ESCUELA NACIONAL DE MARINA MERCANTE

ALMIRANTE MIGUEL GRAU

PROGRAMA ACADÉMICO DE MARINA MERCANTE

ESPECIALIDAD PUENTE y MAQUINAS

"NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS EN LA TRIPULACIÓN DE LA FLOTA DE LA EMPRESA NAVIERA “ELCANO, S.A”, LIMA - 2020"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE OFICIAL DE MARINA MERCANTE MENCION EN PUENTE

PRESENTADA POR:

MANTARI MUCHAYPIÑA, MARICELA YANNET

GUEVARA ROMERO, BILLY JEREMY GROWER

CALLAO, PERÚ

2020

"NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS EN LA TRIPULACIÓN DE LA FLOTA DE LA EMPRESA NAVIERA “ELCANO, S.A”, LIMA - 2020"

DEDICATORIA

A nuestras familias por su apoyo incondicional en cada etapa de nuestras vidas, enseñándonos que con perseverancia y esfuerzo lograremos nuestros objetivos. A los oficiales que nos ayudaron en nuestra formación profesional en la escuela y a durante nuestro periodo de embarque.

AGRADECIMIENTO

A dios quien es nuestro guía en el caminar de nuestra vida. A nuestros asesores por su dedicación y paciencia. En especial agradecimiento al Capitán Jorge del Monte jefe de Gestión Náutica de la empresa Naviera “Elcano S.A” por su apoyo incondicional en mi carrera profesional y en el desarrollo de la presente investigación.

ÍNDICE

Páginas

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

El objetivo principal de la investigación fue determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima – 2020, desarrollado bajo una metodología de diseño de investigación no experimental de corte transversal y alcance descriptivo, por recolectar los datos directamente de los tripulantes en la aplicación única del instrumento, abordando una muestra de estudio conformada por 272 tripulantes de la naviera, a quienes se les aplico un cuestionario que permitió medir el nivel de conocimiento en los mismos, y cuya validez fue determinada por juicio de expertos que asentaron su aplicabilidad, demostrando una confiabilidad aceptable expuesta por el Kuder–Richardson (0,762).

En los resultados se obtuvo que el 60% de los tripulantes presenta un nivel medio de conocimiento de los riesgos cibernéticos marítimos presentes en la empresa, el 32% presenta un alto nivel de conocimiento, y el 8% de los tripulantes presentan un nivel bajo de conocimiento, datos asociados a un p valor= 0,000 del estadístico de la prueba Chi-cuadrado, menor al nivel de significancia establecido en la investigación ($p<0,05$), lo que conllevo al rechazo de la hipótesis nula y la

aceptación de la hipótesis planteada en la investigación, concluyendo que: Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.

Palabras claves: Riesgo cibernéticos marítimos; equipos y sistemas vulnerables, tipos de amenazas, protocolos de seguridad.

ABSTRACT

The main objective of the investigation was to determine the level of knowledge of maritime cyber risks in the crew of the fleet of the shipping company “ElCano, SA”, Lima - 2020, developed under a cross-sectional non-experimental research design methodology and descriptive scope, for collecting the data directly from the crew members in the unique application of the instrument, addressing a study sample made up of 272 crew of the shipping company, to whom a questionnaire was applied that allowed to measure the level of knowledge in them, and whose validity was determined by the judgment of experts who established its applicability, demonstrating an acceptable reliability set forth by the Kuder-Richardson (0.762).

In the results it was obtained that 60% of the crew members present a medium level of knowledge of the maritime cyber risks present in the company, 32% have a high level of knowledge, and 8% of the crew members have a low level of knowledge, data associated with a p value = 0.000 of the Chi-square test statistic, lower than the level of significance established in the investigation ($p < 0.05$), which led to the rejection of the null hypothesis and the acceptance of the hypothesis raised in the

investigation, concluding that: There is a significant level of knowledge of maritime cyber risks in the crew of the fleet of the shipping company “ElCano, SA”.

Keywords: Maritime cyber risk; vulnerable computers and systems, types of threats, security protocols..

INTRODUCCIÓN

De acuerdo a la Organización Marítima Internacional (2017), el “riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posible, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas”. (MSC-FAL, 2017, p.1)

En este sentido las empresas navieras deben adoptar todos los mecanismos disponibles para prevenir cualquier circunstancia que coloque en peligro a los tripulantes por un ataque cibernético, ante ello “los interesados deberían tomar las medidas necesarias para salvaguardar el transporte marítimo de las amenazas y vulnerabilidad actuales y emergentes relacionadas con la digitalización, la integración y automatización de los procedimientos y sistemas del transporte marítimo” (MSC-FAL, 2017, p.1).

De esta manera es de destacar que el mayor riesgo cibernético para cualquier organización que opere en el mundo interconectado de hoy es el capital humano, según NEP&I (2017), las amenazas humanas pueden ser catalogadas como no intencional y surge a través de individuos con poca o ninguna capacitación

sobre riesgos cibernéticos, que pueden dejar a las organizaciones vulnerables a las amenazas cibernéticas, debido a su falta de capacitación o conocimiento, estas personas pueden ser altamente susceptibles al malware entregado a través de un correo electrónico de apariencia inofensiva (por ejemplo, *phishing*), sitios web falsos (ataque de abrevaderos) y manipulación a través de las redes sociales y otros medios (ingeniería social).

A efectos de este planteamiento surge como objetivo de investigación determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima – 2020, para ello el estudio se estructura en IV Capítulos, los cuales se describen a continuación:

En el Capítulo I, Planteamiento del problema: Se expone la realidad problemática, la formulación del problema, objetivos de la investigación, la justificación, las limitaciones y, por último, la viabilidad de la investigación.

En el Capítulo II, Marco teórico: Se presentan los antecedentes de las investigaciones tanto nacionales como internacionales, al igual que las bases teóricas que sustentan el estudio ahondando en las diversas teorías que sustentan la variable y sus dimensiones.

El Capítulo III, Hipótesis y variables: Se efectúa la declaración de hipótesis general y específica, así como las variables en su definición conceptual y operacional, además de las dimensiones de estudio.

El Capítulo IV, Diseño metodológico: Se expone el diseño de la investigación, la población y muestra; la operacionalización de las variables, así como las técnicas

para la recolección de datos, y las etapas del procesamiento y análisis de los datos, más los aspectos éticos respetados en el estudio.

El Capítulo V, Resultados: Se evidencian la descripción de cada una de las dimensiones y variables, a través de tablas y gráficos procesados mediante el programa estadístico Excel y SPSS v23.

En el Capítulo VI, Discusiones, conclusiones y recomendaciones: Apartado que incluye el análisis de los resultados, así como su contrastación con las teorías formuladas y los antecedentes de investigación, promoviendo las conclusiones y sugerencias derivadas de los resultados.

Por último, se presentan las fuentes de información o referencias bibliográficas, y los anexos que sustentan la viabilidad del estudio.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

Hoy en día el mundo depende más de la tecnología que antes, numerosas aplicaciones de tecnología se han convertido en una parte fundamental en el transporte de mercancías, proporcionando información real y comunicación efectiva en todo el mundo de manera instantánea. La tecnología digital ha avanzado y aumentado exponencialmente en los últimos años, tanto la tecnología de la información (TI) como la tecnología operativa (TO) están más frecuentemente conectadas a la red mundial, y la industria del transporte marítimo no escapa de esta realidad (BIMCO, et. al., 2017). Sin embargo, la tecnología también conlleva ciertos riesgos con respecto a la seguridad de las operaciones en los buques y el transporte de mercancías que posiblemente podrían extenderse al dominio económico, considerando que tanto la tecnología de la información como la tecnología operativa son esenciales para la operación diaria y la sostenibilidad de la industria naviera. El hecho de que más de un 90 por ciento del comercio mundial sea realizado por la industria naviera, demuestra que es un factor crítico en la economía mundial, donde el transporte intermodal de carga y los sistemas

integrados juegan un papel esencial, al mismo tiempo, estos sistemas son muy vulnerables a los ciberataques (Saul, 2017).

En este sentido, se destaca que el riesgo de ciberataques se expandió exponencialmente a fines del siglo XX, con la llegada de Internet, el uso de sistemas de redes informáticas y la aparición del ciberespacio como base de los negocios. Los ciberataques se refieren a la explotación deliberada de sistemas informáticos que utilizan códigos maliciosos para alterar computadoras y datos. Los piratas cibernéticos, hackers, delincuentes cibernéticos, motivados por beneficios monetarios u otros, obtienen acceso y control del sistema de un objetivo para causar daños con fines criminales o terroristas. Como ya se señaló, acceder a sistemas delicados y utilizar el transporte marítimo para actos sin escrúpulos puede comprometer la seguridad de las operaciones del transporte marítimo (DiRenzo, Drumhiller y Roberts, 2017).

Bajo esta perspectiva dentro de la industria marítima moderna, hay sistemas electrónicos, cada uno con vulnerabilidades significativas: el sistema de información automático (AIS), Sistema de posicionamiento global (GPS), el sistema de control interno (ICS) y los sistemas de gestión de carga. La cadena de suministro global, tanto terrestre como marítima, depende en gran medida del Sistema mundial de navegación por satélite, el mismo es vulnerable a los ciberataques. En 2017, más de 20 embarcaciones que operan en el Mar Negro informaron haber recibido una posición de embarcación GPS muy diferente de sus ubicaciones físicas reales (Hambling, 2017). Lo interesante de este incidente es la proximidad de los buques a Rusia y la señal de entrada final que coloca a todos los buques en un espacio dentro del territorio ruso (Goward, 2017). Debido a la gran área de mar que se vio

afectada por este evento, parece haber sido un ataque o ejercicio de suplantación de propiedad del estado por un actor sofisticado. Es probable que este ataque involucrara tecnología de interferencia de grado militar. Sin embargo, esto no impide que las organizaciones terroristas realicen algo similar en un nivel mucho más pequeño. Por ejemplo, los grupos podrían apuntar a una sola embarcación y convencer al operador de tomar una acción deliberada que, sin saberlo, pondría la nave en peligro.

En 2013, los investigadores de la Universidad de Texas pudieron piratear la señal GPS de un yate de 65 m en el mar Mediterráneo. Una vez que establecieron el control de la señal, alteraron las entradas digitales al barco y convencieron al operador de ajustar el barco rumbo a una línea de navegación ficticia y desviando el barco de su ubicación prevista (Bhatti y Humphreys, 2017). Este evento simulado demuestra que la señal puede ser hackeada, lo que hace que los oficiales de navegación tomen medidas que pongan en peligro a sus barcos y tripulaciones. La aparente falsificación de GPS por parte del gobierno ruso y el pirateo de un solo barco en curso indican una dependencia excesiva de estos sistemas, así como su vulnerabilidad.

De acuerdo al Centro de navegación de la Guardia Costera de EE. UU. (2016), junto con el GPS, el sistema AIS es un componente clave de navegación para los buques mercantes, ya que proporciona una posición, velocidad y punto de aproximación más cercano a todos los buques que utilizan AIS en el área inmediata al barco. Según Balduzzi, Wilhoit, y Pasta (2014), mientras que el sistema GPS es vulnerable solo a través de la radio señal, el AIS es vulnerable a través de la World Wide Web (www) y la señal de radio, debido a la interconexión del AIS con GPS y

RADAR, un pirata informático puede pintar objetivos en la pantalla de la carta del oficial de navegación o producir información de posicionamiento falsa para un barco o las naves a su alrededor. Esta combinación de desinformación puede hacer que el oficial realice maniobras que conduzcan a una colisión o encallamiento de la embarcación.

Hoy en día, las embarcaciones modernas dependen casi por completo de sistemas electrónicos de navegación; también dependen en gran medida del software de gestión logística. Debido a la complejidad de la cadena de suministro global, las empresas de logística han convertido sus sistemas completos de gestión de carga en bases de datos interconectadas, como todos los sistemas electrónicos estos pueden ser manipulados.

En 2017, *Maersk Shipping Lines* fue pirateado por un ataque de ransomware NotPetya, lo que resultó en un apagado total de todos sus sistemas de seguimiento de carga. Este ataque provocó que la compañía reemplazara completamente toda su infraestructura de TI, lo que resultó en un 20 por ciento de reducción en la capacidad operativa (Chirgwin, 2018).

En septiembre de 2018, el Puerto de San Diego también fue blanco de un ataque de ransomware. Aunque aparentemente no fue tan paralizante como el incidente de Maersk, los impactos sobre la gobernanza y el funcionamiento de este puerto han persistido (Freeman, 2018). De igual manera, en un giro diferente en el uso de la tecnología, las organizaciones de narcotraficantes piratearon las computadoras de gestión de carga en el puerto de Amberes para monitorear y controlar el movimiento de los envíos de drogas en contenedores hacia Europa (Bateman, 2013).

Estos ejemplos de ataques cibernéticos indican claramente que el número y la variedad de ataques a la industria marítima aumentarán en el futuro. Según una encuesta marítima realizada en 2016 por HIS Fairplay en asociación con el Báltico y el Consejo Marítimo Internacional (BIMCO), el malware representa el 77 por ciento de todos los ataques cibernéticos marítimos (Di Rollo, 2017), por lo tanto, desarrollar políticas de seguridad cibernética e implementar múltiples estrategias para abordar las amenazas y los riesgos cibernéticos, junto con priorizar la acción interna y aumentar la cultura de seguridad cibernética para promover la conciencia de seguridad y la capacitación de los recursos humanos, serán vitales para las operaciones seguras de una empresa naviera.

Cabe destacar que el mayor riesgo cibernético para cualquier organización que opere en el mundo interconectado de hoy es el Humano. Con el uso de sitios de redes sociales, teléfonos inteligentes y una amplia gama de dispositivos móviles, motiva que el punto de entrada más efectivo para que un actor de amenaza cibernética acceda a una organización es a través del Humano.

Según NEP&I (2017), hay dos tipos distintos de amenazas humanas a las que las organizaciones pueden ser vulnerables. La primera es a través de la persona que tiene la intención de causar daño a los sistemas o la seguridad de la empresa. Esto puede ser impulsado por diferentes motivaciones, por codicia, ira hacia un colega o empleador, chantaje por parte de un tercero, ideología política o religiosa. En cuanto a la segunda amenaza, se cataloga como no intencional y surge a través de individuos con poca o ninguna capacitación sobre riesgos cibernéticos, que pueden dejar a las organizaciones de manera significativa y persistente, vulnerables a las amenazas cibernéticas, debido a su falta de

capacitación o conocimiento, estas personas pueden ser altamente susceptibles al malware entregado a través de un correo electrónico de apariencia inofensiva (por ejemplo, *phishing*), sitios web falsos (ataque de abrevaderos) y manipulación a través de las redes sociales y otros medios (ingeniería social).

Se cree que el riesgo interno es la mayor amenaza cibernética para una empresa naviera, cabe señalar que unos de los medios más frecuentes de acceso a la red sin privilegios es el uso inapropiado de “unidades de memoria USB". Los tripulantes también a menudo usan dispositivos móviles para el entretenimiento, y acortar el tiempo en rutas marítimas largas, por ejemplo: es muy riesgoso desde la perspectiva de la ciberseguridad la descarga de imágenes y / o videos en sistemas de puentes en red (NEP & I, 2017).

Hirst (2017), señala que “donde hay personas y sistemas de información siempre habrá vulnerabilidades. Los sistemas de control industrial (ICS) tienden a ser operados por ingenieros y personal de campo que pueden no ser conscientes de los peligros y vulnerabilidades de dichos sistemas”. (p.1)

En este sentido, las empresas también deben tener en cuenta los errores humanos al planificar las medidas de seguridad, ya que estos suelen ser el eslabón débil de un sistema de información, también es importante que todos los empleados estén capacitados para cumplir con los estándares requeridos en cualquier nivel de una empresa, y que se incentive una cultura de seguridad y cumplimiento dentro de la misma para garantizar que todas las grietas vulnerables de una organización están adecuadamente protegidos (Hirst, 2017).

No obstante, en la industria marítima las operaciones son interconectados, donde las nuevas aplicaciones tecnológicas y los sistemas digitales evolucionan continuamente, el tiempo operativo y la efectividad de cada proceso son esenciales para las transacciones comerciales, por tal razón es necesario señalar que el desarrollo de medidas de ciberseguridad va de la mano con los avances tecnológicos. Sin embargo, todavía hay una falta de comprensión relacionada con problemas complejos de ciberseguridad y los desafíos futuros que enfrentarán las empresas con respecto a los ciberataques, siendo indispensable considerar que el factor humano juega un papel fundamental en la efectividad de los ataques como un elemento de vulnerabilidad significativo para las empresas.

La Naviera en estudio, es una empresa la cual posee un potencial respecto a las actividades que realiza en virtud de la demanda del transporte marítimo, para lo cual siguiendo los principios y recomendaciones que vinculan los daños relacionados con los riesgos cibernéticos, resulta de suma importancia verificar el nivel de conocimiento sobre aspectos que involucra capacidad cognitiva en los oficiales, tripulantes y colaboradores que forman parte de la empresa en mención.

Ante lo expuesto, el presente estudio busca establecer y determinar un parámetro, con el objetivo de asentar un conocimiento base en aras de mejorar una condición que podría afectar el desarrollo normal del transporte marítimo que encausa a las naves de la naviera en cuestión, buscando afianzar procedimientos o acciones que coadyuven a mejorar los sistemas de gestión, particularizando en el elemento humano en correspondencia con lo que se establece en el Código internacional sobre gestión operacional del buque, en adelante, Código IGS.

. Por esa razón, esta disertación examina la situación actual de seguridad cibernética en la industria marítima, y surgen las siguientes interrogantes.

1.2. Formulación del problema

1.2.1. Problema general

¿Cuál es el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020?

1.2.2. Problemas específicos

1. ¿Cuál es el nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020?
2. ¿Cuál es el nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020?
3. ¿Cuál es el nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

1.3.2. Objetivo específico

1. Determinar el nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.
2. Determinar el nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.
3. Determinar el nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

1.4. Justificación de la investigación

Teórica, A lo largo de la historia, los mares y los océanos se han asociado con el peligro y la inseguridad, como consecuencia de disputas geopolíticas y ataques de piratería. Por esa razón, los problemas de seguridad marítima ante ataques cibernéticos se han convertido en una preocupación entre las partes interesadas e involucradas en el sector marítimo, la agenda de la Organización Marítima Internacional ha reflejado estas preocupaciones en los últimos años con ciertas iniciativas regulatorias. Evidenciando que con el tiempo el panorama ha sido modificado, pero la amenaza permanece; y todos los tripulantes de las embarcaciones son responsables de prevenir estas amenazas, bien sea potenciando una cultura de ciberseguridad, conscientes de las vulnerabilidades y las consecuencias de los ataques informáticos a los sistemas operativos y de información manejados en los buques.

La complejidad de los sistemas y la interconectividad en la operación marítima requieren que cada empresa considere las amenazas desde diferentes perspectivas, de acuerdo con el servicio prestado, la capacitación de los tripulantes, el profesionalismo en el ejercicio de sus funciones y las vulnerabilidades de los sistemas. Aunque la investigación ha sugerido que la industria marítima es sensible a los ciberataques, se ha hecho muy poco para prevenirlos o disuadirlos, de tal manera que el desarrollo de esta investigación ofrece un balance de los avances en ciberseguridad, riesgos de equipos y sistemas, las incidencias y consecuencias generadas por los mismos, aportando resultados a las teorías actuales sobre este evento significativo, y promoviendo instrumentos guías para futuros investigadores.

Social, La industria marítima es reactiva al establecer estándares y procedimientos basados en eventos catastróficos. En respuesta, la comunidad internacional en 1913 se unió para la Convención de Seguridad de la Vida en el Mar (SOLAS) y establecer prácticas y regulaciones de embarque internacional para embarcaciones marítimas. Respondiendo al desastre del Titanic, en 1914, los líderes marítimos de todo el mundo exigieron requisitos de seguridad, incluida de duración, la carga, la capacidad y los requisitos específicos de construcción de botes salvavidas, y exigieron que todas las personas a bordo tengan acceso a un chaleco salvavidas debido a la negligencia de la comunidad marítima para detectar estos problemas desde el principio.

Esto significa que la comunidad internacional generalmente actúa solo en respuesta a eventos extraordinarios que ponen a los estados en pánico, pero hoy la industria marítima tiene un nuevo peligro inminente, establecido en el contexto de las amenazas cibernéticas, amenazas que repercuten en el medio ambiente y

la sociedad en general, y pueden impactar en la seguridad de los tripulantes, la economía y el ecosistema de una nación. El análisis de los ciberataques en la investigación proporcionará una visión general de la situación real de los problemas de ciberseguridad, y la orientación actual a la práctica de la industria del transporte marítimo, proporcionando un sustento para posibles recomendaciones que deben tenerse en cuenta para abordar este riesgo.

Prácticas, La industria del transporte marítimo es un sector que, en términos de red y conectividad, tiene un largo alcance, pero al mismo tiempo, muchos interesados están involucrados en el desarrollo de los diferentes procesos. Por lo tanto, este estudio se establece específicamente a los sistemas de información y operativos de los barcos, como medios vulnerables ante cualquier amenaza cibernética de origen intencional por delincuentes informáticos, o no intencionales generados por la falta de conocimiento o concientización de los tripulantes.

Los ciberataques marítimos ocurren con más frecuencia de lo que creen los miembros de la comunidad marítima debido a la cantidad de ataques no notificados y no detectados, de modo tal que se deben promover acciones que permitan un registro continuo de las incidencias y prevalencias de las ataques cibernéticos al alcance de toda la industria naviera, ofreciendo un alcance de los diferentes virus cibernéticos a los que son vulnerables y las posibles consecuencias, con el fin de promover acciones que permitan su identificación, detección, respuestas y recuperación de los sistemas en los buques, aporte que esta disertación permitirá dar un alcance, en la cual se fundamenta la relevancia social de la investigación.

Metodológica, El estudio de los aspectos de seguridad cibernética en el sector marítimo identificará ideas y consideraciones clave con respecto a esta área,

a nivel nacional e internacional y sitúa el tema de la seguridad cibernética en el sector marítimo como el siguiente paso lógico en el esfuerzo de protección global de la infraestructura de las TIC. Este documento identifica áreas problemáticas esenciales, así como las iniciativas que se están implementando, que podrían servir como línea de base para ayudar al desarrollo de la seguridad cibernética en este contexto particular. Finalmente, se presentan recomendaciones de alto nivel para cada observación, lo que sugiere los posibles enfoques que podrían adoptarse para abordar estos riesgos.

1.5. Limitaciones de la investigación

La investigación se vio limitada principalmente por la dificultad de obtener la información acerca de riesgos cibernéticos en el ámbito marítimo, dado que existen muy pocos registros sobre los ciberataques en las operaciones marítimas, suprimiendo un poco el estudio de este hecho; en este particular se destaca la falta de regulaciones nacionales e internacionales que atienden esta necesidad actual de las navieras, siendo que las normativas en gestión de ciberseguridad serán emitidas por la OMI hasta el año 2021, valiéndose en la actualidad de directrices producto de los diferentes eventos de alto impacto, que han llevado a entidades de alta envergadura a explorar y sugerir algunos parámetros preventivos sobre el tema; todo este panorama conlleva al estudio de la ciberseguridad en otras áreas industriales, alejadas del contexto marítimo, pero que de alguna u otra manera refieren la complejidad e importancia de la situación, abordadas en los antecedentes de investigación.

1.6. Viabilidad de la investigación

La investigación se hace viable, por el hecho de contar con los recursos necesarios exigidos para llevar a cabo el desenlace factible del estudio, en este sentido se cuenta con la participación activa de los integrantes, con el apoyo incondicional de los profesores de la escuela, y la cooperación de los tripulantes de la empresa naviera “ElCano, S.A” para aplicar la encuesta de recolección de datos; así mismo se cuenta con el aporte financiero que exija el estudio, gastos que serán financiados por los autores, lo cual infiere un aspecto viable, en este particular se incluyen los materiales e insumos que requiere la investigación en su proceso, que se extiende a bienes de papelería, en la reproducción de los instrumentos, servicios de impresión y espiralado de los ejemplares de la tesis en sí, u otros insumos a disponer, que bien como se explican no deducen impedimento alguno.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Nacionales

Rivera (2019), en su tesis titulada: *Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016*, presentada en la Universidad Nacional Daniel Alcides Carrión, tuvo como objetivo general conocer de qué manera los riesgos de ciberseguridad tienen consecuencias en la prevención de fraudes en las empresas industriales, desarrollado bajo una metodología de tipo explicativo y de alcance descriptivo, con una muestra de 176 trabajadores a quienes se les aplico una encuesta. Entre los resultados determinan que el conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de fraudes en las empresas industriales, expuesta por un valor de Chi-cuadrado X^2_c 422.014 > X^2_t 26.296, asociado a un nivel de sig. 0,000< 0,05 lo que permitió el rechazo de la hipótesis nula. Entre sus conclusiones destaca que a mayor conocimiento de los

componentes que originan riesgos de seguridad cibernética por parte de los trabajadores, se reduciría significativamente de manera integral los fraudes en las empresas, así mismo concluyen que el gobierno del Perú debe identificar la seguridad de su ciberespacio como un objetivo estratégico de la seguridad nacional, puesto que la materialización de una amenaza sobre nuestro ciberespacio puede afectar muy negativamente al desarrollo social, económico y cultural de nuestro país.

Mendoza y Vega (2019), en su tesis de maestría titulada *"Evaluación de la Capacidad de Detección y Respuesta a Riesgos de Ciberseguridad, caso de la Empresa SISC"*, presentada ante la Universidad del Pacífico, tuvo como objetivo general identificar las brechas en materia de ciberseguridad que están relacionadas con la detección y respuesta a los eventos de ciberseguridad en la empresa, desarrollado mediante una metodología con enfoque cualitativo bajo la forma de estudios de casos, con diseño no experimental. Los resultados de la evaluación de capacidad realizada a los procesos de detección y de respuesta en ciberseguridad, confirma que el enfoque actual de protegerse a través de la gestión técnica de herramientas de seguridad no es suficiente para detectar y responder a posibles incidentes de ciberseguridad. De tal manera que el nivel de capacidad de ciberseguridad debe alcanzar de acuerdo con el marco de referencia de ciberseguridad del NIST un nivel de proceso ejecutado (nivel 1), para ello deberá cumplir completamente los atributos definidos para cada proceso en el marco de referencia indicado. Concluyendo que los principales riesgos de ciberseguridad encontrados en la empresa son la intrusión de malware sobre los servidores operacionales críticos de la empresa, la falta de procedimientos para el tratamiento de incidentes de ciberseguridad,

la falta de personal técnico especializado en ciberseguridad y el uso de medios de almacenamiento externo (USB).

Inoguchi y Macha (2017), en su tesis de grado titulada: *Gestión de la Ciberseguridad y Prevención de los Ataques Cibernéticos en las Pymes del Perú, 2016*, presentada ante la Universidad San Ignacio de Loyola, tuvo como objetivo principal determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES, desarrollado bajo una metodología con enfoque cuantitativo, de diseño no experimental y de nivel descriptivo. Los resultados generales que se derivan de la encuesta demuestran que para el personal consultado la ciberseguridad es importante; sin embargo, la empresa no cuenta con procedimientos ni políticas que orienten a las buenas prácticas en el uso de la tecnología, no ha formado a sus empleados en materia de ciberseguridad para prevenir y evitar posibles amenazas; no invierten en herramientas de ciberseguridad y no tienen personal responsable de la seguridad de la empresa en la red. Concluyendo que los gerentes deben conocer, analizar e implementar los elementos que componen el concepto de ciberseguridad, mediante un análisis de riesgos, para establecer la probabilidad de ocurrencia de los mismos y el impacto que este genere al concretarse una amenaza, lo que implica identificarlos y analizarlos para determinar las posibles consecuencias, proponiendo medidas a efectuar para tratarlos de forma adecuada.

Sánchez y Sumiano (2017), en su tesis de grado titulada: *Conocimiento de Normas de Seguridad y la Conducta de Riesgo en la Tripulación de los Buques de una Naviera Peruana*, presentado en la Escuela Nacional de Marina

Mercante Almirante Miguel Grau, tuvo como objetivo general determinar la relación que existe entre el conocimiento de normas de seguridad y la conducta de riesgo en la tripulación de los buques de una naviera peruana, a través de una metodología de diseño no experimental, de corte transversal y de alcance correlacional, con enfoque cuantitativo, y bajo una muestra de estudio conformada por 90 tripulantes a quienes se les aplico una encuesta. Determinando en los resultados una correlación inversa entre las variables expuesta por un coeficiente de correlación de Rho de Sperman -0,233 asociado a un nivel de significancia que conllevo al rechazo de la hipótesis nula (p valor 0,027 < 0,05), es decir a mayor conocimiento por parte de los tripulantes de las normas de seguridad menor será el riesgo que estos puedan generar en el ejercicio de sus funciones. En tal sentido, concluyen que el riesgo en la tripulación de los buques es mayor ante la falta de conocimientos de las normas de seguridad que deben cumplirse.

Delgado y Puch (2016), en su tesis titulada: *Relación entre la Actitud y el Nivel de Conocimiento de Medidas Alternativas Ante Fallas del GPS, ECDIS y ARPA en Egresados de la Especialidad de Puente de la Escuela Nacional de Marina Mercante "Almirante Miguel Grau" del año 2015*, presentada ante la Escuela Nacional de Marina Mercante Almirante Miguel Grau, tuvo como finalidad determinar la relación entre la Actitud y el Nivel de Conocimiento de medidas alternativas ante fallas del GPS, ECDIS Y ARPA en oficiales egresados de la especialidad de puente de la ENAMM, bajo una metodología de tipo básica no experimental, y diseño descriptivo – correlacional, con una muestra conformada por 45 egresados a quienes se les aplico un cuestionario para medir el nivel de conocimiento. Los resultados validan la hipótesis alterna

que sugiere que “Si existe relación entre la actitud y el nivel de conocimiento de medidas alternativas ante fallas del GPS, ECDIS y ARPA en oficiales egresados de la especialidad de puente de la ENAMM, dado por un valor de significancia de 0,046 asociado al Chi-cuadrado, menor al nivel de significancia 0,05 establecido en la investigación. Concluyendo que a medida que los egresados de la especialidad de puente de la ENAMM adquieran más conocimiento de medidas alternativas ante fallas del GPS, ECDIS y ARPA, su actitud para resolver las fallas que presenten estos equipos se determinara de manera oportuna y apropiada.

2.1.2. Internacionales

Torres (2018), en su tesis de maestría titulada: *Protección Marítima del Marino Mercante Español en el Contexto Internacional*, presentado en la Escuela Técnica Superior de Náutica, Universidad de Cantabria, España. Tuvo como objetivo identificar las áreas conflictivas para el tráfico marítimo internacional, determinar los riesgos de protección marítima existentes y como pueden afectar a nuestros profesionales de la Mar, siendo los más comunes: la piratería, el terrorismo marítimo, el polizonaje, la inmigración irregular y el tráfico de drogas u otros más contemporáneos, como el ciberdelito en el ámbito marítimo. Estudio desarrollado bajo una metodología cualitativa de análisis documental con la aplicación de una entrevista a marinos mercantes para obtener una visión real de esta problemática. Destacando entre sus conclusiones que la ciberseguridad a bordo, se verá mermada si no establecen unas normas claras por parte de la compañía naviera o del capitán del buque, en relación a la conexión de dispositivos electrónicos personales de la tripulación con los

sistemas de navegación o equipos informáticos de administración o acciones de mantenimiento del software, que podrían infectar a los mismos de forma accidental. Así mismo el uso mayor del Radar en detrimento del ECDIS aumenta la seguridad de la navegación en caso de manipulación del sistema GPS por parte de organizaciones criminales.

Crawford (2019), en su artículo de investigación titulado: *Ciberataque al Transporte Marítimo. ¿Una Amenaza Real o Ciencia Ficción?*, expone los riesgos de ciberataques en la industria marítima, con una clasificación en los sistemas que pueden ser intervenidos, analizando varios casos de ciberataques y las medidas que se han adoptado a nivel global y en Chile, bajo un análisis documental y estudio de los antecedentes ocurridos en la industria marítima en los últimos años a causa de los ataques informáticos. Concluyendo que, los ataques al ciberespacio marítimo, son un hecho real, que se han registrado durante los últimos años, derivado del aumento de los sistemas críticos a bordo que impulsan las amenazas cibernéticas, competencia técnica de los atacantes y complejidad de los mismos. Lo anterior, ha significado pérdidas económicas, materiales, daño a la vida humana y potencial beneficio para el tráfico ilegal de productos a través de recintos portuarios. Asimismo, podría entenderse, como un periodo de entrenamiento para ataques más grandes y de mayor impacto.

Ahokas (2018), en su tesis de maestría titulada: *El sector marítimo finlandés dentro del huracán de ciberseguridad*, presentada en la Universidad de Turku, Finlandia, tuvo como objetivo comprender las percepciones y opiniones de los operadores clave del sector marítimo finlandés, que son las autoridades portuarias, los operadores portuarios y las compañías navieras,

con respecto a la ciberseguridad. Desarrollada como una investigación cualitativa que se basó en una revisión exhaustiva de la literatura y se mejoró con entrevistas en profundidad con los operadores clave del sector marítimo finlandés. Los resultados muestran que ha aumentado la conciencia dentro del sector marítimo finlandés, pero aún se producen algunas diferencias entre los diferentes operadores marítimos en términos de comprensión de los factores de ciberseguridad. Los operadores marítimos finlandeses han tomado medidas para mejorar la ciberseguridad, pero aún existe una gran necesidad de estándares para toda la industria y una coordinación práctica de nivel. La Directiva NIS tiene la oportunidad de mejorar aún más las operaciones de seguridad cibernética y simplificar los conceptos y procedimientos en términos de una mejor situación de seguridad cibernética. En conclusión, este sentido el estudio tiene el potencial de mejorar la conciencia de la importancia de la ciberseguridad para diferentes operadores marítimos en Finlandia, y tal vez dar algunas pautas para las autoridades clave de seguridad de Finlandia sobre cómo abordar los desarrollos de ciberseguridad desde la perspectiva de Sector marítimo finlandés.

Miranda (2018), en su tesis de maestría *"Ciberataques: una realidad de amenaza digital que afecta a la industria marítima"*, presentada en la Universidad Marítima Mundial - Suecia, tuvo como objetivo crear una lista de casos recientes de ciberataques con información detallada, mediante un análisis documental a través de una recopilación de informes, principalmente de revistas electrónicas marítimas, y artículos, que muestran las áreas específicas afectadas y las consecuencias de los ciberataques, para demostrar la importancia de las medidas de ciberseguridad para la industria marítima. Los

resultados muestran que la industria marítima es claramente vulnerable a los ciberataques, dado que, las compañías navieras, los buques, los puertos y las administraciones marítimas tienen varios sistemas electrónicos modernos, lo que facilita el beneficio y la conducción de sus operaciones diarias. Sin embargo, esta tecnología, si no se usa adecuadamente y junto con las medidas de seguridad apropiadas, podría tener serias repercusiones. Hay una falta de comprensión dentro de la industria marítima de lo que realmente significan los ciberataques y las consecuencias que siguen a estos incidentes. Concluyendo que es necesario comprender que los riesgos que enfrenta la industria marítima en términos de ciberseguridad son reales. Por esa razón, es necesario que la gestión de la empresa atienda los problemas de seguridad cibernética porque un ataque cibernético es un problema organizacional, no solo relacionado con el departamento de TI, dado que estos problemas pueden afectar directamente toda la estructura organizativa y la operación de la empresa.

