GRUPO DE SEGURIDAD MARÍTIMA

GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN BUQUES E INSTALACIONES PORTUARIAS

CONSEJO NACIONAL DE SEGURIDAD MARÍTIMA

JUNIO 2020

Nombre documento	Autores	Fecha	Versión
GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN BUQUES E INSTALACIONES PORTUARIAS	GRUPO DE TRABAJO DE SEGURIDAD MARÍTIMA	JUNIO 2020	01

CONTENIDO

1. PREÁMBULO

La interacción creciente del entorno marítimo con el ciberespacio, ambos considerados "espacios globales comunes", es objeto de especial atención tanto en la Estrategia de Seguridad Nacional de 2017 como en la Estrategia de Seguridad Marítima Nacional de 2013.

Una de las Líneas de Acción Estratégicas de esta última es, precisamente, "la mejora de la ciberseguridad en el ámbito marítimo".

La presente Guía nace como uno de los trabajos derivados de esa línea de acción, para lo cual se creó un grupo de trabajo interministerial, que contó con el apoyo y asesoramiento de expertos independientes, con el mandato de **"elaborar, desde un enfoque integral y con objeto de ser difundidas tanto a nivel administración como a nivel comunidad marítima, guías de buenas prácticas en ciberseguridad enfocadas a elementos concretos del sector marítimo; en particular, a buques e instalaciones portuarias"**.

2. INTRODUCCIÓN

Las Tecnologías de la Información y las Comunicaciones 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 los últimos años, las nuevas tecnologías han penetrado de forma arrolladora en el sector, apoyando todas las actividades que lo soportan. Así, hoy en día se dispone de infinidad de sistemas que dependen del ciberespacio para su funcionamiento: posicionamiento global, cartografía digital, ayuda a la navegación, información y previsión meteorológica, controles de plataforma, comunicaciones digitales por satélite, conectividad inalámbrica, movimiento de cargas, seguridad de instalaciones, relaciones con los clientes, etc.

Esta situación ha creado una enorme dependencia de estos sistemas, sin que el proceso de cambio haya llevado convenientemente aparejados los aspectos relativos a su seguridad (requisitos, arquitecturas, procedimientos, formación, concienciación, etc.), si bien, como se verá más adelante, en los últimos años se han puesto en marcha algunas iniciativas para paliar esta situación.

Por motivos muy diversos, las ciberamenazas encuentran el ámbito marítimo especialmente atractivo para sus actividades, sea cual sea su naturaleza y motivación. Las grandes sumas de dinero que mueve este sector estratégico, la complejidad y heterogeneidad de los sistemas que apoyan su actividad, la convivencia de tecnologías obsoletas con otras muy avanzadas, la creciente conectividad, el funcionamiento permanente de muchos de sus servicios, la elevada movilidad del personal (turnos, dotaciones múltiples, guardias), la dependencia de terceras empresas, el elevado impacto mediático que puede suponer un accidente en la mar o la paralización de la actividad de un puerto, hacen que este sector sea de enorme interés para cibercriminales, ciberterroristas y hacktivistas y también para las ciberamenazas apoyadas por estados.

Ello, unido a la todavía grave falta de conocimientos y de concienciación y carencia de medios de ciberseguridad, se ha traducido en los últimos años en un alarmante crecimiento de los ciberincidentes en este sector.

El espectro de activos que pueden encontrarse en el ámbito marítimo es muy amplio y heterogéneo. Muchos de ellos, además, no son específicos de este entorno, sino comunes a otros sectores de actividad. Por tal motivo, esta Guía se centra en dos elementos principales y exclusivos de este ámbito, como son los **buques y puertos**.

La seguridad absoluta es imposible de alcanzar. No obstante, existen medidas relativamente sencillas de aplicar y de coste razonable que pueden reducir notablemente el riesgo.

En línea con lo anterior, la pretensión de esta Guía es la de proporcionar unas **recomendaciones de base** que deberían ser incluidas por las compañías y organizaciones como apartados específicos dentro de los procedimientos contenidos en el Código de Gestión de la Seguridad (ISM) y el Código de Protección de Buques e Instalaciones Portuarias (ISPS) de forma que sirvan de prolongación natural de las prácticas existentes para la gestión de la seguridad y la protección de buques y puertos.

3. SISTEMAS DE BUQUES Y PUERTOS

Entre los sistemas empleados en buques y puertos podemos encontrar, entre otros, los siguientes:

- Sistemas del puente.
- Sistemas de control de plataforma.
- Sistemas de manipulación y gestión de la carga.
- Sistemas de propulsión y suministro eléctrico.
- Sistemas de control de acceso.
- Sistemas de comunicaciones.
- Sistemas administrativos y de habilitación.
- Sistemas de servicio a los pasajeros y tripulación (incluyendo los de ocio y bienestar).

En este conjunto, podemos distinguir dos grandes grupos: las Tecnologías de la Información (IT), que se centran en el uso de los datos como información, y los sistemas de Tecnología Operativa (OT), que utilizan los datos para controlar o vigilar procesos físicos (tal y como sucede con los sistemas de control industrial).

Si bien estos sistemas y tecnologías ofrecen ventajas importantes para el sector marítimo, también presentan una serie de riesgos derivados de la posible explotación por parte de actores amenaza de vulnerabilidades de sus activos, entendiendo como tales cualquiera de los siguientes elementos: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos, que pueden ser susceptibles de ser atacados, deliberada o accidentalmente, con consecuencias (impacto) sobre el funcionamiento (servicio) o sobre la seguridad física de las personas y los bienes, así como sobre el entorno marítimo, incluyendo el costero.

