PÚBLICO

D.G.T.M. Y M.M. ORDINARIO N° 12600/**204** Vrs.

APRUEBA CIRCULAR DE LA DIRECCIÓN GENERAL DEL TERRITORIO MARÍTIMO Y DE MARINA MERCANTE, ORDINARIO N° O-75/006.

VALPARAÍSO, **08 JUN 2023**

VISTO: los artículos 3º y 4º del D.F.L. (H.) Nº 292, de 1953, que aprueba la Ley Orgánica de la Dirección General del Territorio Marítimo y de Marina Mercante; lo dispuesto en los artículos 5°, 29°, 88° y 91° del D.L. (M.) Nº 2.222, de 1978, Ley de Navegación; lo dispuesto en el artículo 3° del D.L. (I.) N° 3.607, de 1981, que establece nuevas normas sobre funcionamiento de vigilantes privados; el Decreto (RR.EE.) N° 384, de 2003, y el Decreto (RR.EE.) N° 71, de 2005, que promulgan las enmiendas al Convenio Internacional para la Seguridad de la Vida Humana en el Mar, SOLAS 1974, adoptadas por el Comité de Seguridad Marítima de la Organización Marítima Internacional sobre la implementación del Código Internacional de gestión de la seguridad (IGS) y sobre el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP); la resolución MSC 428 (98), sobre Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad (Comité de Seguridad Marítima (MSC) OMI, 2017); la resolución MSC-FAL.1/Circ.3, sobre directrices para la Gestión de los Riesgos Cibernéticos Marítimos (Comité de Seguridad Marítima (MSC) - Comité de Facilitación (FAL) OMI, jul 2017); el artículo 345° del D.S. (M.) N° 1340 bis, de 1941, y teniendo presente las atribuciones que me confiere la reglamentación vigente,

R E S U E L V O :

1.- **APRUÉBASE** la siguiente circular que establece disposiciones relativas a la implementación de medidas de seguridad de la información y protección cibernética por parte de Buques, Instalaciones Portuarias y Compañías en el marco de la gestión de riesgos cibernéticos marítimos.

CIRCULAR D.G.T.M. Y M.M. ORDINARIO N° O-75/006

OBJ.: Establece disposiciones relativas a la implementación de medidas de seguridad de la información y protección cibernética por parte de buques, instalaciones portuarias y compañías en el marco de la gestión de riesgos cibernéticos marítimos.

I.- INFORMACIONES:

A.- Lo dispuesto en el artículo 5° del D.L. (M.) N° 2.222, de 1978, Ley de Navegación, el cual establece que: *"la Autoridad Marítima corresponderá a la Dirección General del Territorio Marítimo y Marina Mercante y, como tal, aplicará y fiscalizará el cumplimiento de esta ley, de los convenios internacionales y de las normas legales o reglamentarias relacionadas con sus funciones, con la preservación de la ecología en el mar y con la navegación en las aguas sometidas a la jurisdicción nacional".*

B.- El artículo 3° del D.L. N° 3.607, de 1981**,** que regula el funcionamiento de las Empresas Estratégicas, dispone que estas deben contar con su propio servicio de vigilantes privados, un estudio de seguridad y mantener un organismo de seguridad interno. Las Empresas Estratégicas son aquellas designadas por Decreto Supremo.

C.- El Convenio Internacional para la Seguridad de la Vida Humana en el Mar, SOLAS, promulgado mediante el Decreto (RR.EE.) Nº 328, del 11 de junio de 1980, está compuesto por 14 capítulos, entre los que destacan los capítulos IX "Gestión de la Seguridad Operacional de los Buques", que implementa el Código Internacional de Gestión de la Seguridad (Código IGS) y el XI-2 "Medidas Especiales para Incrementar la Protección Marítima" e implementa el Código Internacional para la Protección de Buques e Instalaciones Portuarias (Código PBIP).

D.- El Código IGS, según el capítulo IX del SOLAS, contiene las prescripciones relativas a la gestión de la seguridad, obligando tanto a las compañías que explotan comercialmente a los buques como a los buques, a garantizar normas adecuadas de seguridad y prevención de la contaminación, como también garantizar que las Administraciones implementen y hagan cumplir eficazmente dichas normas y reglas.