Hamrock (2019), en su tesis titulada: *Seguridad Cibernética Marítima: Un Análisis Comparativo de la Regulación Internacional y de EE. UU. Sobre los Receptores de datos AIS*, presentada en la Universidad Texas A & M, tuvo como objetivo examinar la regulación sobre los transmisores y receptores de datos AIS, mediante una comparación de las leyes internacionales y nacionales. La referencia internacional es la OMI (Organización Marítima Internacional) y como Nacional (Estados Unidos), como uno de los principales países objetivo de ataques cibernéticos. Los resultados muestran que la regulación internacional es amplia y la regulación de los Estados Unidos es más restringida y específica. Entre sus conclusiones se destaca que la ciberseguridad marítima es un área que no debe pasar desapercibida, en este

sentido el AIS dentro de la seguridad cibernética está subestimado y subvalorado, especialmente cuando se compara con otras políticas conocidas que se han convertido en un gran impulso y enfoque. Centrándose en los Estados Unidos, es obvio afirmar que estas vulnerabilidades son un problema que no debe tomarse a la ligera dentro de las compañías marítimas, resaltando que a medida que las regulaciones para los datos de AIS se vuelvan más específicas hacia los transpondedores y receptores, habrá más conciencia sobre estos delitos cibernéticos, así como formas de mitigarlos.

2.2. Bases teóricas

2.2.1. Ciberespacio

Para comprender los riesgos cibernéticos, se debe identificar el ciberespacio, el cual se puede definir como “un conjunto de redes y sistemas de comunicación que están interconectados, directa o indirectamente” (Pastor, Pérez, Arnáiz, y Taboso, 2009). El ciberespacio en el ámbito marítimo es, por lo tanto, el entorno que engloba los componentes tecnológicos, es decir, las vulnerabilidades inherentes a su empleo y las amenazas que pueden afectarlos, como los factores humanos ya que son estos los que caracterizan a los usuarios de este entorno. Para comprender adecuadamente su funcionamiento y sus riesgos, se debe prestar especial atención a las personas que acceden al ciberespacio, así como a sus diferentes culturas y motivaciones.

Sin embargo, el ciberespacio tiene una serie de características particulares, que es necesario estudiar detenidamente, para que podamos identificar su relevancia en las áreas de seguridad y defensa marítima. Rodrigues, (2013) clasifica estas características en: dinámico, costo de acceso, potencial de

crecimiento, alta capacidad de procesamiento, asimétrico, anonimato, alta capacidad para producir efectos físicos, y transversalidad.

- **Carácter dinámico:** El ciberespacio tiene una alta frecuencia de cambio. Los diferentes sistemas que lo integran, cambian y se modifican constantemente, especialmente sus interconexiones. Las vulnerabilidades se descubren casi a diario y las amenazas surgen y cambian constantemente.
- **Costo de acceso irrelevante:** La barrera económica para acceder al ciberespacio es muy pequeña, y se estima que actualmente más de un tercio de la población mundial tiene acceso a Internet.
- **Gran potencial de crecimiento:** Tanto en términos de características como de velocidad de intercambio de información.
- **Alta capacidad de procesamiento:** Alta capacidad para buscar, procesar y a su vez almacenar información.
- **Carácter asimétrico:** En este nuevo dominio, con muy pocos recursos, se pueden desarrollar acciones hostiles de gran impacto. La asimetría se revela tanto en términos de recursos como del conocimiento necesario para desarrollar estas acciones.
- **Anonimato:** Es muy difícil detectar y rastrear el origen de un ataque, lo que dificulta la capacidad de disuadir y responder a estos eventos.
- **Alta capacidad para producir efectos físicos:** Se refleja en la posibilidad de llegar a una amplia gama de industrias y dispositivos al mismo tiempo, compartiendo información.

- **Transversalidad:** Una acción o evento que ocurrió en el ciberespacio puede afectar una o más áreas de actividad de las sociedades modernas, como el área política, económica, social o incluso la seguridad y defensa de los Estados.

Marsh y McLennan (2014), añaden que el ciberespacio abre la puerta a los atacantes inteligentes para que realicen sus actos criminales, considerando que el negocio en el sector marítimo tiene un perfil muy alto por sus ingresos notables, en este sentido el objetivo de seguridad más importante de Internet de las cosas (IoT), término que se refiere a una interconexión digital de objetos con internet, es garantizar que los mecanismos de seguridad utilizados en el sistema puedan cumplir su función, utilizando los tres componentes de la tríada de la CIA (confidencialidad, integridad y disponibilidad) (ver Figura 1).

Figura 1. Tríada de la CIA.

Fuente: Adaptado Farooq, Wasseem, Khairi y Mazhar (2015).

La confidencialidad de los datos representa el uso de información solo por parte del personal autorizado, proporcionando los mecanismos de seguridad para

mantener la privacidad de los datos y el sistema. La integridad mencionada en la tríada de la CIA se refiere a la protección de información y datos valiosos de actores externos e internos durante el uso diario del sistema. Además, la disponibilidad permite el acceso inmediato del personal autorizado a la información y los datos para el funcionamiento normal o en situaciones peligrosas, lo que proporciona independencia a la empresa en términos de uso de sus recursos. Sin embargo, una ruptura en uno de estos elementos puede provocar graves daños al sistema de seguridad, afectando las operaciones y exponiendo los procesos involucrados en la compañía (Farooq, *et. al.,* 2015).

Una vez comprendido que constituye el ciberespacio, sus características propias y los componentes que garantizan su seguridad, se abre el panorama de los riesgos cibernéticos a los que la empresa marítima está expuesta, dada por los múltiples equipos y sistemas interconectados que posibilitan su vulnerabilidad.

2.2.2. Riesgos cibernéticos marítimos

De acuerdo a NEP&I (2017), el “Riesgo cibernético, significa cualquier riesgo de accidentes, incidentes, pérdida financiera, interrupción del negocio o daño a la reputación de una organización debido a la falla de sus sistemas electrónicos o por las personas que usan esos sistemas.” (p.1)

El riesgo cibernético, según Biener, Eling y Wirfs (2014), se refiere a una variedad de riesgos que afectan los activos de la empresa de manera informativa y tecnológica. El riesgo cibernético también se refiere a la participación en eventos electrónicos maliciosos que causan la interrupción de la empresa, pérdida comercial y monetaria (Mukhopadhyay, Saha, Mahanti, *et. al.,* (2005). Además,

existen riesgos involucrados en un sistema de información defectuoso; teniendo esto en cuenta, el riesgo cibernético también se conoce como riesgo de seguridad de la información.

La ciberseguridad marítima es un tema en rápido crecimiento dentro de la industria naviera, debido a las continuas innovaciones y avances tecnológicos, que resultan en una desconexión del sector para adecuarse a las nuevas exigencias informáticas, causando vulnerabilidades y amenazas en los equipos a bordo, por lo que la Organización Marítima Internacional y otros organismos involucrados al ámbito marítimo identifican que estos problemas deben ser reconocidos y se deben coordinar esfuerzos para mitigar y evitar que estos sucesos ocurran.

En este sentido el Comité de Facilitación y el Comité de Seguridad Marítima (MSC-FAL) de la Organización Marítima Internacional (OMI) señala que:

> El riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posible, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas. (MSC-FAL, 2017, p.1)

Bajo esta primicia las empresas navieras deben adoptar todos los mecanismos disponibles para prevenir cualquier circunstancia que coloque en peligro a los tripulantes por un ataque cibernético, ante ello “los interesados deberían tomar las medidas necesarias para salvaguardar el transporte marítimo de las amenazas y vulnerabilidad actuales y emergentes relacionadas con la digitalización, la integración y automatización de los procedimientos y sistemas del transporte marítimo” (MSC-FAL, 2017, p.1).

En esta perspectiva, las investigaciones recientes de Wang y Mileski (2018) han demostrado que la industria marítima está atrasada con respecto a la aplicación de la estrategia comercial en comparación con otros sectores comerciales internacionales. Esto incluye la infraestructura cibernética de barcos, puertos, plataformas en alta mar y submarinos, que se incorporan continuamente como resultado del avance de tecnología a la automatización y la digitalización de procesos. Teniendo en cuenta su naturaleza, propósito y funcionalidades, la industria marítima está expuesta al riesgo cibernético, que potencialmente aumenta con el uso exponencial de Internet de las cosas (IoT). Según Robinson (2015), la utilización de IoT es eficiente y rápida, pero está significativamente desestructurada.

Esta incorporación tecnológica constituye una fuerza revolucionaria en la industria marítima debido a un aumento en la velocidad, variedad y volumen de información disponible. Sin embargo, como resultado de su uso, se agregaron nuevas vulnerabilidades a la industria marítima y los incidentes recientes muestran que el sector ha adoptado un enfoque más reactivo que proactivo. Kusi (2015) ha identificado amenazas y vulnerabilidades de ciertos puertos, dando una breve idea de otros problemas que pueden promover las amenazas y vulnerabilidades de seguridad cibernética. De hecho, el riesgo cibernético es parte de la evaluación de riesgos que cualquier organización (comercial, militar, etc.) debería tener y como tal, se podrían tener en cuenta varios aspectos dependiendo de las amenazas y consecuencias identificadas. Fitton, Prince, Germond y Lacy (2015) muestran que los efectos de la amplia seguridad de los aspectos cibernéticos, como la defensa y la ofensiva y el patrón de inversión, cambiarán en el futuro. Cualquier evaluación de riesgos debe considerar al menos tres niveles de análisis, incluidos el físico, el

legal y el económico. Salem (2018) aborda que la acción principal para encontrar amenazas y vulnerabilidades cibernéticas es “realizar evaluaciones de riesgos de ciberseguridad”.

El problema del riesgo cibernético es precisamente sus posibles consecuencias devastadoras en estos tres niveles (como la reputación financiera y los daños ambientales) que a diferencia de otras industrias, como la aviación, en el sector marítimo no existe una visión centralizada sobre el flujo de información a través de los controladores de tráfico, en otras palabras, Robinson (2015), señala que esto significa que cualquier dispositivo en un barco que use IoT puede transmitir y recibir información que se captura, almacena y comparte con varios propósitos (desconocidos).

2.2.2. Evaluación del riesgo cibernético

De acuerdo a Hsia (2017), el riesgo cibernético puede evaluarse desde la identificación de las vulnerabilidades y consecuencias de las amenazas. La Figura 2 ilustra esa superposición, siendo los activos la variable correspondiente para las consecuencias.

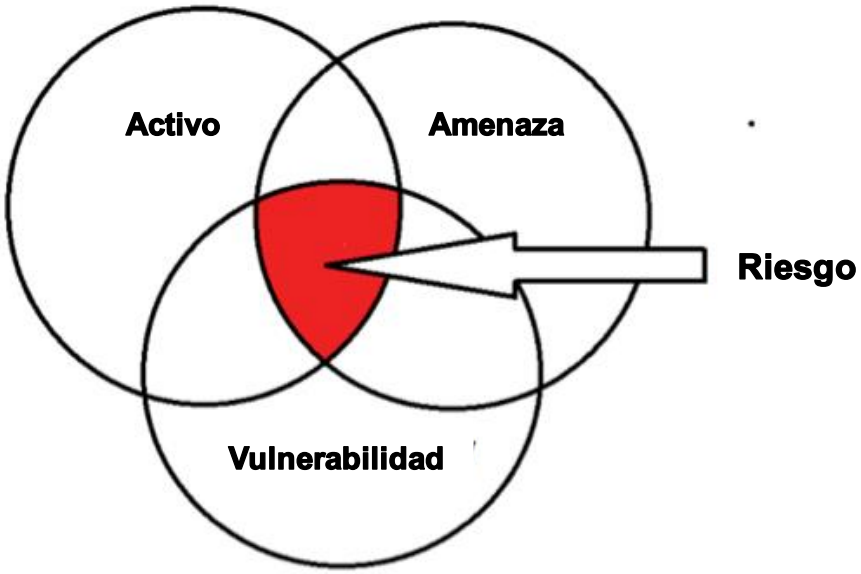


Figura 2. La evaluación del riesgo cibernético.

Fuente: Adaptado de Hsia (2017, p.1)

Hsia (2017) explica además que una compañía no solo debe identificar sus amenazas y vulnerabilidades, sino también evaluar los activos de la compañía que tienen el mayor impacto junto con el valor y el riesgo, representados en la Figura 2.

Para comprender de manera integral cómo las principales regulaciones de seguridad marítima han remodelado la industria en su conjunto, es crucial analizar los conceptos de riesgo, vulnerabilidad y amenaza marítima. El riesgo y la amenaza junto con la seguridad son conceptos necesarios al examinar cualquier entorno empresarial. Un riesgo puede verse como la probabilidad de un evento que tiene la oportunidad de tener consecuencias positivas o negativas (Prezelj y Ziberna 2013). La principal diferencia entre riesgo y seguridad es que lo último implica también incertidumbre (Marlow, 2010).

El ***riesgo*** puede entenderse como la potencialidad del daño, que se alcanzará bajo las condiciones de uso y / o exposición, y la posible extensión del

daño (Fransas, Nieminen, Salokorpi y Rytkönen, 2012). El sector marítimo es vulnerable especialmente en términos de riesgos operativos, como accidentes, fallas en el equipo o mal manejo de cargas peligrosas, e infracciones de seguridad, que incluyen ataques físicos directos, sabotaje y robos (Kouwenhoven, Borrett y Wakankar, 2016). En el Código ISPS, la OMI (2012) ha identificado que un riesgo contiene aspectos como amenaza, impacto y vulnerabilidad. Polemi (2018) ha ampliado la definición de riesgo al agregar otras dimensiones, como la probabilidad de amenaza, la pérdida promedio de amenaza y la probabilidad de incidente.

Rodrigue, Notteboom y Pallis (2011), han identificado las siguientes cinco categorías de riesgo dentro del sector marítimo: 1) Técnico, 2) Financiero, 3) Político, 4) Mercado y 5) Ambiental. Los riesgos técnicos son a menudo internos y ocurren desde la construcción y proporción de tecnologías. Los riesgos financieros incluyen, por ejemplo, las fluctuaciones de la tasa de interés, la moneda de los impuestos y los riesgos de capital propios de la organización, como la disponibilidad de préstamos. Los riesgos políticos incluyen riesgos legales, regulatorios y morales. Los riesgos de mercado se producen por cambios económicos en las áreas productivas e incluyen diversos factores que afectan los modelos y entornos comerciales. Los riesgos ambientales se relacionan con los cambios de las leyes ambientales y las sensibilidades sociales imprevistas.

Los factores de ***vulnerabilidad*** más comunes del sector marítimo incluyen situaciones en las que un barco es atacado por terroristas en una forma de acto político, o piratas/grupos criminales que secuestran la carga. Detrás de estos secuestros de carga, los motivos varían de ser un acto político a la generación de fondos. Los contenedores son usados como método de transporte en diferentes

delitos transnacionales, como el contrabando de drogas, armas entre otros. (Kouwenhoven, *et. al.,* 2016)

Se identifica el ***peligro*** como “una condición o un objeto con el potencial de causar lesiones al personal, daños a equipos o estructuras, pérdida de material o reducción de la capacidad para realizar una función prescrita”. (OACI, 2013)

La ***amenaza*** puede entenderse como un acto o acción que puede causar daño o dañar a un país, organización, persona o instalación (Polemi, 2018). En el contexto marítimo, las amenazas consisten en todas las posibles actividades dañinas o perjudiciales que llevan a cabo los estados-nación y sus representantes o terroristas, y grupos criminales o individuos que no actúan en nombre de una nación (Edgerton, 2013). Las amenazas marítimas incluyen, por ejemplo, desastres físicos, sabotaje, ataques terroristas, pérdidas financieras y robo de carga o información (McNicholas, 2008).

2.2.3. Dimensiones del riesgo cibernético

2.2.3.1. Equipos y sistemas vulnerables

La tendencia de digitalización global, las políticas y regulaciones recientes requieren que los puertos enfrenten nuevos desafíos con respecto a las tecnologías de la información y la comunicación (TIC). Los puertos tienden a depender más de las tecnologías para ser más competitivos, cumplir con algunos estándares y políticas y optimizar las operaciones. Esto trae nuevas apuestas y desafíos en el área de la ciberseguridad, tanto en el mundo de las tecnologías de la información (TI) como de las tecnologías de operación (OT). (BINCO, *et. al.,* 2018)

Durante varios años, los puertos han experimentado una transformación digital para enfrentar los desafíos emergentes, optimizar los procesos existentes e introducir nuevas capacidades, como la automatización y el monitoreo en tiempo real de las operaciones. Esta digitalización se ha centrado en la interconectividad de los activos de Tecnología de la Información (TI) y Tecnología de Operación (OT) y la introducción de nuevos habilitadores tecnológicos, tales como la computación en la nube, big data e Internet de las cosas (IoT). (Heilig, Lalla-Ruiz, y Voss, 2017)

Los barcos utilizan cada vez más sistemas que dependen de la digitalización, la integración y la automatización, los cuales requieren una gestión del riesgo cibernético a bordo. A medida que la tecnología continúa desarrollándose, la tecnología de la información (TI) y la tecnología operativa (OT) a bordo de los buques se conectan en red de Internet con mayor frecuencia. (BINCO, *et. al.,* 2018)

Tanto la ciberseguridad como la ciberdefensa son importantes debido a su potencial efecto en el personal, el barco, el medio ambiente, la empresa y la carga. La seguridad cibernética se refiere a la protección de TI y OT, información y datos de accesos no autorizados, la manipulación y la interrupción, cubriendo los riesgos de la pérdida de disponibilidad o integridad de los datos críticos de seguridad y OT. (BINCO, *et. al.,* 2018)

Los sistemas de OT controlan el mundo físico y los sistemas de TI administran los datos. OT es un hardware y software que monitorea / controla directamente los dispositivos y procesos físicos. Por otro lado, la TI cubre los aspectos de tecnologías para el procesamiento de la información, incluidas las tecnologías de software, hardware y comunicación. Tradicionalmente, los OT y TI se han separado, pero con el uso de Internet, se están acercando a medida que los

sistemas históricamente independientes se están integrando. La interrupción de la operación de los sistemas OT puede imponer un riesgo significativo para la seguridad del personal a bordo, la carga, los daños al medio marino y obstaculizar la operación del barco. (BINCO, *et. al.,* 2018)

Al considerarse la distinción entre la tecnología de la información y los sistemas de tecnología operacional, vemos que este último, se centra en el uso de los datos para controlar o vigilar procesos físicos, esto lleva a considerar la protección de la información y el intercambio de datos dentro de esos sistemas. (MSC-FAL, 2017)

La OMI (2017), señala que:

> Si bien dichas tecnologías y sistemas ofrecen ventajas importantes al sector marítimo desde el punto de vista de la eficacia, también presentan riesgos para sistemas y procedimientos cruciales vinculados al funcionamiento de los sistemas que son parte integral del transporte marítimo. Dichos riesgos pueden derivar de la vulnerabilidad originada por el funcionamiento, integración, mantenimiento y proyecto inadecuados de los sistemas de índole cibernética, y de amenazas cibernéticas intencionadas o no intencionadas. (MSC-FAL, 2017, p.2)

En general, cuando se pone de manifiesto o se aprovecha alguna vulnerabilidad de la tecnología operacional y/o de la información, directamente (por ejemplo, con contraseñas poco seguras que dan lugar a accesos no autorizados) o indirectamente (por ejemplo, por la ausencia de segregación de las redes), puede haber implicaciones para la protección y confidencialidad, integridad y disponibilidad de la información. Asimismo, cuando se pone de manifiesto o se aprovecha alguna vulnerabilidad de la tecnología operacional y/o de la información, puede haber implicaciones para la seguridad, sobre todo poniendo en peligro sistemas cruciales (la navegación en el puente o de sistemas principales de

propulsión). (MSC-FAL, 2017)

En el entorno marítimo, los equipos, sistemas y dispositivos están aumentando rápidamente la conectividad a la red, lo que facilita la accesibilidad y la funcionalidad, proporcionando operaciones más eficientes. Entre los dispositivos conectados incluyen el sistema de navegación, sistema de comunicación, sistema de gestión de carga, sistema de máquinas, sistema de propulsión, sistema de gestión de terminales, sistema de seguimiento, sistema logístico y muchos más. Sin embargo, el crecimiento de los dispositivos conectados genera un alto riesgo para la industria marítima, lo que aumenta la vulnerabilidad de todos los sistemas integrados de puentes, maquinas, carga, comunicación y tierra mencionadas. Por esa razón, es necesario que el sector marítimo evalúe las vulnerabilidades en los sistemas sofisticados e interconectados, que se incorporan en las operaciones diarias, y comprenda la complejidad de estas en los sistemas marítimos (Clark y Keaney, 2017).

Por su parte MSC-FAL (2017), señalan que:

> Las tecnologías cibernéticas se han convertido en esenciales para el funcionamiento y la gestión de los numerosos sistemas cruciales para la seguridad y la protección del transporte marítimo, y la protección del medio marino. En algunos casos, estos sistemas han de cumplir las normas internacionales y las prescripciones de las Administraciones de abanderamiento. No obstante, la vulnerabilidad generada por el acceso, la interconexión o el establecimiento de redes entre estos sistemas puede dar lugar a riesgos cibernéticos que deberían abordarse. (p. 1)

Entre estos sistemas vulnerables a un ataque cibernético por su interconectividad y funcionalidad eléctrica, la MSC-FAL (2017) destaca los siguientes:

- ✓ Los sistemas del puente
- ✓ Los sistemas de manipulación y gestión de la carga

- ✓ Los sistemas de propulsión y gestión de las máquinas y de control de suministro eléctrico
- ✓ Los sistemas de control de acceso
- ✓ Los sistemas de servicio a los pasajeros y de organización de los mismos
- ✓ Las redes públicas para los pasajeros
- ✓ Los sistemas administrativos y de bienestar de la tripulación
- ✓ Los sistemas de comunicación (p.2)

DiRenzo, *et. al.,* (2015), sostiene que la exposición en los buques modernos ha aumentado enormemente en los últimos años debido a su dependencia de medios electrónicos sofisticados como AIS (Sistema de identificación automática), ECDIS (Sistema de visualización e información de cartas electrónicas), GPS (Sistema de posicionamiento global), VDR (Registrador de datos de viaje), Radar / ARPA (Radio Dirección y Rango) (Ayuda de trazado de radar automático), GMDSS (Sistema de seguridad y socorro marítimo global) y otro sistema conectado a la red de la embarcación de uso para la tripulación. Todo esto da como resultado un peligro significativo para la seguridad de la operación del barco que, debido a su interconectividad y uso recurrente está abierto a ataques cibernéticos.

En la Figura 3, se visualiza con mayor precisión los sistemas electrónicos y equipos a bordo, vulnerables ante un ataque cibernético.

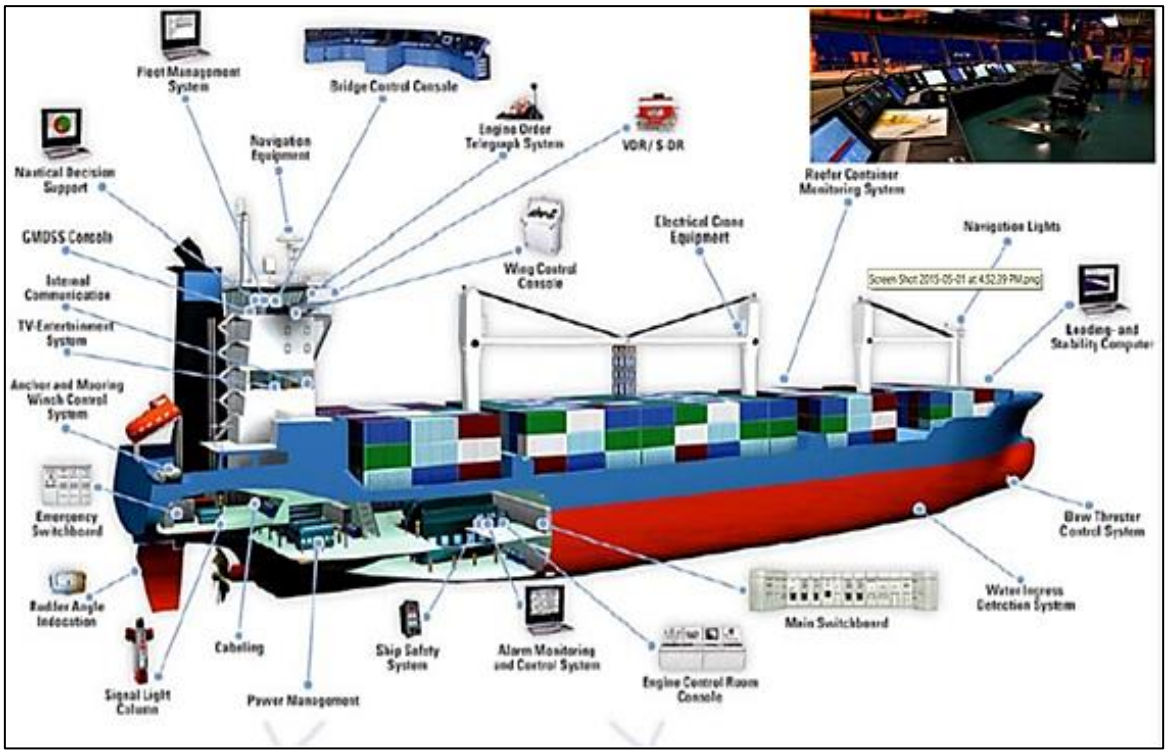


Figura 3. Sistema electrónico y equipo a bordo de embarcaciones.

Fuente: HudsonAnalytix Cía

De acuerdo a la Figura 3, los sistemas independientes serán menos vulnerables a los ciberataques externos en comparación con los conectados a redes no controladas o directamente a Internet. Se debe tener cuidado para comprender cómo los sistemas críticos de a bordo podrían estar conectados a redes no controladas. Al hacerlo, se debe tener en cuenta el elemento humano, ya que muchos incidentes son iniciados por las acciones del personal. (BINCO, *et. al.,* 2018)

Según BINCO, *et. al.,* (2018) las vulnerabilidades de los sistemas a bordo podrían incluir:

- ✓ **Sistemas de gestión de carga**

Los sistemas tecnológicos actuales utilizados para la operación, gestión y

control de carga, pueden interactuar con una variedad de sistemas en tierra, incluidos puertos y terminales marítimas. Dichos sistemas pueden incluir herramientas de seguimiento de envíos disponibles para los operadores a través de Internet. Sin embargo, el seguimiento generalmente se realiza a través de los sistemas de la compañía conectados al barco y no directamente entre el remitente y el barco. Las interfaces de este tipo hacen que los sistemas de gestión de carga, los datos en manifiestos de carga y listas de carga sean vulnerables a los ciberataques. (BINCO, *et. al.,* 2018)

Como hecho relevante en este aspecto, en agosto del año 2011, piratas informáticos penetraron en los servidores de la empresa naviera iraní IRISL, dañando datos de las tarifas, cargando secuencias de carga, fechas de entrega y lugares. Lo anterior, trajo como consecuencia, el descontrol sobre la ubicación de un gran número de contenedores. Asimismo, una cantidad considerable de carga se entregó a los destinos equivocados o incluso se perdió. (Crawford, 2019)

El año 2012, piratas informáticos pusieron en peligro el sistema de carga controlado por la agencia del Servicio de Aduanas y Protección Fronteriza de Australia. Los ciberdelincuentes querían saber qué contenedores se encontraban bajo sospecha de la policía o las autoridades aduaneras. Con esta información sabrían si necesitaban abandonar contenedores particulares con carga de contrabando (Crawford, 2019). Asimismo, entre los años 2011 y 2013, ataques similares al señalado precedentemente, se desarrollaron en el puerto de Antwerp, Bélgica, logrando la pérdida de

información sobre la ubicación de los contenedores, el cambio de fechas y lugares de entrega y la confidencialidad de los números de seguridad. Cuando se descubrió la violación de seguridad, el puerto instaló un firewall, sin embargo, los delincuentes ingresaron al puerto e instalaron puentes inalámbricos en las computadoras, lo que hizo posible el acceso directo al sistema operativo. La administración del puerto tardó aproximadamente dos años en encontrar el motivo de la desaparición de los contenedores en sus instalaciones (Crawford, 2019).

- ✓ **Sistemas de puente**

El uso cada vez mayor de sistemas de navegación interconectados en red, con interfaces a las redes costeras para la actualización y provisión de servicios, hace que dichos sistemas sean vulnerables a los ataques cibernéticos. Los sistemas de puente que no están conectados a otras redes pueden ser igualmente vulnerables, ya que los medios extraíbles (bien sea: USB, CD, Disco duro portátil) a menudo se utilizan para actualizar dichos sistemas desde otras redes controladas o no controladas. Un incidente cibernético puede extenderse a la denegación o manipulación del servicio y, por lo tanto, puede afectar a todos los sistemas asociados con la navegación, incluidos ECDIS, GNSS, AIS, VDR y Radar / ARPA. (BINCO, *et. al.,* 2018)

- **Sistema de identificación automática (AIS):** Es un sistema de seguimiento de buques que es obligatorio para todos los barcos comerciales (no pesqueros) de más de 300 toneladas métricas, así como para los buques de pasajeros (independientemente de su tamaño

y peso). El sistema AIS opera mediante coordenadas GPS e intercambia datos sobre la posición de un barco, su rumbo e información con los buques y las instalaciones de otros barcos cercanos en alta mar y en la costa. Actualmente, unos 400.000 buques cuentan con este sistema instalado. (Trend Micro, 2014)

El AIS es un transpondedor no encriptado responsable de transmitir el rumbo, la velocidad, el tipo de buque, el tipo de carga, estado de anclaje o en marcha, y otra información para la seguridad en el mar (Middleton, 2015). Es un sistema de radiodifusión de radio de muy alta frecuencia (VHF) en barco y en tierra, utilizado para los servicios de tráfico de buques (VTS), operaciones de búsqueda y rescate, investigación de accidentes y pronóstico del tiempo. La confianza en la información transmitida es crítica para el conocimiento situacional y la prevención de colisiones en el mar. Los transpondedores AIS se comunican por aire sin ninguna verificación de autenticación o integridad, por tal razón los atacantes pueden inyectar señales a través de una Radio definida por software (SDR) y colocar faros falsos de “hombre en el agua”, hacer que el barco sea invisible y reportar informes de clima falso (Balduzzi, Wihoit y Pasta, 2014). Confiar en la información potencialmente incorrecta puede conducir a decisiones equivocadas y resultados catastróficos.

Las vulnerabilidades en el sistema AIS son ampliamente conocidas. Por ejemplo, un estudio realizado por el equipo de amenazas con visión de futuro de Trend Micro, grupo de defensa contra amenazas que se

centra en el sector de la tecnología, pudo recrear una frecuencia VHF en AIS que simulaba un “barco falso” en un puerto y alertó a las embarcaciones cercanas que estaban en curso de colisión con otra embarcación (Ferran, 2013). Además, Trend Micro expuso una lista completa de habilidades de “falsificación” de AIS, incluyendo rumbo falso, velocidad, bandera y nombre del barco; alertas meteorológicas falsas que causan desviaciones del plan original del movimiento previsto; falsificación como autoridad de aplicación de la ley marítima (USCG); plataformas de rescate marítimo falso, situaciones de hombre al agua por la borda; y abrumador de AIS que conduce a informes dobles y datos falsos que causan sobrecargas del sistema. (CyberKeel, 2014)

- **Sistema de posicionamiento global (GPS):** Hoy, con la gran dependencia del mundo marítimo en la tecnología, los datos GPS son cruciales para mantener la seguridad de la navegación en el mar para todos los buques. La suplantación de identidad y la interferencia son dos técnicas diferentes que causan estragos en la comunidad marítima cuando se emplean con éxito. La suplantación de identidad de GPS se define como “un ataque electrónico que involucra señales enviadas a un receptor para controlar la navegación”, mientras que la interferencia de GPS involucra a un actor que bloquea intencionalmente las señales de GPS (Thompson, 2015).

  La Oficina de Análisis Cibernético e Infraestructura (OCIA), ha identificado preocupaciones por la interferencia y falsificación de GPS

para envíos comerciales, principalmente por la excesiva dependencia de los marinos en los sistemas GPS y el abandono de las ayudas visuales tradicionales en la navegación de canales estrechos. Operar cerca de aguas poco profundas o en un canal estrecho aumenta naturalmente el riesgo de desastres de navegación como la puesta a tierra o la colisión. La pérdida de las entradas de navegación, la dirección o la propulsión de un barco serían catastrófica y causaría daños significativos, demoras en los servicios y tensiones financieras. (OCIA, 2016)

En el 2013, el equipo de investigación de la Universidad de Texas-Austin pudo comprobar que si se puede controlar un buque de forma remota mediante la manipulación de su GPS. Como ejemplo se usó al yate White Rose of Drax, el cual, en tan solo 30 minutos se pudo hackear las señales de su GPS durante su navegación en el Mediterráneo. De esta manera los investigadores lograron controlar la navegación del yate. Los encargados de navegación al ver la desviación del rumbo decidieron volver a rumbo, sin percatarse que iban al rumbo definido por los investigadores. Ante esto Todd Humphreys dijo que, “el yate comenzó a alterar su rumbo, pero en la pantalla del radar solo se apreciaba una línea recta” (Crawford, 2019).

Figura 4. Fotografía del yate White Rose of Drax y la representación de la alteración obtenida en su rumbo de navegación.

Fuente: Crawford (2019).

- **Sistema electrónico de información de visualización de cartas (ECDIS):** Las cartas de papel se están convirtiendo en una reliquia del pasado. El Sistema Electrónico de Visualización e Información de Cartas (ECDIS), una pantalla de cartas de navegación basada en computadora, ha reemplazado las cartas de papel. Los diferentes sensores alrededor de un barco comercial típico alimentan la siguiente entrada en el ECDIS: AIS, datos de GPS, velocidad, rumbo y radar (CyberKeel, 2014). Como el principal medio de navegación, el sistema ECDIS proporciona cartas digitales electrónicas que permiten al oficial de puente (OOD) navegar adecuadamente. Recibir la información de cartas más actualizada requiere que los sistemas ECDIS establezcan una conexión a través de redes de Internet no seguras a bordo de los barcos, lo que podría poner en riesgo la integridad de los datos de navegación de un barco (OCIA, 2016).

  En enero de 2014, NCC Groups, una empresa de aseguramiento, desempeñó el papel de un pirata informático que intentaba acceder al ICS de un barco. Según CyberKeel (2014), después de someterse a

pruebas, “se encontraron varias debilidades de seguridad, incluida la capacidad de leer, descargar, reemplazar o eliminar cualquier archivo almacenado en la computadora que aloja el ECDIS”.

La dependencia excesiva de los datos del ECDIS puede ser costosa. El 17 de enero de 2013, un dragaminas de la Marina de los EE. UU., El USS Guardián (MCM), encalló en el arrecife Tubbatatha frente a las costas de Filipinas. A pesar de las numerosas alarmas y advertencias de la versión de la Armada del ECDIS (ECDIS-N), el equipo de navegación y puente no tuvo en cuenta las señales visuales y las correcciones, según lo requerido bajo la dirección de la marina. Tras una investigación, la armada determinó que el dragaminas cargó las cartas equivocadas antes del zarpe, encallando así el barco. Este evento, aunque no es un ciberataque, muestra la excesiva dependencia del barco de la armada de los datos electrónicos (OCIA, 2016).