Esas vulnerabilidades explotables pueden proceder de factores muy diversos: falta de actualización y/o de mantenimiento, inadecuada configuración de los elementos de seguridad de los sistemas, interconexiones inapropiadas, emanaciones electromagnéticas no deseadas, políticas o procedimientos inadecuados, etc.). Especial mención merecen las vulnerabilidades software de día 0, que son aquellas que aún no disponen de una solución por parte del fabricante.

Las amenazas, una vez que se materializan aprovechando la vulnerabilidad de algún activo, afectan a una o varias dimensiones de seguridad: la **confidencialidad** (los activos sólo están disponibles para personas y procesos autorizados), la **integridad** (los activos no han sido modificados ni alterados por personas o procesos no autorizados) y la **disponibilidad** (los activos están cuando son requeridos por personas y procesos autorizados). Estas dimensiones son complementadas con otras como la **autenticidad** (evitación de la suplantación), la **responsabilidad** (imputación de acciones), el **no repudio** (prevención de la negación de la autoría) y la **fiabilidad** (evitación de resultados inconsistentes). Además, hay que tener en cuenta que los incidentes podrían tener repercusión sobre otros aspectos muy relevantes (reputación de la empresa, costes, seguros) y derivar en daños colaterales muy diversos (daños al medio ambiente, accidentes, etc.).

Además, estas dimensiones están claramente enfocadas a los sistemas IT, por lo que al abordar los sistemas OT han de considerarse también otros aspectos.

4. PECULIARIDADES DE BUQUES Y PUERTOS EN MATERIA DE CIBERSEGURIDAD

Buques y puertos acumulan una serie de peculiaridades que han de ser muy tenidas en cuenta a la hora de abordar su ciberseguridad.

Tanto en unos como en otros, un gran número de actividades se apoya en Tecnologías de la Información (IT) y Operativas (OT), muy heterogéneas en cuanto a su naturaleza y empleo. En muchos casos, existirá algún tipo de interconexión entre sistemas, siendo especialmente preocupantes aquellas que conecten los sistemas a redes abiertas, especialmente a Internet; y teniendo en cuenta el principio de transitividad de las interconexiones, si un sistema A está conectado con B, y B está conectado con C, en la práctica A está interconectado con C.

Por lo general, en el diseño e implantación de estos sistemas prevalecen los criterios de funcionalidad y fiabilidad sobre los de seguridad. El que su régimen de operación sea continuo o muy prolongado exige que los sistemas sean capaces de operar en entornos degradados y de ser restaurados de la forma más pronta posible. Por tal motivo, aspectos como las arquitecturas, interconexiones o la redundancia de activos críticos han de ser contemplados durante la fase de construcción; y determinados procedimientos y políticas (copias de seguridad, equipos de respuesta inmediata, restauración de activos,…) resultan indispensables durante la fase de operación.

La operación continua de puertos y buques implica trabajar en regímenes de guardias o turnos. En el caso de los buques, además, esta actividad se alterna tanto en puerto como en la mar, siendo muy diferentes las circunstancias en uno y otro entorno, lo que tiene sus implicaciones en materia de ciberseguridad. En la mar o en puertos diferentes al de su base habitual, lo normal será que las actividades de ciberseguridad sean llevadas a cabo por la propia tripulación, por lo general muy reducida en número. Actividades que, además, tendrán muy probablemente que ser compatibilizadas con otros cometidos abordo.

Un aspecto crítico en entornos en los que se trabaja a turnos/guardias es una adecuada gestión de credenciales de acceso a los sistemas, que habrá de estar condicionada al principio de “necesidad de conocer (o de acceder)”. Así mismo, también resulta crucial una adecuada estructura de administración de esos sistemas y del control de los privilegios en función de los diferentes perfiles. Por desgracia, es muy habitual encontrar en estos entornos políticas laxas de control de acceso a los sistemas, mala gestión de credenciales (compartidas, mal custodiadas o mantenidas por tiempo excesivo) y dispersión de responsabilidades (administración, actualizaciones, control de activos,…).

En los buques de pasajeros, además, habrá de tenerse en cuenta el conveniente aislamiento de los sistemas que puedan ser empleados para el entretenimiento o conectividad del pasaje de aquellos que solo deban ser utilizados por la tripulación.

Otro aspecto a tener en muy cuenta es el limitado ancho de banda con el que cuentan los buques en la mar o fuera de su puerto base, que limitará y condicionará la forma en que puedan monitorizarse remotamente sus sistemas.

Por lo general, buques y puertos son elementos que forman parte de organizaciones complejas. Por tal motivo, los planes de ciberseguridad de esas organizaciones han de extenderse hasta ellos y abarcarlos de forma particularizada. Algo que habrán de

contemplar estos planes es, por ejemplo, que el personal de la dotación responsable de la ciberseguridad cuente con un apoyo especializado en tierra para auxilio en caso de necesidad.

5. GESTIÓN DE RIESGOS PARA LA CIBERSEGURIDAD

En ciberseguridad, se entiende por riesgo la probabilidad de que una amenaza pueda explotar las vulnerabilidades de un activo que represente un cierto impacto para una organización.

Estos riesgos deben afrontarse de manera integral (es decir, teniendo en cuenta todos y cada uno de los factores que pueden influir en la exposición de los activos a determinadas amenazas) a fin de identificar las salvaguardas (técnicas, organizacionales, procedimentales, contractuales o legales) que ayudarán a reducir ese riesgo a límites aceptables.

