

CIRCULAR

No. CR-20200155

Bogotá, 21/09/2020

PARA: Instalaciones Portuarias.
Compañías Marítimas.

ASUNTO: Seguridad Cibernética y Seguridad de Drones.

Con el objetivo de seguir desarrollando buenas prácticas para la mejora continua del Sistema de Gestión de la Protección Marítima a nivel nacional, y con el fin de proteger el transporte marítimo específicamente en esta ocasión en relación con buques e instalaciones portuarias; de los riesgos asociados con drones, ataques cibernéticos y las vulnerabilidades tanto existentes como emergentes, como Autoridad Designada nos permitimos presentar las siguientes directrices.

Basado en la carta circular No. 36/2019, el informe sobre el 101° periodo de sesiones del Comité de Seguridad Marítima de la OMI (MSC 101) de junio del 2019, la circular del Comité de Facilitación de la OMI, en su 41° periodo de sesiones (4 a 7 de abril de 2017) y el Comité de Seguridad Marítima, en su 98° periodo de sesiones (7 a 16 de junio de 2017), donde se toma en consideración la necesidad urgente de elevar el nivel de concienciación sobre las amenazas y las vulnerabilidades conexas con los riesgos cibernéticos.

Así mismo, se tiene en consideración los análisis de riesgos presentados por las capitanías de puerto a nivel nacional, con respecto a la implementación e inclusión en las evaluaciones y planes de protección, aspectos relacionados con los riesgos cibernéticos, la seguridad física de la ciber-seguridad, la seguridad de artefactos tipo drones y seguridad física con estos equipos.

INTRODUCCIÓN

El propósito de estas directrices es ofrecer recomendaciones de alto nivel para la gestión de los riesgos cibernéticos marítimos y la seguridad de artefactos tipo drones. 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, así mismo de los riesgos que puede generar la intrusión de artefactos tipo drones en las instalaciones portuarias con fines terroristas.

“Consolidemos nuestro país marítimo”

Dirección Carrera 54 N°. 26-50 CAN, Bogotá

Teléfono (1) 220 0490. Línea Anticorrupción 01 8000 911 670

Línea gratuita de Atención al Ciudadano: Nacional 01800 115 966 – Bogotá 328 6800

dimar@dimar.mil.co - www.dimar.mil.co

A2-00-FOR-022-V1

Se deben 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, como también de acciones o intromisiones de drones dentro del espacio físico de las instalaciones portuarias y los buques que arriban a estas.

Las compañías e instalaciones portuarias usuarios de estas directrices, deberán remitirse también 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 en protección marítima.

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, integración, automatización y los sistemas basados en redes ha creado una necesidad creciente de gestionar los riesgos cibernéticos dentro del sector del transporte marítimo, así mismo la evolución de artefactos voladores de mediano y pequeño tamaño con capacidades que hasta hoy no eran tenidas en cuenta.

Tomando como base el objetivo de contribuir a la seguridad y a la protección del transporte marítimo, operacionalmente resiliente ante los riesgos cibernéticos y drones, se incluyen en las presentes directrices recomendaciones que se pueden incorporar en los procedimientos existentes de gestión de los riesgos, como complemento a las prácticas sobre gestión de la seguridad y la protección marítima en cada compañía e instalación portuaria.

GENERALIDADES

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 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 puede dar lugar a riesgos cibernéticos que deben abordarse. Dichos sistemas vulnerables pueden ser, entre otros:

- ✓ Control de acceso.
- ✓ Manipulación y gestión de la carga (operaciones).
- ✓ Equipos de vigilancia.
- ✓ Administrativos.
- ✓ Comunicación.
- ✓ Del puente.
- ✓ Propulsión y gestión de las máquinas y de control de suministro eléctrico.
- ✓ Servicio a los pasajeros y de organización de los mismos.