- ✓ **Sistemas de control de potencia y administración de maquinaria y propulsión**

El uso de sistemas automatizados para monitorear y controlar la maquinaria, propulsión y dirección a bordo hace que dichos sistemas sean vulnerables a los ataques cibernéticos. La vulnerabilidad de estos sistemas puede aumentar cuando se utiliza junto con monitoreo remoto basado en la integración con equipos de navegación y comunicaciones en barcos manipulando sistemas de puentes integrados. (BINCO, *et. al.,* 2018)

Respecto a este punto en el año 2010, Mientras se trasladaba desde Corea del Sur a Brasil, una plataforma de perforación petrolera a de perforación petrolera se escoro hacia una banda, causando múltiples heridos. En el transcurso de los 19 días de investigación, se confirmó que la causa fue por un ataque cibernético, debido a los virus alojados en las computadoras y los sistemas de control de la plataforma (Crawford, 2019). Además, hubo otro ciberataque a una plataforma petrolera, la *Noble Regina*, fue anunciad el 3 de diciembre de 2012, cuando se encontraba en su proceso de construcción. Los ciberatacantes accedieron a sus controles de sus sistemas de bombas, logrando producir una escora de 17º, esto provoco un accidente que dejo a 89 heridos y también pérdidas económicas a la empresa. (Crawford, 2019).

Figura 5. Plataforma petrolera Noble Regina, escorada posterior al ataque.

Fuente: Crawford (2019, p.19).

- ✓ **Sistemas de control de acceso**

Los sistemas digitales utilizados para soportar el control de acceso para garantizar la seguridad física, la del barco y su carga, incluida la vigilancia, las alarmas y los sistemas electrónicos de “personal a bordo” son vulnerables a los ataques cibernéticos. (BINCO, *et. al.,* 2018)

- ✓ **Sistemas de servicio y gestión de pasajeros**

Los sistemas computarizados utilizados para la gestión de pasajeros, embarque y control de acceso pueden contener datos valiosos relacionados con los pasajeros. Los dispositivos inteligentes (tabletas, escáneres portátiles, etc.) constituyen un vector de ataque, ya que, en última instancia, los datos recopilados se transmiten a otros sistemas. (BINCO, *et. al.,* 2018)

- ✓ **Redes públicas para pasajeros**

Las redes fijas o inalámbricas conectadas a Internet, instaladas a bordo para el beneficio de los pasajeros, por ejemplo, los sistemas de entretenimiento para invitados, deben considerarse incontroladas y no deben conectarse a ningún sistema crítico de seguridad a bordo. (BINCO, *et. al.,* 2018)

- ✓ **Sistemas administrativos y de bienestar de la tripulación**

Las redes informáticas a bordo utilizadas para la administración del barco o el bienestar de la tripulación son particularmente vulnerables cuando se proporciona acceso a Internet y correo electrónico. Los ciberatacantes pueden explotar esto para obtener acceso a los sistemas y datos a bordo.

Estos sistemas deben considerarse incontrolados y no deben conectarse a ningún sistema crítico de seguridad a bordo. El software proporcionado por las compañías o propietarios de gestión de buques también se incluye en esta categoría. (BINCO, *et. al.,* 2018)

- ✓ **Sistemas de comunicación**

La disponibilidad de conectividad a Internet vía satélite u otra comunicación inalámbrica puede aumentar la vulnerabilidad de los barcos al pertenecer a un ciberespacio, en este sentido los mecanismos de defensa cibernética implementados por el proveedor de servicios deben utilizarse cuidadosamente, pero no deben confiarse únicamente en ellos para asegurar todos los sistemas y datos de a bordo. En estos sistemas se incluyen enlaces de comunicación con las autoridades públicas para la transmisión de la información requerida de notificación del buque. Los requisitos de gestión de autenticación y control de acceso aplicables por estas autoridades deben cumplirse estrictamente. (BINCO, *et. al.,* 2018)

En este particular el 25 de septiembre de 2018, el puerto de San Diego sufrió una interrupción en sus sistemas de tecnología de la información, habiendo informado que había recibido una nota de rescate de los atacantes que exigieron el pago en Bitcoin (Port Technology, 2018a.). Otro evento se registró el 25 de julio de 2018, la compañía naviera COSCO encontró un ciberataque, que afectó sus canales de comunicación y aplicaciones de red en sus mercados estadounidenses. (Port Technology, 2018b.)

Los sistemas a bordo mencionados anteriormente consisten en equipos potencialmente vulnerables, que deben revisarse durante la evaluación.

2.2.3.2. Tipos de amenazas

La complejidad de los sistemas y las partes interesadas involucradas en la operación marítima requieren que cada empresa considere las amenazas desde diferentes perspectivas, de acuerdo con el servicio prestado y las vulnerabilidades del sistema. Sin embargo, de acuerdo a la Boyes, Isbell y Luck (2016), las amenazas presentadas en la industria marítima se pueden clasificar en dos elementos principales: las amenazas directas intencionales y las amenazas directas no intencionales.

- **Las amenazas directas intencionales**, pueden atribuirse a:
  - ✓ **Hacktivismo o grupo activista:** Estos grupos están formados por individuos con motivaciones ideológicas, para lo cual la acción principal es una protesta en línea con el objetivo de acceder al sistema y robar información y datos confidenciales para usar con fines maliciosos (Boyes, *et. al.,* 2016).
  - ✓ **Competidor industrial de espionaje:** Están organizados para realizar actos de espionaje con el objetivo principal de obtener acceso a información confidencial, destruir datos y robar propiedad intelectual para usarlos con ventaja competitiva o interrumpir las operaciones comerciales (Boyes, *et. al.,* 2016).

- ✓ **Impulsado por el gobierno o patrocinado por el estado:** En la industria marítima se reconoce que muchos países están involucrados en ciberataques. Su propósito es obtener acceso a secretos de estado, información altamente sensible, información comercial y documentos valiosos, para ser utilizados con la intención de afectar directamente a otro estado o institución de gran importancia para una nación, y con este acto crear desestabilización o caos nacional, u obtener una ventaja económica o control de la información (Boyes, *et. al.,* 2016).

  Por ejemplo, en abril de 2016, Corea del Sur informó que 280 embarcaciones sufrieron problemas con sus sistemas de navegación. La señal de GPS fue atacada por piratas informáticos; en consecuencia, algunas de las señales de GPS murieron y otras recibieron información falsa. En algunos casos, el GPS mostró la posición de las embarcaciones que navegaban en el mar como aparentemente en tierra (Saul, 2017). Corea del Sur afirmó que Corea del Norte estuvo involucrada en los incidentes (Graham, 2017).

  En 2017, más de 20 embarcaciones que operan en el Mar Negro informaron haber recibido una posición de embarcación GPS muy diferente de sus ubicaciones físicas reales (Hambling, 2017). Lo interesante de este incidente es la proximidad de los buques a Rusia y la señal de entrada final que coloca a todos los buques en un espacio dentro del territorio ruso (Goward, 2017). Debido a la gran área de mar que se vio afectada por este evento, parece haber sido un ataque o ejercicio de suplantación de propiedad del estado por un actor sofisticado. Es probable que este ataque involucrara tecnología de interferencia de grado militar.

- ✓ **Terrorismo:** Los grupos terroristas pueden usar los medios electrónicos e informatizados como un nuevo modus operandi para llevar a cabo sus actos terroristas contra otros grupos, naciones y empresas, obteniendo acceso e interrumpiendo el sistema operativo, para fines o intereses ideológicos, religiosos o políticos (Boyes, *et. al.,* 2016).
- ✓ **Delincuentes:** Los individuos u organizaciones criminales usan ataques cibernéticos contra sistemas y redes interconectados, con la intención de llevar a cabo actividades delictivas, principalmente enfocadas en operaciones fraudulentas, extorsiones o robo de propiedad intelectual. También se reconoce que estos delincuentes, cuando obtienen acceso a los diferentes sistemas, pueden controlar los sistemas operativos para facilitar el tráfico de drogas, armas y dinero de contrabando para obtener beneficios económicos o vender información valiosa a otro (Boyes, *et. al.,* 2016).

  En este sentido un ataque cibernético importante tuvo lugar en el puerto de Amberes en Bélgica entre 2011 y 2013, cuando una banda de narcotraficantes pudo contrabandear drogas dentro de contenedores ocultos, que fueron engañados sin el reconocimiento temprano de los operadores del puerto. La banda de narcotraficantes había contratado a algunos piratas informáticos para instalar cámaras ocultas dentro de las oficinas del puerto de Amberes y, por lo tanto, tenían acceso a las contraseñas y la información de los contenedores. (Clark y Keaney 2017)

- **Las amenazas directas no intencionales,** están relacionados con:
  - ✓ **Amenaza interna o naturaleza:** pueden ser errores de empleados o proveedores de servicios. Los empleados internos pueden comprometer los sistemas de la industria marítima por negligencia, descuido, ignorancia o simplemente error humano, abriendo accidentalmente correos electrónicos maliciosos, utilizando medios extraíbles infectados o accediendo a sitios web y redes sociales falsas. Estos actos no intencionales exponen los sistemas o datos confidenciales a amenazas, poniendo la seguridad de las empresas en diferentes niveles de riesgo dependiendo del acceso que tengan a los sistemas (Boyes, *et. al.,* 2016). Se reconoce que este tipo de amenaza representa una falta de capacitación y conciencia de los tripulantes, representando el máximo riesgo para las empresas. Además, “por naturaleza” puede describirse como un error en un sistema, software o aplicación derivado de una mala instalación o fabricación, que no proporciona las medidas de seguridad necesarias para mantener el sistema seguro (NEP&I, 2017).

    Un incidente significativo involucró una plataforma petrolera en los Estados Unidos de América, específicamente Houston, en 2013. El incidente se produjo por un software malicioso descargado involuntariamente por trabajadores petroleros en alta mar. El malware se descargó a bordo de computadoras portátiles, unidades USB o directamente de fuentes en línea a través de satélites (Shauk, 2013). Los archivos, que estaban infectados con malware de tierra como pornografía y música, incapacitaban computadoras y sistemas operativos en algunos equipos y plataformas (Hayes, 2016). Un efecto directo fue que una

plataforma estaba paralizada e incapaz de comunicarse con el sistema de plataforma de navegación, lo que resultó en la inmovilización de los propulsores y el sistema de navegación. Como consecuencia, la Unidad Móvil de Perforación Offshore (MODU) salió del sitio de perforación. Este incidente muestra claramente que el elemento de disponibilidad del modelo de la CIA se vio comprometido, creando un alto riesgo para el medio ambiente y demoras en las operaciones (Belmont, 2016).

El Consejo Marítimo Internacional Báltico (BIMCO, *et al*., 2018) han dividido los ataques cibernéticos en dos categorías: 1) ataques dirigidos y 2) ataques no dirigidos. La diferencia entre los ataques dirigidos y no dirigidos es que en los ataques dirigidos hay un objetivo previsto, que puede ser una organización o un sistema y sus datos. Por otro lado, en los ataques no dirigidos tiene muchos objetivos diferentes.

Es probable que los ataques no dirigidos usen herramientas y técnicas disponibles en Internet, que pueden usarse para localizar, descubrir y explotar vulnerabilidades generalizadas que también pueden existir en una empresa y a bordo de un barco.

En este sentido BINCO, *et. al.,* (2018), señala que algunas herramientas y técnicas que pueden usarse en los ataques no dirigidos incluyen:

- ✓ **Malware:** software malicioso que está diseñado para acceder o dañar una computadora sin el conocimiento del propietario. Existen varios tipos de malware, incluidos troyanos, ransomware, spyware, virus y gusanos. El ransomware cifra los datos en los sistemas hasta que se haya pagado un

rescate. El malware también puede explotar deficiencias y problemas conocidos en el software comercial desactualizado / sin parches. El término “exploit” generalmente se refiere al uso de un software o código, que está diseñado para aprovechar y manipular un problema en otro software o hardware de computadora. Este problema puede ser, por ejemplo, un error de código, vulnerabilidad del sistema, diseño incorrecto, mal funcionamiento del hardware y / o error en la implementación del protocolo. Estas vulnerabilidades pueden explotarse de forma remota o activarse localmente. A nivel local, el usuario puede ejecutar un fragmento de código malicioso, a veces a través de enlaces distribuidos en archivos adjuntos de correo electrónico o a través de sitios web maliciosos. (BINCO, *et. al.,* 2018)

Conforme los resultados obtenidos en la encuesta realizada por HIS Fairplay en asociación con el Báltico y el Consejo Marítimo Internacional (BIMCO), en el año 2016 a *stakeholders* marítimos, el 77% de los ataques perpetrados en la industria marítima, responden a *malware*, y cerca de un 20% a robo de credenciales (Di Rollo, 2017). Entre los eventos más resaltantes, se reporta el suceso del año 2017, cuando la empresa Maersk sufrió un ataque informático del tipo *Ransomware*, impidiendo o limitando el acceso de los usuarios de sus sistemas de administración y control, a su propio sistema informático (Crawford, 2019). El 25 de septiembre de 2018, el puerto de San Diego sufrió una interrupción en sus sistemas de tecnología de la información, habiendo informado que había recibido una nota de rescate de los atacantes que exigieron el pago en Bitcoin, presumiendo un ataque cibernético del tipo *Ransomware* (Port

Technology 2018a). Otro suceso se evidencio el 25 de julio de 2018, cuando la compañía naviera COSCO encontró un ciberataque, que afectó sus canales de comunicación y aplicaciones de red en sus mercados estadounidenses, reconociendo un ataque cibernético de tipo malware, que deshabilitó todo acceso al sitio web de COSCO en las Américas (Port Technology, 2018b).

- ✓ **Phishing (Suplantación de identidad):** Enviar correos electrónicos a una gran cantidad de objetivos potenciales que solicitan piezas particulares de información confidencial o confidencial. Tal correo electrónico también puede solicitar que una persona visite un sitio web falso utilizando un hipervínculo incluido en el correo electrónico. (BINCO, *et. al.,* 2018)

- ✓ **Agujero de agua:** Establecer un sitio web falso o comprometer un sitio web genuino para explotar a los visitantes. (BINCO, *et. al.,* 2018)

- ✓ **Escaneo:** Atacando grandes porciones de internet al azar. (BINCO, *et. al.,* 2018)

BINCO, *et. al.,* (2018), señala que los ataques dirigidos pueden ser más sofisticados y utilizar herramientas y técnicas creadas específicamente para atacar a una empresa o barco. Entre estas se incluyen:

- ✓ **Ingeniería social:** Técnica utilizada por los posibles ciberatacantes con el fin de manipular a personas internas para que rompan los procedimientos de seguridad, a través de la interacción con las redes sociales. (BINCO, *et. al.,* 2018)

- ✓ **Fuerza bruta:** Un ataque que prueba muchas contraseñas con la esperanza de eventualmente adivinar correctamente. El atacante verifica sistemáticamente todas las contraseñas posibles hasta encontrar la correcta. (BINCO, *et. al.,* 2018)

- ✓ **Denegación de servicio (DoS):** Evita que los usuarios legítimos y autorizados accedan a la información, generalmente inundando una red con datos. Un ataque distribuido de denegación de servicio (DDoS) toma el control de múltiples computadoras y / o servidores para implementar un ataque DoS. (BINCO, *et. al.,* 2018)

- ✓ **Spear-phishing:** Al igual que el phishing, las personas son blanco de correos electrónicos personales, que a menudo contienen software malicioso o enlaces que descargan automáticamente software malicioso. (BINCO, *et. al.,* 2018)

- ✓ **Subvertir la cadena de suministro:** Atacar a una empresa o nave comprometiendo equipos, software o servicios de apoyo que se entregan a la empresa o nave. (BINCO, *et. al.,* 2018)

Los ejemplos anteriores no son exhaustivos. Otros métodos están evolucionando, como hacerse pasar por un empleado legítimo en tierra en una compañía naviera para obtener información valiosa, que se puede utilizar para un ataque adicional. El número potencial y la sofisticación de las herramientas y técnicas utilizadas en los ataques cibernéticos continúan evolucionando y solo están limitadas por el ingenio de las organizaciones y las personas que las desarrollan. (BINCO, *et. al.,* 2018)

En virtud de profundizar sobre los tipos de amenazas más significativos en la industria marítima, se destaca la siguiente información.

Malware

Los *malwares* son softwares maliciosos diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información. Los tipos de malware incluyen spyware (software espía), adware (software publicitario), phishing, virus, troyanos, gusanos, rootkits, ransomware y secuestradores del navegador. (Significados.com, 2019)

- **Procedencia de los malwares:** Frecuentemente, el malware accede a su dispositivo a través de Internet y del correo electrónico, aunque también puede conseguir acceder a través de sitios web hackeados, demos de juegos, archivos de música, barras de herramientas, software, suscripciones gratuitas o cualquier otra cosa que descargue de Internet en un dispositivo que no esté protegido con software antimalware. (Significados.com, 2019)
- **Prevención de malwares:** La forma más efectiva de prevenir *malwares* es la instalación de programas que los detecten como, por ejemplo, antivirus, antim*alware* o antis*pyware*, que puedan escanear el computador regularmente, prevenir ataques y mantener una protección actualizada. (Significados.com, 2019)
- **Síntomas de infección por *malwares*:** Algunos de los síntomas que el computador puede presentar al ser infectado con *malwares* son:
    - Procesamiento lento
    - Ejecuta procesos desconocidos

- Interrumpe su conexión a Internet
- Aparecen ventanas con mensajes de advertencia
- Se comporta de manera extraña. (Significados.com, 2019)

- **Formas de contagio de malwares:**
  - Abrir archivos desconocidos enviados por correo electrónico,
  - Navegar por Internet sin actualizar los programas de antivirus o antimalware,
  - Navegar en redes poco seguras,
  - Descargar programas y softwares de fuentes desconocidas,
  - Abrir archivos con extensiones desconocidas. (Significados.com, 2019)

Phishing

El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso. (Avast.com, 2019)

- **Procedencia del phishing:** Los mensajes de phishing parecen provenir de organizaciones legítimas como PayPal, UPS, una agencia gubernamental o su banco. Sin embargo, en realidad se trata de imitaciones. Los correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa y se le embaucada para que

facilite información sobre su cuenta, lo que puede provocar el robo de su identidad. (Avast.com, 2019)

- **Reconocimiento del phishing:** Recibe mensajes pidiendo que revele información personal, normalmente mediante correo electrónico, sitio web o mensajes de texto (celular). (Avast.com, 2019)
- **Prevención del phishing:**
    - No responda a enlaces en correos electrónicos no solicitados, Facebook o mensajes de texto (celular)
    - No abra archivos adjuntos de correos electrónicos no solicitados.
    - Proteja sus contraseñas y no las revele a nadie.
    - No proporcione información confidencial a nadie por teléfono, en persona o a través del correo electrónico.
    - Mantenga actualizado su navegador y aplique los parches de seguridad.
    - Introduce tus datos confidenciales sólo en sitios web seguros. Para que un sitio se pueda considerar como ‘seguro’, el primer paso -aunque no el único- es que empiece por "https://", lo que implica que sigue el protocolo de transferencia de hipertexto, y que el navegador muestre el icono de un candado cerrado. (Avast.com, 2019a)

Spear-phishing

A diferencia de los correos electrónicos de phishing normales, los de spear-phishing están muy personalizados. El objetivo final es el mismo, engañar al destinatario para que haga clic en un enlace URL o un archivo adjunto maliciosos; pero, en este caso, el mensaje contiene el nombre, la empresa o el cargo de la víctima, o se mencionan a sus compañeros de trabajo y contactos. Estos detalles personales

hacen mucho más probable que el usuario abra o ejecute el contenido malicioso. Además, dada la proliferación de redes sociales y sitios web para hacer contactos profesionales, a los ciberdelincuentes les resulta relativamente sencillo reunir la información personal necesaria para redactar un mensaje convincente (Akamai.com, 2019).

Las medidas preventivas, de procedencia y reconocimiento de este virus se establecen igual a las del virus informático *phishing.*

Spyware

El spyware es un tipo de malware difícil de detectar. Recopila información sobre sus hábitos y su historial de navegación o información personal (como números de tarjetas de crédito) y a menudo utiliza Internet para enviar esta información a terceros sin su conocimiento. Los keyloggers son un tipo de spyware que monitoriza sus pulsaciones en el teclado. (Avast.com, 2019b)

- **Procedencia del spyware:** A menudo, el spyware está incluido dentro de otro software o en descargas de sitios de intercambio de archivos (por ejemplo, sitios donde descarga música o películas gratis) o se instala cuando abre un adjunto de un correo electrónico. Debido a la naturaleza secreta del spyware, la mayoría de la gente ni siquiera sabe cuándo tiene spyware en su equipo. (Avast.com, 2019b)
- **Reconocimiento del spyware:** Pueden aparecer iconos nuevos o no identificados en la barra de tareas en la parte inferior de su pantalla, y las búsquedas pueden provocar que se le redirija a un motor de búsqueda

diferente. Aparecen mensajes de error aleatorios cuando realiza operaciones que antes funcionaban correctamente. (Avast.com, 2019b)

- **Prevención del spyware:**
  - Asegúrese de que su navegador, su sistema operativo y su software tienen las actualizaciones y los parches de seguridad más recientes.
  - Establezca niveles más altos de seguridad y privacidad en su navegador.
  - Extreme las precauciones si frecuenta sitios de intercambio de archivos.
  - No haga clic en las ventanas emergentes de publicidad. (Avast.com, 2019b)

Ransomware

El ransomware restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado ransomware como WannaCry, Petya, Cerber, Cryptolocker y Locky. (Avast.com, 2019c)

- **Procedencia del ransomware:** El ransomware lo crean estafadores con un gran conocimiento en programación informática. Puede entrar en su PC mediante un adjunto de correo electrónico o a través de su navegador si visita una página web infectada con este tipo de malware. También puede acceder a su PC a través de su red. (Avast.com, 2019c)
- **Reconocimiento del ransomware:** Es obvio cuando su dispositivo ha sido infectado con ransomware, ya que probablemente no podrá acceder a su equipo. (Avast.com, 2019c)

- **Prevención del ransomware:**
    - Asegúrese de que todo el software de su equipo está actualizado, incluyendo su sistema operativo, su navegador y cualquier complemento de barra de herramientas que utilice.
    - Asegúrese de que su software antivirus y su protección cortafuegos están actualizados. (Avast.com, 2019c)

2.2.3.3. Protocolos de seguridad

Para comprender el vínculo entre la motivación de este estudio, es necesario resaltar la diferencia entre seguridad y protección en contraste con el sector marítimo. Cualquier teoría clara o común para la seguridad no se puede encontrar en la literatura existente. La conexión entre seguridad y protección se puede ver de varias maneras. Muchos autores e investigadores han indicado que la seguridad forma un concepto más amplio y más completo, y la protección se puede colocar dentro de las medidas de seguridad, y esta relación se indica en la Figura 4. (Helmick, 2008; Polemi, 2018).

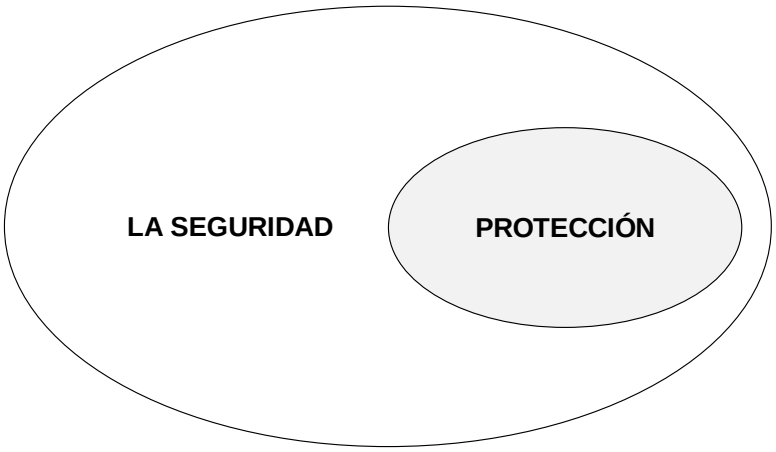


Figura 6. La relación entre seguridad y protección.

Fuente: Polemi (2018).

La seguridad marítima puede verse como el conjunto de medidas preventivas proyectadas para proteger al sector marítimo mundial y para reducir el efecto de peligro, daño, riesgo o pérdida no intencional o natural (Edgerton, 2013). La seguridad marítima también puede identificarse como la seguridad de la vida y la protección de los activos en el mar frente a las amenazas ambientales y operativas, y también la seguridad del medio ambiente marítimo contra la contaminación de los barcos. La mayoría de las veces, la seguridad marítima incluye todos los aspectos relacionados con la combinación de seguridad y protección. (Fransas, *et al.* 2012.)

Los siguientes cuatro factores 1) seguridad externa; 2) seguridad interna; 3) factor humano; y 4) los impactos ambientales se utilizan para describir la seguridad marítima. La seguridad externa incluye, por ejemplo, calles, puertos, equipos relacionados y condiciones ambientales. La seguridad interna influye en la estructura y estabilidad de daños de los buques, y la evaluación de locales comerciales. El factor humano es un aspecto importante relacionado con la seguridad marítima, porque casi el 80% de los incidentes y accidentes son causados por el hombre. Los impactos ambientales son causados por las complicadas interacciones entre todos los factores mencionados anteriormente. (Fransas, *et. al.,* 2012)

El sector de la seguridad marítima con todos sus institutos operativos está regido por un régimen global fuerte. Pero se puede ver que todas las normas y directrices nacionales de seguridad marítima siguen los puntos y estructuras principales de los Convenios y Códigos de seguridad marítima de la Organización Marítima Internacional (OMI). El Código y los reglamentos de la OMI son más fáciles

de reconocer e implementar en las operaciones de los operadores marítimos. (Guldbrandsen, 2013) Debido a accidentes graves dentro del sector marítimo, se han desarrollado dos normas principales de seguridad marítima: el Convenio internacional para la seguridad de la vida humana en el mar (SOLAS) y el Código internacional de gestión de la seguridad (ISM) (Attard, 2014).

El objetivo actual del Convenio SOLAS es proporcionar estándares mínimos de seguridad para la construcción, el equipamiento y la operación de los buques (Attard, 2014; Polemi 2018), también incluyen estándares internacionales para áreas, tales como requisitos para salvar vidas, seguridad de navegación, licencias y competencia de la tripulación y gestión de embarcaciones (Edgerton, 2013).

En este sentido el Comité de Facilitación de la OMI (FAL) y el Comité de Seguridad Marítima (MSC) definieron las Directrices de la OMI sobre la gestión del riesgo cibernético marítimo en MSC-FAL.1 / Circ.319. Ambos reconocieron la necesidad urgente de crear conciencia sobre las amenazas y vulnerabilidades del riesgo cibernético y proporcionar recomendaciones de alto nivel sobre cómo gestionar este hecho actual y emergente, incluyendo las áreas principales que apoyan la gestión eficaz del riesgo cibernético (identificar, proteger, detectar, responder y recuperarse). (MSC-FAL, 2017)

Por lo tanto, es importante que la alta gerencia se mantenga comprometida durante todo el proceso para garantizar que la planificación de protección, contingencia y respuesta esté equilibrada en relación con las amenazas, vulnerabilidades, exposición al riesgo y consecuencias de un posible incidente cibernético. Tal como se explica en la Figura 7 (BINCO, *et. al.,* 2018)

Figura 7. Enfoque de gestión del riesgo cibernético.

Fuente: BINCO, *et. al.,* (2018)

Según BINCO, *et. al.,* (2018), las actividades de estas medidas de gestión del riesgo cibernético expuestas en la Figura 7, incluye:

- **Identificar amenazas:** Comprender las amenazas externas de ciberseguridad para el barco, y la amenaza interna de seguridad cibernética que plantea el uso inapropiado y la falta de conciencia.

- **Identificar vulnerabilidades:** Desarrollar inventarios de sistemas a bordo con enlaces de comunicaciones directas e indirectas, comprendiendo las consecuencias de una amenaza de seguridad cibernética en estos sistemas.

- **Evaluar la exposición al riesgo:** Determinar la probabilidad de que las vulnerabilidades sean explotadas por amenazas externas, así como la

probabilidad de que estas estén expuestas por el uso inapropiado de los equipos, por tanto, también se debe determinar el impacto de seguridad y protección de cualquier individuo o combinación de vulnerabilidades que se exploten.

- **Desarrollar medidas de protección y detección:** Reducir la probabilidad de que las vulnerabilidades sean explotadas a través de medidas de protección, al igual de reducir el impacto potencial de una vulnerabilidad que se explota.

- **Establecer planes de contingencia:** Desarrollar un plan de contingencia prioritario para mitigar cualquier posible riesgo cibernético identificado.

- **Responder y recuperarse de incidentes de seguridad cibernética:** Responder y recuperar los incidentes de seguridad cibernética utilizando el plan de contingencia, y evaluar el impacto de la efectividad del plan de respuesta y reevaluar las amenazas y vulnerabilidades.

Otra medida que contribuye al aumento de la seguridad del sector marítimo se enmarca en Código Internacional de Gestión de Seguridad (ISM), al indicar a los operadores marítimos que asuman la responsabilidad de los problemas de seguridad de sus operaciones (Fransas, *et. al.,* 2012). El código fue adoptado en 1993, y cinco años tarde en 1998 se convirtió en obligatorio para embarcaciones de pasajeros, embarcaciones de pasajeros de alta velocidad, petroleros y petroleros químicos, graneleros y embarcaciones de carga de alta velocidad de 500 toneladas brutas o más. (McNicholas, 2008; OMI 2014)

Ante las amenazas emergentes de ciberseguridad para la industria marítima

y con la resolución del MSC, la OMI ha tomado la decisión de incorporar los requisitos obligatorios de ciberseguridad en el Código Internacional de Gestión de Seguridad, a partir del 1 de enero de 2021, la seguridad cibernética debe ser abordada por todos los actores de la industria del transporte marítimo e incorporada en sus sistemas de gestión de seguridad.

Los objetivos del Código ISM son garantizar la seguridad en el mar, la prevención de lesiones humanas o la pérdida de vidas, y evitar daños al medio ambiente, en particular al medio marino y a la propiedad, en este sentido los objetivos según Gómez, (2019), deberían:

- Proporcionar prácticas seguras en la operación del buque y un entorno de trabajo seguro.
- Evaluar todos los riesgos identificados para sus barcos, el personal y el medio ambiente y establecer protecciones apropiadas.
- Mejorar continuamente las habilidades de gestión de seguridad del personal en tierra y a bordo de los barcos, incluida la preparación para emergencias relacionadas tanto con la seguridad como con la protección del medio ambiente.

Gómez (2019), señala que cada empresa naviera debe desarrollar, implementar y mantener un sistema de gestión de seguridad SMS que incluya los siguientes requisitos funcionales:

- Una política de seguridad y protección del medio ambiente.
- Instrucciones y procedimientos para garantizar la operación segura de los

buques y la protección del medio ambiente de conformidad con la legislación internacional y del Estado del pabellón pertinente.

- Niveles definidos de autoridad y líneas de comunicación entre, personal de tierra y a bordo.

- Procedimientos para reportar accidentes en conformidades con las disposiciones de este Código.

- Procedimientos para prepararse y responder a situaciones de emergencia.

- Procedimientos para auditorías internas y revisiones de gestión.

El objetivo clave de ISM es avanzar en la cultura de seguridad dentro del sector marítimo y mejorar continuamente este problema, ya que ha afectado los niveles de seguridad del sector marítimo (Lappalainen, *et. al.,* 2010).

Concerniente al Código Internacional de Seguridad de Buques e Instalaciones Portuarias (ISPS), este se agregó al Convenio de Seguridad de la Vida en el Mar (SOLAS) en 2004 para reconocer el papel de las instalaciones portuarias en la seguridad marítima y definir los requisitos y recomendaciones obligatorios que los buques y las instalaciones portuarias deben seguir. Este capítulo se ha definido para abordar la seguridad de los puertos, pero los requisitos también pueden estar relacionados con la seguridad cibernética de los puertos (requisitos de control de acceso y autenticación). (OMI, 2019)

El código ISPS se aplica a los buques que participan en viajes internacionales, incluidos los buques de pasajeros y buques de carga de más de

500 toneladas de arqueo bruto y comprende una primera parte (A) de disposiciones obligatorias y una segunda parte (B) de disposiciones opcionales a discreción de las autoridades nacionales (Gómez, 2019). Los objetivos del código ISPS son:

- Establecer un marco internacional que implique la cooperación entre gobiernos, agencias gubernamentales, administraciones locales y las industrias navieras y portuarias para detectar amenazas a la seguridad y tomar medidas preventivas contra incidentes de seguridad que afecten a buques o instalaciones portuarias utilizadas en el comercio internacional.

- Establecer las funciones y responsabilidades respectivas de los gobiernos, las agencias gubernamentales, las administraciones locales y las industrias navieras y portuarias, a nivel nacional e internacional para garantizar la seguridad marítima.

- Garantizar la recopilación e intercambio temprano y eficiente de información relacionada con la seguridad.

- Proporcionar una metodología para las evaluaciones de seguridad a fin de tener planes y procedimientos establecidos para reaccionar a los niveles cambiantes de seguridad.

- Garantizar la confianza de que existen medidas de seguridad marítima adecuadas y proporcionadas.

En este sentido Gómez (2019), sostiene que de acuerdo con el código ISPS, se debe crear un plan de seguridad del buque SSP. La organización y los procedimientos de los planes de seguridad del buque SSP deben establecer:

- Los deberes y responsabilidades de todo el personal de a bordo con un rol de seguridad.

- Los procedimientos necesarios para permitir que tales comunicaciones continuas se mantengan en todo momento.

- Los procedimientos necesarios para evaluar la efectividad continua de los procedimientos de seguridad y cualquier equipo y sistema de seguridad y vigilancia, incluidos los procedimientos para identificar y responder a fallas o mal funcionamiento del equipo o sistema.

El Plan de seguridad del buque SSP y el Manual de gestión de seguridad SMM pueden ser los documentos apropiados para incluir referencias a políticas y controles de ciberseguridad marítima, tales como (Gómez, 2019):

- Análisis de riesgos de los sistemas informáticos de tecnología de la información.

- Medidas de seguridad preventivas implementadas en el barco y en tierra para mitigar los riesgos en los sistemas de TI a un nivel aceptable.

- Política de seguridad de acceso a Internet que indica restricciones aplicables según las operaciones que se realicen en el barco.

- Política para el uso de medios de almacenamiento extraíbles, como memorias USB, unidades externas, CD y DVD.

- Política y controles de acceso a la red para la tripulación y las redes inalámbricas WiFi.

- Política y procedimientos para actualizar y mantener los sistemas de información y navegación.

- Controles de acceso físicos y lógicos a los diversos sistemas de barcos en función de su nivel de sensibilidad.

- Criterios de autorización para conexiones remotas desde la oficina de la compañía para el monitoreo y mantenimiento del sistema.

- Plan de contingencia para sistemas informáticos de tecnología de la información.

- Procedimientos de gestión de incidentes cibernéticos: detección, notificación, evaluación y decisión, respuesta, recuperación y lecciones aprendidas.

- Capacitación y conocimiento de capitanes, oficiales, ingenieros y tripulación sobre riesgos y controles de ciberseguridad.

Según Gómez (2019), los manuales, procedimientos y listas de verificación de seguridad cibernética deben tener su propia identidad y la documentación de respaldo debe incorporarse en un Manual de seguridad cibernética del buque (MCSEC), el mismo podría derivarse del SSP y SMM como en los siguientes ejemplos:

- La existencia de un plan de contingencia para los sistemas de navegación ECDIS debe estar en el SMM. En caso de que haya una contingencia, los detalles del Plan de Contingencia de los Sistemas de TI, incluido el ECDIS, deben encontrarse en el MCSEC.

- El control de acceso físico a diferentes áreas del barco debe indicarse en el SSP. Los controles de acceso lógico para los sistemas de TI en las diferentes áreas físicas se deben encontrar en el MCSEC.

- Las lecturas de posición del barco en ECDIS no corresponden con las lecturas anteriores de ECDIS o las correcciones visuales actuales que sugieren un mal funcionamiento del sistema o una intercepción deliberada. Además de seguir los procedimientos recomendados por SMM para la navegación segura del barco, se debe consultar el procedimiento de gestión de incidentes cibernéticos MCSEC para evaluar el posible ciberincidente y responder adecuadamente.