Este proceso, además, debe ser iterativo, ya que todos los elementos citados son cambiantes: incorporación de nuevos dispositivos, instalación de nuevas aplicaciones, actualizaciones de éstas, interconexiones, nuevas amenazas conocidas, descubrimiento de nuevas vulnerabilidades,… Todo ese conjunto de acciones constituye el ciclo de la función de la ciberseguridad conocido como “Gestión del Riesgo”.

Para que la gestión del riesgo para la Ciberseguridad sea eficaz, deben considerarse tanto las amenazas intencionadas (ciberespionaje, ciberdelincuencia, ciberterrorismo, ciberguerra, hacktivismo, personal con acceso que desea causar un daño por cualquier motivación) como aquellas de carácter no intencionado (comportamiento indebido o negligente por parte de los responsables de su administración o mantenimiento y/o los usuarios de los sistemas), sin olvidar las derivadas del entorno (acción de la mar y los elementos, fuego, inundación, etc).

Por lo general, las ciberamenazas explotarán alguna vulnerabilidad de las Tecnologías Operacionales o de la Información. Entre las más habituales: arquitecturas inadecuadas, programas informáticos anticuados o no actualizados, controles de acceso ineficaces o inexistentes, configuraciones deficientes, mal funcionamiento, inadecuada integración, mantenimiento incorrecto o insuficiente, carencia de procedimientos o incumplimiento de estos por desconocimiento o desinterés de administradores o usuarios.

La velocidad de los cambios de las tecnologías y la sofisticación creciente de las ciberamenazas dificultan la gestión de este tipo de riesgos únicamente con controles de tipo técnico, motivo por el cual la gestión debe contemplar también controles de gestión y de procedimiento operativo.

A los efectos de la presente Guía, se entiende por “Gestión del Riesgo” el proceso integral de identificación, análisis, evaluación y comunicación de riesgos de ciberseguridad y de aceptación, evitación, transferencia o mitigación de esos riesgos hasta un nivel aceptable.

La gestión eficaz de los riesgos de ciberseguridad deberá empezar en el más alto nivel de dirección y exigirá la implicación de todos los niveles de la organización, empresa o compañía en la adopción de una cultura de conocimiento de los riesgos, de manera que se garantice un régimen global y flexible de gestión de estos riesgos a través de un proceso de actualización continua que utilice mecanismos eficaces de retroalimentación.

El planteamiento más adecuado para conseguir lo anterior es evaluar y comparar de forma completa la situación actual con la situación deseada. Mediante esa comparación podrán resolverse posibles lagunas implantando controles y medidas proporcionales al riesgo en

función de la prioridad y valor de los activos, lo que permitirá aplicar los recursos de la manera más eficaz y eficiente.

Existe profusa normativa internacional al respecto, pero quizás el estándar más reconocido sea la serie de normas UNE ISO 27000. Entre ellas, la ISO 27001 recoge los requerimientos para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) y la ISO 27002 muestra una serie de controles que podrían ser considerados como necesarios.

Hay que tener en cuenta que la implantación de un Sistema de Gestión de la Seguridad de la Información debe adaptarse a la tipología de la organización, a los activos que deben protegerse y a los riesgos a los que están expuestos. Una implantación inadecuada podría dar lugar a una inversión y a unos costes de mantenimiento excesivos, o a un nivel de seguridad no apropiado para los activos a proteger y riesgos que se desean mitigar. La implantación de algunas buenas prácticas puede requerir de un análisis de riesgos formal y un estudio previo coste/beneficio que permita a la dirección entender en profundidad las razones de la inversión en seguridad y la toma de las decisiones adecuadas.

El modelo de gestión más aceptado en ciberseguridad se basa en 5 áreas funcionales:

IDENTIFICAR	• Definir las funciones y responsabilidades del personal en la gestión de riesgos de ciberseguridad e identificar los sistemas, medios, datos e información, procesos y capacidades que, de resultar afectados, supondrían un riesgo para la organización.
PROTEGER	• Implementar procesos y medidas de seguridad adecuadas para garantizar los servicios, así como un planeamiento de contingencia que proporcione medidas para limitar y/o contener el impacto sobre ellos ante un ciberincidente y asegure su continuidad.
DETECTAR	• Desarrollar e implementar los procesos y actividades necesarias para identificar la ocurrencia de un incidente de seguridad de manera oportuna.
RESPONDER	• Desarrollar e implementar actividades y planes que proporcionen medidas de contingencia y mitigación que reduzcan el impacto sobre los sistemas IT/OT y los servicios que se vean afectados por un ciberincidente.
RECUPERAR	• Frente a un incidente, identificar medidas para respaldar y restaurar los sistemas afectados que sean necesarios para la continuidad de las operaciones/servicios.

Estas áreas funcionales abarcan la totalidad de actividades para la gestión eficaz de los riesgos de ciberseguridad y constituyen un proceso cíclico y permanente (dinámico), con mecanismos eficaces de retroalimentación. Su implantación debería ser simultánea y continua y estar imbuida en un marco de gestión de riesgos que afronte las ciberamenazas de manera global, con una estructura coordinada que comparta información sobre la amenaza, que disponga de normativa legal que la soporte y respalde y que adopte las medidas necesarias en función del riesgo.

Ha de prestarse especial atención a la prevención, ya que el objetivo de una óptima gestión de ciberincidentes es que no ocurran nunca, y para lo cual la concienciación y la formación del personal resultan fundamentales.

