ORGANIZACIÓN MARÍTIMA INTERNACIONAL

S

4 ALBERT EMBANKMENT
LONDRES SE1 7SR
Teléfono: +44(0)20 7735 7611 Facsímil: +44(0)20 7587 3210

MSC-FAL.1/Circ.3
5 julio 2017

DIRECTRICES SOBRE LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS

1 El Comité de facilitación, en su 41º periodo de sesiones (4 a 7 de abril de 2017) y el Comité de seguridad marítima, en su 98º periodo de sesiones (7 a 16 de junio de 2017), tras haber tomado en consideración la necesidad urgente de elevar el nivel concienciación sobre las amenazas y las vulnerabilidades conexas con los riesgos cibernéticos, aprobó las Directrices sobre la gestión de los riesgos cibernéticos marítimos que figuran en el anexo.

2 Las Directrices facilitan recomendaciones de alto nivel sobre la gestión de los riesgos cibernéticos marítimos para proteger el transporte marítimo de los riesgos cibernéticos y las vulnerabilidades, tanto existentes como emergentes. Las Directrices también recogen elementos funcionales para apoyar una gestión efectiva de los riesgos cibernéticos.

3 Se invita a los Gobiernos Miembros a que pongan el contenido de la presente circular en conocimiento de todas las partes interesadas.

4 La presente circular revoca las Directrices provisionales que figuran en la circular MSC.1/Circ.1526.

***

ANEXO

DIRECTRICES SOBRE LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS

1 INTRODUCCIÓN

1.1 El propósito de estas directrices es ofrecer recomendaciones de alto nivel para la gestión de los riesgos cibernéticos marítimos. A efectos de las presentes directrices, el riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posibles, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas.

1.2 Los interesados deberían tomar las medidas necesarias para salvaguardar el transporte marítimo de las amenazas y vulnerabilidad actuales y emergentes relacionadas con la digitalización, la integración y automatización de los procedimientos y sistemas del transporte marítimo.

1.3 Los usuarios de estas directrices deberían remitirse a las prescripciones de los Gobiernos Miembros y de las Administraciones de los Estados de abanderamiento, así como a las normas internacionales pertinentes, normas del sector y mejores prácticas, para obtener información y orientaciones a la hora de elaborar e implantar los procedimientos específicos de gestión de los riesgos.

1.4 La gestión de los riesgos es fundamental para la seguridad y la protección de las operaciones del transporte marítimo. Tradicionalmente, la gestión de los riesgos se ha centrado en operaciones de ámbito físico, pero la mayor dependencia en la digitalización, la integración, la automatización y los sistemas basados en redes ha creado una necesidad creciente de gestionar los riesgos cibernéticos dentro del sector del transporte marítimo.

1.5 Tomando como base el objetivo de contribuir a la seguridad y a la protección del transporte marítimo, operacionalmente resiliente ante los riesgos cibernéticos, se incluyen en las presentes directrices recomendaciones que se pueden incorporar en los procedimientos existentes de gestión de los riesgos. A este respecto, las siguientes directrices complementan las prácticas sobre gestión de la seguridad y la protección establecidas por esta Organización.

2 GENERALIDADES

2.1 Antecedentes

2.1.1 Las tecnologías cibernéticas se han convertido en esenciales para el funcionamiento y la gestión de los numerosos sistemas cruciales para la seguridad y la protección del transporte marítimo, y la protección del medio marino. En algunos casos, estos sistemas han de cumplir las normas internacionales y las prescripciones de las Administraciones de abanderamiento. No obstante, la vulnerabilidad generada por el acceso, la interconexión o el establecimiento de redes entre estos sistemas puede dar lugar a riesgos cibernéticos que deberían abordarse. Dichos sistemas vulnerables podrían ser, entre otros:

- Los sistemas del puente
- Los sistemas de manipulación y gestión de la carga
- Los sistemas de propulsión y gestión de las máquinas y de control de suministro eléctrico

– Los sistemas de control de acceso
– Los sistemas de servicio a los pasajeros y de organización de los mismos
– Las redes públicas para los pasajeros
– Los sistemas administrativos y de bienestar de la tripulación
– Los sistemas de comunicación

2.1.2 Debería considerarse la distinción entre la tecnología de la información y los sistemas de tecnología operacional. Podría decirse que los sistemas de tecnología de la información se centran en el uso de los datos como información. Los sistemas de tecnología operacional, a su vez, se centran en el uso de los datos para controlar o vigilar procesos físicos. Además, debería considerarse la protección de la información y el intercambio de datos dentro de esos sistemas.