“Consolidemos nuestro país marítimo”

Dirección Carrera 54 N°. 26-50 CAN, Bogotá

Teléfono (1) 220 0490. Línea Anticorrupción 01 8000 911 670

Línea gratuita de Atención al Ciudadano: Nacional 01800 115 966 – Bogotá 328 6800

dimar@dimar.mil.co - www.dimar.mil.co

A2-00-FOR-022-V1

Debe considerarse la distinción entre la tecnología de la información y los sistemas de tecnología operacional. Puede 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, debe considerarse la protección de la información y el intercambio de datos dentro de esos sistemas.

Las amenazas aparecen mediante actuaciones malintencionadas, por ejemplo, piratería informática o introducción de programas informáticos maliciosos o como una consecuencia no deliberada de actuaciones bien intencionadas, como 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, evaluaciones y planes de protección o bien aprovechan alguna vulnerabilidad de la tecnología operacional o de la información. Para que la gestión de los riesgos cibernéticos sea eficaz, deben considerarse ambos tipos de amenazas.

La vulnerabilidad puede derivarse de un proyecto, integración y/o mantenimiento inadecuado de los sistemas, así como de lapsus en la disciplina cibernética. Cuando se pone de manifiesto o se aprovecha alguna vulnerabilidad de la tecnología operacional y/o de la información, como contraseñas poco seguras que dan lugar a accesos no autorizados o indirectamente 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.

Algo semejante ocurre con el segundo tema en interés, se conoce que los drones son útiles, pero con una cara oscura. Pueden ser un riesgo para la navegación aérea y un arma terrible el día que los terroristas reparen en ellos. Incluso constituyen una amenaza para la intimidad, pues están ya en condiciones de convertirse en un elemento que invade nuestra intimidad desde el aire.

Estos abren también una oportunidad para los grupos terroristas, comprar un dron está al alcance de cualquiera. Los drones en la versión más pesimista serán fuente de accidentes y de acosos, pero la auténtica pesadilla es imaginarlos en manos de terroristas.

Finalmente, 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 y de drones, los cuales son resilientes y evolutivos como prolongación natural de las prácticas existentes para la gestión de la seguridad y la protección.

Al examinar las fuentes posibles de amenazas y de la vulnerabilidad, así como las estrategias posibles para mitigar los riesgos, las instalaciones portuarias y buques deberían examinar varias opciones de control de la gestión de los riesgos cibernéticos y de drones. Entre estos

“Consolidemos nuestro país marítimo”

Dirección Carrera 54 N°. 26-50 CAN, Bogotá

Teléfono (1) 220 0490. Línea Anticorrupción 01 8000 911 670

Línea gratuita de Atención al Ciudadano: Nacional 01800 115 966 – Bogotá 328 6800

dimar@dimar.mil.co - www.dimar.mil.co

A2-00-FOR-022-V1

controles posibles cabe mencionar los controles de la gestión, los operacionales o de procedimiento, y los controles técnicos.

ÁMBITO DE APLICACIÓN

Las presentes directrices se dirigen a los buques de bandera colombiana de tráfico internacional y a las instalaciones portuarias, cobijadas por el código PBIP.

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, con el carácter recomendatorio.

ELEMENTOS DE LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS

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.

La gestión eficaz de los riesgos cibernéticos debería empezar en el nivel de la alta gerencia, que debe establecer 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.

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

- ✓ **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.
- ✓ **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.
- ✓ **Detectar:** crear las actividades necesarias para detectar un suceso cibernético oportunamente.
- ✓ **Responder:** crear e implantar actividades y planes para dar resiliencia y restaurar los sistemas necesarios para las operaciones que hayan sido afectados por un suceso cibernético.

“Consolidemos nuestro país marítimo”

Dirección Carrera 54 N°. 26-50 CAN, Bogotá

Teléfono (1) 220 0490. Línea Anticorrupción 01 8000 911 670

Línea gratuita de Atención al Ciudadano: Nacional 01800 115 966 – Bogotá 328 6800

dimar@dimar.mil.co - www.dimar.mil.co

A2-00-FOR-022-V1

- ✓ **Recuperar:** determinar medidas para copiar y restaurar sistemas cibernéticos necesarios para las operaciones que hayan sido objeto de un suceso cibernético.