6. ESTADO DEL ARTE DE LA CIBERSEGURIDAD EN EL SECTOR MARÍTIMO

Hasta hace muy pocos años, en el sector marítimo en general, y en buques y puertos en particular, no ha existido una excesiva preocupación por la ciberseguridad en comparación con otros sectores de actividad. Sistemas operativos obsoletos, software no actualizado, configuraciones de seguridad inadecuadas, carencia de buenas prácticas y procedimientos, administración de redes ineficaz o inexistente, uso de cuentas y contraseñas de administrador predeterminadas, sistemas sin elementos de protección y con arquitecturas inadecuadas, ausencia de segmentación de redes, interconexiones no conocidas o no debidamente configuradas, equipos o sistemas críticos de seguridad conectados permanentemente a redes abiertas, controles de acceso inadecuados, incluidos contratistas y proveedores de servicios, eran (y siguen siendo en muchos casos) lo habitual.

La profusión de ciberincidentes y la constatación del enorme interés de las ciberamenazas por el sector han ido provocando un progresivo cambio de mentalidad. En los últimos años varias organizaciones del ámbito marítimo, con el apoyo de un gran número de compañías, han unido esfuerzos para hacer frente a este problema.

La **IMO (*International Maritime Organization*)** es una agencia especial perteneciente a las Naciones Unidas que desarrolla estándares internacionales y que ha creado un marco de referencia para la industria naval, velando por la seguridad y la conservación del medio ambiente en las navegaciones, para que sea adoptado e implementado de forma universal.

En 2017, la IMO adoptó la **resolución MSC.428(98)** sobre la gestión de riesgos de ciberseguridad marítimos en el Sistema de Gestión de la Seguridad (SMS). La Resolución establecía que un SMS aprobado debía tener en cuenta la gestión de riesgos de ciberseguridad de acuerdo con los objetivos y requisitos funcionales del International safety Management (ISM) Code. Además, alentaba a las administraciones a garantizar que estos riesgos se abordaran adecuadamente en los sistemas de gestión de la seguridad a más tardar en la primera verificación anual del Documento de Cumplimiento de la empresa después del 1 de enero de 2021. El mismo año, la IMO elaboró recomendaciones de alto nivel sobre la gestión de riesgos de ciberseguridad en el transporte marítimo, en las que se resalta que una gestión eficaz de estos riesgos debe comenzar en la alta dirección y abarcar todos los niveles.

Alineada con las recomendaciones anteriores y teniendo en cuenta el marco de referencia de ciberseguridad del ***US National Institute of Standards and Technology*** **(NIST)**, se publica en 2018 una guía de ciberseguridad para barcos[1] (***The Guidelines on Cyber Security on Board Ships***) que contiene recomendaciones elaboradas y aprobadas por varias asociaciones líderes a nivel internacional en la industria marítima. Esta publicación ha sido objeto de diversas mejoras y actualizaciones, siendo la última versión disponible del documento la número 3.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) también ha prestado un especial interés a la Ciberseguridad en el ámbito marítimo, siendo la primera agencia de la

[1] http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf

UE en publicar un informe al respecto[2] (septiembre de 2011). Más recientemente (noviembre 2019), ha publicado una guía de buenas prácticas enfocada a puertos[3].

Por lo tanto, se constata la atención creciente hacia el problema. No obstante, para que los esfuerzos sean efectivos, es necesario que esas medidas se extiendan y apliquen en todos los aspectos de las operaciones y demás actividades que se desarrollan en una compañía marítima. Por ello, tal y como se hizo en su momento con la inclusión de la cultura *safety*, la IMO decidió incluir requisitos de ciberseguridad en el ISM Code (*International Safety Management Code*)[4], de carácter obligatorio para todos los propietarios de buques, operadores y compañías implicadas del sector. Algunos de estos requisitos son:

- Evaluación de riesgos de todos los dispositivos TI y TO, tanto a bordo como en tierra.
- Políticas de seguridad relacionadas con el uso de dispositivos de almacenamiento externo.
- Políticas y procedimientos sobre el uso de las redes y comunicaciones por parte de la tripulación.
- Políticas y procedimientos sobre la monitorización y actualización de sistemas de navegación y comunicación.
- Políticas sobre los criterios de autorización del uso de conexiones remotas.
- Inventario de todos los sistemas OT.
- Políticas de acceso a Internet, estableciendo restricciones cuando se estén desarrollando operaciones a bordo.
- Elaboración de planes de contingencia para respuestas de emergencia.

Estos nuevos requisitos cubren las operaciones de los siguientes buques en operaciones internacionales:

- Naves de pasajeros, incluidos los de alta velocidad.
- Buques de transporte de crudo, químicos, gas, buques cargueros y cargueros de alta velocidad de 500 toneladas de registro bruto o superior.
- Otros buques de carga y unidades móviles de perforación de alta mar de 500 toneladas de registro bruto o superior.

Otra organización que ha reaccionado ante estos cambios y actualizado rápidamente sus guías a las nuevas circunstancias es la **OCIMF (*Oil Companies International Marine Forum*),** asociación voluntaria de compañías relacionadas con el transporte marítimo de crudo, petróleo y gas, que tiene como misión ser la principal autoridad en la operación segura y responsable con el medio ambiente en buques de petróleo, terminales y buques de apoyo

[2] https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

[3] https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

[4] http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

en alta mar. En enero de 2018 actualizó su programa ***TMSA*[5] *(Tanker Management and Self Assessment)***, que provee a dichas compañías de medios para mejorar y medir sus SMS, incluyendo en él aspectos y requisitos de ciberseguridad aplicables a estos sectores, entre los que se encuentran:

- Procedimientos sobre la gestión de parches y software.
- Procesos y guías para la identificación y mitigación de ciberamenazas.
- Procedimientos para la gestión de contraseñas.
- Desarrollo de un plan de concienciación y formación en ciberseguridad para todo el personal involucrado.