E.- El Código PBIP cuenta con ciertos objetivos principales, a saber: establecer un marco internacional en el ámbito marítimo portuario, con el fin de detectar amenazas a los activos de información y telecomunicaciones y adoptar medidas preventivas contra sucesos que afecten a la protección en los buques e instalaciones portuarias utilizadas para el comercio internacional; definir funciones y responsabilidades, a todo nivel, para garantizar la confidencialidad, integridad y disponibilidad de la información, considerando los datos, redes, sistemas y telecomunicaciones para una adecuada protección marítima; garantizar la recopilación, procesamiento, almacenamiento, intercambio y destrucción de información; ofrecer metodología para las evaluaciones de la protección mediante planes, estándares y procedimientos; y garantizar la

confianza de que se cuente con medidas de protección marítima adecuadas y proporcionadas.

F.- La resolución del Comité de Seguridad Marítima (MSC) de la OMI, MSC 428 (98), sobre “Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad”, solicita a las Administraciones garantizar que los riesgos cibernéticos se aborden debidamente en un nivel adecuado y aceptable, a más tardar, en la primera verificación anual del documento de cumplimiento de las compañías después del 1 de enero de 2021.

G.- La Organización Marítima Internacional (OMI), ha propuesto mediante la Circular MSC-FAL.1/Circ.3, recomendaciones de alto nivel para la gestión de los riesgos cibernéticos marítimos, mediante la utilización de un sistema de gestión de riesgos para enfrentar esta problemática, el cual se basa en las prácticas que se han llevado a nivel internacional por organismos tales como: la Organización Internacional de Normalización (ISO); la Comisión electrotécnica internacional (IEC); la Norma ISO/IEC 27001 y el Instituto Nacional de Normas y Tecnología de los Estados Unidos (NIST), con su marco de mejora de la ciberseguridad de la infraestructura crítica.

H.- De acuerdo con lo expresado en la Norma NCh-ISO/IEC 27005:2020[1] para referirse a la *“gestión del riesgo de la seguridad de la información”*, se entenderá por gestión de los riesgos cibernéticos al “*proceso estructurado, consistente y continuo, implementado a través de toda la organización que permite establecer el contexto interno y externo, e identificar y evaluar los riesgos y tratarlos usando un plan de tratamiento de riesgos para implementar las recomendaciones y decisiones*”.

I.- La gestión de los riesgos cibernéticos 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. Sin embargo, en la actualidad, y en consideración a la mayor dependencia de las tecnologías de la información y telecomunicaciones, la digitalización, integración, automatización y de sistemas basados en redes, se ha hecho una necesidad creciente de gestionar los riesgos cibernéticos dentro del ámbito marítimo. La gestión de riesgos cibernéticos deberá ceñirse, al menos, o incluir los siguientes subprocesos, los cuales se basan en aquellos definidos en la Norma NCh-ISO/IEC 27005:2020:

[1] Instituto Nacional de Normalización (INN). 2020. 5 Antecedentes. En *Norma NCh-ISO/IEC 27005:2020.* p. 3.

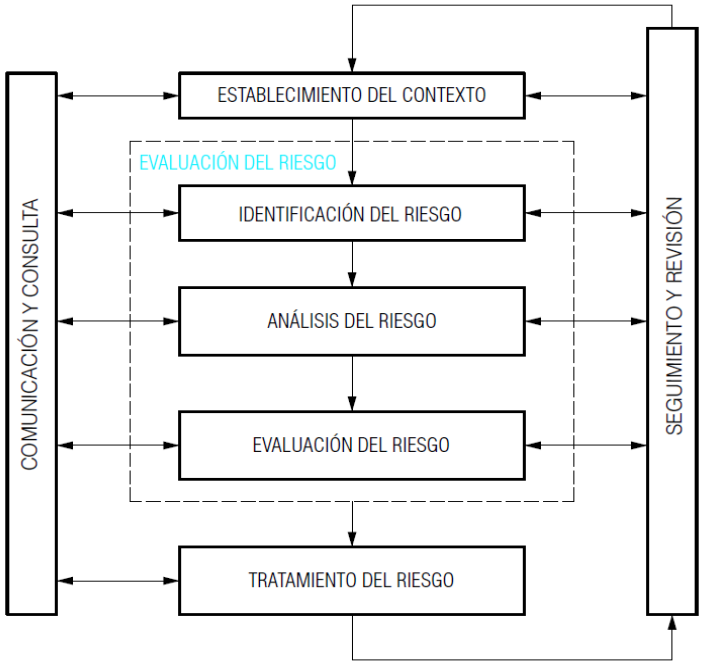

Imagen N° 1: *Proceso de Gestión del Riesgo Cibernético.*
Fuente: NCh-ISO/IEC 27005:2020, p. 5.