Es muy importante darse cuenta de que la definición y documentación del manual y las políticas de MCSEC es solo un primer paso, también es necesario implementar los procedimientos, controles y listas de verificación de ciberseguridad, proporcionar capacitación, realizar pruebas regularmente y verificar los resultados para mejorar, para ello los elementos requeridos por ISPS e ISM podrían interactuar con las políticas y procedimientos de ciberseguridad marítima.

2.3. Definiciones conceptuales

Teniendo en cuenta la complejidad y los diferentes enfoques en la terminología utilizada para discutir los problemas de seguridad cibernética, se necesita un marco rígido de análisis. A continuación, se proporciona una lista de los términos y palabras esenciales utilizados en el esfuerzo de investigación actual.

- **Ciberataques:** Cualquier tipo de maniobra ofensiva dirigida a sistemas de TI y OT, redes de computadoras y / o dispositivos de computadoras personales que

intentan comprometer, destruir o acceder a los sistemas y datos de la compañía y de los barcos (BIMCO, *et. al.,* 2017).

- **Ciberseguridad:** La actividad o proceso, habilidad o capacidad, o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y / o defendidos contra daños, uso o modificación no autorizados, o explotación. (ABS, 2016).

- **Incidente cibernético:** Es una ocurrencia que en realidad que potencialmente da como resultado consecuencias adversas para un sistema, red y computadora a bordo o para la información que procesan, almacenan o transmiten, y que puede requerir una acción de respuesta para mitigar las consecuencias (BIMCO, *et. al.,* 2017).

- **Malware:** Es un término genérico para una variedad de software malicioso que puede infectar sistemas informáticos y afectar su rendimiento (BIMCO, *et. al.,* 2017).

- **Peligro:** Origen, situación o acto con potencial de daño, en términos de lesiones o problemas de salud, daños a la propiedad, daños al entorno laboral o una combinación de estos (ABS, 2016).

- **Riesgo:** Según los diccionarios de Oxford, el riesgo se define como una situación que implica la exposición al peligro, con la posibilidad de que ocurra algo desagradable o inoportuno (Oxforddictionaries, 2018).

- **Tecnología de la información:** La tecnología de la información (TI) es un sector empresarial que se ocupa de la informática, incluido el hardware, el

software, las telecomunicaciones y, en general, todo lo relacionado con la transmisión de información o los sistemas que facilitan la comunicación (Techopedia, 2018).

- **Tecnología operativa:** Incluye dispositivos, sensores, software y redes asociadas que monitorean y controlan los sistemas a bordo (BIMCO, *et. al.,* 2017).

- **Virus:** Es una sección oculta y auto-replicante de software que infecta y manipula maliciosamente el funcionamiento de un programa o sistema informático (BIMCO, *et. al.,* 2017).

- **Vulnerabilidad:** Una debilidad de un activo, o grupo de activos, que puede ser explotada por una o más amenazas (Boyes, *et. al.,* 2016).

CAPÍTULO III: HIPOTESIS Y VARIABLES

3.1. Formulación de la hipótesis

3.1.1. Hipótesis general

Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

3.1.2. Hipótesis específicas

1. Existe un nivel de conocimiento significativo sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.
2. Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

3. Existe un nivel de conocimiento significativo de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

3.1.3. Variables y Dimensiones

Variable: Conocimiento de los riesgos cibernéticos marítimos.

Definición conceptual:

El riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posible, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas. (MSC-FAL, 2017, p.1)

Definición operacional:

Para efectos de la investigación el conocimiento de los riesgos cibernéticos marítimos se mide a través de las dimensiones: equipos y sistemas vulnerables en la empresa naviera, los tipos de amenazas y agentes de un ataque cibernético, y los protocolos de seguridad que deben gestionar la empresa para evitar este riesgo.

Dimensiones:

- Equipos y sistemas vulnerables
- Tipos de amenazas
- Protocolos de seguridad

CAPÍTULO IV: DISEÑO METODOLÓGICO

4.1. Diseño de la investigación

El presente estudio tiene un diseño de investigación no experimental de corte transversal y alcance descriptivo. De acuerdo a Hernández, Fernández y Baptista (2014), la investigación no experimental “son estudios realizados sin cambiar intencionalmente las variables y solo se analizan los fenómenos en su entorno natural para analizarlas” (p.152), en este sentido se establece el nivel de conocimiento de los riesgos cibernéticos en la empresa naviera, directamente de la aplicación del instrumento a los tripulantes.

La recolección de datos se efectuó mediante la aplicación única y directa de un cuestionario, por tal razón es de corte transversal dado que, según Hernández, *et. al.,* (2014), el estudio “tiene la intención de explicar la variable y analizar la incidencia y la relación de manera oportuna. Es como “tomar fotos” de lo que sucede” (p.154).

Es de alcance descriptivo porque se determina el nivel de conocimiento, la investigación que “examinan la incidencia de las propiedades en cuanto al tipo o

nivel de una o muchas variables en la población estudiada, son estudios que se hacen de modo descriptivos" (Hernández, *et. al.,* 2014, p.155)

Bajo esta perspectiva la investigación de diseño no experimental de corte transversal y alcance descriptivo, se explica a través del siguiente diagrama:

Figura 8. Investigación no experimental, transversal de alcance descriptivo.

Dónde: **M:** Muestra de la investigación.

X: Variable: Conocimiento de los riesgos cibernéticos marítimos.

4.2. Población y muestra

Población:

De acuerdo a Hernández, *et. al.,* (2014), "La población o el universo es un conjunto de todos los casos que cumplen requisitos específicos" (p.174).

En este sentido, la población se establece en la flota de la empresa naviera el "ElCano, S.A" España, la cual está constituida por un total de 11 buques, que conforman en su totalidad 272 tripulantes, la cantidad de tripulantes por cada buque se detalla en la siguiente tabla (Ver Tabla 1).

Tabla 1. *Distribución de la población.*

N°	Buque	Cantidad de Tripulantes
1	Castillo de Caldelas	33
2	Castillo de Merida	29
3	Castillo de Villalba	26
4	Castillo de Malpica	24
5	Castillo de Valverde	24
6	Castillo de Catoira	24
7	Castillo de Navia	24
8	Castillo de Artega	23
9	Castillo de Trujillo	23
10	Castillo de Monterreal	23
11	Castillo de Pambre	19
	Total	**272**

Fuente: Empresa Naviera “ElCano, S.A”.

De esta manera la población objeto de estudio se conforma por 272 tripulantes pertenecientes a la flota de 11 buques de la Empresa Naviera el “ElCano, S.A”.

Muestra:

La muestra a decir Hernández *et. al.,* (2014), son “subgrupos del universo o población donde se recopilan datos para luego ser representados” (p.173).

Bajo esta perspectiva la investigación se plantea mediante una muestra de tipo censal, constituida por el universo de estudio en su totalidad, es decir los 272 tripulantes pertenecientes a los 11 Buques de la flota de la Empresa Naviera el “ElCano, S.A” conforman la muestra. En este sentido Ramírez (2007) establece que

la muestra censal es aquella donde todas las unidades de investigación son consideradas como muestra.

4.3. Operacionalización de variables

En la Tabla 2, se presenta la operacionalización de la variable conocimiento de los riesgos cibernéticos marítimos, exponiendo su definición operacional, dimensiones e indicadores que permiten un mejor acercamiento de su análisis.

Tabla 2. *Operacionalización de variables.*

Variables	Definiciones Operacional	Dimensiones	Indicadores	Niveles y Rangos	Escala de Medición
Conocimiento de los riesgos cibernéticos marítimos	Para efectos de la investigación el conocimiento de los riesgos cibernéticos marítimos se mide a través de las dimensiones: equipos y sistemas vulnerables en la empresa naviera, los tipos de amenazas y agentes de un ataque cibernético, y los protocolos de seguridad que deben gestionar la empresa para evitar este riesgo.	- Equipos y sistemas vulnerables.	- Sistemas de información (TI). - Sistemas operacionales (TO). - Equipos electrónicos.	Alto (13-18) Medio (7-12) Bajo (0-6)	Nominal, Dicotómica: Correcto (1) Incorrecto (0)
		- Tipos de amenazas.	- Atacantes. - Softwares informáticos.		
		- Protocolos de seguridad.	- Directrices. - Códigos. - Gestión de la empresa.		

Fuente: Elaboración propia.

4.4. Técnicas e instrumentos para la recolección de datos.

4.4.1. Técnicas

Como técnica se llevó a cabo una encuesta tipo cuestionario, en función de la variable en estudio y las dimensiones planteadas, aplicada a los tripulantes de la empresa naviera para analizar el nivel de conocimiento ante los riesgos cibernéticos marítimos.

Según Parreño (2016), esta técnica se utiliza “para recopilar información; se relaciona íntimamente con la entrevista y el cuestionario, caracterizándose básicamente por recoger información por escrito; por lo tanto, el investigador debe preparar y planificar el cuestionario por escrito y el informante deberá contestar también por escrito” (p.72).

4.4.2. Instrumentos, validez y confiabilidad

Instrumentos

De acuerdo a Hernández, *et. al.,* (2014), un instrumento de medición es el “recurso que utiliza el investigador para registrar información o datos sobre las variables que tiene en mente.” (p.199).

En este sentido, para medir el nivel de conocimientos que tienen los tripulantes en la empresa naviera el “ElCano, S.A” sobre los riesgos cibernéticos marítimos, se utilizó un cuestionario con preguntas orientadas a la variable y sus dimensiones, con opciones de respuesta en selección simple, representando una medida en escala dicotómica, con una codificación: correcta (1) e incorrecta (0); el mismo se compone por 18 preguntas, distribuidas de la siguiente manera:

dimensión, equipos y sistemas vulnerables 6 preguntas; dimensión, tipos de amenazas 5 preguntas; y dimensión, protocolos de seguridad 7 preguntas (Ver Anexo 2).

Los datos recolectados se representan en niveles: alto, medio y bajo, estableciendo de esta manera el nivel de conocimiento de los tripulantes sobre los riesgos cibernéticos marítimos, según las respuestas otorgadas, los mismos se detallan en la Tabla 3.

Tabla 3. *Niveles y rangos de la variable y sus dimensiones.*

Baremos	**Variable**	**Dimensión**		
	Conocimiento de los Riesgos Cibernéticos	**Equipos y sistemas vulnerables**	**Tipos de amenazas**	**Protocolos de seguridad**
Pregunta	1 al 18	1 al 6	7 al 11	12 al 18
Nivel	**Rangos**			
Alto	13 – 18	5 - 6	4 - 5	5 - 7
Medio	7 – 12	3 - 4	2 - 3	3 - 4
Bajo	0 – 6	0 - 2	0 - 1	0 - 2

Fuente: Elaboración propia.

Validez

La validez del instrumento se determinó recurriendo al juicio de expertos, quienes, una vez revisados los mismos y verificada su coherencia con los objetivos de la investigación, la variable y dimensiones definidas, en base a su experiencia estuvieron en la capacidad de certificar si el instrumento es válido, sugiriendo, en caso necesario, ajustes que aporten mayor claridad en la formulación de los mismos, con lo cual se elaboraron las versiones definitivas.

Según Parreño (2016), la validez, “se considera al grado en que un instrumento realmente mida la variable que pretende medir” (p.95).

De acuerdo a lo anteriormente planteado, la Tabla 4 presenta en resumen el juicio considerado por los expertos consultados, respecto a los instrumentos de recolección de datos, los cuales por su experiencia en el área de marítima bien sea académicamente o directamente dentro de una organización, los cataloga como expertos (Ver Anexo 3).

Tabla 4. *Validez del instrumento por juicio de expertos.*

Expertos	Juicio
Dr. Rodríguez Eguizábal José Luis	Aceptable
Cap. Arestizabal Altube Esteban	Aceptable
Cap. Del Monte Sánchez Jorge Francisco	Aceptable
Ing. Dieguez Alberte Andres	Aceptable
Mg. Chafloque Castro John	Aceptable

Fuente: Elaboración propia.

Confiabilidad

De acuerdo a Parreño (2016), la confiabilidad “se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce iguales resultados” (p.95).

Para determinar la confiabilidad del instrumento, se empleó la fórmula de Kuder–Richardson, por contener preguntas de medición dicotómica, determinando el coeficiente mediante el siguiente procedimiento:

- Primero se determinó una muestra piloto de 15 tripulantes.
- Se aplicó el instrumento para determinar la confiabilidad;

- Se procedió a estimar mediante el uso de Microsoft Excel la confiabilidad por la consistencia interna de Kuder–Richardson, por estipular opciones de respuesta dicotómicas en el instrumento.
- Según la bibliografía, se compara el resultado de la confiabilidad con los siguientes criterios:

Tabla 5. *Criterios para evaluar la confiabilidad de los instrumentos.*

Valores	Nivel de Confiabilidad
-1 a 0.24	No es confiable
0.25 a 0.49	Baja confiabilidad
0.5 a 0.75	Media o regular
0.76 a 0.89	Aceptable confiabilidad
0.90 a 1	Elevada confiabilidad

Fuente: Hernández, *et. al.,* (2010, p. 302).

La Tabla 6 muestra el resultado del coeficiente de consistencia interna Kuder–Richardson después de aplicar la prueba piloto para el instrumento Conocimiento de los Riesgos Cibernéticos Marítimos, obteniendo un valor de Kr20 = 0.762, indicando una aceptable confiabilidad del instrumento.

Tabla 6. *Estadística de fiabilidad para las variables comunicación interna y logística de entrada.*

Variable	Kuder–Richardson	N de elementos
Conocimiento de los Riesgos Cibernéticos Marítimos	0.762	18

Fuente: Elaboración propia.

4.5. Técnicas para el procesamiento y análisis de los datos.

La técnica utilizada para el análisis de los datos, se describe mediante las siguientes etapas:

- **Primero,** se realizó una revisión teórica mediante la recopilación de datos de diversas fuentes y la preparación de herramientas de recopilación de datos.
- **Segundo,** se estableció la validez y confiabilidad de los instrumentos, determinando su claridad y consistencia.
- **Tercero,** se aplicó la técnica de recolección de datos a la muestra de estudio.
- **Cuarto,** se tabularon los datos recolectados de forma organizada y sistemáticamente en bases de datos, haciendo uso del software Microsoft Excel y SPSS v.23.
- **Quinto,** se analizaron e interpretaron los datos recolectados, en el análisis descriptivo: Se presentan los resultados por niveles de conocimiento, mediante frecuencias simples y relativas porcentuales; en el análisis inferencial: se determinó la normalidad de los datos a través de la prueba Kolmogorov-Smirnov, para muestras mayores a 50 elementos, lo que permitió elegir para la contrastación de las hipótesis entre una prueba paramétrica (*t de Student* para muestras únicas) o no paramétrica (Chi-cuadrado de ajuste e independencia), el nivel de significancia establecido es de 0,05, rechazando la Ho, Si $p<0,005$, y aceptando la Ho, Si $p>0,005$, con un nivel de confianza del 95%.
- **Sexto,** se realizó la presentación de resultados en tablas y gráficos.
- **Séptimo,** se hizo la generación de conclusiones y recomendaciones en base a los resultados contrastados.

4.6. Aspectos éticos

En esta investigación se respeta la propiedad intelectual de los autores, así mismo la honorabilidad para presentar los datos empleados, haciendo uso adecuado de las citas y referencias bibliográficas, en base a las normativas actuales; planteando las bases teóricas según las normas APA; estructurando y esquematizando el contenido, dispuestos por las normas que dictan la casa de estudio; y respetando el anonimato de los tripulantes consultados.

CAPÍTULO V: RESULTADOS

5.1. Análisis estadístico descriptivo

Variable: Riesgos cibernéticos marítimos

Como objetivo general, al determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, se obtuvieron los siguientes resultados:

Tabla 7. *Nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.*

Nivel de Conocimiento	Frecuencia (fx)	Porcentaje (%)
Alto	86	31.6%
Medio	164	60.3%
Bajo	22	8.1%
Total	**272**	**100.0%**

Fuente: Elaboración propia.

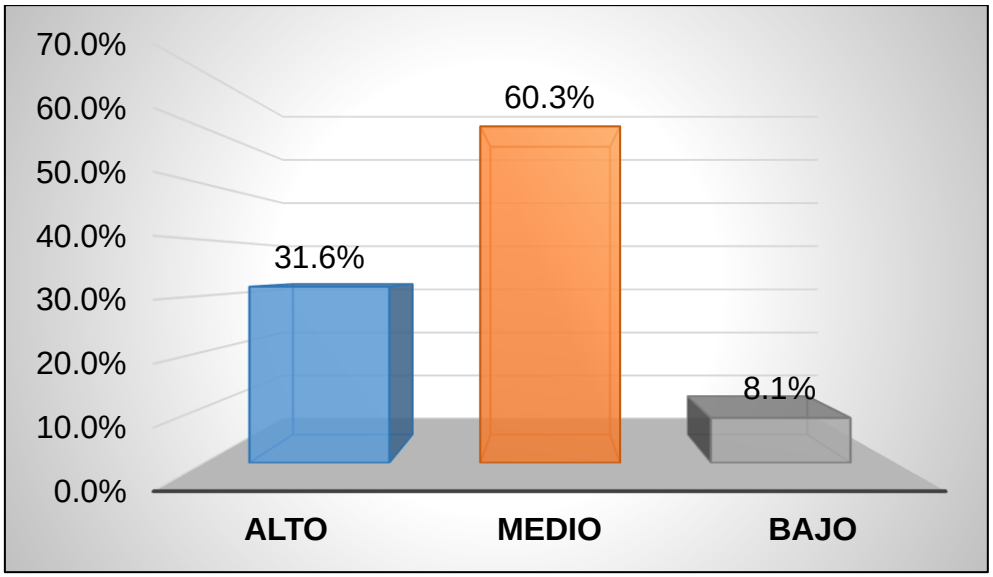


Figura 9. Nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.

En la Tabla 7 y Figura 9, se presentan los resultados del nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, donde se evidencia que del total de tripulantes evaluados, el 60% presenta un nivel medio de conocimiento acerca de los riesgos cibernéticos marítimos persistentes en la empresa naviera, el 32% presenta un nivel alto de conocimiento sobre estos riesgos, y tan solo el 8% de los tripulantes presentan un bajo nivel de conocimiento.

Dimensión: Equipos y sistemas vulnerables

En cuanto al primer objetivo específico, se determinó el nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, presentando los siguientes resultados:

Tabla 8. *Nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A".*

Nivel de Conocimiento	Frecuencia (fx)	Porcentaje (%)
Alto	103	37.9%
Medio	137	50.4%
Bajo	32	11.8%
Total	**272**	**100.0%**

Fuente: Elaboración propia.

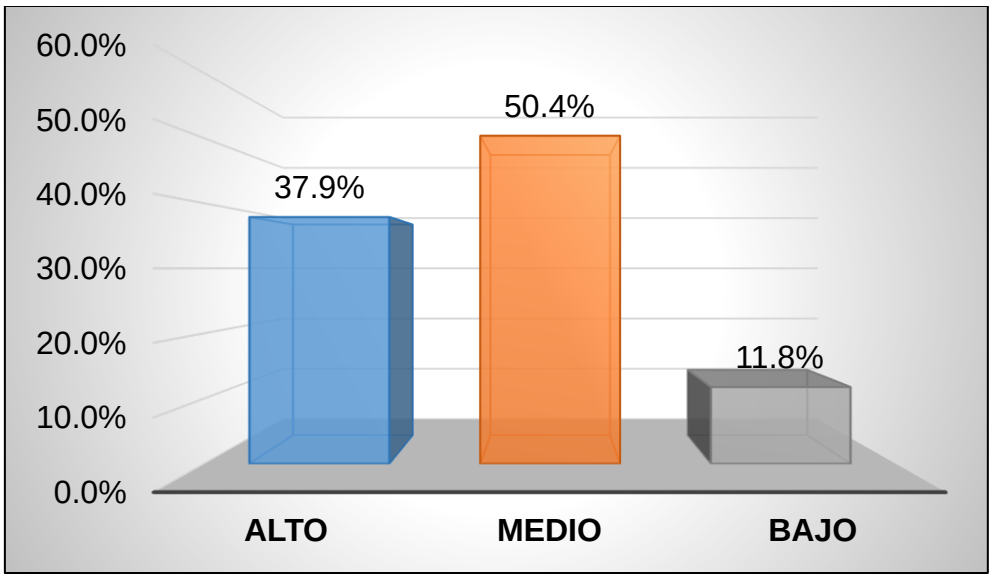


Figura 10. Nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A".

En la Tabla 8 y Figura 10, se presentan los resultados del nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", donde se evidencia que del total de tripulantes evaluados, el 50% presenta un nivel medio de conocimiento de los equipos y sistemas vulnerables a riesgos cibernéticos marítimos, el 38%

presenta un nivel alto de conocimiento sobre estos equipos y sistemas, y tan solo el 12% de los tripulantes presentan un nivel bajo de conocimiento.

Tabla 9. *Resultados a la pregunta 1: ¿Un ataque cibernético al Sistema de Identificación Automática (AIS) puede generar?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	230	85%
Incorrecta	42	15%
Total	**272**	**100%**

Fuente: Elaboración propia.

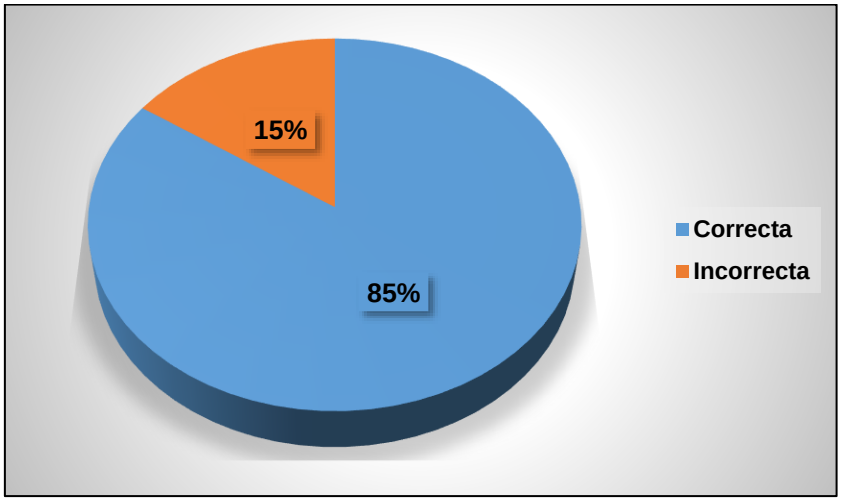


Figura 11. Resultados a la pregunta 1: ¿Un ataque cibernético al Sistema de Identificación Automática (AIS) puede generar?

En la Tabla 9 y Figura 11, se evidencia que el 85% del total de los tripulantes evaluados respondieron correctamente sobre las afecciones que puede generar un ataque cibernético al Sistema de Identificación Automática (AIS), mientras que el 15% desconoce del tema respondiendo incorrectamente.

Tabla 10. *Resultados a la pregunta 2: ¿El Sistema Electrónico de Visualización e Información de Cartas (ECDIS), puede ser afectado cibernéticamente por?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	107	39%
Incorrecta	165	61%
Total	**272**	**100%**

Fuente: Elaboración propia.

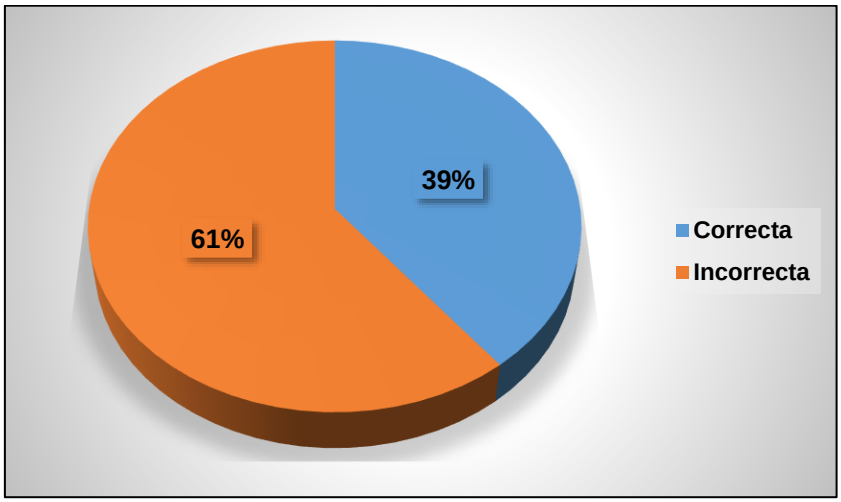


Figura 12. Resultados a la pregunta 2: ¿El Sistema Electrónico de Visualización e Información de Cartas (ECDIS), puede ser afectado cibernéticamente por?

En la Tabla 10 y Figura 12, se evidencia que el 61% del total de los tripulantes evaluados respondieron incorrectamente sobre el porqué el Sistema Electrónico de Visualización e Información de Cartas (ECDIS) puede ser afectado cibernéticamente, mientras que el 39% conoce porque es vulnerable el ECDIS respondiendo correctamente.

Tabla 11. *Resultados a la pregunta 3: ¿Si los operadores de navegación toman medidas que desvíen a la embarcación de su ruta poniendo en riesgo a la tripulación, pueden estar frente a un ataque cibernético al?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	168	62%
Incorrecta	104	38%
Total	**272**	**100%**

Fuente: Elaboración propia.

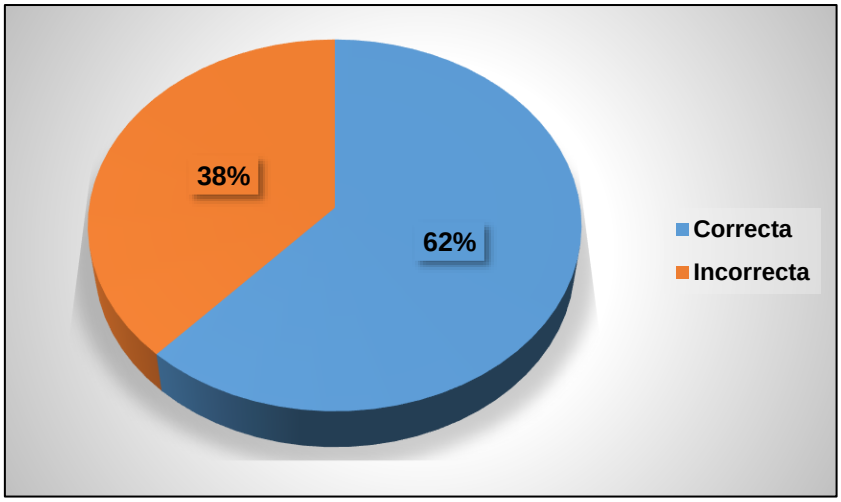


Figura 13. Resultados a la pregunta 3: ¿Si los operadores de navegación toman medidas que desvíen a la embarcación de su ruta poniendo en riesgo a la tripulación, pueden estar frente a un ataque cibernético al?

En la Tabla 11 y Figura 13, se evidencia que el 62% del total de los tripulantes evaluados respondieron correctamente sobre la identificación de un ataque cibernético al Sistema de Posicionamiento Global (GPS), mientras que el 38% no conoce identificar este riesgo al GPS respondiendo incorrectamente.

Tabla 12. *Resultados a la pregunta 4: ¿Cuál de los siguientes sistemas considera usted que son vulnerables ante un ataque cibernético?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	203	75%
Incorrecta	69	25%
Total	**272**	**100%**

Fuente: Elaboración propia.

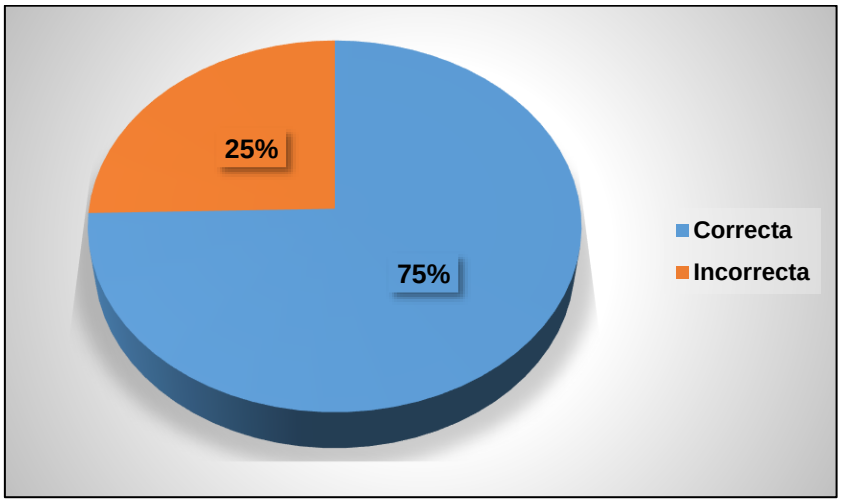


Figura 14. Resultados a la pregunta 4: ¿Cuál de los siguientes sistemas considera usted que son vulnerables ante un ataque cibernético?

En la Tabla 12 y Figura 14, se evidencia que el 75% del total de los tripulantes evaluados respondieron correctamente sobre cuáles son los diferentes sistemas vulnerables ante un ataque cibernético, mientras que el 25% no conoce cuales son los sistemas vulnerables a un ataque cibernético, respondiendo incorrectamente.

Tabla 13. *Resultados a la pregunta 5: ¿Los principales ataques cibernéticos reportados en la industria marítima están enfocados a los equipos?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	171	63%
Incorrecta	101	37%
Total	**272**	**100%**

Fuente: Elaboración propia.

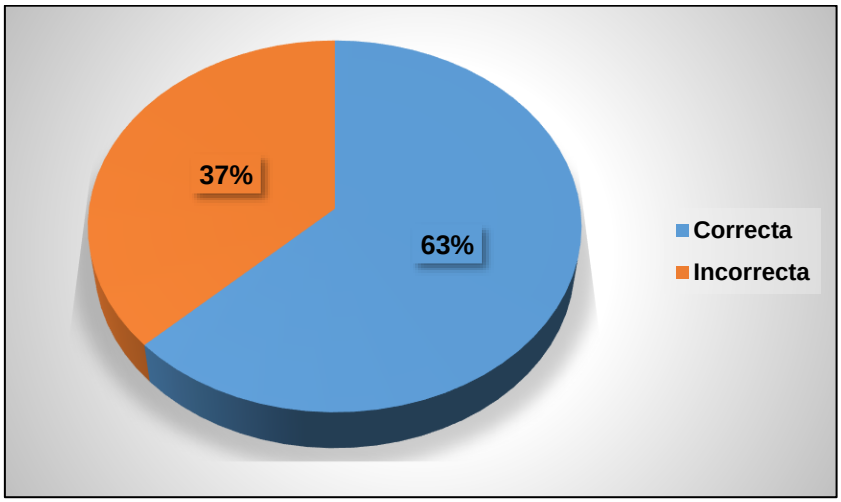


Figura 15. Resultados a la pregunta 5: ¿Los principales ataques cibernéticos reportados en la industria marítima están enfocados a los equipos?

En la Tabla 13 y Figura 15, se evidencia que el 63% del total de los tripulantes evaluados respondieron correctamente sobre los equipos que están principalmente enfocados a ataques cibernéticos reportados en la industria marítima, mientras que el 37% no conoce cuales son los equipos de mayor enfoque a un ataque cibernético, respondiendo incorrectamente.

Tabla 14. *Resultados a la pregunta 6: ¿Si una persona mal intencionada infecta con un virus las computadoras de las consolas de máquina, que fallas ocasionaría?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	171	63%
Incorrecta	101	37%
Total	**272**	**100%**

Fuente: Elaboración propia.

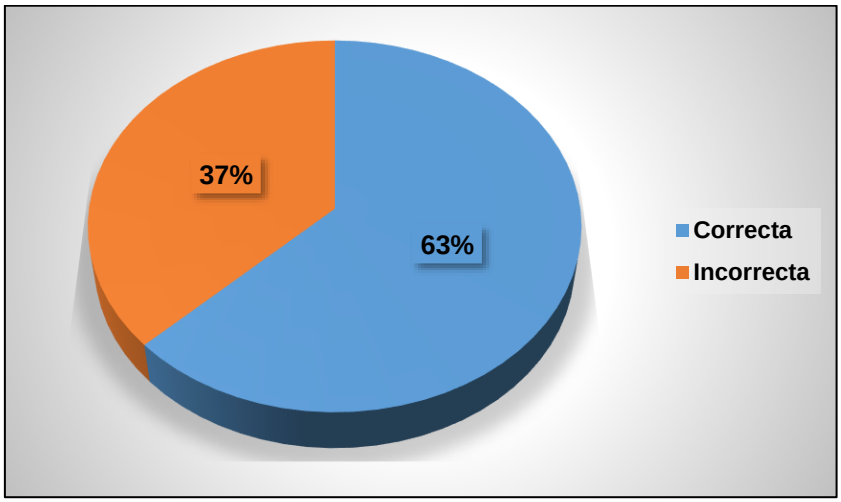


Figura 16. Resultados a la pregunta 6: ¿Si una persona mal intencionada infecta con un virus las computadoras de las consolas de máquina, que fallas ocasionaría?

En la Tabla 14 y Figura 16, se evidencia que el 63% del total de los tripulantes evaluados respondieron correctamente sobre las fallas ocasionadas si se infecta con un virus las computadoras de las consolas de máquina, mientras que el 37% no conoce cuales serían las fallas ocasionadas a estos equipos por un ciberataque, respondiendo incorrectamente.

Dimensión: Tipos de amenazas

Como segundo objetivo específico, se determinó el nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, mostrando los resultados en la siguientes tablas y gráficos:

Tabla 15. *Nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.*

Nivel de Conocimiento	Frecuencia (fx)	Porcentaje (%)
Alto	87	32.0%
Medio	135	49.6%
Bajo	50	18.4%
Total	**272**	**100.0%**

Fuente: Elaboración propia.

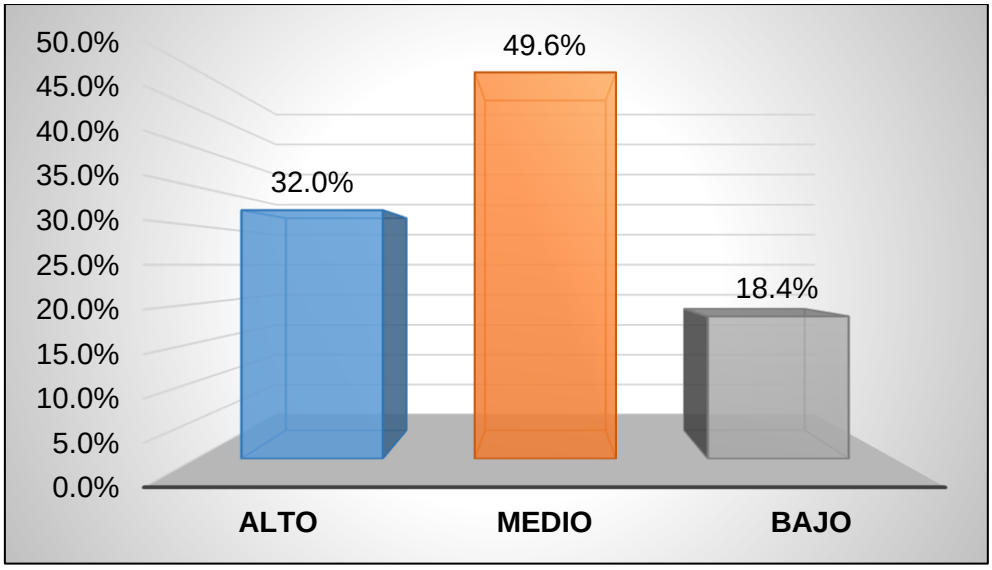


Figura 17. Nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.