La **IMCA (*International Maritime Contractors Association*)**, que representa a la mayoría de los contratistas y cadenas de producción asociadas a la industria de construcción marítima en alta mar y cuyo principal objetivo es la de ayudar a las organizaciones a priorizar la defensa contra los ataques actuales más comunes y más dañinos a las infraestructuras TO y TI, también ha actualizado recientemente sus recomendaciones en ciber amenazas, las cuales se encuentran incluidas en su guía ***Security Measures and Emergency Response Guidance* (IMCA SEL 037/M 226)**, que consta de 20 controles y sub-controles centrados en varias medidas y actividades técnicas, entre los que se incluyen:

- Gestión activa del inventario de dispositivos y del software autorizado y no autorizado.
- Bastionado de dispositivos finales y de red.
- Evaluación y solución continua de vulnerabilidades.
- Defensa contra el malware.
- Control de acceso a redes inalámbricas.
- Capacidad de recuperación de datos.
- Evaluación de las habilidades en ciberseguridad del equipo y programa de formación.
- Control de acceso a los puertos de red.
- Control del uso de privilegios administrativos.
- Defensa perimetral.
- Mantenimiento, monitorización y análisis de logs.
- Control de acceso basado en el principio de “Necesidad de Conocer”.
- Monitorización y control de las cuentas de usuario.
- Protección de la información.
- Respuesta y gestión ante incidentes de ciberseguridad.

[5] https://www.ocimf.org/sire/about-tmsa.aspx

- Ingeniería de red segura.
- Realización de pruebas de penetración para evaluar la fortaleza de las defensas de una organización.

7. BUENAS PRÁCTICAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN BUQUES E INSTALACIONES PORTUARIAS

La siguiente selección de recomendaciones se ha basado en el modelo IDENTIFICAR-PROTEGER-DEFENDER-RESPONDER-RECUPERAR, buscando un enfoque eminentemente práctico.

Algunas de las medidas están dirigidas a las fases previas a la operación de la infraestructura o sistema (diseño, construcción) y otras a todo el ciclo de vida, si bien la mayoría se centran en la fase de operación. Con antelación a la entrada en servicio y con ocasión de obras de modernización y ante la implantación de nuevos sistemas, son especialmente importantes las enfocadas a la IDENTIFICACIÓN, así como las básicas de PROTECCIÓN (arquitecturas, configuraciones, procedimientos). En la fase de operación, cobran especial relevancia las encaminadas a la PROTECCIÓN (actualizaciones, inspecciones, concienciación), DETECCIÓN, RESPUESTA y RECUPERACIÓN.

Como se ha señalado anteriormente, se trata de **unas recomendaciones de base** que en su mayor parte puedan ser aplicadas en entornos no especialmente propicios (por ejemplo, con personal reducido, de alta movilidad, no altamente especializado y sin dedicación completa, y con limitaciones de ancho de banda para monitorización remota) y que deberán ser complementadas por otras medidas técnicas, organizativas, procedimentales y legales en el ámbito de la organización/compañía.

La tabla se ha inspirado en modelos sobradamente probados y maduros, entre ellos los referidos en los apartados anteriores, adaptándolos a las peculiaridades de los entornos a los que se enfoca esta Guía.

Nº	TÍTULO	FUNCIÓN	DESCRIPCIÓN
1	**Control de activos**	**IDENTIFICAR**	Se debe elaborar una documentación técnica de cada sistema, que incluya el inventario y la configuración detallada de cada elemento. Esto permitirá abordar en un tiempo reducido la sustitución de hardware o software averiado u obsoleto y poder restablecer así el sistema a las condiciones previas al suceso. Así mismo, se deben designar responsables del mantenimiento al día y comprobación periódica del inventario del hardware y software de los diferentes sistemas. Otro aspecto a tener en cuenta es la adecuación del material de repuesto a lo que establezca el plan de contingencia y continuidad, teniendo previsto el funcionamiento del sistema en modo degradado (sin todas las funcionalidades), lo cual permitirá reducir el material a transportar/almacenar. Además, tener un inventario actualizado de activos permite identificar rápidamente los elementos (software y hardware) que estén próximos a finalizar su vida útil (fin de soporte), lo que facilita planificar su renovación antes de que se produzca su obsolescencia.
2	**Identificación de activos críticos**	**IDENTIFICAR**	Ya durante la fase de diseño, es preciso identificar los activos críticos, de forma que puedan diseñarse las soluciones técnicas que permitan potenciar su protección y resiliencia (*back-ups*, redundancias de elementos o cableado, etc.). Así mismo, esta identificación se deberá mantener durante todo el ciclo de vida y especialmente durante fases de modernización o con ocasión de la incorporación de nuevos sistemas. En la identificación de activos críticos es fundamental tener en cuenta las mutuas dependencias entre los distintos elementos del sistema: un activo crítico puede depender de forma indirecta de otro que no se considera en principio crítico, pero que cambia su categoría debido a esta dependencia. Las metodologías de análisis de riesgos permiten identificar este tipo de dependencias, por lo que es fundamental efectuar un análisis formal de riesgos en todo sistema crítico.

