cumplimiento de la normativa nacional e internacional vigente, mantener el registro de las empresas navieras y su certificación; y garantizar la seguridad marítima dentro de su jurisdicción.

***LAS OPINIONES AQUÍ EXPUESTAS REFLEJAN LA POSICIÓN PERSONAL DEL AUTOR Y NO DE LA ASOCIACIÓN VENEZOLANA DE DERECHO MARÍTIMO (AVDM), NI DE SUS MIEMBROS.**

[12] Decreto con Rango, Valor y Fuerza de Ley Orgánica de los Espacios Acuáticos. Gaceta Oficial de la República Bolivariana de Venezuela. N° 6.153 Extraordinario del 18 de noviembre de 2014.