1.- **Establecimiento del Contexto**: se debe establecer el contexto interno y externo para la gestión del riesgo cibernético, lo que involucra fijar los criterios básicos necesarios para la gestión del riesgo cibernético, definir la identificación, el alcance, límites, análisis de riesgo y establecer un ordenamiento adecuado que opere la gestión del riesgo cibernético.

2.- **Evaluación del Riesgo**: se debe identificar, cuantificar o describir cualitativamente los riesgos y asignarles prioridad en contraste con criterios de evaluación del riesgo y objetivos relevantes para la organización. Este subproceso se descompone, a su vez, en 3 actividades a saber:

a.- Identificación del riesgo: "*El propósito es determinar qué puede pasar para causar una pérdida potencial y ganar comprensión sobre cómo, dónde y por qué las pérdidas pueden ocurrir. Los pasos descritos en las siguientes subcláusulas deberían recopilar datos de entrada para la actividad de análisis del riesgo*"[2].

b.- Análisis del Riesgo: "*Este se puede llevar a cabo en variados grados de detalle dependiendo de la criticidad de los activos, extensión de las vulnerabilidades conocidas e incidentes previos involucrados en la organización. Una metodología de análisis del riesgo puede ser*

[2] Instituto Nacional de Normalización (INN). 2020. 8.2.1 Introducción a la Identificación del Riesgo. En *Norma NCh-ISO/IEC 27005:2020.* p. 11.

cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. En la práctica, a menudo primero se usan análisis cualitativos para obtener una indicación general del nivel de riesgo y para revelar los riesgos más graves. Posteriormente, se puede necesitar llevar a cabo análisis más específicos o cuantitativos para los riesgos más graves debido a que normalmente es menos complejo y más barato realizar análisis cualitativos que cuantitativos"[3].

c.- Evaluación del Riesgo: "*En esta actividad se compara el nivel de riesgos en contraste con los criterios de evaluación del riesgo y criterios de aceptación del riesgo*"[4].

Para el desarrollo de las actividades antes mencionadas, se deberán utilizar las estrategias de procesamiento de información "*Bottom-up*" o "T*op-down*".

3.- **Tratamiento del Riesgo**: se deberán establecer controles, ya sean administrativos, tecnológicos o físicos, para mitigar, retener, evitar o compartir los riesgos y definir un plan de tratamiento de este.

4.- **Comunicación y Consulta del Riesgo**: se intercambia la información sobre el/los riesgos detectados en el subproceso de "Evaluación de Riesgo" y se le comunica a la alta dirección y a las otras partes interesadas.

5.- **Seguimiento y Revisión del Riesgo: "***se debe hacer seguimiento y revisar los riesgos y sus factores (es decir, valor de activos, impactos, amenazas, vulnerabilidades, probabilidad de ocurrencia) para identificar cualquier cambio en el contexto de la organización en una etapa temprana y para mantener una visión general del panorama del riesgo completo*"[5].

J.- El riesgo cibernético marítimo, para efectos del presente documento se definirá como el grado de exposición a la materialización de una amenaza (a través de un evento o incidente), que puedan causar daños a una organización (por ejemplo: fallas operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o poner en peligro la información y los sistemas).

RIESGO = PROBABILIDAD X IMPACTO

K.- Se debe tener presente la diferencia entre lo que se denomina T.I., que son los Sistemas de Tecnologías de la Información, refiriéndose en general a las estaciones de trabajo (computadoras, servidores, etc.) de las organizaciones,

[3] Instituto Nacional de Normalización (INN). 2020. 8.3.1 Metodologías de análisis del riesgo. En *Norma NCh-ISO/IEC 27005:2020.* p. 16.

[4] Instituto Nacional de Normalización (INN). 2020. 8.4 Evaluación del riesgo. En *Norma NCh-ISO/IEC 27005:2020.* p. 19.