En la Tabla 15 y Figura 17, se presentan los resultados del nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, donde se evidencia que del total de tripulantes evaluados, el 50% presenta un nivel medio de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos, el 32% presenta un nivel alto de conocimiento sobre los tipos de amenazas, mientras que el 18% de los tripulantes presentan un nivel bajo de conocimiento.

Tabla 16. *Resultados a la pregunta 7: ¿En un ataque cibernético donde el atacante encripta los datos, secuestrando los sistemas y la información para solicitar que paguen un rescate, se debe a una amenaza informática de tipo?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	144	53%
Incorrecta	128	47%
Total	**272**	**100%**

Fuente: Elaboración propia.

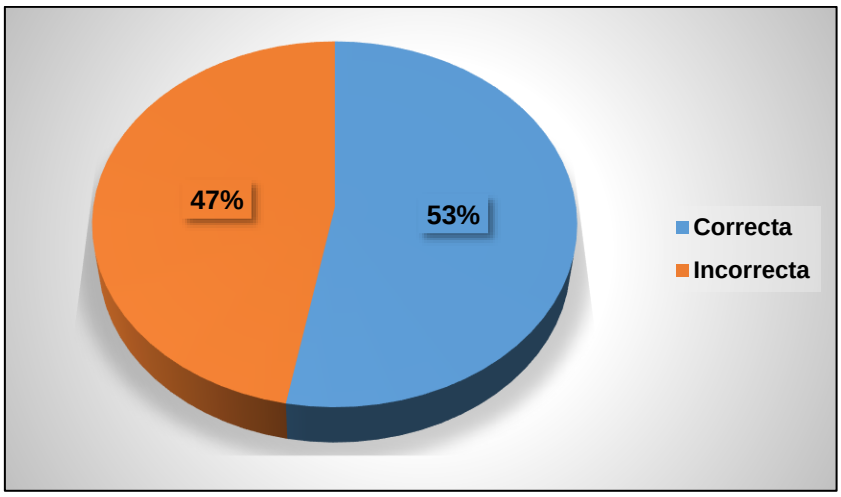


Figura 18. Resultados a la pregunta 7: ¿En un ataque cibernético donde el atacante encripta los datos, secuestrando los sistemas y la información para solicitar que paguen un rescate, se debe a una amenaza informática de tipo?

En la Tabla 16 y Figura 18, se evidencia que el 53% del total de los tripulantes evaluados respondieron correctamente al identificar un ataque informático de tipo Ransomware, mientras que el 47% no conoce cómo identificar este tipo de ataque, respondiendo incorrectamente.

Tabla 17. *Resultados a la pregunta 8: ¿En la empresa naviera los ciberatacantes pueden infiltrarse, dañar y causar acciones autenticadas y no deseadas en los sistemas de información mediante?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	162	60%
Incorrecta	110	40%
Total	**272**	**100%**

Fuente: Elaboración propia.

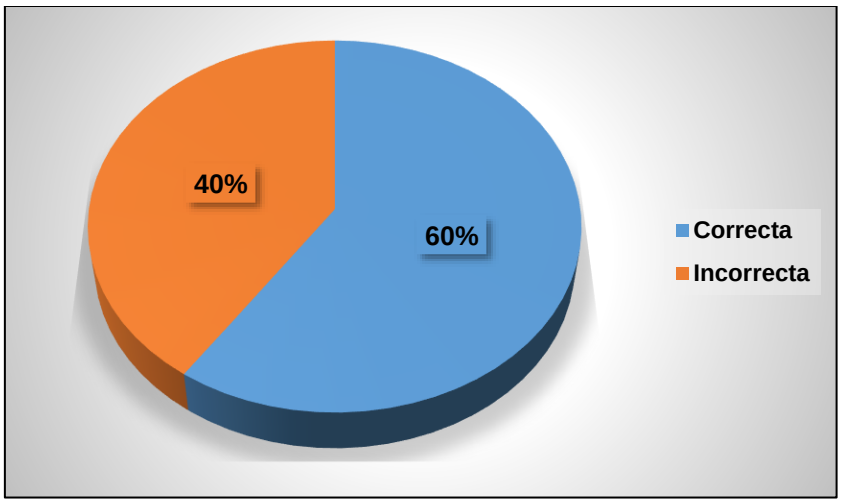


Figura 19. Resultados a la pregunta 8: ¿En la empresa naviera los ciberatacantes pueden infiltrarse, dañar y causar acciones autenticadas y no deseadas en los sistemas de información mediante?

En la Tabla 17 y Figura 19, se evidencia que el 60% del total de los tripulantes evaluados respondieron correctamente sobre las acciones y daños que pueden

ocasionar los ciberatacantes al infiltrar un virus o software malicioso, mientras que el 40% no conoce cómo sobre estas acciones y daños, respondiendo incorrectamente.

Tabla 18. *Resultados a la pregunta 9: ¿Los ataques cibernéticos mediante phishing permiten a los ciberatacantes generar en una empresa naviera?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	78	29%
Incorrecta	194	71%
Total	**272**	**100%**

Fuente: Elaboración propia.

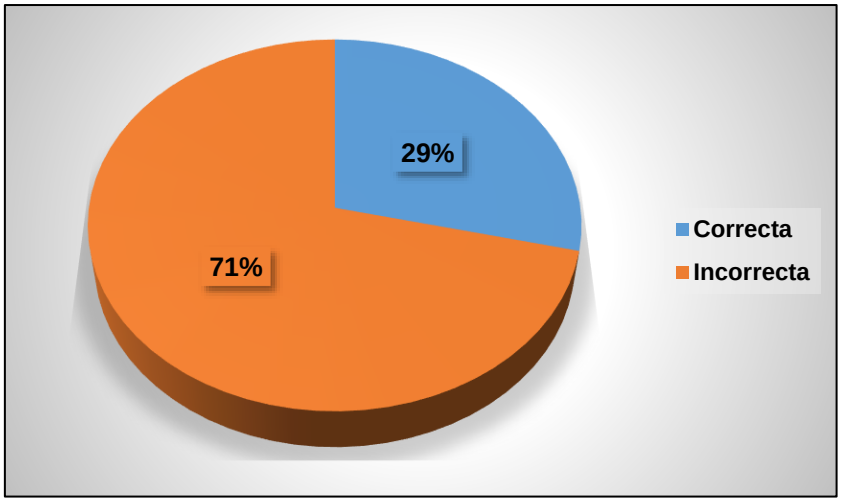


Figura 20. Resultados a la pregunta 9: ¿Los ataques cibernéticos mediante phishing permiten a los ciberatacantes generar en una empresa naviera?

En la Tabla 18 y Figura 20, se evidencia que el 71% del total de los tripulantes evaluados no conocen lo que puede generar un ataque cibernético mediante phishing a la empresa naviera, respondiendo incorrectamente, mientras que el 39% respondiendo correctamente sobre lo que puede generar este tipo de ataque.

Tabla 19. *Resultados a la pregunta 10: ¿Los tripulantes de un barco pueden comprometer los sistemas de la industria marítima ante un riesgo cibernético?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	176	65%
Incorrecta	96	35%
Total	**272**	**100%**

Fuente: Elaboración propia.

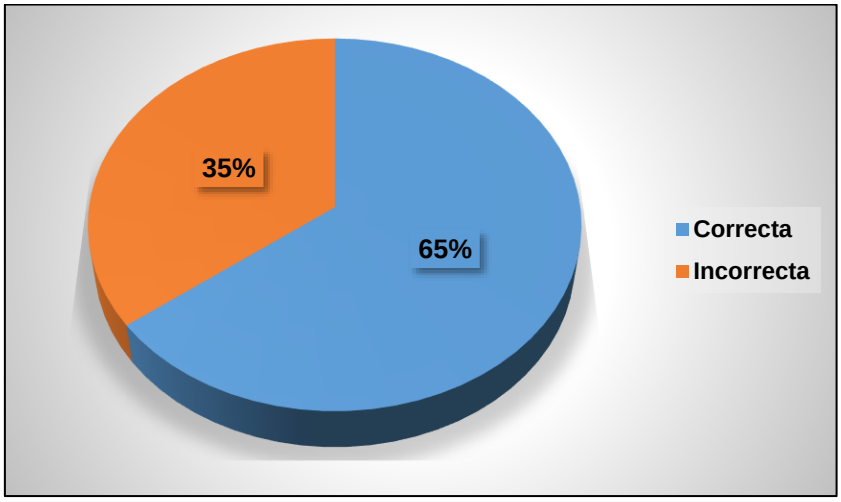


Figura 21. Resultados a la pregunta 10: ¿Los tripulantes de un barco pueden comprometer los sistemas de la industria marítima ante un riesgo cibernético?

En la Tabla 19 y Figura 21, se evidencia que el 65% del total de los tripulantes evaluados reconocen bajo qué acciones ellos pueden comprometer los sistemas de la industria marítima ante un riesgo cibernético, respondiendo correctamente, mientras que el 25% no conocen estas acciones, respondiendo incorrectamente.

Tabla 20. *Resultados a la pregunta 11: ¿En la empresa naviera se pueden generar atacantes cibernéticos que ponen en peligro la seguridad de las embarcaciones y sus tripulantes, motivados por?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	151	56%
Incorrecta	121	44%
Total	**272**	**100%**

Fuente: Elaboración propia.

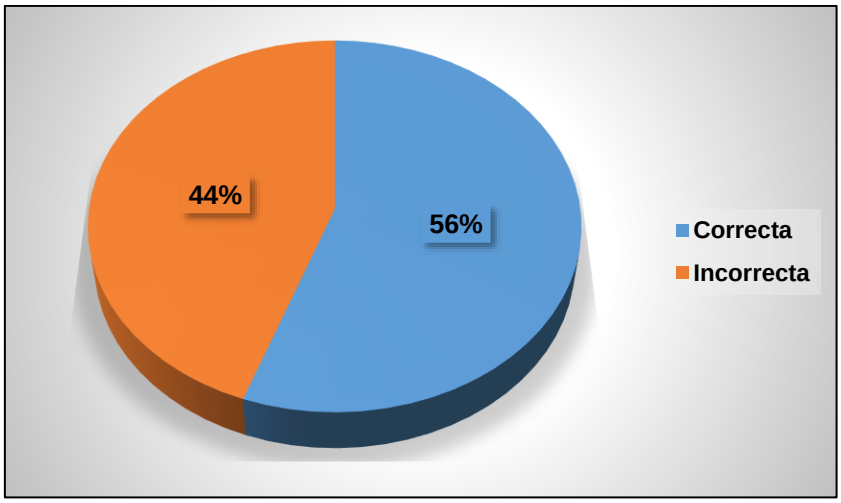


Figura 22. Resultados a la pregunta 11: ¿En la empresa naviera se pueden generar atacantes cibernéticos que ponen en peligro la seguridad de las embarcaciones y sus tripulantes, motivados por?

En la Tabla 20 y Figura 22, se evidencia que el 56% del total de los tripulantes evaluados saben cuáles son los motivos que podrían generar un ataque cibernético a la empresa naviera, respondiendo correctamente, mientras que el 44% no reconoce estos motivos, respondiendo incorrectamente.

Dimensión: Protocolos de seguridad

En el tercer objetivo específico, al determinar el nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, se obtuvieron los siguientes resultados:

Tabla 21. *Nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.*

Nivel de Conocimiento	Frecuencia (fx)	Porcentaje (%)
Alto	130	47.8%
Medio	109	40.1%
Bajo	33	12.1%
Total	**272**	**100.0%**

Fuente: Elaboración propia.

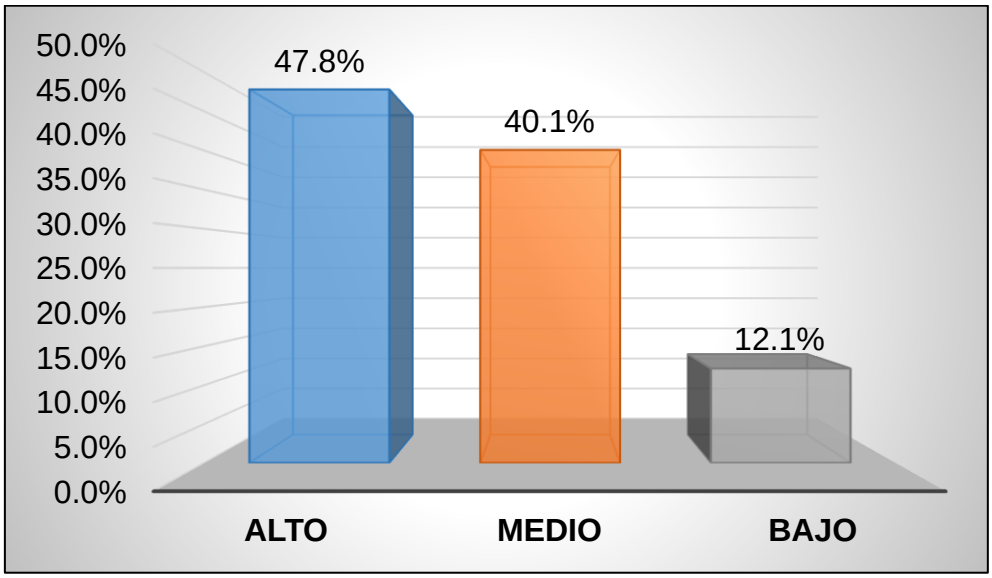


Figura 23. Nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”.

En la Tabla 21 y Figura 23, se presentan los resultados del nivel de conocimiento acerca de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, evidenciando que del total de tripulantes evaluados, el 48% presenta un nivel alto de conocimiento acerca de los protocolos de seguridad para abordar los riesgos cibernéticos marítimos, el 40% presenta un nivel medio de conocimiento sobre los protocolos de seguridad, mientras que el 12% de los tripulantes presentan un nivel bajo de conocimiento.

Tabla 22. *Resultados a la pregunta 12: ¿La empresa naviera para atender un ataque cibernético y garantizar la operatividad de la embarcación, debe contar con?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	157	58%
Incorrecta	115	42%
Total	**272**	**100%**

Fuente: Elaboración propia.

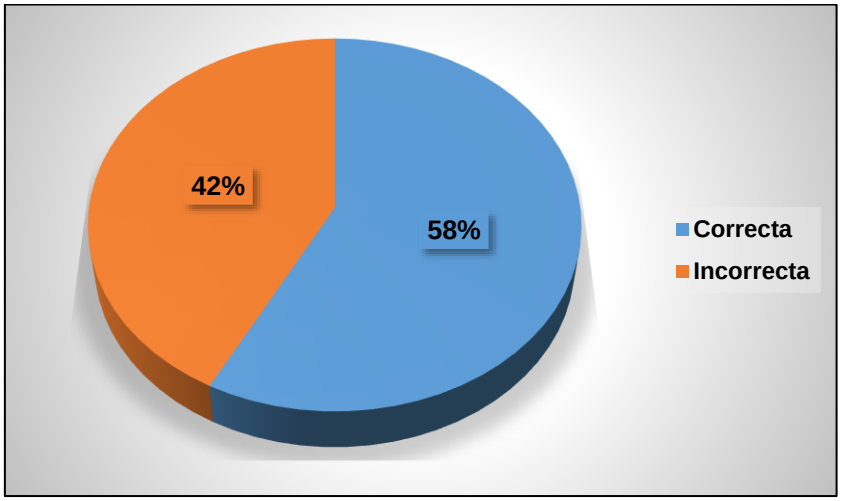


Figura 24. Resultados a la pregunta 12: ¿La empresa naviera para atender un ataque cibernético y garantizar la operatividad de la embarcación, debe contar con?

En la Tabla 22 y Figura 24, se evidencia que el 58% del total de los tripulantes evaluados saben qué un equipo de emergencia cibernética interna y externa es una medida que debe tomar la empresa naviera para atender un ataque cibernético y garantizar la operatividad de la embarcación, respondiendo correctamente, mientras que el 42% no reconoce estas medidas, respondiendo incorrectamente.

Tabla 23. *Resultados a la pregunta 13: ¿Para prevenir y abordar automáticamente la presencia de amenazas / actividades maliciosas en los sistemas a bordo, se deben?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	147	54%
Incorrecta	125	46%
Total	**272**	**100%**

Fuente: Elaboración propia.

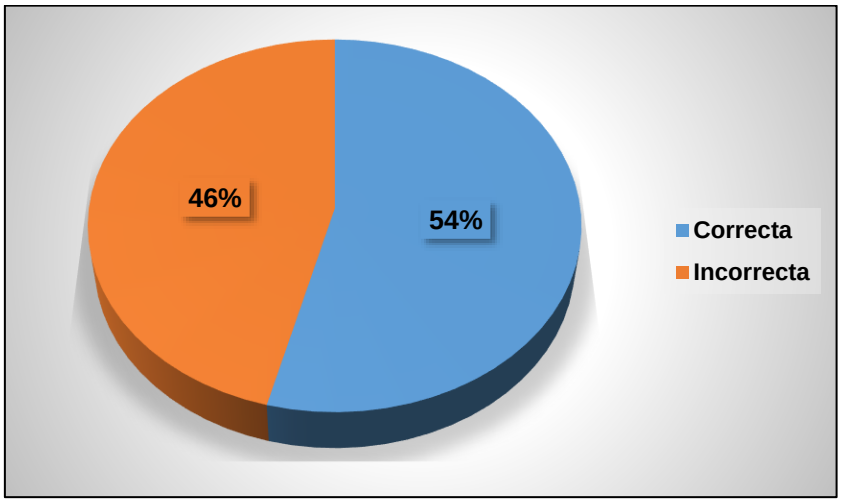


Figura 25. Resultados a la pregunta 13: ¿Para prevenir y abordar automáticamente la presencia de amenazas / actividades maliciosas en los sistemas a bordo, se deben?

En la Tabla 23 y Figura 25, se evidencia que el 54% del total de los tripulantes evaluados saben qué la instalación en la empresa de un software de escaneo informático permite prevenir y abordar automáticamente la presencia de amenazas / actividades maliciosas en los sistemas a bordo, respondiendo correctamente, mientras que el 46% no reconoce esta medida de seguridad, respondiendo incorrectamente.

Tabla 24. *Resultados a la pregunta 14: ¿Cómo medida de seguridad ante un ataque cibernético, en la embarcación debe existir la provisión de un medio alternativo de comunicación, que funcione independientemente de todos los demás sistemas de a bordo?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	168	62%
Incorrecta	104	38%
Total	**272**	**100%**

Fuente: Elaboración propia.

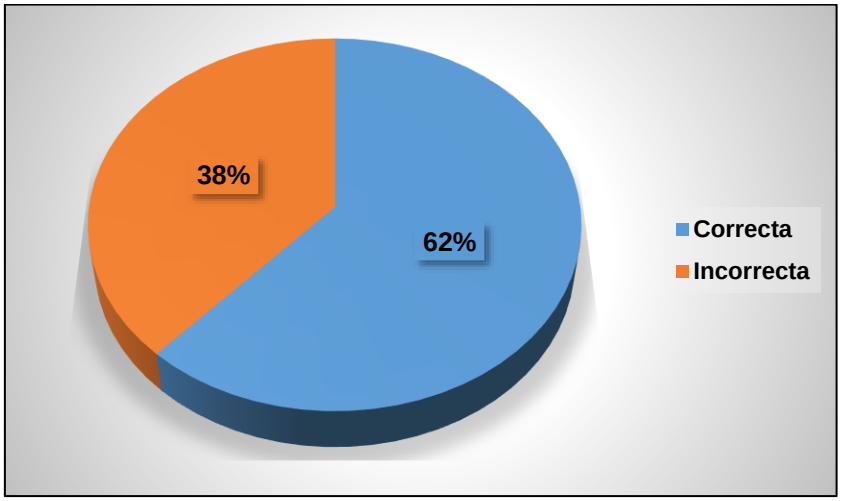


Figura 26. Resultados a la pregunta 14: ¿Cómo medida de seguridad ante un ataque cibernético, en la embarcación debe existir la provisión de un medio

alternativo de comunicación, que funcione independientemente de todos los demás sistemas de a bordo?

En la Tabla 24 y Figura 26, se evidencia que el 62% del total de los tripulantes evaluados están de acuerdo que en la embarcación como medida de seguridad ante un ataque cibernético debe existir la provisión de un medio alternativo de comunicación, que funcione independientemente de todos los demás sistemas de a bordo, mientras que el 38% no está de acuerdo o desconoce esta medida.

Tabla 25. *Resultados a la pregunta 15: ¿Cómo protocolo de seguridad todos los tripulantes de la embarcación?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	250	92%
Incorrecta	22	8%
Total	**272**	**100%**

Fuente: Elaboración propia.

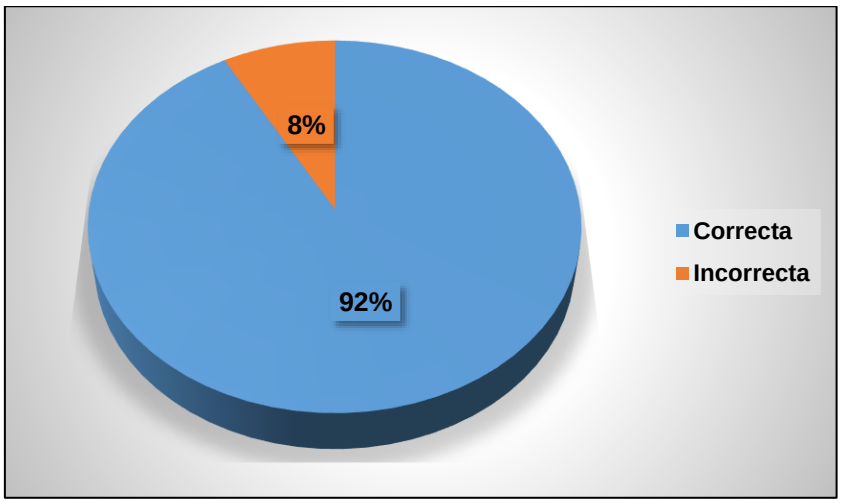


Figura 27. Resultados a la pregunta 15: ¿Cómo protocolo de seguridad todos los tripulantes de la embarcación?

En la Tabla 25 y Figura 27, se evidencia que el 92% del total de los tripulantes evaluados reconocen como protocolo de seguridad que todos deben tener capacitación básica sobre los riesgos cibernéticos, vulnerabilidades de los equipos y medidas preventivas, mientras que el 8% no reconoce esta medida, respondiendo incorrectamente.

Tabla 26. *Resultados a la pregunta 16: ¿Las regulaciones para abordar los problemas de seguridad cibernética, estipulan directrices orientadas a?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	200	74%
Incorrecta	72	26%
Total	**272**	**100%**

Fuente: Elaboración propia.

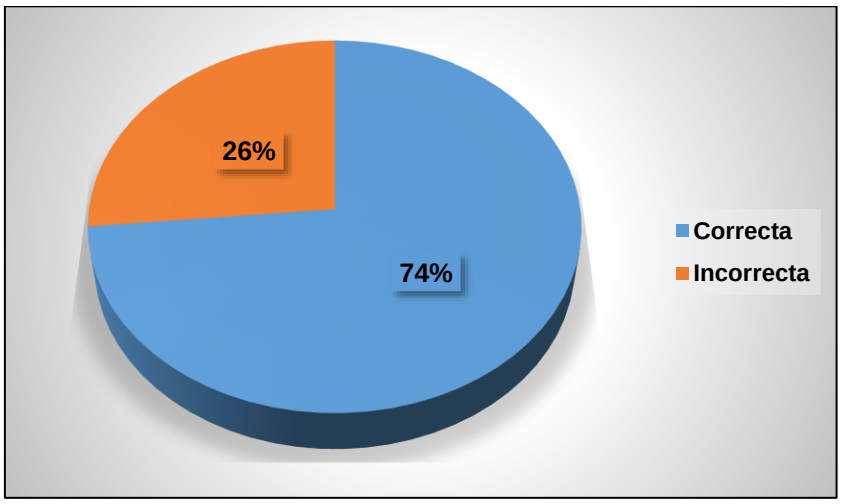


Figura 28. Resultados a la pregunta 16: ¿Las regulaciones para abordar los problemas de seguridad cibernética, estipulan directrices orientadas a?

En la Tabla 26 y Figura 28, se evidencia que el 74% del total de los tripulantes evaluados conocen cuales son las directrices en las regulaciones para abordar los

problemas de seguridad cibernética, mientras que el 26% no conoce estas directrices, respondiendo incorrectamente.

Tabla 27. *Resultados a la pregunta 17: ¿Cuál de las siguientes normativas regulan la gestión ante los riesgos cibernéticos en una empresa naviera?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	173	64%
Incorrecta	99	36%
Total	**272**	**100%**

Fuente: Elaboración propia.

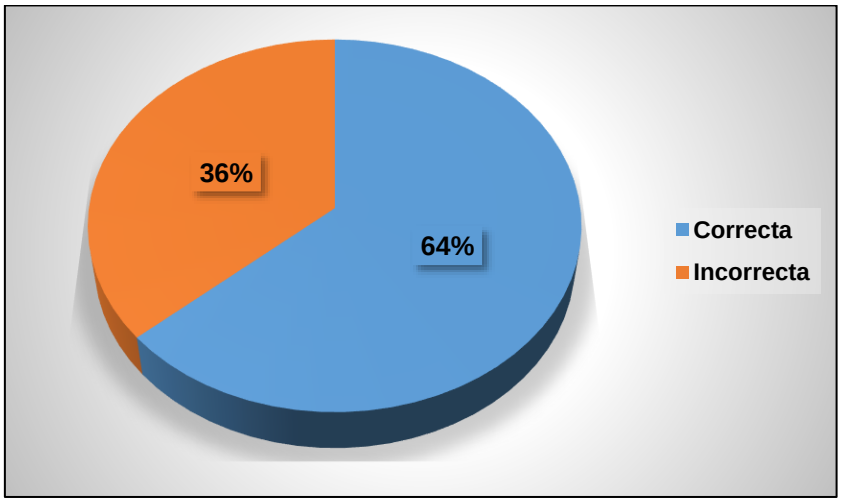


Figura 29. Resultados a la pregunta 17: ¿Cuál de las siguientes normativas regulan la gestión ante los riesgos cibernéticos en una empresa naviera?

En la Tabla 27 y Figura 29, se evidencia que el 64% del total de los tripulantes evaluados conocen cuales son las normativas regulan la gestión ante los riesgos cibernéticos en una empresa naviera, mientras que el 36% no conoce estas normativas, respondiendo incorrectamente.

Tabla 28. *Resultados a la pregunta 18: ¿Hasta cuándo la OMI otorgó a los propietarios y gerentes de buques incorporar la gestión del riesgo cibernético en el sistema de seguridad del buque?*

Respuesta	Frecuencia (fx)	Porcentaje (%)
Correcta	84	31%
Incorrecta	188	69%
Total	**272**	**100%**

Fuente: Elaboración propia.

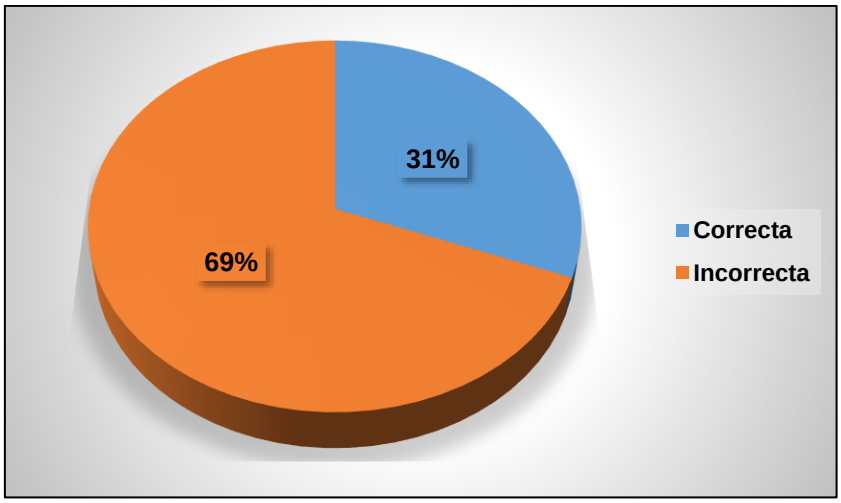


Figura 30. Resultados a la pregunta 18: ¿Hasta cuándo la OMI otorgó a los propietarios y gerentes de buques incorporar la gestión del riesgo cibernético en el sistema de seguridad del buque?

En la Tabla 28 y Figura 30, se evidencia que el 69% del total de los tripulantes evaluados no conocen a partir de cuándo la OMI otorgó a los propietarios y gerentes de buques incorporar la gestión del riesgo cibernético en el sistema de seguridad del buque, mientras que el 31% si conoce a partir de cuándo deben incorporar la gestión del riesgo cibernético en el sistema de seguridad del buque, respondiendo correctamente.

5.2. Análisis estadístico inferencial

5.2.1. Prueba estadística para la determinación de la normalidad

La prueba de normalidad se establece a través del estadístico Kolmogorov-Smirnov prueba utilizada para determinar si los datos provienen de una distribución teórica específica, en muestras mayores a 50 elementos, con la finalidad de elegir para la contrastación de las hipótesis entre una prueba paramétrica (*t de Student para muestras únicas*) o no paramétrica (*Chi- cuadrado de ajuste e independencia*).

Su contrastación se realiza mediante la siguiente hipótesis de trabajo:

Ho: Los datos de la variable riesgos cibernéticos marítimos y sus dimensiones tienen una distribución normal.

Ha: Los datos de la variable riesgos cibernéticos marítimos y sus dimensiones no tienen una distribución normal.

Tabla 29. *Resultados de la prueba de normalidad para la variable riesgos cibernéticos marítimos y sus dimensiones.*

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Equipos y sistemas vulnerables	,276	272	,000
Tipos de amenazas	,257	272	,000
Protocolos de seguridad	,303	272	,000
Riesgos Cibernéticos	,340	272	,000

a. Corrección de significación de Lilliefors

En la Tabla 29, se presentan los resultados de la prueba de normalidad para la variable riesgos cibernéticos marítimos y sus dimensiones, evidenciando un p valor= 0,000 asociado al estadístico Kolmogorov-Smirnov tanto para la variable como sus dimensiones, menor al nivel de significancia establecido en la

investigación (p<0,05), por tanto, se rechaza la **Ho** y se acepta la **Ha**, es decir los datos de la variable riesgos cibernéticos marítimos y sus dimensiones no tienen una distribución normal, de acuerdo a estos resultados la contrastación de hipótesis se realizará mediante la prueba no paramétrica Chi- cuadrado de ajuste e independencia.

5.2.2. Prueba de hipótesis general

La prueba de hipótesis general se efectúa mediante el siguiente enunciado:

Ha: Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Ho: No Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Tabla 30. *Frecuencias observadas y esperadas para la variable conocimiento de los riesgos cibernéticos marítimos.*

	N observado	N esperada	Residuo
Bajo	22	45,3	-23,3
Medio	164	90,7	73,3
Alto	86	136,0	-50,0
Total	272		

Fuente: SPSS v23.

En la Tabla 30, se evidencia la probabilidad de los valores esperados según la distribución de la variable, esperando en el conocimiento de riesgos cibernéticos un valor para el nivel alto de 136 tripulantes, con una diferencia en cuanto a lo observado de menos 50 tripulantes, para el nivel medio se esperaba un valor de 90,7 tripulantes, con una diferencia en comparación a lo observado de más 73,3 tripulantes y en cuanto al nivel bajo de conocimiento se esperaba un valor de 45,3 tripulantes con una diferencia en cuanto a lo observado de menos 23,3 tripulantes.

Tabla 31. *Estadístico de la prueba Chi-cuadrado para la variable riesgos cibernéticos marítimos.*

	Riesgos Cibernéticos
Chi-cuadrado	89,706[a]
gl	2
Sig. asintótica	,000

a. 0 casillas (0,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 45,3.

En la Tabla 31, se presentan los resultados del estadístico de la prueba Chi-cuadrado para la variable riesgos cibernéticos marítimos, observando un p valor= 0,000 asociado a la prueba, menor al nivel de significancia establecido en la investigación ($p<0,05$), por tanto, se rechaza la hipótesis nula (**Ho**) y se acepta la hipótesis planteada en la investigación (**Ha**), concluyendo que: Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima – 2020, es decir no existe variación de los conocimientos probabilísticamente esperados en los tripulantes.

5.2.3. Prueba de hipótesis específica 1

La prueba de la primera hipótesis específica, se efectúa mediante el siguiente enunciado:

H_1: Existe un nivel de conocimiento significativo sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Ho: No Existe un nivel de conocimiento significativo sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Tabla 32. *Frecuencias observadas y esperadas sobre el conocimiento de los equipos y sistemas vulnerables a riesgos cibernéticos marítimos.*

	N observado	N esperada	Residuo
Bajo	32	45,3	-13,3
Medio	137	90,7	46,3
Alto	103	136,0	-33,0
Total	272		

Fuente: SPSS v23.

En la Tabla 32, se evidencia la probabilidad de los valores esperados según la distribución de la variable, esperando en el conocimiento de los equipos y sistemas vulnerables a riesgos cibernéticos marítimos un valor para el nivel alto de 136 tripulantes, con una diferencia en cuanto a lo observado de menos 33 tripulantes, para el nivel medio se esperaba un valor de 90,7 tripulantes, con una diferencia en comparación a lo observado de más 46,3 tripulantes y en cuanto al

nivel bajo de conocimiento se esperaba un valor de 45,3 tripulantes con una diferencia en cuanto a lo observado de menos 13,3 tripulantes.

Tabla 33. *Estadístico de la prueba Chi-cuadrado para la dimensión equipos y sistemas vulnerables a riesgos cibernéticos marítimos.*

	Equipos y sistemas vulnerables
Chi-cuadrado	35,607[a]
gl	2
Sig. asintótica	,000

a. 0 casillas (0,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 45,3.

En la Tabla 33, se presentan los resultados del estadístico de la prueba Chi-cuadrado para la dimensión equipos y sistemas vulnerables a riesgos cibernéticos marítimos, observando un p valor= 0,000 asociado a la prueba, menor al nivel de significancia establecido en la investigación ($p<0,05$), por tanto, se rechaza la hipótesis nula (**Ho**) y se acepta la primera hipótesis específica planteada en la investigación (**H_1**), concluyendo que: Existe un nivel de conocimiento significativo sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020, es decir no existe variación de los conocimientos probabilísticamente esperados en los tripulantes.

5.2.4. Prueba de hipótesis específica 2

La prueba de la segunda hipótesis específica, se efectúa mediante el siguiente enunciado:

H_2: Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Ho: No Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Tabla 34. *Frecuencias observadas y esperadas acerca del conocimiento de los tipos de amenazas de riesgos cibernéticos marítimos.*

	N observado	N esperada	Residuo
Bajo	50	45,3	4,7
Medio	135	90,7	44,3
Alto	87	136,0	-49,0
Total	272		

Fuente: SPSS v23.

En la Tabla 34, se evidencia la probabilidad de los valores esperados según la distribución de la variable, esperando en el conocimiento de los tipos de amenazas de riesgos cibernéticos marítimos un valor para el nivel alto de 136 tripulantes, con una diferencia en cuanto a lo observado de menos 49 tripulantes, para el nivel medio se esperaba un valor de 90,7 tripulantes, con una diferencia en comparación a lo observado de más 44,3 tripulantes y en cuanto al nivel bajo de conocimiento se esperaba un valor de 45,3 tripulantes con una diferencia en cuanto a lo observado de más 4,7 tripulantes.

Tabla 35. *Estadístico de la prueba Chi-cuadrado para la dimensión tipos de amenazas de riesgos cibernéticos marítimos.*

	Tipos de amenazas
Chi-cuadrado	39,813[a]
gl	2
Sig. asintótica	,000

a. 0 casillas (0,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 45,3.