3	**Estructura de seguridad de los sistemas**	**IDENTIFICAR**	Se debe definir y mantener actualizada una estructura de seguridad de los sistemas (gobernanza), integrada en el plan de seguridad del buque/instalación, que designe responsables en las diferentes áreas y establezca de forma clara sus cometidos.
4	**Actualizaciones y gestión de parches**	**PROTEGER**	Las actualizaciones y parches de software y de firmware resuelven problemas funcionales y de seguridad, por lo que es muy importante que sistemas operativos, drivers, programas ofimáticos, antivirus, Java, etc. estén permanentemente actualizados a su última versión. Para ello, es necesario que exista personal específicamente designado para este cometido. Es conveniente, además, el mantenimiento de un registro donde queden reflejadas las actualizaciones realizadas.
5	**Aislamiento de redes**	**PROTEGER**	Durante la fase de diseño y construcción se han de detectar todas las posibles conexiones entre sistemas y aplicar las soluciones técnicas adecuadas para cada tipo de conexión. Han de ser objeto de especial atención las conexiones con redes públicas (fundamentalmente, Internet). Dependiendo de la criticidad de la red, esto se llevará a cabo bien mediante separación física (sin conexión) o bien con medidas de seguridad específicas que controlen dichas conexiones (segmentación mediante sistemas de protección del perímetro y el establecimiento de zonas desmilitarizadas DMZ). Posteriormente, durante la fase de servicio hasta el final de ciclo de vida, en función de la incorporación de nuevos sistemas, se habrán de evitar o controlar debidamente las conexiones entre las redes públicas y aquellas redes consideradas sensibles o críticas para el funcionamiento del buque o instalación (comunicaciones, operaciones, sistemas de mando y control, redes corporativas, sistemas de navegación y posicionamiento, etc.). Deberá prestarse especial atención al conveniente aislamiento entre las redes y sistemas que estén a disposición del pasaje de aquellas otras cuyo acceso deba estar restringido a la tripulación.
6	**Segmentación y bastionado**	**PROTEGER**	Con antelación a la entrada en servicio y durante todo el ciclo de vida, se han de definir y crear segmentos de red (subredes o VLANs) que contengan cada uno sólo los recursos específicos (ordenadores, servidores, impresoras,…) necesarios para dar un servicio, creando entornos de mínimo privilegio, al objeto de

			controlar su acceso, reducir el tráfico en la red sin afectar a su rendimiento y reducir la superficie del ataque. Se deben limitar los puertos de red, protocolos y servicios de red a los estrictamente necesarios. Se debe asegurar que los accesos *wireless* a la red son accesos controlados y realizados a través de dispositivos autorizados, utilizando protocolos considerados seguros. Así mismo, se deben cambiar las contraseñas por defecto en la electrónica de red (*routers* y *switches*) y establecer un mecanismo de filtrado que sólo permita la conexión de equipos autorizados.
7	**Política y procedimientos**	**PROTEGER**	Además de las medidas técnicas, enfocadas en asegurar que los sistemas de abordo se encuentran diseñados y configurados para ser resilientes en caso de ataque, es necesario contemplar medidas procedimentales, centradas en definir el modo en que esos sistemas han de ser operados por el personal. Deben desarrollarse y actualizarse procedimientos operativos que contemplen aspectos tales como alta y baja de usuarios, acceso de terceros, entradas y salidas de información, gestión de copias de seguridad, instalación de aplicaciones, uso del correo electrónico, etc.
8	**Concienciación y formación**	**PROTEGER**	Los usuarios participan de forma no intencionada en un alto porcentaje de los incidentes de seguridad en los sistemas, motivo por el cual resulta fundamental su formación y conocimiento de los riesgos y amenazas. Tanto en lo relativo a su dimensión física como lógica, todo el personal del buque/instalación debe conocer las normas básicas de seguridad. Aquellos perfiles encargados de sistemas críticos deben recibir formación específica sobre su seguridad. Además, deben desarrollarse campañas periódicas de concienciación mediante conferencias, boletines, guías, etc. que permitan a todos los niveles de la organización conocer las formas de actuación de la ciberamenaza y desarrollar comportamientos y actitudes de “ciberhigiene” que reduzcan las vulnerabilidades derivadas del elemento humano. Así mismo, es conveniente distribuir boletines especiales ante amenazas en curso que puedan afectar a la organización tan pronto como sean detectadas.

9	**Seguridad de aplicaciones**	**PROTEGER**	Sólo deben estar instaladas las aplicaciones autorizadas por el responsable del sistema. Las aplicaciones han de ejecutarse con el mínimo de privilegios posible. Otra práctica muy recomendable es la de la normalización de los equipos clientes, para limitar sus funcionalidades a las estrictamente necesarias.
10	Correo electrónico	**PROTEGER**	**El correo electrónico es uno de los principales vectores de entrada empleados por los atacantes, por lo que ha ser objeto de especial atención. Únicamente podrán utilizarse las herramientas y programas de correo electrónico autorizados. Se debe incidir en este aspecto en las acciones de concienciación, de forma que el usuario desconfíe de los correos de los que desconozca el remitente y no ejecute o abra archivos o ficheros de remitentes desconocidos. Sería conveniente disponer de unas instrucciones básicas a nivel usuario que oriente la actuación ante la recepción de este tipo de correos.**
11	**Control de privilegios**	**PROTEGER**	Los privilegios de administración sobre los equipos deben estar limitados a sus administradores. Los usuarios no deberán tener permisos de modificación del hardware y software (instalación de programas, modificación de configuraciones, instalación de equipos no autorizados, USBs, etc.). Así mismo, se ha de limitar el personal autorizado para la entrada y salida de información en el sistema y restringirlo a los equipos que se determinen, considerando como acción complementaria la inhabilitación de los puertos USB y lectores de CD/DVD del resto de los equipos. Las cuentas de administración deben ser utilizadas exclusivamente para tareas de administración. Los administradores tendrán y usarán normalmente cuentas sin privilegios cuando accedan al sistema para tareas que no requieran acceso privilegiado.
12	**Seguridad en la cadena de suministro**	**PROTEGER**	Buques y puertos constituyen sistemas complejos vulnerables a los incidentes de ciberseguridad que puedan proceder de la cadena de suministro que los apoya tanto en situación de actividad operativa como en períodos de obras y mantenimientos. Por tal motivo, reviste especial importancia que los elementos de hardware y software, especialmente aquellos que se empleen en los sistemas críticos del buque o instalación, procedan de proveedores de