[5] Instituto Nacional de Normalización (INN). 2020. 12.1 Seguimiento y revisión de factores de riesgo. En *Norma NCh-ISO/IEC 27005:2020.* p. 27.

como también a los dispositivos electrónicos de la tripulación (computadores personales, teléfonos inteligentes, relojes inteligentes, computadores de tamaño reducido (SBC, tablets, etc.); y lo conocido como T.O. (Tecnologías operacionales) que son los controles programables, sistemas o dispositivos diseñados para dirigir, monitorear o interactuar con sistemas que facilitan procesos físicos, tales como sistemas de control industrial, administración de carga, seguridad, controles de motores, etc.

L.- Chile, como miembro de la OMI, a través de la Dirección General del Territorio Marítimo y de Marina Mercante, debe supervisar el cumplimiento de las exigencias específicas de los instrumentos internacionales en las naves de bandera nacional, las compañías y las instalaciones portuarias, con el objetivo de contribuir a la seguridad y a la protección del transporte marítimo, ante los constantes riesgos cibernéticos.

II.- ÁMBITO DE APLICACIÓN:

Las prescripciones de la presente circular se aplicarán a los buques de bandera nacional, compañías e instalaciones portuarias de acuerdo con lo siguiente:

A.- Buques de tráfico internacional en el marco del Código Internacional de Gestión de la Seguridad (Código IGS).

B.- Compañías que cumplan con el Código Internacional de Gestión de la Seguridad (Código IGS).

C.- Instalaciones Portuarias que den cumplimiento al Código PBIP y aquellas consideradas como empresas estratégicas del ámbito marítimo portuario.

III.- INSTRUCCIONES:

A.- GENERALES:

1.- Las compañías, buques e instalaciones portuarias deberán adoptar las medidas pertinentes y necesarias para salvaguardar el transporte marítimo respecto de las amenazas actuales y emergentes relacionadas con la digitalización, integración y la automatización de los procedimientos y sistemas relacionados con el transporte marítimo.

2.- Las compañías, buques e instalaciones portuarias deberán incorporar en los procesos existentes un sistema de gestión de riesgos cibernéticos.

3.- El sistema de gestión de riesgos cibernético podrá ser desarrollado e implementado siguiendo las recomendaciones de la familia de Normas ISO 27000, para la gestión de la seguridad de la información e ISO 27001/ NCh-ISO/IEC 27001.

4.- Las compañías, buques e instalaciones portuarias deberán identificar y analizar las posibles fuentes de amenazas y/o vulnerabilidades que puedan afectar a sus redes y sistemas informáticos (T.I. y T.O.), objeto puedan adoptar las estrategias necesarias para mitigar los riesgos en su plan de protección, mediante la incorporación del proceso de Gestión de Riesgo Cibernético, que debe considerar todas las actividades indicadas en el anexo “A” de la presente circular.

5.- Las compañías e instalaciones portuarias deberán considerar, dentro de su sistema de gestión de riesgos cibernéticos, a una persona responsable denominado CISO (Chief Information Security Officer) quien deberá prevenir y resolver los ciberincidentes. Además, los ciberincidentes que detecte en sus redes y sistemas informáticos (T.I. y T.O.), que tengan o puedan tener consecuencias contra la integridad de las personas, la seguridad y protección marítima, deberán ser reportados al Capitán de Puerto correspondiente para el caso de las instalaciones portuarias y al MRCC para el caso de los buques, de acuerdo con las instrucciones y plazos especificados en el anexo “B”.

6.- El CISO o la persona que designe la compañía o instalación portuaria, deberá efectuar la respectiva denuncia al Ministerio Público al detectar ciberincidentes que constituyan delito de acuerdo a la Ley N° 21.459 de fecha 20 de junio de 2022, que establece normas sobre delitos informáticos.

B.- COMPAÑÍAS Y BUQUES:

1.- Se deberá, al menos, considerar en el sistema de gestión de riesgos cibernéticos los sistemas vulnerables o sensibles y plan de recuperación ante desastres tecnológicos (DRP), tales como:

a.- Los sistemas de puente.
b.- Sistemas de manipulación y gestión de la carga.
c.- Sistemas de propulsión y gestión de las máquinas y de control de suministros eléctricos.
d.- Sistemas de servicio a los pasajeros y de organización de los mismos.
e.- Redes públicas de tripulación y pasajeros.
f.- Sistemas de comunicaciones.
g.- Sistemas administrativos y de bienestar de la tripulación (redes físicas e inalámbricas).

h.- Sistemas de proveedores que interactúen con sistemas anteriores.
i.- Cualquier otro sistema informático que interactúe con los sistemas anteriores.