2.1.3 Si bien dichas tecnologías y sistemas ofrecen ventajas importantes al sector marítimo desde el punto de vista de la eficacia, también presentan riesgos para sistemas y procedimientos cruciales vinculados al funcionamiento de los sistemas que son parte integral del transporte marítimo. Dichos riesgos pueden derivar de la vulnerabilidad originada por el funcionamiento, integración, mantenimiento y proyecto inadecuados de los sistemas de índole cibernética, y de amenazas cibernéticas intencionadas o no intencionadas.

2.1.4 Las amenazas aparecen mediante actuaciones malintencionadas (por ejemplo, piratería informática o introducción de programas informáticos maliciosos) o como una consecuencia no deliberada de actuaciones bienintencionadas (por ejemplo, mantenimiento de los programas informáticos o permisos de usuarios). En general, estas actuaciones ponen de manifiesto alguna vulnerabilidad (por ejemplo, programas informáticos anticuados o barreras de control de acceso ineficaces) o bien aprovechan alguna vulnerabilidad de la tecnología operacional o de la información. Para que la gestión de los riesgos cibernéticos sea eficaz, deberían considerarse ambos tipos de amenazas.

2.1.5 La vulnerabilidad puede derivarse de un proyecto, integración y/o mantenimiento inadecuados de los sistemas, así como de lapsus en la disciplina cibernética. En general, cuando se pone de manifiesto o se aprovecha alguna vulnerabilidad de la tecnología operacional y/o de la información, bien directamente (por ejemplo, con contraseñas poco seguras que dan lugar a accesos no autorizados) o indirectamente (por ejemplo, por la ausencia de segregación de las redes), puede haber implicaciones para la protección y confidencialidad, e integridad y disponibilidad de la información. Asimismo, cuando se pone de manifiesto o se aprovecha alguna vulnerabilidad de la tecnología operacional y/o de la información, puede haber implicaciones para la seguridad, sobre todo poniendo en peligro sistemas cruciales (la navegación en el puente o de sistemas principales de propulsión).

2.1.6 Para que la gestión de los riesgos cibernéticos sea eficaz, también se deberían considerar las repercusiones que tienen en la seguridad y en la protección la manifestación o el aprovechamiento de la vulnerabilidad de los sistemas de tecnología de la información. La causa podría ser la conexión indebida a sistemas de tecnología operacional o lapsus de procedimiento que hayan tenido el personal operacional o terceras partes, que ponen en peligro dichos sistemas (por ejemplo, el uso indebido de medios extraíbles, como un lápiz de memoria).

2.1.7 Para más información sobre la vulnerabilidad y las amenazas, véanse las orientaciones adicionales y normas a que se hace referencia en la sección 3.

2.1.8 La velocidad de los cambios de las tecnologías y de las amenazas dificulta el tratamiento de estos riesgos solamente mediante normas técnicas. Al ser directrices, en ellas se recomienda un planteamiento para gestionar los riesgos cibernéticos, el cual es resiliente y evolutivo como prolongación natural de las prácticas existentes para la gestión de la seguridad y la protección.

2.1.9 Al examinar las fuentes posibles de amenazas y de la vulnerabilidad, así como las estrategias posibles para mitigar los riesgos, las organizaciones deberían examinar varias opciones de control de la gestión de los riesgos cibernéticos. Entre estos controles posibles cabe mencionar los controles de la gestión, los controles operacionales o de procedimiento, y los controles técnicos.

2.2 Ámbito de aplicación

2.2.1 Las presentes directrices se dirigen principalmente al conjunto de las organizaciones del sector del transporte marítimo y están concebidas para fomentar las prácticas de gestión de la seguridad y la protección dentro del ámbito cibernético.

2.2.2 Al reconocer que en el sector del transporte marítimo no hay dos organizaciones que sean iguales, las presentes directrices se expresan en términos generales para que tengan una aplicación generalizada. En el caso de los buques con sistemas de índole cibernética limitados, la simple aplicación de estas directrices puede ser suficiente; sin embargo, los buques con sistemas de índole cibernética complejos requerirán un mayor nivel de atención y deberían encontrar recursos adicionales a través de socios del sector reputados y del Gobierno.

2.2.3 Las presentes directrices tienen carácter recomendatorio.

3 ELEMENTOS DE LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS

3.1 A los efectos de las presentes directrices, se entiende por gestión de los riesgos cibernéticos el proceso de identificación, análisis, evaluación y comunicación de riesgos de índole cibernética y de aceptación, evitación, transferencia o mitigación de esos riesgos hasta un nivel aceptable, teniendo en cuenta los costos y las ventajas para los interesados de las actuaciones emprendidas.