			garantía, que cuenten con el adecuado soporte técnico y que su vida útil sea lo suficientemente prolongada y la continuidad tecnológica esté garantizada para evitar su obsolescencia prematura. Otro aspecto a tener en cuenta son los posibles efectos que para el buque, instalación o compañía pueda tener un ciberincidente que afecte a un proveedor; por tal motivo, la exigencia de que el proveedor cuente con un SGSI puede ser un criterio a incluir en la definición de requisitos para la contratación.
13	**Cumplimiento normativa protección de datos**	**PROTEGER**	Los sistemas de información almacenan datos sensibles (personales, relativos al cargo del buque, etc.) deberán ser protegidos conforme a la legislación en vigor.
14	**Registro de la actividad**	**PROTEGER Y DETECTAR**	Los sistemas deben almacenar registros de auditoría a todos los niveles (eventos del sistema, registros de acceso, registro de errores) y en todos los dispositivos críticos (red, sistema operativo, dispositivos de protección, bases de datos,…) que, en caso necesario, permitan conocer los accesos y operaciones realizados. Se debe dotar al sistema de la capacidad de almacenamiento adecuada en función de los eventos generados.
15	**Inspecciones y Auditorías**	**PROTEGER Y DETECTAR**	De forma periódica, ha de procederse a la inspección y auditoría de los sistemas por parte de personal especializado. Estas inspecciones han de contemplar aspectos de seguridad física, políticas y procedimientos operativos, y descubrimiento de vulnerabilidades e identificar y proponer las medidas correctivas más adecuadas para la mitigación de las deficiencias y vulnerabilidades encontradas. Cuando un sistema crítico sufra modificaciones importantes deberá someterse a una auditoría fuera de ciclo. Aquellos sistemas considerados críticos deberían ser sometidos, además, a pruebas de penetración y revisión exhaustiva de las medidas de seguridad.
16	**Seguridad física y del entorno**	**PROTEGER Y DETECTAR**	El entorno físico de los sistemas y su cableado debe disponer de medidas de control de acceso físico para evitar y detectar los accesos no autorizados (videovilgilancia, acceso por clave, acceso por biométrica, etc.). Esto es especialmente importante en los buques de pasaje o en las zonas de las instalaciones portuarias a las que puedan acceder personas ajenas a la organización.

			Así mismo, se deben contemplar medidas para la supervisión y acompañamiento de personal de terceras empresas que haya de acceder a los sistemas o áreas restringidas. No se debería permitir la conexión de elementos ajenos al sistema (portátiles, periféricos, almacenamiento extraíble, etc), ni siquiera para tareas de mantenimiento, si no han pasado previamente una inspección de seguridad por personal de confianza cualificado para ello. Las tareas de mantenimiento de sistemas críticos se realizaran preferentemente usando equipos bajo control y supervisión del responsable del sistema.
17	**Software antivirus**	**PROTEGER Y DETECTAR**	Se debe prestar especial atención a la protección a nivel de equipo, como ordenadores de usuario, consolas de los sistemas de control y navegación (ECDIS, AIS, Control de Plataforma, etc.). Todos los equipos que lo soporten deberán tener un software antivirus instalado y actualizado. Además, deberán estar adecuadamente configurados los cortafuegos locales en los diferentes equipos.
18	**Instalación de dispositivos de defensa perimetral**	**PROTEGER Y DETECTAR**	En función de la criticidad de los activos, deberá considerarse la instalación adicional de elementos y dispositivos específicos de defensa perimetral, como cortafuegos, sistemas de prevención y detección de intrusiones (IDS/IPS), sistemas anti-spam, *proxies web*, recolección centralizada de logs, etc.
19	**Control de acceso lógico**	**PROTEGER Y DETECTAR**	Deben existir controles para el acceso a las redes (protocolos y servicios autorizados), al sistema operativo, a las aplicaciones y a la información (carpetas de red, etc.). El acceso a los sistemas y aplicaciones debe basarse en la “necesidad de conocer/acceder”, de forma que solo tengan acceso a un dispositivo o sistema aquellas personas que lo necesiten para realizar su trabajo o función. Se recomienda establecer controles de doble factor para el acceso a los sistemas (por ejemplo, contraseña + token). En el caso de usar control de acceso mediante usuario y contraseña, se recomienda establecer una política que defina el tamaño, complejidad y periodicidad de cambio. Los usuarios y las contraseñas deben ser unipersonales y no compartirse. Aquella información considerada crítica, debería almacenarse cifrada y estar disponible sólo para usuarios autorizados.