2.- Cuando el servicio tecnológico sea otorgado por uno o varios proveedores, este deberá asegurar la disponibilidad, confidencialidad e integridad objeto los proveedores protejan la información propia y la de sus clientes.

3.- De acuerdo con lo establecido en Código IGS, las compañías deberán implementar en su sistema de gestión los procedimientos necesarios para mitigar los riesgos detectados en la actividad de evaluación de riesgos del proceso de gestión del riesgo cibernético.

4.- Tanto para compañías como para buques, la verificación de la adecuada implementación del sistema gestión de riesgos cibernéticos, se efectuará mediante auditorías internas o externas, que se realizarán de acuerdo lo establecen el Código IGS.

C.- INSTALACIONES PORTUARIAS:

1.- Se deberá considerar en el sistema de gestión de riesgos cibernéticos, al menos, los sistemas vulnerables o sensibles y plan de recuperación ante desastres tecnológicos (DRP), tales como:

a.- Los sistemas de control de acceso.
b.- Los sistemas de servicio a los pasajeros y de organización de los mismos.
c.- Los sistemas de comunicaciones en el marco de lo dispuesto en cada plan de protección marítima.
d.- Sistemas operacionales de manipulación de la carga y sus respectivos procesos.
e.- Las ayudas a la navegación electrónicas, propiedad de las instalaciones portuarias.
f.- Sistemas de proveedores que interactúen con sistemas anteriores.
g.- Cualquier otro sistema informático que interactúe con los sistemas anteriores.

2.- Cuando el servicio tecnológico sea otorgado por uno o varios proveedores, este deberá asegurar la disponibilidad, confidencialidad e integridad, objeto los proveedores protejan la información propia y la de sus clientes.

3.- Las instalaciones portuarias deberán incorporar en la respectiva evaluación de protección el proceso de gestión del riesgo cibernético.

4.- Las instalaciones portuarias deberán implementar en su sistema de gestión de riesgos, los procedimientos necesarios para mitigar los riesgos detectados en la actividad de evaluación de riesgos del proceso de gestión del riesgo cibernético.

5.- El plan de protección de la instalación portuaria deberá incorporar los procedimientos necesarios para mitigar los riesgos detectados en la evaluación de protección.

6.- La evaluación de protección y el plan de protección de la instalación portuaria, serán aprobados por la Dirección de Seguridad y Operaciones Marítimas, conforme lo establece el Código PBIP.

7.- La verificación de la adecuada implementación del sistema de gestión de riesgos cibernéticos, se efectuará mediante auditorías internas y los procesos de auditorías externas ejecutadas por los auditores dependientes de la Autoridad Marítima, de acuerdo al plan anual de auditorías respectivo, que se realizarán de acuerdo lo establece el Código PBIP.

8.- Las instalaciones portuarias consideradas estratégicas deberán incorporar un Sistema de Gestión de Riesgos Cibernéticos en el Estudio de Seguridad y Plan General de Seguridad.

IV.- VIGENCIA:

Las exigencias establecidas en la presente circular entrarán en vigencia dos años después de la fecha de su publicación en el Diario Oficial. La prevención de las disposiciones de la presente circular, no excluyen el cumplimiento de las demás normas jurídicas que se encuentran vigentes.

V.- ANEXOS:

"A" : Lineamientos para la Gestión del Riesgo Cibernético.

"B" : Contenido de los Reportes y su Periodicidad.

2.- **ANÓTESE,** comuníquese y publíquese en el Diario Oficial de la República de Chile extracto de la presente resolución y su forma íntegra en la página Web internet de esta Dirección General.

(ORIGINAL FIRMADO)

FERNANDO CABRERA SALAZAR
VICEALMIRANTE
DIRECTOR GENERAL

DISTRIBUCIÓN:
1.- D.G.T.M. Y M.M. (Depto. Jurídico – Div. RR. y PP.MM.)
2- ARCHIVO.