En la Tabla 35, se presentan los resultados del estadístico de la prueba Chi-cuadrado para la dimensión tipos de amenazas de riesgos cibernéticos marítimos, observando un p valor= 0,000 asociado a la prueba, menor al nivel de significancia establecido en la investigación (p<0,05), por tanto, se rechaza la hipótesis nula (**Ho**) y se acepta la segunda hipótesis específica planteada en la investigación (**H_2**), concluyendo que: Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020, es decir no existe variación de los conocimientos probabilísticamente esperados en los tripulantes.

5.2.5. Prueba de hipótesis específica 3

La prueba de la tercera hipótesis específica, se efectúa mediante el siguiente enunciado:

H_3: Existe un nivel de conocimiento significativo de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Ho: No Existe un nivel de conocimiento significativo de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.

Tabla 36. *Frecuencias observadas y esperadas acerca del conocimiento de los protocolos de seguridad ante riesgos cibernéticos marítimos.*

	N observado	N esperada	Residuo
Bajo	33	45,3	-12,3
Medio	109	90,7	18,3
Alto	130	136,0	-6,0
Total	272		

Fuente: SPSS v23.

En la Tabla 36, se evidencia la probabilidad de los valores esperados según la distribución de la variable, esperando en el conocimiento de los protocolos de seguridad ante riesgos cibernéticos marítimos un valor para el nivel alto de 136 tripulantes, con una diferencia en cuanto a lo observado de menos 6 tripulantes, para el nivel medio se esperaba un valor de 90,7 tripulantes, con una diferencia en comparación a lo observado de más 18,3 tripulantes y en cuanto al nivel bajo de conocimiento se esperaba un valor de 45,3 tripulantes con una diferencia en cuanto a lo observado de menos 12,3 tripulantes.

Tabla 37. *Estadístico de la prueba Chi-cuadrado para la dimensión protocolos de seguridad ante riesgos cibernéticos marítimos.*

	Protocolos de seguridad
Chi-cuadrado	7,327[a]
gl	2
Sig. asintótica	,026

a. 0 casillas (0,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 45,3.

En la Tabla 37, se presentan los resultados del estadístico de la prueba Chi-cuadrado para la dimensión protocolos de seguridad ante riesgos cibernéticos marítimos, observando un p valor= 0,026 asociado a la prueba, menor al nivel de significancia establecido en la investigación (p<0,05), por tanto, se rechaza la hipótesis nula (**Ho**) y se acepta la tercera hipótesis específica planteada en la investigación (**H_3**), concluyendo que: Existe un nivel de conocimiento significativo de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020, es decir no existe variación de los conocimientos probabilísticamente esperados en los tripulantes.

CAPÍTULO VI: DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

6.1. Discusión

De acuerdo al objetivo general planteado en la investigación, al determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, los resultados obtenidos en la investigación muestran que el 60% de los tripulantes presenta un nivel medio de conocimiento de los riesgos cibernéticos marítimos presentes en la empresa, el 32% presenta un nivel alto de conocimiento sobre estos riesgos, y tan solo el 8% de los tripulantes presentan un nivel bajo de conocimiento, valores que al contrastar con la probabilidad de los valores esperados según la prueba estadística de Chi-cuadrado, se obtuvo un p valor= 0,000 asociado a la prueba, menor al nivel de significancia establecido en la investigación ($p<0,05$), lo que conllevo al rechazo de la hipótesis nula y la aceptación de la hipótesis planteada en la investigación, comprobando que Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, es decir

no existe variación de los conocimientos probabilísticamente esperados sobre riesgos cibernéticos marítimos en los tripulantes.

Los resultados expuestos dan cuenta que la mayoría de los tripulantes que integran la flota de la empresa naviera “ElCano, S.A”, tienen una cultura preventiva que permita mitigar los riesgos cibernéticos que se puedan generar en la empresa, comprendida en el uso adecuado de los equipos electrónicos personales, concientización y conocimiento de los riesgos de infección al sistemas y equipos críticos por virus informáticos, previniendo la apertura de correos y páginas web con agentes maliciosos que exponga la funcionalidad de los equipos y sistemas, y ponga en peligro a toda la tripulación, en este sentido los tripulantes son conscientes y conocen los acontecimientos actuales y las nuevas amenazas que atentan contra el sector marítimo, bajo esta perspectiva Crawford (2019), en su investigación señala que los ataques al ciberespacio marítimo, son un hecho real, que se han registrado durante los últimos años, derivado del aumento de los sistemas críticos a bordo que impulsan las amenazas cibernéticas, bajo esta situación se han gestionado directrices que permitan minimizar estos ataques, más sin embargo Ahokas (2018), en los resultados de su investigación muestran que ha aumentado la conciencia dentro del sector marítimo, pero aún se producen algunas diferencias entre los diferentes operadores marítimos en términos de comprensión de los factores de ciberseguridad, se han tomado medidas para mejorar la ciberseguridad, pero aún existe una gran necesidad de estándares para toda la industria y una coordinación práctica de nivel.

Cabe destacar que un adecuado conocimiento sobre las vulnerabilidades de los equipos y sistemas, las amenazas cibernéticas que atentan contra la industria

marítima y los mecanismos de seguridad para prevenir esta situación, se constituye como una fortaleza para evitar un riesgo cibernético en la empresa, dado que “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”. (MSC-FAL, 2017, p.1)

En cuanto al primer objetivo planteado, sobre determinar el nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, los hallazgos obtenidos en la investigación evidencian que el 50% de los tripulantes presenta un nivel medio de conocimiento de los equipos y sistemas vulnerables a riesgos cibernéticos marítimos, el 38% presenta un alto nivel de conocimiento sobre estos equipos y sistemas, y tan solo el 12% de los tripulantes presentan un nivel bajo de conocimiento, valores que al comparar con parámetros probabilísticos obtenidos por la prueba Chi-cuadrado, ofrecen un nivel de significancia p valor= 0,000 asociado a la prueba, menor al establecido en la investigación ($p<0,05$), lo que conllevo al rechazo de la hipótesis nula y la aceptación de la primera hipótesis específica planteada en la investigación, evidenciando a nivel inferencial que Existe un nivel de conocimiento significativo sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, es decir no existe variación de los conocimientos probabilísticamente esperados sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en los tripulantes.

En este sentido los resultados ofrecen que los tripulantes de la flota de la empresa naviera “ElCano, S.A” tienen un amplio conocimiento de cuáles y porque los equipos o sistema a bordo son vulnerables ante un ataque cibernético, lo cual ofrece estabilidad a la operatividad de la nave, seguridad a los tripulantes y prevención y cuidado del medio ambiente, ya que si un equipo es afectado por un virus informático se puede ocasionar algún accidente, tales como, colisiones entre buques, derrames petroleros, secuestro de la embarcación, entre otros, por tanto a mayor conocimiento de las fallas que puedan presentarse en los equipos y sistemas de una embarcación, se logra prevenir y contrarrestar las consecuencias derivadas de un ataque cibernético.

Hallazgos que se sustentan en Delgado y Puch (2016), quienes concluyendo en su investigación, que a medida que los egresados de la especialidad de puente de la ENAMM adquieran más conocimiento de medidas alternativas ante fallas de los equipos de puente, su actitud para resolver las fallas que presenten estos equipos se determinara de manera oportuna y apropiada, dado por un valor de significancia de 0,046 asociado al Chi-cuadrado, menor al nivel de significancia 0,05 establecido en la investigación. Así mismo Hamrock (2019), afirma este hallazgo, al concluir que estas vulnerabilidades son un problema que no debe tomarse a la ligera dentro de las compañías marítimas, resaltando en su estudio que a medida que las regulaciones para los datos de AIS se vuelvan más específicas hacia los transpondedores y receptores, habrá más conciencia sobre estos delitos cibernéticos, así como formas de mitigarlos. Por su parte Torres (2018), en su estudio destaca entre sus conclusiones que la ciberseguridad a bordo, se verá mermada si no establecen unas normas claras por parte de la compañía naviera o del capitán del buque, en relación a la conexión de dispositivos electrónicos

personales de la tripulación con los sistemas de navegación o equipos informáticos de administración o acciones de mantenimiento del software, que podrían infectar a los mismos de forma accidental.

En el segundo objetivo específico, al determinar el nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, se observa en los resultados presentados que el 50% de los tripulantes presenta un nivel medio de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos, el 32% presenta un alto nivel de conocimiento sobre los tipos de amenazas, mientras que el 18% de los tripulantes presentan un nivel bajo de conocimiento, valores que al comparar con la probabilidad de los valores esperados según la prueba estadística de Chi-cuadrado, se obtuvo un nivel de significancia p valor= 0,000 asociado a la prueba, menor al establecido en la investigación ($p<0,05$), lo que permitió el rechazo de la hipótesis nula y la aceptación de la segunda hipótesis específica planteada en la investigación, concluyendo que Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, es decir no existe variación de los conocimientos probabilísticamente esperados acerca de los tipos de amenazas de riesgos cibernéticos marítimos en los tripulantes.

En base a los hallazgos obtenidos se evidencia que los tripulantes de la empresa naviera “ElCano, S.A” contribuyen a prevenir cualquier amenaza cibernética, dado que la mayoría de los tripulantes conocen las medidas para identificar, detectar, y prevenir cualquier situación que comprometa a los equipos, sistemas de información y sistemas operativos en los buques ante un ataque

cibernético, mas sin embargo se debe procurar que toda la tripulación este capacitada en ciberseguridad, de esta manera los tripulantes no serían un eslabón débil para generar riesgos informáticos, tal como lo describe Boyes, *et. al.* (2016), en su teoría, quien establece que los empleados internos pueden comprometer los sistemas de la industria marítima por negligencia, descuido, ignorancia o simplemente error humano, dado que estos actos no intencionales exponen los sistemas o datos confidenciales a amenazas, poniendo la seguridad de las empresas en diferentes niveles de riesgo dependiendo del acceso que tengan a los sistemas. De tal manera se reconoce que este tipo de amenaza representa una falta de capacitación y conciencia de los empleados y representa el máximo riesgo para las empresas.

En esta misma línea el análisis de los resultados se afianza en los hallazgos descritos por Rivera (2019), en su investigación, al concluir que a mayor conocimiento de los componentes que originan riesgos de seguridad cibernética por parte de los trabajadores, se reduciría significativamente de manera integral los fraudes en las empresas, expuesta por un valor de Chi-cuadrado X^2_c 422.014 > X^2_t 26.296, asociado a un nivel de sig. 0,000< 0,05 lo que permitió el rechazo de la hipótesis nula.

Por último en el tercer objetivo específico, se determinó el nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, evidenciando en los resultados que el 48% de los tripulantes presentan un alto nivel de conocimiento acerca de los protocolos de seguridad para abordar los riesgos cibernéticos marítimos, el 40% presenta un nivel medio de conocimiento sobre los protocolos de

seguridad, mientras que el 12% de los tripulantes presentan un nivel bajo de conocimiento, valores que al contrastar con los parámetros probabilísticamente esperados dispuestos por la prueba estadística de Chi-cuadrado, arrojan un nivel de significancia p valor= 0,026, menor al nivel de significancia establecido en la investigación (p<0,05), lo cual condujo al rechazo de la hipótesis nula y la aceptación de la tercera hipótesis específica, contrastando estadísticamente que Existe un nivel de conocimiento significativo de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, es decir no existe variación de los conocimientos probabilísticamente esperados de los protocolos de seguridad ante riesgos cibernéticos marítimos en los tripulantes.

En virtud de los hallazgos obtenidos se entiende que los tripulantes de la flota de la empresa naviera “ElCano, S.A” tienen un amplio conocimiento sobre las medidas de seguridad actuales, dispuestas en las directrices y convenios que permite la buena gestión de riesgos cibernéticos, es de destacar que en todos los niveles funcionales dentro de la empresa es necesario una actualización constante de las nuevas normativas dispuestas por la OMI y sus organismos aliados, esto constituye un compromiso con la empresa y garantiza la seguridad de toda tripulación en todos los ámbitos operativos, en esta perspectiva los resultados se apoyan en Sánchez y Sumiano (2017), quienes determinaron en su investigación que a mayor conocimiento por parte de los tripulantes de las normas de seguridad menor será el riesgo que estos puedan generar en el ejercicio de sus funciones, expuesta por un coeficiente de correlación de Rho de Sperman -0,233 asociado a un nivel de significancia que conllevo al rechazo de la hipótesis nula (p valor 0,027 < 0,05)

Estas medidas de seguridad también reflejan la buena gestión de la empresa, respecto al seguimiento y cumplimiento de las normativas nacionales e internacionales, acoplándose a las necesidades y acontecimientos actuales en pro de salvaguardar el ecosistema y la seguridad de los tripulantes, de acuerdo a lo planteado Miranda (2018), en su investigación concluyendo que es necesario comprender que los riesgos que enfrenta la industria marítima en términos de ciberseguridad son reales. Por esa razón, es necesario que la gestión de la empresa atienda los problemas de seguridad cibernética porque un ataque cibernético es un problema organizacional, no solo relacionado con el departamento de TI, dado que estos problemas pueden afectar directamente toda la estructura organizativa y la operación de la empresa. En este sentido Inoguchi y Macha (2017), añaden que los gerentes deben conocer, analizar e implementar los elementos que componen el concepto de ciberseguridad, mediante un análisis de riesgos, para establecer la probabilidad de ocurrencia de los mismos y el impacto que este genere al concretarse una amenaza, lo que implica identificarlos y analizarlos para determinar las posibles consecuencias, proponiendo medidas a efectuar para tratarlos de forma adecuada. En este contexto Mendoza y Vega (2019) sostienen que la gestión de la empresa no solo debe protegerse de los riesgos cibernéticos mediante la gestión técnica de herramientas operativas de seguridad sino debe establecer protocolos de seguridad cibernética para que los trabajadores puedan detectar y responder a los principales riesgos cibernéticos, de esta forma la empresa pueda cumplir con cada parámetro establecido en el marco de referencia del NIST para poder adquirir un nivel aceptable o nivel ejecutado ,de esta forma toda la organización de la empresa pueda estar capacitada para confrontar los incidentes de ciberseguridad.

A efectos de este análisis las empresas navieras deben tomar acciones estratégicas que les permita identificar sus debilidades y fortalezas. Por cuanto los resultados ofrecidos en esta disertación dan reflejo de superación de una de las vulnerabilidades que presenta la empresa naviera “ElCano, S.A”, en cuanto al nivel de conocimiento que varían de medio a alto sobre los riesgos cibernéticos en su tripulación, a tal fin una estrategia oportuna seria ahondar más sobre este tema y capacitar al personal en función de ello. Bajo este análisis Salem (2018), aborda que la acción principal para encontrar amenazas y vulnerabilidades cibernéticas es “realizar evaluaciones de riesgos de ciberseguridad”.

Con nuestra investigación, demostramos que los riesgos cibernéticos marítimos han crecido exponencialmente en los últimos años tanto en el ámbito internacional como Nacional. Sin embargo, en el sector nacional aún no ha tomado las medidas adecuadas para protegerse de los riesgos cibernéticos. Según el reporte anual de ciberseguridad 2018 de Cisco, los incrementos de ataques cibernéticos en el país son debido a la inexistencia de protocolos de seguridad cibernética por parte de la gestión de la empresa, colocándonos en el quinto país en Latinoamérica con más ataques cibernéticos.

En la actualidad, las empresas navieras peruanas están utilizando políticas de seguridad cibernética únicamente para tratar de eliminar el riesgo a un nivel parcial. Sin embargo, las empresas navieras internacionales como ElCano S.A tiene como objetivo principal eliminar el riesgo cibernético marítimo de esta forma la gestión de la empresa con respecto a seguridad cibernética se encuentre e n el nivel adaptativo número 4 del marco de referencia del Nist. Esta forma de gestión que están adoptando empresas internacionales, es el punto clave que deberían

seguir las navieras nacionales para tener un nivel de conocimiento significativo de los riesgos cibernéticos marítimos tanto en la tripulación de los buques como el ámbito administrativo.

Por lo tanto, La empresa incluye políticas de ciberseguridad que abarquen los 5 elementos funcionales claves para la gestión del riesgo cibernético marítimo, como:

-Políticas de acceso a internet, en el cual incluye un registro de las horas de acceso por cada tripulante, bloqueo de páginas web que pongan en vulnerabilidad los sistemas conectados del buque, el capitán si lo ve necesario puede restringir el acceso al internet, si encuentra alguna vulnerabilidad del sistema.

-Políticas de control y registro de todos los medios de almacenamiento que se encuentren abordo. Además, los medios de almacenamiento de los tripulantes son revisados por un programa de antivirus antes de su uso a bordo, también está totalmente prohibido utilizar un dispositivo en algún sistema conectado del buque con la compañía.

-La empresa ha creado protocolos de actualización de los sistemas informáticos y equipos ECDIS mediante redes controladas, estas redes de internet únicamente se utilizan para las actualizaciones de los sistemas mencionados únicamente mediante personas encargadas usando claves para cada actualización.

-La empresa naviera ElCano S.A ha implementado un software únicamente para la gestión de seguridad en la empresa y para realizar los pedidos utiliza un programa para pedidos , el cual no tiene enlace con los sistemas y programas

conectados del buque con la empresa. Sin embargo, algunas navieras peruanas permiten que su software para la gestión de la seguridad, este conectado con el software de pedidos como “SERTICA “, poniendo en riesgo el ciberespacio de las navieras nacionales. En consecuencia, los delincuentes cibernéticos pueden acceder a la información de las navieras nacionales sin ninguna restricción mediante las comunicaciones que se realizan entre el buque, la compañía y las autoridades en tierra, mediante los pedidos que se solicitan a diferentes organismos. Por tal motivo, un paso fundamental para mitigar el riesgo cibernético marítimo, es que el sector marítimo nacional separe sus sistemas de tecnología de información, y que todo sistema conectado entre el buque y la compañía cuente con una red independiente, como hacen en empresas internacionales.

6.2. Conclusiones

Primera conclusión

Los resultados obtenidos en la investigación permiten concluir que Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, dado que el 60% de los tripulantes presenta un nivel medio de conocimiento de los riesgos cibernéticos marítimos presentes en la empresa, el 32% presenta un nivel alto, y el 8% de los tripulantes presentan un nivel bajo de conocimiento, asociado a un p valor= 0,000 del estadística de la prueba Chi-cuadrado, menor al nivel de significancia establecido en la investigación ($p<0,05$), lo que conllevo al rechazo de la hipótesis nula y la aceptación de la hipótesis planteada en la investigación.

Segunda conclusión

En base a los hallazgos obtenidos, se concluye que Existe un nivel de conocimiento significativo sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “

, S.A”, por cuanto el 50% de los tripulantes presenta un nivel medio de conocimiento, el 38% presenta un alto nivel de conocimiento, y el 12% de los tripulantes presentan un nivel bajo de conocimiento, valores que ofrecen un nivel de significancia p valor= 0,000 asociado a la prueba Chi-cuadrado, menor al establecido en la investigación ($p<0,05$), lo que conllevo al rechazo de la hipótesis nula y la aceptación de la primera hipótesis específica planteada en la investigación.

Tercera conclusión

Conforme a los resultados obtenidos, se concluye que Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, sustentado porque el 50% de los tripulantes presenta un nivel medio de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos, el 32% presenta un alto nivel de conocimiento, mientras que el 18% de los tripulantes presentan un nivel bajo de conocimiento, asociado a un p valor= 0,000 de la prueba estadística de Chi-cuadrado, menor al establecido en la investigación ($p<0,05$), lo que permitió el rechazo de la hipótesis nula y la aceptación de la segunda hipótesis específica planteada en la investigación.

Cuarta conclusión

En virtud de los resultados presentados, se logra concluir que Existe un nivel de conocimiento significativo de los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, por cuanto el 48% de los tripulantes presentan un alto nivel de conocimiento acerca de los protocolos de seguridad, el 40% presenta un nivel medio de conocimiento, mientras que el 12% de los tripulantes presentan un bajo nivel de conocimiento, valores que arrojan un nivel de significancia p valor= 0,026 asociado a la prueba estadística de Chi-cuadrado, menor al nivel de significancia establecido en la investigación ($p<0,05$), lo cual condujo al rechazo de la hipótesis nula y la aceptación de la tercera hipótesis específica.

6.3. Recomendaciones

Primera recomendación

Conforme de que la tripulación tiene un nivel de conocimiento de medio a alto sobre los riesgos cibernéticos, se recomienda a la empresa naviera “ElCano, S.A”, impulsar en su gestión la capacitación de toda la tripulación y en general obtener un nivel alto de conocimiento, partiendo de un análisis de las vulnerabilidades y fallas que puedan presentar los equipos y sistemas a bordo, explicando que acciones comprometen la seguridad de los mismos y llevando al alcance de todos las nuevas directrices y normativas dispuestas en el ámbito nacional e internacional, con la finalidad de reforzar y mantener una conciencia preventiva ante un ataque cibernético, garantizando la seguridad de toda la tripulación, el ecosistema y la sociedad en general.

Finalmente, las empresas navieras nacionales deben crear estrategias de ciberseguridad en el cual incluyan evaluaciones constantes a la tripulación y a los trabajadores de la empresas, ya que la evaluación constante permitirá identificar las brechas que puedan existir en la cadena de protección y prevención que están adoptando las compañías internacionales .Según OMI (2017) señala que la mejor política de prevención de los riesgos cibernéticos es mediante evaluaciones y capacitaciones constantes a toda la organización , de esta forma se identificara cual es la mayor vulnerabilidad que tiene la empresa .

Por tal razón la empresa Naviera ElCano S.A nos brindó las autorizaciones y facilidades necesarias para poder realizar nuestra investigación, ya que mediante nuestra investigación ellos pudieron identificar en que aspectos de la gestión de riesgos cibernéticos marítimos están fallando, permitiéndoles identificar sus

vulnerabilidades, enfocándose ahora en que su tripulación obtenga un nivel de conocimiento alto en riesgos cibernéticos marítimos. De esta manera nuestra investigación permite que investigaciones a futuro puedan realizar investigaciones que puedan crear estrategias o programas de prevención ante los riesgos cibernéticos marítimos que puedan adoptarse en las empresas navieras nacionales, logrando que la gestión del riesgo cibernético el sector marítimo nacional pueda competir con la gestión de las empresas navieras nacionales.

Es importante fomentar en las escuelas de formación tanto nacional como internacional y organizaciones no gubernamentales desarrollar investigación sobre temas afines vinculados a los riesgos cibernéticos de tal manera que se puedan consolidar soportes teóricos que brinden un panorama con mayor evidencia científica dentro del contexto marítimo internacional.

Segunda recomendación

En virtud de que se determinó que los tripulantes tienen un nivel de conocimiento de medio a alto sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos, se recomienda a la empresa naviera “ElCano, S.A”, la necesidad de aclarar en todos los tripulantes que los equipos interconectados electrónicamente en todos los espacios de la embarcación están expuestos a un ataque cibernético, mostrando las consecuencias que se puedan generar de concretarse un ciberataque y cuáles serían los medios para revertir este hecho, partiendo primeramente de la expansión del conocimiento mediante la formación en gestión de riesgos cibernéticos.

Tercera recomendación

En base a los hallazgos encontrados de que los tripulantes tienen un nivel medio de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos, es de recomendar a la empresa naviera “ElCano, S.A”, mantener a bordo un registro de los acontecimientos actuales sobre los ataques cibernéticos en la industria marítima, identificando los diferentes escenarios, el tipo de atacante, los medios utilizados y las consecuencias de los mismos, con el fin de ofrecer a la tripulación un mecanismo claro y real de los tipos de amenazas a los que se enfrenta la empresa naviera en la actualidad, resaltando el impacto que puede generar esta situación y despertar en todos el interés al conocimiento de la ciberseguridad.

Cuarta recomendación

Dado que los tripulantes tienen un nivel alto de conocimiento acerca de los protocolos de seguridad ante riesgos cibernéticos marítimos, es de recomendar a la empresa naviera “ElCano, S.A”, potenciar y expandir a toda la tripulación este conocimiento sobre las medidas de seguridad dispuestas por la Organización Marítima Internacional y los Organismo cooperantes para mitigar cualquier riesgo cibernético en la industria, con la finalidad de que los tripulantes se alineen a las medidas y directrices internacionales y puedan estructurar su comportamiento en pro de salvaguardar la seguridad de todos en el ejercicio de sus funciones, para ello la empresa debe ofrecer las herramientas necesarias dentro de su entorno que permita la integración del binomio empresa-tripulante dejando por sentado una buena gestión.

FUENTES DE INFORMACIÓN

ABS - Oficina Americana de Transporte de Mercancías (2016). Nota de orientación sobre; La Aplicación de los Principios de Ciberseguridad a las Operaciones Marinas y Offshore. Volumen 1: Ciberseguridad. Recuperado de: https://safety4sea.com/wp-content/uploads/2018/04/ABS-Cyber_Security-2016_02.pdf

Ahokas, J. (2018). El sector marítimo finlandés dentro del huracán de ciberseguridad. (Tesis de maestría) Universidad de Turku, Finlandia. Recuperado de: https://www.utupub.fi/bitstream/handle/10024/146355/Ahokas_Jenna_opinnayte.pdf?sequence=1&isAllowed=y

Akamai.com (2019). ¿Qué es el phishing? Recuperado de: https://www.akamai.com/es/es/resources/what-is-phishing.jsp

Attard, F. (2014) Contribución de la OMI al derecho internacional que regula la seguridad marítima. Revista de Derecho Marítimo y Comercio, Vol. 45 (4), 479–565.

Avast.com (2019a). Phishing. Recuperado de: https://www.avast.com/es-es/c-phishing

Avast.com (2019b). Spyware. Recuperado de: https://www.avast.com/es-es/c-spyware

Avast.com (2019c). Ransomware. Recuperado de: https://www.avast.com/es-es/c-spyware

Balduzzi, M. Wilhoit, K. y Pasta, A. (2014). Una evaluación de seguridad de AIS. Trend Micro. Recuperado de: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

Bateman, T. (2013). Advertencia policial después del ciberataque de narcotraficantes. BBC. Recuperado de: https://www.bbc.com/news/world-europe-24539417

Belmont, K.B, (2016). Ciberseguridad marítima: casos cibernéticos en el entorno marítimo. Asociación americana de autoridades portuarias. Recuperado de: https://www.ahcusa.org/uploads/2/1/9/8/21985670/k._belmont_-_aapa_maritime_cybersecurity_final.pdf

Bhatti, J. y Humphreys, T. (2017). Control hostil de barcos a través de falsas señales de GPS: demostración y detección. Navegación 64(1): 51–66. Doi: https://doi.org/10.1002/navi.183

Biener, C., Eling, M. y Wirfs, J. (2014). Asegurabilidad del riesgo cibernético: un análisis empírico. Los Documentos de Ginebra sobre Riesgo y Seguros - Problemas y práctica, Vol. 40 (1), 131-158.

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL (2018) Las Pautas Sobre Los

Buques de Seguridad Cibernética a Bordo, Vol 3. BIMCO, Copenhagen. Recuperado de: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Boyes, H., Isbell, R. y Luck, A. (2016). Código de Prácticas. Ciberseguridad para puertos y sistema portuario. Institución de Ingeniería y Tecnología (IET), Londres, Reino Unido. Recuperado de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Centro de navegación de la Guardia Costera de EE. UU. (2016) Cómo funciona AIS. Centro de navegación de la Guardia Costera de EE. UU. Recuperado de: https://www.navcen.uscg.gov/?pageName=AISworks#

Chirgwin, R. (2018). Los 'héroes' de TI salvaron a Maersk de NotPetya con un bombardeo de reinstalación de diez días. The Register. Recuperado de: https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

Clark, J. y Keaney, D. (2017) Cerrando la puerta del establo después de que el Cyber Horse se haya desbocado. Revista Internacional de Tecnología, Vol. 76, 18–19.

Comité de Facilitación y el Comité de Seguridad Marítima (MSC-FAL, 2017) Directrices sobre la Gestión de los Riesgos Cibernéticos Marítimos. Londres: Organización Marítima Internacional (OMI). Recuperado de: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-

%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Crawford, J. (2019) Ciberataque al Transporte Marítimo. ¿Una Amenaza Real o Ciencia Ficción? Revista de Marina Nº 970, pp. 15-23. Recuperado de: https://revistamarina.cl/revistas/2019/3/jcrawfordc.pdf

CyberKeel (2014). “Riesgos cibernéticos marítimos: piratas virtuales en general en los mares cibernéticos”. Recuperado de: https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

Delgado, J. y Puch, M. (2016). Relación entre la Actitud y el Nivel de Conocimiento de Medidas Alternativas Ante Fallas del GPS, ECDIS y ARPA en Egresados de la Especialidad de Puente de la Escuela Nacional de Marina Mercante "Almirante Miguel Grau" del año 2015. (Tesis de grado) Escuela Nacional de Marina Mercante Almirante Miguel Grau. Callao – Perú. Recuperado de: http://repositorio.enamm.edu.pe/bitstream/ENAMM/49/1/TESIS%2040%20-%20DELGADO-PUCH.pdf

Di Rollo, J. (2017). Cyber Tsunami. BREAKBULK MAGAZINE. ISSUE 3 / 2017. Recuperado de: https://issuu.com/breakbulk/docs/2017_issue_3_issuu/58

DiRenzo, J., Drumhiller, N. y Roberts, F. (2017). Problemas en ciberseguridad marítima. Washington DC: Fred Roberts.

DiRenzo, J., Goward, D. y Roberts, F. (2015). El desafío poco conocido de la ciberseguridad marítima. En Información, Inteligencia, Sistemas y Aplicaciones (IISA), 2015 6ª Conferencia Internacional sobre IEEE Recuperado de:

http://dimacs.rutgers.edu/archive/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf

Edgerton, M. (2013). "Una guía profesional para la seguridad marítima y portuaria efectiva", Nueva Jersey, Hoboken: John Wiley & Sons, Inc.

Farooq, M. U., Waseem, M., Khairi, A. y Mazhar, S. (2015). Un análisis crítico sobre las preocupaciones de seguridad de internet de las cosas (IoT). Revista internacional de aplicaciones informáticas, 111 (7). Recuperado de: http://www.pcporoje.com/filedata/592496.pdf

Ferran, L. (2013). “Los chicos que pueden hacer que los petroleros desaparezcan, virtualmente”, ABC News. Recuperado de: http://abcnews.go.com/Blotter/guys-make-oil-tankers-disappear-virtually/story?id=20565851

Fitton, O., Prince, D., Germond, B. y Lacy, M. (2015). El futuro de la ciberseguridad marítima. Universidad de Lancaster. Recuperado de: http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf

Fransas, A., Nieminen, E., Salokorpi, M. y Rytkönen, J. (2012) Seguridad marítima: revisión de la literatura. Publicaciones de la Universidad de Ciencias Aplicadas de Kymenlaakso, Serie B Investigación e Informes, No 77. Recuperado de: https://www.theseus.fi/bitstream/handle/10024/46235/B77_raportti_2.pdf?sequence=3&isAllowed=y

Freeman, M. (2018). El puerto de San Diego continúa la recuperación del ciberataque. San Diego UnionTribune. Recuperado de:

https://www.sandiegouniontribune.com/business/technology/sd-fi-port-update-20181004-story.html

Gómez, A. (2019). “Ciberseguridad marítima utilizando códigos ISPS e ISM”. Gerente de Ciberseguridad y Consultor. Recuperado de: https://www.he-alert.org/filemanager/root/site_assets/standalone_article_pdfs_1220-/he01335.pdf

Goward, D. (2017) ¿Ataque masivo de suplantación de GPS en el Mar Negro? Ejecutivo Marítimo. Recuperado de: https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

Graham, L. (2017). Industria naviera vulnerable a ciberataques y bloqueo de GPS, CNBC. Recuperado de: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html

Guldbrandsen, C. (2013) Neptuno o Poseidón: implementando la ley de seguridad marítima global y de la UE en una agencia nacional. Revista Internacional de Ciencias Administrativas, Vol. 79 (3), 505–522.

Hambling, D. (2017). Las naves engañadas en el ataque de suplantación de GPS sugieren arma cibernética rusa. New Scientist. Recuperado de: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

Hamrock, S. (2019). Ciberseguridad marítima: un análisis comparativo de la regulación estadounidense e internacional sobre receptores de datos AIS. (Tesis de pregrado) Texas A&M University. Recuperado de: https://oaktrust.library.tamu.edu/bitstream/handle/1969.1/175401/HAMROCK-FINALTHESIS-2020.pdf?sequence=1&isAllowed=y

Hayes, C. (2016). Ciberseguridad marítima: el futuro de la seguridad nacional. Escuela Naval de Posgrado. Recuperado de: https://www.hsdl.org/?view&did=794596

Heilig, L., Lalla-Ruiz, E. y Voss, S. (2017). Transformación digital en puertos marítimos: análisis y un marco teórico de juegos. NETNOMICS: Investigación Económica y Redes Electrónicas. V18, pp.227-254. DOI: 10.1007 / s11066-017-9122-x

Helmick, J. (2008) Seguridad portuaria y marítima: una perspectiva de investigación. Revista de Seguridad del Transporte, Vol. 1 (1), 15–28.

Hernández, R., Fernández C., & Baptista P. (2010). Metodología de la Investigación Científica. México D.F. Edit Mc Graw Hill.

Hernández, R., Fernández C., & Baptista P. (2014). Metodología de la Investigación Científica. México D.F. Edit Mc Graw Hill.

Hirst, I. (2017). Post mortem. En: D, MacIntyre. Los ciberataques son reales y llegan a un puerto cerca de usted. Estrategia portuaria. Insight para profesionales de la tecnología marina. Recuperado de: https://www.portstrategy.com/news101/port-operations/planning-and-design/cyber-security-feature

Hsia, J. (2017) “¿Conoces tus riesgos?” Gestión de Seguridad Cibernética Estadounidense. Recuperado de: www.americancsm.com/do-you-know-your-risks/

Inoguchi, A. y Macha, E. (2017). Gestión de la Ciberseguridad y Prevención de los Ataques Cibernéticos en las Pymes del Perú, 2016. (Tesis de grado) Universidad San Ignacio de Loyola. Lima – Perú. Recuperado de:

http://repositorio.usil.edu.pe/bitstream/USIL/2810/1/2017_Inoguchi_Gestion-de-la-ciberseguridad.pdf

Kouwenhoven, N., Borrett, M. y Wakankar, M. (2016) Las implicaciones y amenazas de la seguridad cibernética para los puertos. Revista Internacional de Tecnología, Vol. 72, 58–60.

Kusi, B. (2015). Seguridad Portuaria: Amenazas y vulnerabilidades. Universidad Laurea de Ciencias Aplicadas. Recuperado de: https://core.ac.uk/download/pdf/38128067.pdf

Lappalainen, J., Vepsäläinen, A. y Tapaninen, U. (2010) Análisis del Código Internacional de Gestión de Seguridad. En J. Heijari y U. Tapaninen. Eficiencia del Código ISM en las compañías navieras finlandesas, eds., 10-16. Publicaciones del Centro de Estudios Marítimos de la Universidad de Turku, A52. Recuperado de: https://www.utupub.fi/bitstream/handle/10024/63763/A52_effeciency_of_the_ISM_code.pdf?sequence=3&isAllowed=y

Marlow, P. B. (2010) Seguridad marítima: una actualización de cuestiones clave. Política y Gestión Marítima, Vol. 37 (7), 667–676.

Marsh y McLennan. (2014). El riesgo de ciberataques al sector marítimo. Práctica marina global. Marsh & McLennan Companies. Recuperado de: https://www.ahcusa.org/uploads/2/1/9/8/21985670/the_risk_of_cyber-attack_to_the_maritime_sector-07-2014.pdf

McNicholas, M. (2008) Seguridad Marítima - Una Introducción. Elsevier, Oxford.