20	**Control activo de la configuración**	**DETECTAR**	Se debe disponer de elementos de monitorización que permitan verificar el estado de todos los elementos de una configuración, su correcto funcionamiento y los tiempos de respuesta para hacer un seguimiento al dimensionamiento y a las capacidades de los sistemas. El sistema de monitorización deberá ser capaz de alertar cuando ocurran cambios no autorizados o anomalías en el sistema y de detectar posibles intrusiones a partir de la información. Además, e independientemente de las auditorías e inspecciones periódicas, es recomendable llevar a cabo análisis periódicos de vulnerabilidades con herramientas automáticas que permitan apreciar la situación del sistema a fin de corregir las deficiencias detectadas.
21	**Gestión de incidentes**	**RESPONDER**	Se debe disponer de un procedimiento para comunicación y respuesta a incidentes de ciberseguridad. En dicho procedimiento se describirá qué se entiende por incidente de ciberseguridad y cómo y a quién han de notificarse y escalarse, en caso necesario. Un equipo técnico designado será el encargado de tomar las medidas necesarias para restituir los sistemas IT y/o OT de manera que el buque o instalación pueda reanudar las operaciones con normalidad. Se considera que una respuesta adecuada debería contemplar, como mínimo, las siguientes acciones: 1) valoración inicial; 2) recuperación de los sistemas y la información; 3) investigación del incidente; y 4) implementación de acciones correctivas.
22	**Planes de continuidad**	**RESPONDER**	Deben existir planes que garanticen que, frente a un incidente, los servicios se puedan mantener de forma efectiva, bien por los mismos medios o por medios alternativos, de manera que se reduzca el impacto en las operaciones del buque/instalación y se facilite su recuperación. Los planes deberán tener en consideración: a) las causas potenciales de incidente (ciber, humanas y naturales); b) los sistemas que resultan esenciales para mantener al buque/instalación operando con seguridad; c) la naturaleza y practicidad de métodos alternativos que se puedan utilizar para dar continuidad a las operaciones en caso de incidente; y d) la capacidad real a la que el buque/instalación podría operar dado el caso. Estos planes deberían ser practicados con regularidad mediante ejercicios/simulacros que permitan evaluar la comunicación, la coordinación, la disponibilidad de recursos, los procedimientos y la capacidad de respuesta.

23	**Asistencia Técnica**	**RESPONDER**	Es conveniente disponer de medios para la asistencia técnica remota (por ejemplo, en modalidad *help desk*) que permitan auxiliar al personal en aspectos técnicos que puedan exceder sus conocimientos y capacidades, con independencia de la ubicación del buque. Este servicio puede ser suministrado por la propia compañía o por empresas especializadas contratadas para tal fin.
24	**Intercambio de información**	**RESPONDER**	Es conveniente establecer canales con aquellos organismos de la Administración y del ámbito privado con los que se pueda compartir información sobre amenazas (incluyendo indicadores de compromiso) y vulnerabilidades. Esto se traduce en un mejor conocimiento del entorno del ciberespacio y en un refuerzo de la resiliencia de la propia organización.
25	**Protección frente a la pérdida de información**	**RECUPERAR**	Realizar copias de seguridad con regularidad es muy recomendable para mantener la seguridad de los datos abordo y de la configuración del sistema y supone la principal medida de recuperación frente a incidentes (muy especialmente frente al *ransomware*), permitiendo que la información y la configuración pueda ser restaurada de un modo rápido y sencillo. Para ello deben emplearse soportes de almacenamiento alternativos al principal y desconectados de la red. En la medida de lo posible se debe tender a cumplir la regla 3-2-1 del *back-up*: disponer de tres (3) copias de seguridad de los datos, almacenarlas en dos (2) medios distintos y almacenar una (1) copia del *back-up* en un medio externo. Debe garantizarse que las copias de seguridad se realizan de manera correcta y que el procedimiento de recuperación sea efectivo. Así mismo, se debe considerar la conveniencia del cifrado de la información sensible y de los *back up* almacenados.

8. DOCUMENTACIÓN DE REFERENCIA

- ***NIST Cybersecurity Framework.***
  https://www.nist.gov/cyberframework
- ***Analysis of cyber security aspects in the maritime sector.*** *November 2011. ENISA.*
  https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
- ***Interim Guidelines on Maritime Cyber Risk Management*** (IMO-MSC 1/CIRC 1526, June 1st 2016).
- ***Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*** (DNVGL-RP-0496, Edition September 2016).
- ***Resolution MSC.428(98) (adopted on 16 June 2017) Maritime Cyber Risk Management in Safety Management Systems.***
  http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf
- ***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).
- ***International Safety Management (IMS) Code.***
  http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx
- ***The Guidelines On Cyber Security Onboard Ships Version 3*** (publicada por BIMCO, CLIA, International Chamber of Shipping, INTERCARGO e INTERTANKO).
  https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20
- ***Security Measures and Emergency Response Guidance (IMCA SEL 037/M 226).***
  https://www.imca-int.com/publications/359/security-measures-and-emergency-response-guidelines/
- ***Port Cibersecurity. Good practices for cybersecurity in the maritime sector*** *(November 2019)*
  https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
- **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 (Directiva NIS).**
  https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA&toc=OJ:L:2016:194:TOC
- **Estrategia de Seguridad Marítima Nacional 2013.**
- **Estrategia Nacional de Ciberseguridad 2019.**

- **Guía Nacional de Notificación y Gestión de Ciberincidentes.** Gobierno de España. Febrero 2020. http://www.interior.gob.es/documents/10180/9771228/Guía+Nacional+de+Notificación+y+Gestión+de+Ciberincidentes.pdf