A N E X O “A”

LINEAMIENTOS PARA LA GESTIÓN DEL RIESGO CIBERNÉTICO

Cada organización deberá preparar una matriz de riesgo, donde cada proceso, servicio y/o activo de información debe ser evaluado, considerando también el nivel de exposición a las distintas amenazas cibernéticas que puede asumir la organización, la tolerancia y la capacidad de riesgo los que serán definidos por la alta dirección. Para la confección de la matriz, se pueden utilizar las propuestas presentadas en el Anexo “E” de la Norma NCh-ISO/IEC 27005:2020, u otras plantillas que se estimen pertinentes, mediante el flujo de proceso indicado en la imagen N° 2.

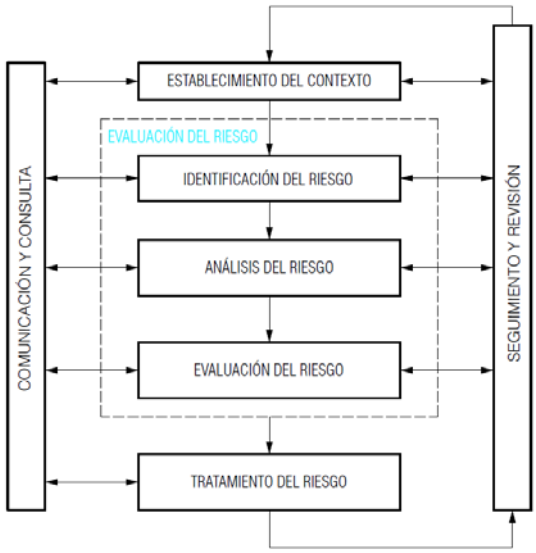

Imagen N° 1: *Proceso de Gestión del Riesgo Cibernético.*
Fuente: NCh-ISO/IEC 27005:2020, p. 5.

El plan resultante de lo anterior será auditado de acuerdo con la Norma ISO 27005/ NCh-ISO/IEC 27001.

APÉNDICE:
N° 1 : Taxonomía de Clasificación de Incidentes.

VALPARAÍSO, **08 JUN 2023.**

(ORIGINAL FIRMADO)

FERNANDO CABRERA SALAZAR
VICEALMIRANTE
DIRECTOR GENERAL

DISTRIBUCIÓN:
Id. Cuerpo Principal.

APÉNDICE N° 1 AL ANEXO "A"

TAXONOMÍA DE CLASIFICACIÓN DE INCIDENTES

Matriz de clasificación de Incidentes			
N°	**Clase de Incidente**	**Tipo de Incidente**	**Descripción**
1	Contenido abusivo.	Pornografía, violencia.	Pornografía, glorificación de la violencia, otros.
		Spam.	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de un grupo masivo de mensajes, todos teniendo un contenido similar.
		Difamación.	Desacreditación o discriminación de alguien
2	Código malicioso.	Malware, Virus, Gusanos, Troyanos, Spyware, +Dialer, Rootkit.	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.
3	Recopilación de información.	Scanning.	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT), escaneo de puertos.
		Sniffing.	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
		Ingeniería social.	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
4	Intentos de intrusión.	Intentos de acceso.	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
		Explotación de vulnerabilidades conocidas.	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc.).
		Nueva firma de ataque.	Un intento de usar un exploit desconocido.

Matriz de clasificación de Incidentes			
N°	**Clase de Incidente**	**Tipo de Incidente**	**Descripción**
5	Intrusión.	Compromiso de credenciales privilegiada.	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede haber sido causado de forma remota por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.
		Compromiso de credenciales sin privilegios.	
		Compromiso de aplicación, Bot.	
6	Disponibilidad.	Ataque de denegación de servicio (DoS / DDoS).	Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema queda indisponible o falla. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail’s. DoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.
		Sabotaje.	
		Intercepción de información.	
7	Información de seguridad de contenidos.	Acceso no autorizado a la información.	Además de un abuso local de datos y sistemas, la seguridad de la información puede ser en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.
		Modificación no autorizada de la información.	
8	Fraude.	Phishing.	Enmascarado como otra entidad para persuadir al usuario a revelar una credencial privada.
		Derechos de autor.	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor (Warez).
		Uso no autorizado de recursos.	Usar recursos para fines no autorizados, incluida la obtención de beneficios empresas (por ejemplo, el uso del correo electrónico para participar en cartas de cadena de ganancias ilegales o esquemas piramidales).