Mendoza, L. y Vega, G. (2019). “Evaluación de la Capacidad de Detección y Respuesta a Riesgos de Ciberseguridad, caso de la Empresa SISC”. (Tesis

de maestría) Universidad del Pacífico. Recuperado de: http://hdl.handle.net/11354/2250

Middleton, A. (2015). “Hide and Seek: Gestión de vulnerabilidades del sistema de identificación automática”. Procedimientos de la Guardia Costera. Vol. 71, N°4: 48-49. Recuperado de: https://www.hsdl.org/?view&did=760822

Miranda, D. (2018). Ciberataques: una realidad de amenaza digital que afecta a la industria marítima. (2018) (Tesis de maestría) Universidad Marítima Mundial. Disertaciones 663. Recuperado de: https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations

Mukhopadhyay, A., Saha, D., Mahanti, A., Chakrabarti, B. y Podder, A. (2005). Seguro de riesgo cibernético: un modelo de utilidad. Decisión, Vol. 32, No.1. Recuperado de: https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model

NEP&I. (2017). Riesgo cibernético en el envío. Información sobre prevención de pérdidas para miembros del Norte. Recuperado de: http://www.nepia.com/media/869527/CyberRisks-in-Shipping-LP-Briefing.PDF

OACI (2013) Manual de gestión de la seguridad. Tercera edición. Organización de Aviación Civil Internacional (OACI), Montreal.

OCIA (2016). “Consecuencias para las operaciones portuarias de la actividad cibernética maliciosa”. Oficina de Análisis Cibernético e Infraestructura (OCIA). Recuperado de: https://homeport.uscg.mil/Lists/Content/Attachments/2203/OCIA_Conseque

nces%20to%20Seaport%20Operations%20from%20Malicious%20Cyber%20Activity.pdf

OMI (2012) Guía de Seguridad Marítima y el Código ISPS. Edición 2012 Organización Marítima Internacional - OMI, Londres.

OMI (2014) Código ISM - Código internacional de gestión de seguridad con pautas para su implementación. 4ta Edición. Organización Marítima Internacional, Londres.

OMI (2018). Protección de la flota de ciberseguridad. Organización Marítima Internacional. Recuperado de: https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5ab3b85f88251b5549a07357/1521727638547/8PeterSchellenberger_OSM_APM18.pdf

OMI (2019). Código internacional para la protección de los buques y de las instalaciones portuarias. Organización Marítima Internacional. Recuperado de: http://www.imo.org/es/OurWork/Security/Guide_to_Maritime_Security/Paginas/SOLAS-XI-2%20ISPS%20Code.aspx

Oxforddictionaries (2018). Definición de riesgo. Recuperado de: https://www.lexico.com/definition/risk

Parreño, A. (2016). Metodología de Investigación en salud. Riobamba: Escuela Superior Politécnica de Chimborazo. Instituto de Investigaciones. La Caracola Editores.

Pastor, O., Pérez, J., Arnáiz, D. y Taboso, P. (2009). Seguridad Nacional y Ciberdefensa, 1a. ed., vol. 6, 7 vols. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Polemi, N. (2018) Ciberseguridad portuaria: asegurar las infraestructuras de información crítica y las cadenas de suministro. Amsterdam, Netherlands: Elsevier, Oxford.

Port Technology (2018a). San Diego sufre un ataque cibernético. Recuperado de: https://www.porttechnology.org/news/san_diego_suffers_cyber_attack

Port Technology (2018b). COSCO lucha contra el ciberataque. Recuperado de: https://www.porttechnology.org/news/cosco_fights_on_against_cyberattack

Prezelj, I. y Ziberna, A. (2013) Evaluación de riesgos basada en las consecuencias, el tiempo y la interdependencia en el campo de la infraestructura crítica. Gestión de riesgos, Vol. 15 (2), 100–131.

Ramírez, T. (2007). ¿Cómo hacer un proyecto de investigación? Caracas: Panapo.

Rivera, A. (2019) Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016. (Tesis de grado) Universidad Nacional Daniel Alcides Carrión. Cerro de Pasco – Perú. Recuperado de: http://repositorio.undac.edu.pe/handle/undac/1372

Robinson, A. (2015). 4 usos de las aplicaciones de la tecnología de la cadena de suministro que llevan a los transportistas al futuro de una gestión eficaz. Cerasis. Recuperado de: https://cerasis.com/supply-chain-technology-applications/

Rodrigue, J., Notteboom, T. y Pallis, A. (2011) La financiarización de la industria portuaria y terminal: revisando el riesgo y la integración. Política y gestión marítimas, vol. 38 (2), 191–213.

Rodrigues, V. (2013). Estrategia de Información y Seguridad en el Espacio Cibernético. Cuadernos del Instituto Nacional de Defensa (IDN), N° 12.

Recuperado de: https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

Salem, W. (2018). Mejores prácticas para encontrar amenazas y vulnerabilidades cibernéticas. El Ejecutivo Marítimo. Recuperado de: https://www.maritime-executive.com/features/best-practices-for-finding-cyber-threats-and-vulnerabilities

Sánchez, R. y Sumiano, A. (2017). Conocimiento de Normas de Seguridad y la Conducta de Riesgo en la Tripulación de los Buques de una Naviera Peruana. (Tesis de grado) Escuela Nacional de Marina Mercante Almirante Miguel Grau. Callao – Perú. Recuperado de: http://repositorio.enamm.edu.pe/bitstream/ENAMM/16/1/TESIS%2005%20-%20S%c3%81NCHEZ-SUMIANO.pdf

Saul, J. (2017). Las amenazas cibernéticas provocan el regreso de la radio para la navegación del barco. Reuters. Recuperado de: https://www.reuters.com/article/us-shipping-gpscyber-idUSKBN1AN0HT

Shauk, Z. (2013). El malware en la computadora de la plataforma petrolera aumenta los temores de seguridad. Houston Chronicle. Recuperado de: https://www.houstonchronicle.com/business/energy/article/Malware-on-oilrig-computers-raises-security-fears-4301773.php

Significados.com (2019). Significado de Malware. Recuperado de: https://www.significados.com/malware/

Techopedia (2018). Diccionario de tecnología. Recuperado de: https://www.techopedia.com/dictionary

Thompson, B. (2015). “GPS Spoofing e Interferencia: Un procesador mundial para todas las embarcaciones”. Procedimientos de la Guardia Costera Vol.71, N°. 4: 50-51. Recuperado de: https://www.hsdl.org/?view&did=760822

Torres, J. (2018). Protección Marítima del Marino Mercante Español en el Contexto Internacional. (Tesis de maestría) Escuela Técnica Superior de Náutica, Universidad de Cantabria, España. Recuperado de: https://repositorio.unican.es/xmlui/bitstream/handle/10902/15489/Torres%20Tubau%2c%20Joan.pdf?sequence=1&isAllowed=y

Trend Micro (2014). Trend Micro descubre serias vulnerabilidades en los Sistemas de Seguimiento de Barcos. Red Seguridad, Revista especializada en Seguridad TIC. Recuperado de: http://www.redseguridad.com/actualidad/info-tic/trend-micro-descubre-serias-vulnerabilidades-en-los-sistemas-de-seguimiento-de-barcos

Wang, P. y Mileski, J.P. (2018). Un marco de contingencia y red en la integración de decisiones de transporte marítimo a través de cadenas de suministro globales. Acta de la Conferencia Anual de la Asociación Internacional de Economistas Marítimos, 2018, Mombasa, Kenia.

ANEXOS

Anexo 1. Matriz de consistencia

Título: "NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS EN LA TRIPULACIÓN DE LA FLOTA DE LA EMPRESA NAVIERA "ELCANO, S.A", LIMA - 2020"

LÍNEA DE INVESTIGACIÓN: Seguridad Marítima.

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLE	DIMENSIÓN	INDICADOR	TIPO MÉTODO DISEÑO
¿Cuál es el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", Lima - 2020?	Determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", Lima - 2020.	Existe un nivel de conocimiento significativo de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", Lima - 2020.	Conocimiento de los riesgos cibernéticos.	• Equipos y sistemas vulnerables	• Sistemas de información (TI). • Sistemas operacionales (TO). • Equipos electrónicos.	**Diseño**: Descriptivo. **De corte** Transversal. **De enfoque** Cuantitativo. **Método** Hipotético deductivo. **Población:** Tripulación de una empresa naviera. **Muestra:** De tipo No probabilística, constituida por la tripulación de una empresa naviera.
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICOS**				
¿Cuál es el nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", Lima - 2020?	Determinar el nivel de conocimiento sobre los equipos y sistemas vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", Lima - 2020.	Existe un nivel de conocimiento significativo sobre los equipos vulnerables a riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "ElCano, S.A", Lima - 2020.		• Tipos de amenazas • Protocolos de seguridad	• Softwares informáticos. • Atacantes externos e internos. • Directrices. • Código ISPS. • Gestión de la empresa.	

¿Cuál es el nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020?	Determinar el nivel de conocimiento acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.	Existe un nivel de conocimiento significativo acerca de los tipos de amenazas de riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.				**Instrumento:** Encuesta tipo cuestionario, con escala Kuder-Richardson 20
¿Cuál es el nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020?	Determinar el nivel de conocimiento de protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.	Existe un nivel de conocimiento significativo sobre los protocolos de seguridad ante riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera “ElCano, S.A”, Lima - 2020.				

Anexo 2. Instrumentos para la recolección de datos

NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS

Estimado Colaborador: Después de haber sido informado adecuadamente sobre el propósito científico de nuestra investigación., agradeceremos su colaboración respondiendo cada una de las preguntas del presente cuestionario. Para ello, sírvase escoger la opción que usted considere correcta:

Preguntas generales:

Años de servicio: _____ Cargo a bordo: _____

Dimensión: Equipos y sistemas vulnerables

1. ¿Un ataque cibernético al Sistema de Identificación Automática (AIS) puede generar?

a) Colisiones entre buques.
b) Afectar la interconectividad de comunicación.
c) Crear la simulación de un barco que puede ser detectado por otros barcos y puertos.
d) Todas las anteriores.

2. ¿El Sistema Electrónico de Visualización e Información de Cartas (ECDIS), puede ser afectado cibernéticamente por?

a) El alto riesgo de exposición que implica el proceso de actualizaciones del sistema.
b) Al no tener antivirus instalado.
c) Estar interconectado a los equipos de navegación.
d) Todas las anteriores.
e) a y b son las correctas.

3. ¿Si los operadores de navegación toman medidas que desvíen a la embarcación de su ruta poniendo en riesgo a la tripulación, pueden estar frente a un ataque cibernético al?

a) Sistema de Identificación Automática (AIS).
b) Sistema de Posicionamiento Global (GPS).
c) Sistema electrónico de visualización e información de cartas (ECDIS).
d) Todas las anteriores.

4. ¿Cuál de los siguientes sistemas considera usted que son vulnerables ante un ataque cibernético?

a) Sistemas de carga y descarga de aguas de lastre.
b) Sistemas de carga y descarga de aguas residuales.
c) Sistemas de emisiones de gases.
d) Ninguna de las anteriores.
e) Todas las anteriores.

5. ¿Los principales ataques cibernéticos reportados en la industria marítima están enfocados a los equipos?

a) Equipos de navegación.
b) Sistemas de comunicación.
c) Plataformas petroleras.
d) Todas las anteriores.

6. ¿Si una persona mal intencionada infecta con un virus las computadoras de las consolas de máquina, que fallas ocasionaría?

a) Bloqueo del motor principal y motores auxiliares.
b) Desactivación de alarmas.
c) Reboce de los tanques.
d) Todas las anteriores.
e) Ninguna de las anteriores.

Dimensión: Tipos de amenazas

7. ¿En un ataque cibernético donde el atacante encripta los datos, secuestrando los sistemas y la información para solicitar que paguen un rescate, se debe a una amenaza informática de tipo?

a) Malware
b) Gusanos
c) Ransomware
d) Troyanos

8. ¿En la empresa naviera los ciberatacantes pueden infiltrarse, dañar y causar acciones autenticadas y no deseadas en los sistemas de información mediante?

a) Gusanos
b) Troyanos
c) Softwares maliciosos
d) Todas las anteriores

9. ¿Los ataques cibernéticos mediante phishing permiten a los ciberatacantes generar en una empresa naviera?

a) La suplantación de identidad mediante el envío de correos electrónicos.
b) Controlar las cargas transportadas en las embarcaciones.
c) Contrabandear mercancías.
d) Todas las anteriores.
e) a y b son correctas.

10. ¿Los tripulantes de un barco pueden comprometer los sistemas de la industria marítima ante un riesgo cibernético?

a) Abriendo correos electrónicos desconocidos.
b) Utilizando medios extraíbles en sitios no permitidos.
c) Accediendo a sitios web y redes sociales sin restricciones.
d) Todas las anteriores.

11. ¿En la empresa naviera se pueden generar atacantes cibernéticos que ponen en peligro la seguridad de las embarcaciones y sus tripulantes, motivados por?

a) Actos criminales y terroristas.
b) Beneficio económico.
c) Competitividad industrial.
d) Espionaje gubernamental.
e) Todas las anteriores.
f) a y b son correctas.

Dimensión: Protocolos de seguridad

12. ¿La empresa naviera para atender un ataque cibernético y garantizar la operatividad de la embarcación, debe contar con?

a) Software de alta tecnología.
b) Equipos y sistemas de última generación.
c) Un equipo de emergencia cibernética interna y externa.
d) Todas las anteriores.

13. ¿Para prevenir y abordar automáticamente la presencia de amenazas / actividades maliciosas en los sistemas a bordo, se deben?

a) Restringir el acceso a la red de internet de la embarcación.
b) No permitir el uso de equipos personales.
c) Instalar en la empresa software de escaneo informático.
d) Todas las anteriores.

14. ¿Cómo medida de seguridad ante un ataque cibernético, en la embarcación debe existir la provisión de un medio alternativo de comunicación, que funcione independientemente de todos los demás sistemas de a bordo?

a) De acuerdo.
b) En desacuerdo.
c) Desconoce.

15. ¿Cómo protocolo de seguridad todos los tripulantes de la embarcación?

a) No deben conectarse a la internet mientras navegan.
b) No deben usar sus dispositivos personales.
c) Deben tener capacitación básica sobre los riesgos cibernéticos, vulnerabilidades de los equipos y medidas preventivas.

d) Todas las anteriores.

16. ¿Las regulaciones para abordar los problemas de seguridad cibernética, estipulan directrices orientadas a?

a) Identificar los sistemas e información vulnerable.
b) Proteger los sistemas y los datos, implantando medidas de control.
c) Crear situaciones para detectar amenazas.
d) Implantar planes de respuesta para dar resiliencia y restaurar los sistemas.
e) Acciones para recuperar los sistemas necesarios para las operaciones.
f) Todas las anteriores.

17. ¿Cuál de las siguientes normativas regulan la gestión ante los riesgos cibernéticos en una empresa naviera?

a) Código Internacional de Seguridad de Buques e Instalaciones Portuarias (ISPS).
b) MSC-FAL.1 / Circ.319.
c) Norma ISO/IEC 27001.
d) Todas la anteriores.
e) a y c son correctas.

18. ¿Hasta cuándo la OMI otorgó a los propietarios y gerentes de buques incorporar la gestión del riesgo cibernético en el sistema de seguridad del buque?

a) A partir del 2019.
b) A partir del 2020.
c) A partir del 2021.
d) A partir del 2022.

BAREMOS DE EVALUACIÓN

NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS

Baremos	Variable	Dimensión		
	Conocimiento de los Riesgos Cibernéticos	Equipos y sistemas vulnerables	Tipos de amenazas	Protocolos de seguridad
Pregunta	1 al 18	1 al 6	7 al 11	12 al 18
Nivel	**Rangos por respuestas correctas**			
Alto	13 - 18	5 - 6	4 – 5	5 - 7
Medio	7 - 12	3 - 4	2 – 3	3 - 4
Bajo	0 - 6	0 - 2	0 – 1	0 - 2
Cuestionario	**Respuestas correctas**			
	Ítems	**Opción**	**Ítems**	**Opción**
Prueba de Conocimiento de los Riesgos Cibernéticos	**1**	D	**10**	D
	2	E	**11**	E
	3	B	**12**	C
	4	E	**13**	C
	5	D	**14**	A
	6	D	**15**	C
	7	C	**16**	F
	8	D	**17**	D
	9	D	**18**	C
Codificación de respuesta	Correcto = 1		Incorrecto = 0	

Fuente: Elaboración propia.

Anexo 3. Ficha de validación del instrumento

FICHA
DATOS DEL EXPERTO

Nombre completo : JOSÉ LUIS RODRÍGUEZ EGUIZÁBAL

Profesión : DOCENTE

Grado académico : LICENCIADO EN EDUCACIÓN

Características que lo determinan como experto:

Se hace una breve síntesis de su experiencia docente o profesional que esté relacionada con la variable a validar, también se puede indicar la experiencia en el ámbito de la investigación o en la elaboración de instrumentos. Se incluye cualquier otra información que sea relevante para caracterizarlo como experto.

- DOCENTE DE LA ENAMM DESDE EL 2013
- DOCENTE DE LA "UNASAM" - 2006 - 2009
- DOCENTE DE LA UNIVERSIDAD "CESAR VALLEJO" 2011 - 2012.
- DOCENTE DE LA UNIVERSIDAD U.T.P.
- PUBLICACIÓN DEL "MÉTODO DE ESTUDIO UNIVERSITARIO" - 2014 LIBRO

Firma
DNI: 41175132

FICHA
DATOS DEL EXPERTO

Nombre completo : **ESTEBAN ARESTIZABAL ALTUBE**

Profesión : **CAPITAN DE LA MARINA MERCANTE**

Grado académico : **LICENCIADO EN NAUTICA**

Características que lo determinan como experto:

Se hace una breve síntesis de su experiencia docente o profesional que esté relacionada con la variable a validar, también se puede indicar la experiencia en el ámbito de la investigación o en la elaboración de instrumentos. Se incluye cualquier otra información que sea relevante para caracterizarlo como experto.

Firma
DNI: 14250700 S

FICHA
DATOS DEL EXPERTO

Nombre completo : JORGE FCO. DEL MONTE SANCHEZ

Profesión : CAPITAN MARINA MERCANTE, INGENIERO INDUSTRIAL

Grado académico : DOCTORADO

Características que lo determinan como experto:

Se hace una breve síntesis de su experiencia docente o profesional que esté relacionada con la variable a validar, también se puede indicar la experiencia en el ámbito de la investigación o en la elaboración de instrumentos. Se incluye cualquier otra información que sea relevante para caracterizarlo como experto.

50 AÑOS RELACIONADO CON LA VIDA DEL MAR, DE ELLOS 10 AÑOS COMO OFICIAL, 20 AÑOS COMO CAPITAN, 20 AÑOS COMO INSPECTOR, SUBDIRECTOR FLOTA, DIRECTOR RECURSOS HUMANOS DE LA FLOTA

Firma
DNI: 14890577D

FICHA
DATOS DEL EXPERTO

Nombre completo : Andres Dieguez Albeite

Profesión : Ingeniero Informatico

Grado académico : Doctorado

Características que lo determinan como experto:

Se hace una breve síntesis de su experiencia docente o profesional que esté relacionada con la variable a validar, también se puede indicar la experiencia en el ámbito de la investigación o en la elaboración de instrumentos. Se incluye cualquier otra información que sea relevante para caracterizarlo como experto.

5 AÑOS COMO TECNICO EN SISTEMAS INFORMATICOS TENF
2 AÑOS COMO JEFE SISTEMAS TENF

Andres Dieguez

Firma
DNI: 14.890.420

FICHA
DATOS DEL EXPERTO

Nombre completo : JOHN CHAFLOQUE CASTRO

Profesión : OFICIAL DE MARINA MERCANTE

Grado académico : MAGISTER EN GERENCIA DE MANTENIMIENTO

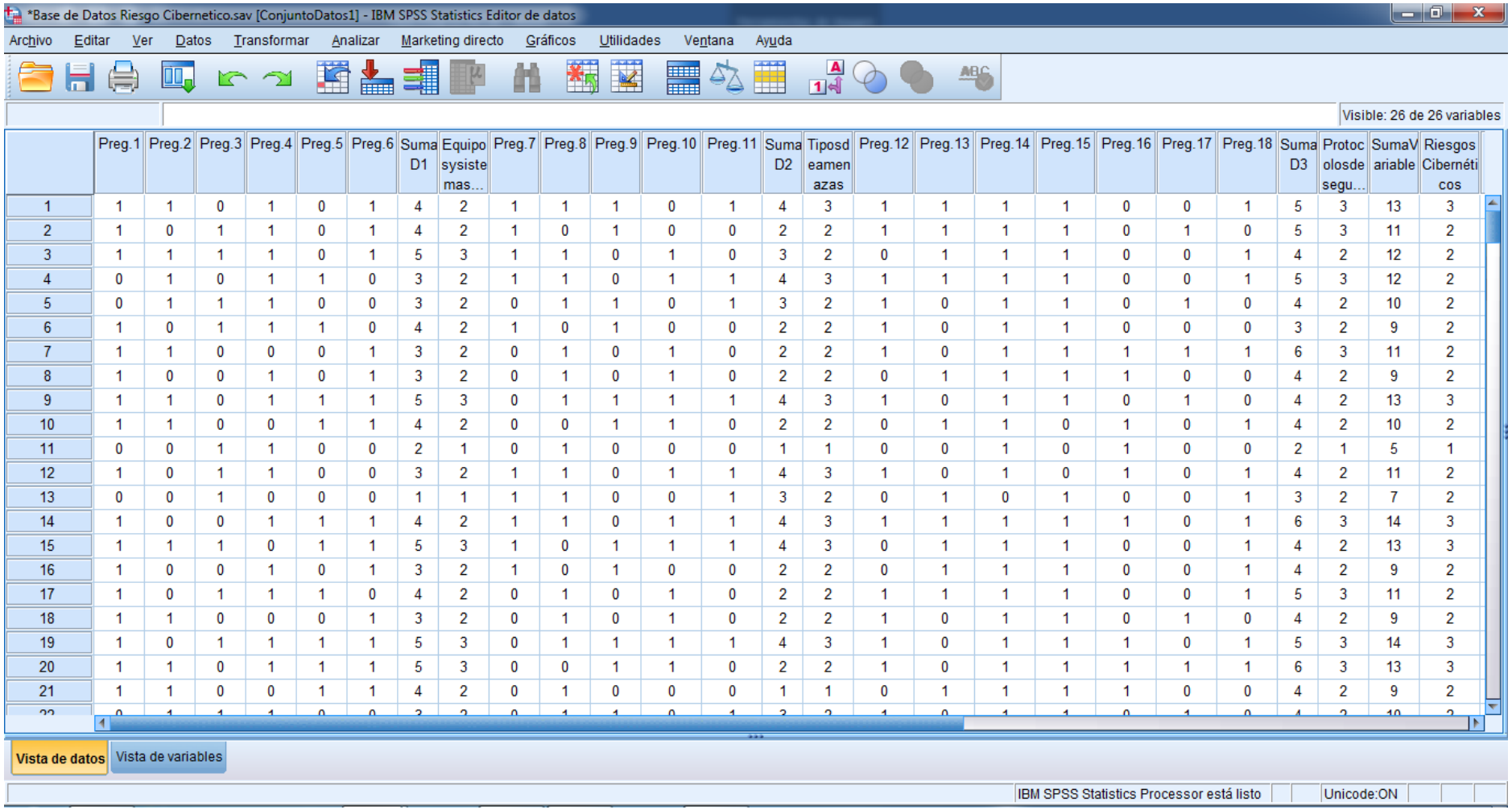
Características que lo determinan como experto:

Se hace una breve síntesis de su experiencia docente o profesional que esté relacionada con la variable a validar, también se puede indicar la experiencia en el ámbito de la investigación o en la elaboración de instrumentos. Se incluye cualquier otra información que sea relevante para caracterizarlo como experto.

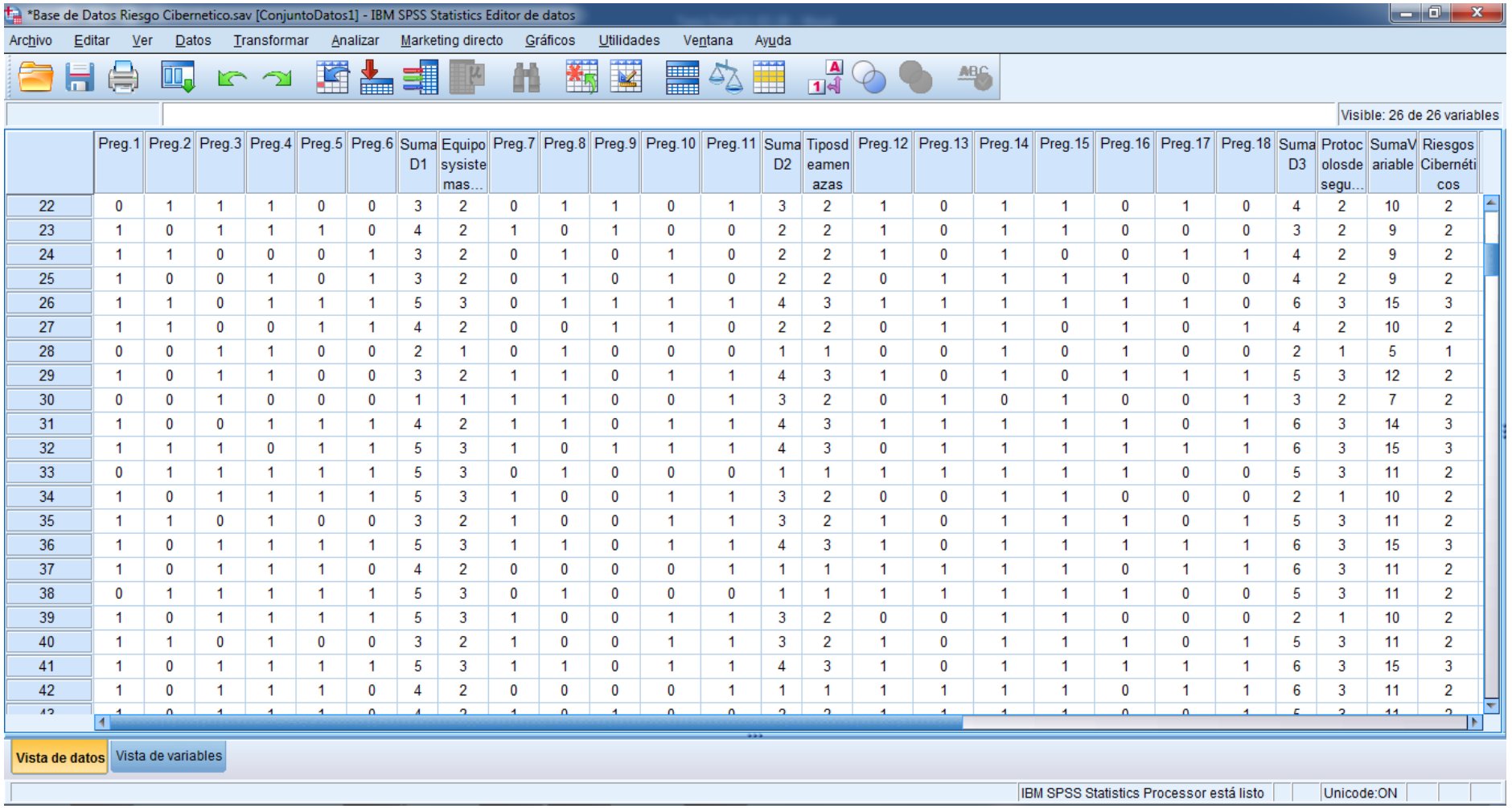
EGRESADO DE LA ENAMM EN EL AÑO 1990,
EXPERIENCIA EN BUQUE CARGUEROS, GASEROS,
PETROLEROS, EMBARCACIONES DE PESCA Y ARRASTRE
ASI COMO REMOLCADORES DE PUERTO Y OCEANICOS.
TITULO DE JEFE DE MAQUINAS Y MG DESEMPEÑO
ACTUALMENTE COMO SUPERINTENDENTE DE
REMOLCADORES EN PETROLERA TRANSOCEANICA S.A.

Firma
DNI: 08717943

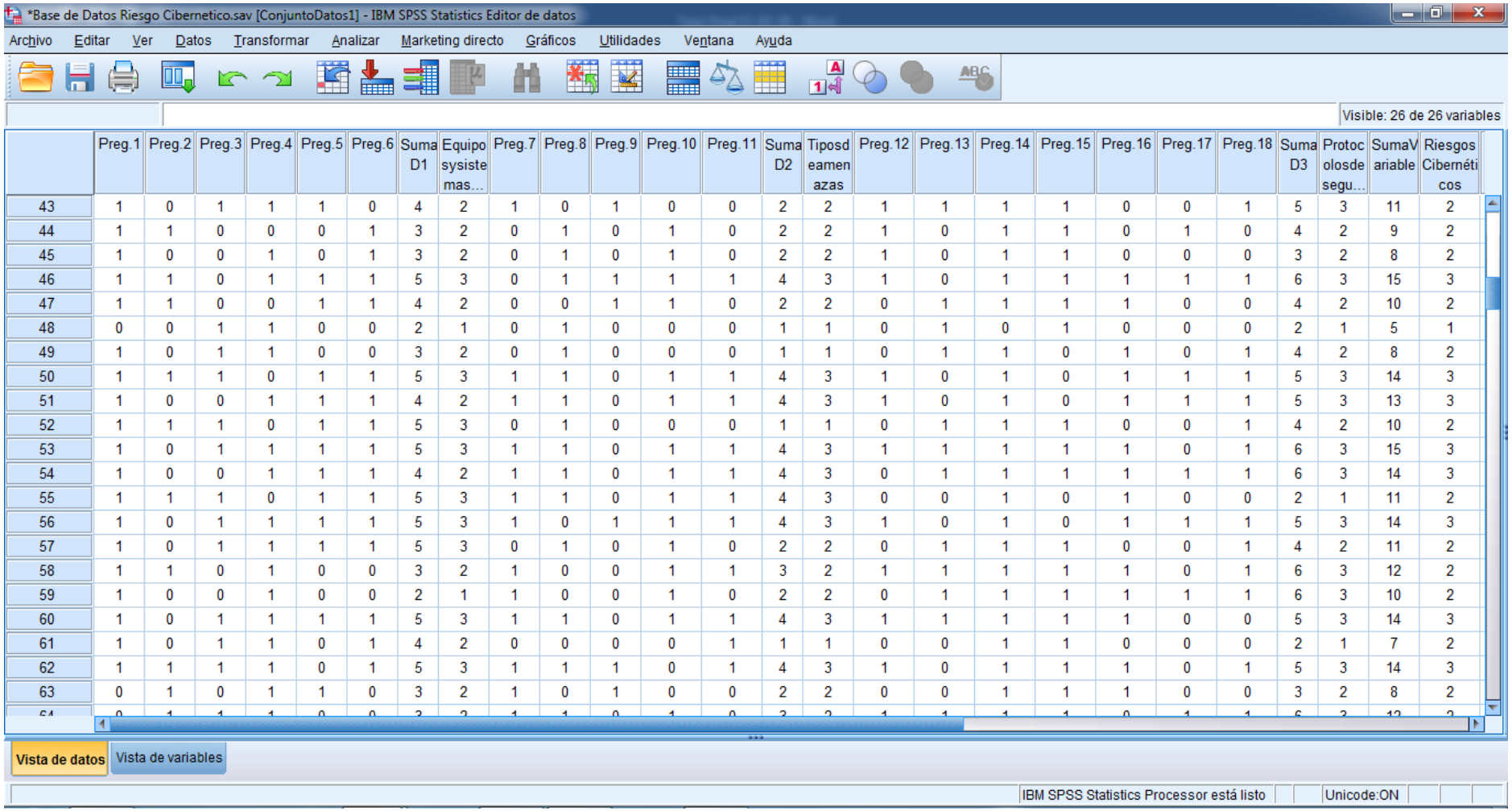
Anexo 4. Base de datos



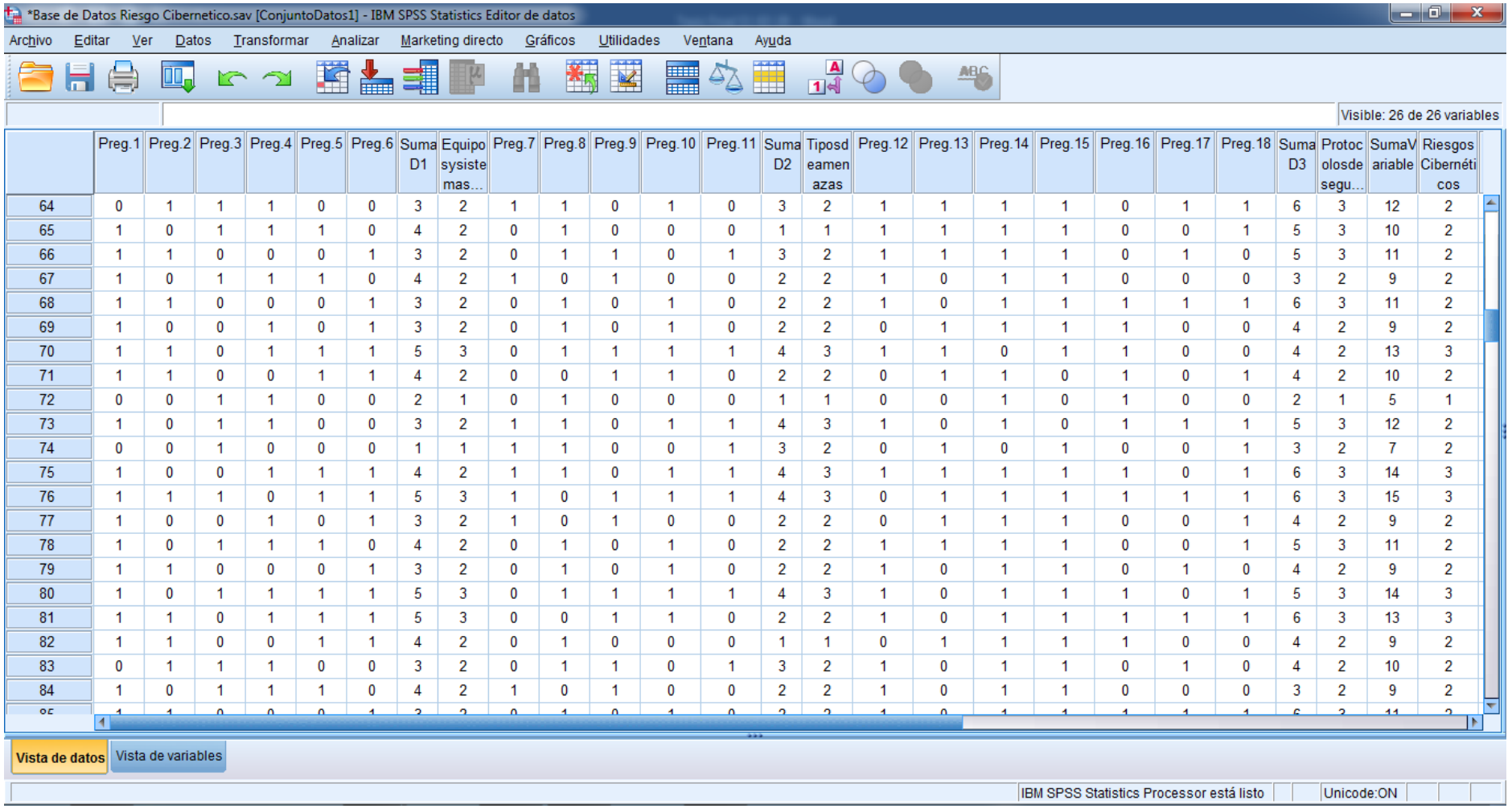
	Preg.1	Preg.2	Preg.3	Preg.4	Preg.5	Preg.6	SumaD1	Equipo sysistemas...	Preg.7	Preg.8	Preg.9	Preg.10	Preg.11	SumaD2	Tiposdeamenazas	Preg.12	Preg.13	Preg.14	Preg.15	Preg.16	Preg.17	Preg.18	SumaD3	Protocolosdesegu...	SumaVariable	Riesgos Cibernéticos
1	1	1	0	1	0	1	4	2	1	1	1	0	1	4	3	1	1	1	1	0	0	1	5	3	13	3
2	1	0	1	1	0	1	4	2	1	0	1	0	0	2	2	1	1	1	1	0	1	0	5	3	11	2
3	1	1	1	1	0	1	5	3	1	1	0	1	0	3	2	0	1	1	1	0	0	1	4	2	12	2
4	0	1	0	1	1	0	3	2	1	1	0	1	1	4	3	1	1	1	1	0	0	1	5	3	12	2
5	0	1	1	1	0	0	3	2	0	1	1	0	1	3	2	1	0	1	1	0	1	0	4	2	10	2
6	1	0	1	1	1	0	4	2	1	0	1	0	0	2	2	1	0	1	1	0	0	0	3	2	9	2
7	1	1	0	0	0	1	3	2	0	1	0	1	0	2	2	1	0	1	1	1	1	1	6	3	11	2
8	1	0	0	1	0	1	3	2	0	1	0	1	0	2	2	0	1	1	1	1	0	0	4	2	9	2
9	1	1	0	1	1	1	5	3	0	1	1	1	1	4	3	1	0	1	1	0	1	0	4	2	13	3
10	1	1	0	0	1	1	4	2	0	0	1	1	0	2	2	0	1	1	0	1	0	1	4	2	10	2
11	0	0	1	1	0	0	2	1	0	1	0	0	0	1	1	0	0	1	0	1	0	0	2	1	5	1
12	1	0	1	1	0	0	3	2	1	1	0	1	1	4	3	1	0	1	0	1	0	1	4	2	11	2
13	0	0	1	0	0	0	1	1	1	1	0	0	1	3	2	0	1	0	1	0	0	1	3	2	7	2
14	1	0	0	1	1	1	4	2	1	1	0	1	1	4	3	1	1	1	1	1	0	1	6	3	14	3
15	1	1	1	0	1	1	5	3	1	0	1	1	1	4	3	0	1	1	1	0	0	1	4	2	13	3
16	1	0	0	1	0	1	3	2	1	0	1	0	0	2	2	0	1	1	1	0	0	1	4	2	9	2
17	1	0	1	1	1	0	4	2	0	1	0	1	0	2	2	1	1	1	1	0	0	1	5	3	11	2
18	1	1	0	0	0	1	3	2	0	1	0	1	0	2	2	1	0	1	1	0	1	0	4	2	9	2
19	1	0	1	1	1	1	5	3	0	1	1	1	1	4	3	1	0	1	1	1	0	1	5	3	14	3
20	1	1	0	1	1	1	5	3	0	0	1	1	0	2	2	1	0	1	1	1	1	1	6	3	13	3
21	1	1	0	0	1	1	4	2	0	1	0	0	0	1	1	0	1	1	1	1	0	0	4	2	9	2