3.2 El objetivo de la gestión de los riesgos cibernéticos marítimos es contribuir a la seguridad y a la protección del transporte marítimo, operacionalmente resiliente ante los riesgos cibernéticos.

3.3 La gestión eficaz de los riesgos cibernéticos debería empezar en el nivel de la dirección superior. La dirección superior debería enraizar en todos los niveles de la Organización la cultura de conocimiento de los riesgos cibernéticos y garantizar que exista un régimen englobador y flexible de gestión de los riesgos cibernéticos, que esté en funcionamiento continuo y se evalúe constantemente mediante mecanismos eficaces de retroalimentación.

3.4 Un planteamiento aceptado para conseguir lo arriba expuesto es evaluar y comparar de forma completa las posturas vigentes, y las posturas deseadas, de la gestión de los riesgos cibernéticos. Gracias a esa comparación, pueden aparecer lagunas que pueden resolverse, con el fin de conseguir los objetivos de la gestión de los riesgos mediante un plan prioritario de gestión de los riesgos cibernéticos. Dicho planteamiento basado en los riesgos permitirá a la Organización aplicar del mejor modo sus recursos, de la manera más eficaz.

3.5 En estas directrices se presentan elementos funcionales que contribuyen a la gestión efectiva de los riesgos cibernéticos. Dichos elementos funcionales no son secuenciales; todos deberían ser simultáneos y continuos en la práctica y deberían incorporarse debidamente en un marco de gestión de los riesgos:

.1 Identificación: definir las funciones y responsabilidades del personal en la gestión de los riesgos cibernéticos, e identificar los sistemas, activos, datos y capacidades que, si se interrumpen, plantean riesgos para las operaciones de los buques.

.2 Proteger: implantar procedimientos y medidas para el control de los riesgos, así como planificación para contingencias, a fin de proteger ante cualquier suceso cibernético y garantizar la continuidad de las operaciones del transporte marítimo.

.3 Detectar: crear las actividades necesarias para detectar un suceso cibernético oportunamente.

.4 Responder: crear e implantar actividades y planes para dar resiliencia y restaurar los sistemas necesarios para las operaciones o servicios de transporte marítimo que hayan sido afectados por un suceso cibernético.

.5 Recuperar: determinar medidas para copiar y restaurar sistemas cibernéticos necesarios para las operaciones de transporte marítimo que hayan sido objeto de un suceso cibernético.

3.6 Estos elementos funcionales abarcan las actividades y los resultados deseados de la gestión eficaz de los riesgos cibernéticos común a todos los sistemas cruciales que afectan a las operaciones marítimas y al intercambio de información, y constituyen un proceso continuo con mecanismos eficaces de retroalimentación.

3.7 La gestión eficaz de los riesgos cibernéticos debería garantizar un nivel de concienciación adecuado sobre los riesgos cibernéticos en todos los niveles de una organización. El nivel de concienciación y de preparación debería ser el adecuado para las funciones y responsabilidades del sistema de gestión de los riesgos cibernéticos.

4 MEJORES PRÁCTICAS PARA IMPLANTAR LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS

4.1 El planteamiento de la gestión de los riesgos cibernéticos aquí descrito sirve de base para entender y gestionar mejor los riesgos cibernéticos, lo que permite un planteamiento de la gestión de los riesgos que aborde las amenazas y la vulnerabilidad cibernéticas. Para contar con orientaciones detalladas sobre la gestión de los riesgos cibernéticos, los usuarios de estas directrices deberían remitirse también a las prescripciones de los Gobiernos Miembros y de las Administraciones del Estado de abanderamiento, así como a las normas internacionales, normas del sector y mejores prácticas pertinentes.

4.2 Entre las orientaciones y las normas adicionales, cabe citar sin carácter exhaustivo:[1]

– Directrices sobre ciberseguridad a bordo de los buques elaboradas y apoyadas por BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF y IUMI.

– Norma ISO/IEC 27001: *Information technology – Security techniques – Information security management systems – Requirements.* Publicada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI).

– Marco de mejora de la ciberseguridad de las infraestructuras críticas del Instituto Nacional de Normas y Tecnologías (NIST) (Marco NIST) de los Estados Unidos.

4.3 Las referencias deberían remitirse a las versiones más actuales de las orientaciones o de las normas utilizadas.

---

[1] Las orientaciones y normas adicionales se enumeran como referencia no exhaustiva para ofrecer información más detallada a los usuarios de estas directrices. Las orientaciones y normas de referencia no han sido publicadas por la Organización y su uso se deja a discreción de los propios usuarios de estas directrices.