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 las operaciones.

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

ELEMENTOS DE LA GESTIÓN DE LOS RIESGOS CON DRONES

En estas directrices se presentan elementos funcionales que contribuyen a la gestión efectiva de los riesgos con drones. Dichos elementos no son secuenciales; todos deben ser simultáneos y continuos en la práctica e incorporarse debidamente en el plan de protección:

- ✓ **Identificación:** definir las funciones y responsabilidades del personal en la gestión de los riesgos con drones, e identificar si generan riesgos para las operaciones.
- ✓ **Proteger:** implantar procedimientos y medidas para el control de los riesgos, así como planificación para contingencias, a fin de proteger ante cualquier suceso y garantizar la continuidad de las operaciones.
- ✓ **Detectar:** crear las actividades necesarias para detectar un artefacto tipo dron oportunamente.
- ✓ **Responder:** crear e implantar actividades y planes para contrarrestar el suceso dentro del espacio físico concesionado, determinar medidas para capturar o detener artefactos tipo dron que hayan sido objetos de sucesos en el espacio físico concesionado.
- ✓ **Recuperar:** establecer procedimientos y medidas para continuar o recuperar la operatividad normal del buque o la instalación portuaria sin afectación del puerto.

CONSIDERACIONES

A continuación, se señalan algunas de las consideraciones y aspectos a tener en cuenta para la actualización de las Evaluaciones y Planes de Protección:

- Establecer medidas para el control en riesgos cibernéticos y ciberseguridad y drones.

“Consolidemos nuestro país marítimo”

Dirección Carrera 54 N°. 26-50 CAN, Bogotá

Teléfono (1) 220 0490. Línea Anticorrupción 01 8000 911 670

Línea gratuita de Atención al Ciudadano: Nacional 01800 115 966 – Bogotá 328 6800

dimar@dimar.mil.co - www.dimar.mil.co

A2-00-FOR-022-V1

- Establecer medidas para tomar acciones frente a riesgos asociados al vuelo de drones al interior de las instalaciones portuarias y/o buques sin autorización alguna.
- Establecer medidas y procedimientos para el uso de drones al interior de las instalaciones portuarias para fortalecer el esquema de protección marítima.

Las instalaciones portuarias y los buques de bandera colombiana de tráfico internacional deberán asegurarse de que dichos análisis de riesgos y procedimientos queden registrados en cada uno de sus evaluaciones y planes de protección, los cuales deberán ser presentados como enmiendas a la Dirección General Marítima para ser aprobados y adicionados en sus respectivos documentos.

Para efectos del tema de drones, se deben considerar las disposiciones emitidas mediante la Resolución No. 04201 del 27 de diciembre de 2018 de la Aeronáutica Civil de Colombia, referente al Sistema de Aeronaves Pilotadas a Distancia RPAS- Drones, cuyo propósito es impartir instrucciones de cumplimiento en referencia a los requisitos de aeronavegabilidad y operaciones necesarios para inscripción de explotadores, operadores y equipos, y para solicitar permiso para realizar vuelos de UAS.

Atentamente,



Contratante: JUAN FRANCISCO HERRERA LEAL
Director General Marítimo

Copia: CP01, CP02, CP03, CP04, CP05, CP06, CP07, CP08, CP09, CP14

"Consolidemos nuestro país marítimo"

Dirección Carrera 54 N°. 26-50 CAN, Bogotá

Teléfono (1) 220 0490. Línea Anticorrupción 01 8000 911 670

Línea gratuita de Atención al Ciudadano: Nacional 01800 115 966 – Bogotá 328 6800

dimar@dimar.mil.co - www.dimar.mil.co

A2-00-FOR-022-V1