Matriz de clasificación de Incidentes			
N°	**Clase de Incidente**	**Tipo de Incidente**	**Descripción**
		Falsificación de registros o identidad.	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
9	Vulnerable.	Sistemas y/o softwares abiertos.	Sistemas «Open Resolvers», impresoras abiertas, vulnerabilidades aparentes detectadas con Nessus u otros aplicativos, firmas de virus no actualizadas, etc.
10	Otros.	Todos los incidentes que no encajan en alguna de las otras categorías dadas.	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
11	Test.	Para pruebas.	Producto de pruebas de seguridad controladas e informadas

***Fuente**: Matriz de clasificación de incidentes del CSIRT Gubernamental. Obtenido desde: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/.*

VALPARAÍSO, **08 JUN 2023**

(ORIGINAL FIRMADO)

FERNANDO CABRERA SALAZAR
VICEALMIRANTE
DIRECTOR GENERAL

DISTRIBUCIÓN:
Id. Cuerpo Principal.

A N E X O “B”

CONTENIDO DE LOS REPORTES Y SU PERIODICIDAD

Los reportes, de acuerdo a su periodicidad, se clasificarán en:

a.- Reporte inicial: es una comunicación consistente en poner en conocimiento y alertar la existencia de un incidente a la ciberseguridad.

b.- Reporte intermedio: actualiza los datos disponibles en ese momento en relación al incidente comunicado. Se efectuarán tantos reportes intermedios como se consideren necesarios, a partir de la hora en que se generó el reporte inicial inmediato.

c.- Reporte final: amplía, ajusta y/o confirma los datos definitivos en relación al incidente reportado a partir del día en que se generó el reporte inicial, considerando además todas las actualizaciones respectivas.

El reporte deberá contener la siguiente información, de acuerdo a la siguiente numeración.

INFORMACIÓN	Inicial	Intermedio	Final
1.- Identificación del buque o Instalación portuaria.	X		
2.- Nombre responsable de ciberseguridad.	X		
3.- Fecha / Hora ocurrencia y detección incidente.	X		
4.- Descripción detallada del evento.		X	X
5.- Equipamiento o sistemas afectados.	X	X	X
6.- Origen o causa identificable.		X	X
7.- Nivel de peligrosidad.		X	X
8.- Nivel de impacto.	X	X	X
9.- Plan de acción o medidas de mitigación.		X	X
10.- Entorno afectado actual y potencial.	X		X
11.- Taxonomía de clasificación de incidentes.		X	X
12.- Otros antecedentes.	X	X	X

NIVEL DE PELIGROSIDAD

Nivel	Clase de Incidente	Tipo de Incidente	Descripción
Crítico	Todos.	Todos.	Amenaza avanzada persistente.
Muy Alto	Contenido abusivo.	Pornografía, violencia.	Distribución de pornografía.
	Código malicioso.	Malware, Virus, Gusanos, Troyanos, Spyware, Dialer, Rootkit.	Distribución de software que se incluye o inserta intencionalmente en un sistema con propósito dañino.
	Recopilación de información.	Scanning.	Ataques a un sistema para descubrir puntos débiles.
	Intrusión.	Compromiso de cuenta privilegiada.	Compromiso exitoso de un sistema o aplicación (servicio).
	Disponibilidad.	Ataque de denegación.	Las operaciones se retrasan o el sistema queda indisponible o falla.
Alto	Contenido abusivo.	Spam.	Distribución de correo masivo a destinatario que no ha otorgado permisos.
	Código malicioso.	Malware, Virus, Gusanos, Troyanos, Spyware, Dialer, Rootkit.	Sistema Infectado.
	Recopilación de información.	Sniffing.	Observar y registrar un sistema (escuchas telefónicas o redes de datos).
	Intentos de intrusión.	Intentos de acceso.	Intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
		Explotación de vulnerabilidades conocidas.	comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas.

Nivel	Clase de Incidente	Tipo de Incidente	Descripción
	Intrusión.	Compromiso de cuenta sin privilegios.	Compromiso exitoso de un sistema o aplicación (servicio).
	Disponibilidad.	Ataque de denegación.	Algunas operaciones se retrasan o quedan indisponible o falla.
	Información de seguridad de contenidos.	Modificación no autorizada de la información.	
	Fraude.	Phishing.	Enmascarado como otra entidad para persuadir al usuario a revelar una credencial privada.
		Falsificación de registros o identidad.	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
Medio	Contenido abusivo.	Difamación.	Desacreditación o discri-minación de alguien.
	Recopilación de información.	Ingeniería social.	Recopilación de información de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
	Intentos de intrusión.	Nueva firma de ataque.	Un intento de usar un exploit desconocido.
	Disponibilidad.	Intercepción de información.	Acción local sobre un sistema.
	Información de seguridad de contenidos.	Acceso no autorizado a la información.	Abuso local de datos y sistemas.
	Fraude.	Derechos de autor.	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor (Warez).
		Uso no autorizado de recursos.	Usar recursos para fines no autorizados, incluida la obtención de beneficios empresas.

Nivel	Clase de Incidente	Tipo de Incidente	Descripción
Bajo	Vulnerable.	Sistemas y/o softwares abiertos.	Sistemas «Open Resolvers», impresoras abiertas, vulnerabilidades aparentes detectadas con Nessus u otros aplicativos, firmas de virus no actualizadas, etc.
	Otros.	Todos los incidentes que no encajan en alguna de las otras categorías dadas.	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
	Test.	Para pruebas.	Producto de pruebas dé seguridad controladas e informadas

Nota: La presente tabla puede ser modificada de acuerdo a las necesidades propias de la Nave, Compañía e Instalación Portuaria.

NIVEL DE IMPACTO

Nivel	Descripción
Crítico	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a elementos o sistemas declarados como infraestructura o equipamiento crítico.
	Afecta a elementos o sistemas clasificados como sensibles.
	Afecta a más del 90% de las operaciones.
	Interrupción en las operaciones por un período superior a 24 hrs.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación nacional.
Muy alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta a la seguridad de la nave con potencial peligro para bienes materiales.
	Afecta a un elemento o sistema esencial.
	Afecta elementos o sistemas clasificados como reservados.
	Afecta a más del 75% de las operaciones.
	Interrupción en las operaciones por un período superior a 12 hrs.
	Daños reputacionales elevados y cobertura en medios de comunicación nacional.
Alto	Afecta algunos elementos o sistemas clasificados.
	Afecta a más del 50% de las operaciones.
	Interrupción en las operaciones por un período superior a superior a 8 hrs.
	Daños reputacionales altos, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
Medio	Afecta a más del 20% de las operaciones.
	Interrupción en las operaciones por un período superior a 5 hrs.
	Daño reputacional con eco mediático (cobertura en los medios de comunicación).
Bajo	Afecta algunos elementos o sistemas en las operaciones.
	Interrupción en las operaciones por un período superior a 1 hr.
	Algunos daños reputacionales (cobertura en algunos medios de comunicación).
Sin impacto	Daño reputacional puntual, sin eco mediático.
	No hay ningún impacto apreciable.

Nota: La presente tabla puede ser modificada de acuerdo a las necesidades propias de la Nave, Compañía e Instalación Portuaria.

PERIODICIDAD

PERIODICIDAD DE REPORTE			
NIVEL DE PELIGROSIDAD O IMPACTO	REPORTE INICIAL.	REPORTE INTERMEDIO.	REPORTE FINAL.
CRÍTICO	INMEDIATO.	MÁXIMO 3 / 6 / 12 / 24 / 48 HORAS POSTERIOR AL INCIDENTE.	MÁXIMO 10 DÍAS POSTERIOR AL INCIDENTE.
ALTO	INMEDIATO.	48 / 72 HORAS.	MÁXIMO 20 DÍAS POSTERIOR AL INCIDENTE.
MEDIO	INMEDIATO.	SIN PLAZO.	MÁXIMO 30 DÍAS POSTERIOR AL INCIDENTE.

VALPARAÍSO, **08 JUN 2023.**

(ORIGINAL FIRMADO)

FERNANDO CABRERA SALAZAR
VICEALMIRANTE
DIRECTOR GENERAL

DISTRIBUCIÓN:
Id. Cuerpo Principal.