	Preg.1	Preg.2	Preg.3	Preg.4	Preg.5	Preg.6	SumaD1	Equipo sysistemas...	Preg.7	Preg.8	Preg.9	Preg.10	Preg.11	SumaD2	Tiposdeamenazas	Preg.12	Preg.13	Preg.14	Preg.15	Preg.16	Preg.17	Preg.18	SumaD3	Protocolosdesegu...	SumaVariable	Riesgos Cibernéticos
22	0	1	1	1	0	0	3	2	0	1	1	0	1	3	2	1	0	1	1	0	1	0	4	2	10	2
23	1	0	1	1	1	0	4	2	1	0	1	0	0	2	2	1	0	1	1	0	0	0	3	2	9	2
24	1	1	0	0	0	1	3	2	0	1	0	1	0	2	2	1	0	1	0	0	1	1	4	2	9	2
25	1	0	0	1	0	1	3	2	0	1	0	1	0	2	2	0	1	1	1	1	0	0	4	2	9	2
26	1	1	0	1	1	1	5	3	0	1	1	1	1	4	3	1	1	1	1	1	1	0	6	3	15	3
27	1	1	0	0	1	1	4	2	0	0	1	1	0	2	2	0	1	1	0	1	0	1	4	2	10	2
28	0	0	1	1	0	0	2	1	0	1	0	0	0	1	1	0	0	1	0	1	0	0	2	1	5	1
29	1	0	1	1	0	0	3	2	1	1	0	1	1	4	3	1	0	1	0	1	1	1	5	3	12	2
30	0	0	1	0	0	0	1	1	1	1	0	0	1	3	2	0	1	0	1	0	0	1	3	2	7	2
31	1	0	0	1	1	1	4	2	1	1	0	1	1	4	3	1	1	1	1	1	0	1	6	3	14	3
32	1	1	1	0	1	1	5	3	1	0	1	1	1	4	3	0	1	1	1	1	1	1	6	3	15	3
33	0	1	1	1	1	1	5	3	0	1	0	0	0	1	1	1	1	1	1	1	0	0	5	3	11	2
34	1	0	1	1	1	1	5	3	1	0	0	1	1	3	2	0	0	1	1	0	0	0	2	1	10	2
35	1	1	0	1	0	0	3	2	1	0	0	1	1	3	2	1	0	1	1	1	0	1	5	3	11	2
36	1	0	1	1	1	1	5	3	1	1	0	1	1	4	3	1	0	1	1	1	1	1	6	3	15	3
37	1	0	1	1	1	0	4	2	0	0	0	0	1	1	1	1	1	1	1	0	1	1	6	3	11	2
38	0	1	1	1	1	1	5	3	0	1	0	0	0	1	1	1	1	1	1	1	0	0	5	3	11	2
39	1	0	1	1	1	1	5	3	1	0	0	1	1	3	2	0	0	1	1	0	0	0	2	1	10	2
40	1	1	0	1	0	0	3	2	1	0	0	1	1	3	2	1	0	1	1	1	0	1	5	3	11	2
41	1	0	1	1	1	1	5	3	1	1	0	1	1	4	3	1	0	1	1	1	1	1	6	3	15	3
42	1	0	1	1	1	0	4	2	0	0	0	0	1	1	1	1	1	1	1	0	1	1	6	3	11	2



	Preg.1	Preg.2	Preg.3	Preg.4	Preg.5	Preg.6	SumaD1	Equipo sysistemas...	Preg.7	Preg.8	Preg.9	Preg.10	Preg.11	SumaD2	Tiposdeamenazas	Preg.12	Preg.13	Preg.14	Preg.15	Preg.16	Preg.17	Preg.18	SumaD3	Protocolosdesegu...	SumaVariable	Riesgos Cibernéticos
43	1	0	1	1	1	0	4	2	1	0	1	0	0	2	2	1	1	1	1	0	0	1	5	3	11	2
44	1	1	0	0	0	1	3	2	0	1	0	1	0	2	2	1	0	1	1	0	1	0	4	2	9	2
45	1	0	0	1	0	1	3	2	0	1	0	1	0	2	2	1	0	1	1	0	0	0	3	2	8	2
46	1	1	0	1	1	1	5	3	0	1	1	1	1	4	3	1	0	1	1	1	1	1	6	3	15	3
47	1	1	0	0	1	1	4	2	0	0	1	1	0	2	2	0	1	1	1	1	0	0	4	2	10	2
48	0	0	1	1	0	0	2	1	0	1	0	0	0	1	1	0	1	0	1	0	0	0	2	1	5	1
49	1	0	1	1	0	0	3	2	0	1	0	0	0	1	1	0	1	1	0	1	0	1	4	2	8	2
50	1	1	1	0	1	1	5	3	1	1	0	1	1	4	3	1	0	1	0	1	1	1	5	3	14	3
51	1	0	0	1	1	1	4	2	1	1	0	1	1	4	3	1	0	1	0	1	1	1	5	3	13	3
52	1	1	1	0	1	1	5	3	0	1	0	0	0	1	1	0	1	1	1	0	0	1	4	2	10	2
53	1	0	1	1	1	1	5	3	1	1	0	1	1	4	3	1	1	1	1	1	0	1	6	3	15	3
54	1	0	0	1	1	1	4	2	1	1	0	1	1	4	3	0	1	1	1	1	1	1	6	3	14	3
55	1	1	1	0	1	1	5	3	1	1	0	1	1	4	3	0	0	1	0	1	0	0	2	1	11	2
56	1	0	1	1	1	1	5	3	1	0	1	1	1	4	3	1	0	1	0	1	1	1	5	3	14	3
57	1	0	1	1	1	1	5	3	0	1	0	1	0	2	2	0	1	1	1	0	0	1	4	2	11	2
58	1	1	0	1	0	0	3	2	1	0	0	1	1	3	2	1	1	1	1	1	0	1	6	3	12	2
59	1	0	0	1	0	0	2	1	1	0	0	1	0	2	2	0	1	1	1	1	1	1	6	3	10	2
60	1	0	1	1	1	1	5	3	1	1	0	1	1	4	3	1	1	1	1	1	0	0	5	3	14	3
61	1	0	1	1	0	1	4	2	0	0	0	0	1	1	1	0	0	1	1	0	0	0	2	1	7	2
62	1	1	1	1	0	1	5	3	1	1	1	0	1	4	3	1	0	1	1	1	0	1	5	3	14	3
63	0	1	0	1	1	0	3	2	1	0	1	0	0	2	2	0	0	1	1	1	0	0	3	2	8	2



	Preg.1	Preg.2	Preg.3	Preg.4	Preg.5	Preg.6	SumaD1	Equipo sysistemas...	Preg.7	Preg.8	Preg.9	Preg.10	Preg.11	SumaD2	Tiposdeamenazas	Preg.12	Preg.13	Preg.14	Preg.15	Preg.16	Preg.17	Preg.18	SumaD3	Protocolosdesegu...	SumaVariable	Riesgos Cibernéticos
64	0	1	1	1	0	0	3	2	1	1	0	1	0	3	2	1	1	1	1	0	1	1	6	3	12	2
65	1	0	1	1	1	0	4	2	0	1	0	0	0	1	1	1	1	1	1	0	0	1	5	3	10	2
66	1	1	0	0	0	1	3	2	0	1	1	0	1	3	2	1	1	1	1	0	1	0	5	3	11	2
67	1	0	1	1	1	0	4	2	1	0	1	0	0	2	2	1	0	1	1	0	0	0	3	2	9	2
68	1	1	0	0	0	1	3	2	0	1	0	1	0	2	2	1	0	1	1	1	1	1	6	3	11	2
69	1	0	0	1	0	1	3	2	0	1	0	1	0	2	2	0	1	1	1	1	0	0	4	2	9	2
70	1	1	0	1	1	1	5	3	0	1	1	1	1	4	3	1	1	0	1	1	0	0	4	2	13	3
71	1	1	0	0	1	1	4	2	0	0	1	1	0	2	2	0	1	1	0	1	0	1	4	2	10	2
72	0	0	1	1	0	0	2	1	0	1	0	0	0	1	1	0	0	1	0	1	0	0	2	1	5	1
73	1	0	1	1	0	0	3	2	1	1	0	1	1	4	3	1	0	1	0	1	1	1	5	3	12	2
74	0	0	1	0	0	0	1	1	1	1	0	0	1	3	2	0	1	0	1	0	0	1	3	2	7	2
75	1	0	0	1	1	1	4	2	1	1	0	1	1	4	3	1	1	1	1	1	0	1	6	3	14	3
76	1	1	1	0	1	1	5	3	1	0	1	1	1	4	3	0	1	1	1	1	1	1	6	3	15	3
77	1	0	0	1	0	1	3	2	1	0	1	0	0	2	2	0	1	1	1	0	0	1	4	2	9	2
78	1	0	1	1	1	0	4	2	0	1	0	1	0	2	2	1	1	1	1	0	0	1	5	3	11	2
79	1	1	0	0	0	1	3	2	0	1	0	1	0	2	2	1	0	1	1	0	1	0	4	2	9	2
80	1	0	1	1	1	1	5	3	0	1	1	1	1	4	3	1	0	1	1	1	0	1	5	3	14	3
81	1	1	0	1	1	1	5	3	0	0	1	1	0	2	2	1	0	1	1	1	1	1	6	3	13	3
82	1	1	0	0	1	1	4	2	0	1	0	0	0	1	1	0	1	1	1	1	0	0	4	2	9	2
83	0	1	1	1	0	0	3	2	0	1	1	0	1	3	2	1	0	1	1	0	1	0	4	2	10	2
84	1	0	1	1	1	0	4	2	1	0	1	0	0	2	2	1	0	1	1	0	0	0	3	2	9	2

Anexo 5. Base de datos prueba piloto

Encuestado	P.1	P.2	P.3	P.4	P.5	P.6	P.7	P.8	P.9	P.10	P.11	P.12	P.13	P.14	P.15	P.16	P.17	P.18	Total
1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	**3**
2	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	1	1	0	**6**
3	0	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	**5**
4	1	0	0	1	1	1	0	1	0	1	1	0	0	1	1	1	0	1	**11**
5	1	0	0	0	1	1	1	0	0	1	1	0	1	1	1	1	1	1	**12**
6	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	0	1	1	**15**
7	1	0	0	1	1	0	0	0	1	0	0	1	0	1	0	1	0	0	**7**
8	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	**16**
9	0	0	0	0	1	0	0	1	0	0	0	1	0	1	1	0	0	1	**6**
10	1	1	0	1	1	1	1	0	1	1	1	0	1	1	1	1	1	1	**15**
11	1	0	1	0	0	1	0	1	0	0	1	1	1	0	0	0	0	0	**7**
12	0	1	1	0	1	1	0	1	1	1	0	1	0	1	1	1	1	1	**13**
13	1	1	0	1	1	0	1	0	1	1	1	1	1	1	0	0	1	1	**13**
14	0	0	0	1	0	1	1	1	0	0	0	0	0	1	1	0	0	1	**7**
15	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	0	0	1	**8**
p	0,60	0,33	0,40	0,47	0,53	0,60	0,47	0,53	0,33	0,53	0,60	0,47	0,53	0,93	0,60	0,47	0,47	0,73	
q (1 - p)	0,40	0,67	0,60	0,53	0,47	0,40	0,53	0,47	0,67	0,47	0,40	0,53	0,47	0,07	0,40	0,53	0,53	0,27	
p*q	0,24	0,222	0,24	0,249	0,249	0,24	0,249	0,249	0,222	0,249	0,24	0,249	0,249	0,062	0,24	0,249	0,249	0,196	
∑ (p*q)	4,14																		
Vt	17,40																		
N	18																		
Kr(20)	***0,762***																		

$$Kr(20) = \frac{K}{K-1}\left[\frac{Vt - \sum(p * q)}{Vt}\right]$$

Kr(20) = Coeficiente de Kuder–Richardson

K = Número de Ítems

p = Proporción de éxito para cada ítems

q = Proporción de incidente para cada ítems

Vt = Varianza total de los ítems

Anexo 6. Evidencias de la investigación

"Año de la Universalización de la salud "

Lima, 23 de enero de 2020

SR.
JORGE FCO. DEL MONTE
EMPRESA NAVIERA ELCANO-GESTION NAUTICA

Presente-

Mediante la presente me dirijo a usted, primeramente, para saludarle y a la vez solicitar de su autorización para desarrollar una investigación a bordo de los buques que integran la flota de tan distinguida empresa, la misma es conllevada por Maricela Yannet Mantari Muchaypiña y Billy Jeremy Guevara Romero, quienes optamos al título académico de Oficial Marina Mercante en la especialidad de puente y maquinas en la Escuela Nacional de Marina Mercante Almirante "Miguel Grau"

La investigación tiene como objetivo: Determinar el nivel de conocimiento de los riesgos cibernéticos marítimos en la tripulación de la flota de la empresa naviera "El Cano", Lima - 2020, para ello se aplicará un cuestionario a la tripulación embarcada en los diferentes buques, destacando la importancia de los riesgos cibernéticos en el transporte y las operaciones marítimas, dado que en la actualidad se han registrados muchos acontecimientos relacionados a este factor, a tal fin los resultados de este estudio ofrecerán un panorama asociado a la ciberseguridad en el entorno de la empresa, que permitirá promover acciones y estrategias para contrarrestar vulnerabilidades en equipos y sistemas a bordo, aumentando el nivel de conocimiento y la concientización en los tripulantes acerca de la seguridad cibernética.

Así mismo se resalta que la información recolectada en este proceso, será de uso confidencial, y exclusivo para fines académicos, los cuestionarios no serán identificados, manteniendo en anonimato la identidad de los participantes.

Agradecidos por toda la colaboración prestada.

Atentamente;

Maricela Yannet Mantari Muchaypiña
DNI:48228952

Billy Jeremy Guevara Romero
DNI: 73061152

JORGE FCO. DEL MONTE
GESTION NAUTICA
DNI : 14890577D

Re: PERMISOS DE ENTRADA

maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
Vie 24/01/2020 08:31
Para: Del Monte, Jorge <JDelMonte@navieraelcano.es>

3 archivos adjuntos (1 MB)
Solicitud a la empresa; Solicitud a la empresa 2; Solicitud a Empresa 1.docx;

Buenos Días Capitán

Adjuntarle recibido el mensaje. Quería preguntarle si podría mandarme la cantidad de tripulación con la que contaremos y si podría enviarme los documentos antes requeridos (el formato de autorización firmado ,ficha de validación)para poder empezar con la parte estadística.

Reiterarle mi más profundo agradecimiento por su apoyo y colaboración con este tema . A espera de su respuesta ,completamente a disposición .

Atentamente

Cdte Mantari M maricela

Obtener Outlook para Android

From: Del Monte, Jorge <JDelMonte@navieraelcano.es>
Sent: Friday, January 24, 2020 8:09:40 AM
To: Secada Juan <JSecada@cosmos.com.pe>
Cc: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
Subject: PERMISOS DE ENTRADA

Buenos días Juan
Por favor solicita los permisos de entrada en Melchorita para nuestro Cadetes Maricela Yannet Mantari Muchaypiña (DNI 48228952) y Billy Jeremy Guevara Romero (DNI 73061152) que tienen prevista realizar una encuesta a bordo del Castillo de Santisteban para su Licenciatura
Gracias por anticipado
Saludos cordiales,
JORGE FCO. DEL MONTE
SUBDIRECTOR FLOTA-GESTION NAUTICA
ELCANO-MADRID

Re: Cdte Mantari Muchaypiña Maricela -Trabajo de Investigacion

Del Monte, Jorge <JDelMonte@navieraelcano.es>
Mié 22/01/2020 12:35

Para: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>

Buenas tardes Maricela
Hoy he estado muy ocupado pero he leído tu encuesta que me parece perfecta,
Se la he pasado a un Inspector
Para cumplimentarla y se la pasaré a nuestro Jefe de sistemas
Mañana te enviaré las listas de tripulantes y mi autorización para COSMOS y le enviaré con copia a ellos
Suerte
Saludos cordiales,
JORGE FCO. DEL MONTE
ELCANO-GESTION NAUTICA

De: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
Fecha: miércoles, 22 de enero de 2020, 17:12
Para: "Del Monte, Jorge" <JDelMonte@navieraelcano.es>
Asunto: Cdte Mantari Muchaypiña Maricela -Trabajo de Investigacion

Date: 01/22/20 - 17:12:50
From: maricela jannet mantari muchaypiña

External email: Do not click links or open attachments if you do not recognize the sender

Buenas tardes Capitán

Me atrevo a escribirle nuevamente el día de hoy para informarle lo siguiente : El día de hoy me he acercado a la empresa Cosmos ,En el cual me derivaron con el señor Juan Secada ,el me solicita mandarle un correo electrónico a la siguiente dirección **melchorita@cosmos.com.pe** especificando los motivos para estar abordo del buque el 01-02-2020 y ademas adjuntarle un documento en el cual usted me autorice el ingreso a la nave emitido por usted con firma y pasaporte o libreta de embarco ,en el cual usted especifica también los motivos .De esta forma el podrá hacer el tramite necesario .Cabe resaltar que ese documento de autorización de su parte también lo anexaría en la tesis ,de esta forma se le daría credibilidad a la investigación .Hoy también me acerque a la escuela y el jefe de investigación ,me aconsejo también sobre ese documento ,donde usted me autorice estar a bordo de la nave ese día para la realización de la encuesta ,ademas de otro documento en el cual usted me autorice hacer la tesis en los buques de la empresa como motivo que se mejore el nivel de conocimiento de los riesgos marítimos y se forme una mayor conciencia y aplicación del tema en la tripulación , de esta forma estos dos documentos serian el respaldo de autorización .
Permanezco atenta a su respuesta y a disposición de cualquier requisito que usted me solicite .

reiterándole mi agradecimiento por el tiempo y ayuda brindada en esta investigación .

Saludos Cordiales

Atentamente

Cdte Mantari M maricela

Re: Cdte Mantari Muchaypiña Maricela (LNG Castillo de Mérida) -trabajo de investigación

Del Monte, Jorge <JDelMonte@navieraelcano.es>
Mar 21/01/2020 02:08

Para: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>

Buenos días Maricela
En el Castillo de Mérida no te van a poder atender debido a que tiene un vetting te sugiero el Castillo de Santisteban que tiene oprevista su llegada a Melchorita el día 01 de Febrero mientras podrías ir pasando la encuesta a los otros buques y por favor envíamela a mi
El Agente en Melchorita es COSMOS en Lima para que puedas pedir el permiso de entrada
Saludos cordiales,
JORGE FCO. DEL MONTE
ELCANO-GESTION NAUTICA

De: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
Fecha: lunes, 20 de enero de 2020, 18:41
Para: "Del Monte, Jorge" <JDelMonte@navieraelcano.es>
Asunto: RE: Cdte Mantari Muchaypiña Maricela (LNG Castillo de Mérida) -trabajo de investigación

Date: 01/20/20 - 18:41:06
From: maricela jannet mantari muchaypiña

External email: Do not click links or open attachments if you do not recognize the sender

Muchas gracias capitán ,el día de mañana le estaría enviando la encuesta para poder real izarla en los buques Castillo de Mérida ,Castillo de Caldelas,Castillo de Santi esteban,Castillo de Malpica,Castillo de Monte real,Castillo de Navia .

Para darle mayor credibilidad a la investigación nos sugieren realizara personalmente a uno de los barcos si es que existe la posibilidad ,he estado investigando y se que el barco Castillo de Mérida ,llegaría a Chile próximamente ,usted cree que es factible poder realizara ,yo estaría llendo a puerto si es que se da a autorización únicamente para poder realizar la encuesta si en caso se autorice .En caso no se podría ,trabajaríamos con lo que usted nos indique.

A espera de su respuesta ,para así saber con el numero exacto de muestra que tendríamos para la validación de datos ,agradeciendo nuevamente con su colaboración y su apoyo en mi trabajo .

Atentamente

CDT Mantari Muchaypiña Maricela

De: Del Monte, Jorge <JDelMonte@navieraelcano.es>
Enviado: lunes, 20 de enero de 2020 12:30
Para: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
Asunto: Re: Cdte Mantari Muchaypiña Maricela (LNG Castillo de Mérida) -trabajo de investigación

Buenas tardes Maricela
Yo te autorizo a efectuar dicha encuesta en los buques que desees
Informame que buques quieres y envíame la encuesta para que la haga circular y llegue a tu destino

Saludos cordiales,

RE: PERMISOS DE ENTRADA

Solis Oswaldo <osolis@cosmos.com.pe>
Jue 30/01/2020 12:30

Para: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
CC: Cosmos - Melchorita <Melchorita@cosmos.com.pe>; Del Monte, Jorge <JDelMonte@navieraelcano.es>; Secada Juan <JSecada@cosmos.com.pe>; Felix Tragodara <ftragodara@seapacific.org>

Estimada Maricela
Buenas tardes ,

De acuerdo a nuestra conversación , la cita de espera de tu compañero Billy Jeremy y el Ud. deberá ser en el Hotel Palmetto San Miguel el día 01 feb a las 1400 Hrs para sus traslados hacia Pampa Melchorita y deberán acomodarse para venir en la movilidad de los tripulantes que desembarcarán el 01feb tarde/noche .

Dejo numero de contacto del Sr Felix Tragodara que se encargará de sus traslados (999 070 007)

Saludos ,

Oswaldo Solis Berrios
Vessel's Operator (Operations Department)

COSMOS
AGENCIA MARITIMA
A DP World Company

T: (511) 7144444 Ext (Anexo) 819
C: (51) 943158976

Cosmos Agencia Marítima S.A.C.
Jr. Mariscal Miller 450
Callao 1
Perú

www.cosmos.com.pe

"La seguridad es sacrosanta; no será y no puede ser comprometida"

De: Solis Oswaldo <osolis@cosmos.com.pe>
Enviado: lunes, 27 de enero de 2020 11:19
Para: maricela jannet mantari muchaypiña <maricella_mm@hotmail.com>
Cc: Cosmos - Melchorita <Melchorita@cosmos.com.pe>; Del Monte, Jorge <JDelMonte@navieraelcano.es>; Secada Juan <JSecada@cosmos.com.pe>
Asunto: RE: PERMISOS DE ENTRADA

Estimada Maricela
De acuerdo a lo conversado agradeceré enviarnos copia de pasaportes y libreta de marino a fin de gestionar sus permisos ante Terminal Melchorita

Saludos ,

Oswaldo Solis Berrios

INSTRUMENTO

NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS

Estimado Colaborador: Después de haber sido informado adecuadamente sobre el propósito científico de nuestra investigación., agradeceremos su colaboración respondiendo cada una de las preguntas del presente cuestionario. Para ello, sírvase escoger la opción que usted considere correcta:

Preguntas generales:

Años de servicio: 4 Cargo a bordo: 3RD MATE

Dimensión: Equipos y sistemas vulnerables

1. **¿Un ataque cibernético al Sistema de Identificación Automática (AIS) puede generar?**

   a) Colisiones entre buques.
   b) Afectar la interconectividad de comunicación.
   c) Crear la simulación de un barco que puede ser detectado por otros barcos y puertos.
   d) Todas las anteriores.

2. **¿El Sistema Electrónico de Visualización e Información de Cartas (ECDIS), puede ser afectado cibernéticamente por?**

   a) El alto riesgo de exposición que implica el proceso de actualizaciones del sistema.
   b) Al no tener antivirus instalado.
   c) Estar interconectado a los equipos de navegación.
   d) Todas las anteriores.
   e) a y b son las correctas.

3. **¿Si los operadores de navegación toman medidas que desvíen a la embarcación de su ruta poniendo en riesgo a la tripulación, pueden estar frente a un ataque cibernético al?**

   a) Sistema de Identificación Automática (AIS).
   b) Sistema de Posicionamiento Global (GPS).
   c) Sistema electrónico de visualización e información de cartas (ECDIS).
   d) Todas las anteriores.

4. **¿Cuál de los siguientes sistemas considera usted que son vulnerables ante un ataque cibernético?**

   a) Sistemas de carga y descarga de aguas de lastre.

b) Sistemas de carga y descarga de aguas residuales.
c) Sistemas de emisiones de gases.
d) Ninguna de las anteriores.
e) Todas las anteriores.

5. **¿Los principales ataques cibernéticos reportados en la industria marítima están enfocados a los equipos?**

a) Equipos de navegación.
b) Sistemas de comunicación.
c) Plataformas petroleras.
d) Todas las anteriores.

6. **¿Si una persona mal intencionada infecta con un virus las computadoras de las consolas de máquina, que fallas ocasionaría?**

a) Bloqueo del motor principal y motores auxiliares.
b) Desactivación de alarmas.
c) Reboce de los tanques.
d) Todas las anteriores.
e) Ninguna de las anteriores.

Dimensión: Tipos de amenazas

7. **¿En un ataque cibernético donde el atacante encripta los datos, secuestrando los sistemas y la información para solicitar que paguen un rescate, se debe a una amenaza informática de tipo?**

a) Malware
b) Gusanos
c) Ransomware
d) Troyanos

8. **¿En la empresa naviera los ciberatacantes pueden infiltrarse, dañar y causar acciones autenticadas y no deseadas en los sistemas de información mediante?**

a) Gusanos
b) Troyanos
c) Software maliciosos
d) Todas las anteriores

9. **¿Los ataques cibernéticos mediante phishing permiten a los ciberatacantes generar en una empresa naviera?**

a) La suplantación de identidad mediante el envío de correos electrónicos.

b) Controlar las cargas transportadas en las embarcaciones.
c) Contrabandear mercancías.
d) Todas las anteriores.
e) a y b son correctas.

10. ¿Los tripulantes de un barco pueden comprometer los sistemas de la industria marítima ante un riesgo cibernético?

a) Abriendo correos electrónicos desconocidos.
b) Utilizando medios extraíbles en sitios no permitidos.
c) Accediendo a sitios web y redes sociales sin restricciones.
d) Todas las anteriores.

11. ¿En la empresa naviera se pueden generar atacantes cibernéticos que ponen en peligro la seguridad de las embarcaciones y sus tripulantes, motivados por?

a) Actos criminales y terroristas.
b) Beneficio económico.
c) Competitividad industrial.
d) Espionaje gubernamental.
e) Todas las anteriores.
f) a y b son correctas.

Dimensión: Protocolos de seguridad

12. ¿La empresa naviera para atender un ataque cibernético y garantizar la operatividad de la embarcación, debe contar con?

a) Software de alta tecnología.
b) Equipos y sistemas de última generación.
c) Un equipo de emergencia cibernética interna y externa.
d) Todas las anteriores.

13. ¿Para prevenir y abordar automáticamente la presencia de amenazas / actividades maliciosas en los sistemas a bordo, se deben?

a) Restringir el acceso a la red de internet de la embarcación.
b) No permitir el uso de equipos personales.
c) Instalar en la empresa software de escaneo informático.
d) Todas las anteriores.

14. ¿Cómo medida de seguridad ante un ataque cibernético, en la embarcación debe existir la provisión de un medio alternativo de comunicación, que funcione independientemente de todos los demás sistemas de a bordo?

a) De acuerdo.

b) En desacuerdo.
c) Desconoce.

15. **¿Cómo protocolo de seguridad todos los tripulantes de la embarcación?**

a) No deben conectarse a la internet mientras navegan.
b) No deben usar sus dispositivos personales.
c) Deben tener capacitación básica sobre los riesgos cibernéticos, vulnerabilidades de los equipos y medidas preventivas.
d) Todas las anteriores.

16. **¿Las regulaciones para abordar los problemas de seguridad cibernética, estipulan directrices orientadas a?**

a) Identificar los sistemas e información vulnerable.
b) Proteger los sistemas y los datos, implantando medidas de control.
c) Crear situaciones para detectar amenazas.
d) Implantar planes de respuesta para dar resiliencia y restaurar los sistemas.
e) Acciones para recuperar los sistemas necesarios para las operaciones.
f) Todas las anteriores.

17. **¿Cuál de las siguientes normativas regulan la gestión ante los riesgos cibernéticos en una empresa naviera?**

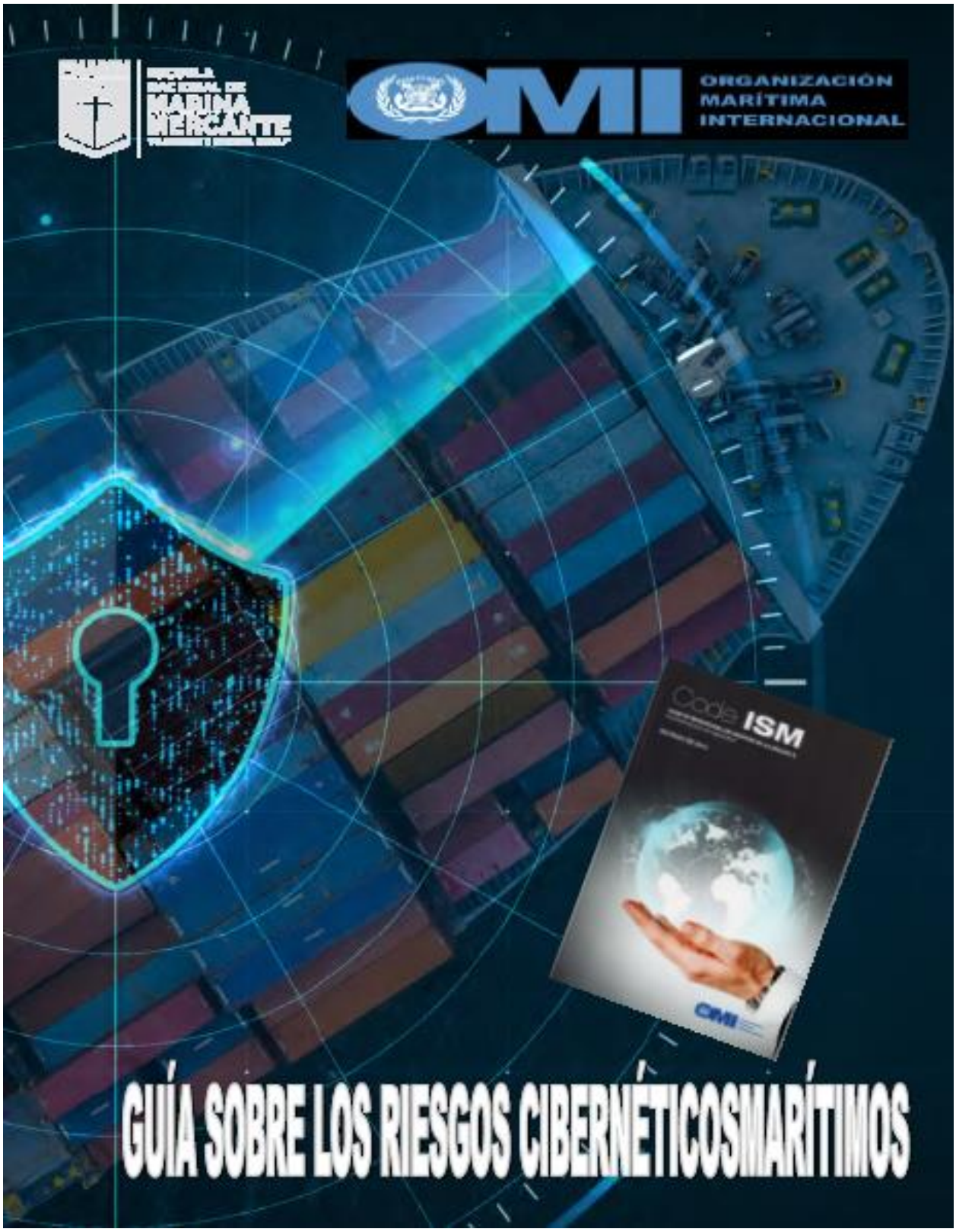
a) Código Internacional de Seguridad de Buques e Instalaciones Portuarias (ISPS).
b) MSC-FAL.1 / Circ.319.
c) Norma ISO/IEC 27001.
d) Todas la anteriores.
e) a y c son correctas.

18. **¿Hasta cuándo la OMI otorgó a los propietarios y gerentes de buques incorporar la gestión del riesgo cibernético en el sistema de seguridad del buque?**

a) A partir del 2019.
b) A partir del 2020.
c) A partir del 2021.
d) A partir del 2022.

Anexo 7. Evidencias fotográficas de aplicación del instrumento

Anexo 8. Guía de los Riesgos Cibernéticos Marítimos




IMO
RIESGOS CIBERNÉTICOS
AUTORES:
Maricela Mantari Muchaypiña
Guevara Romero Billy
La Guia Rápida "Riesgos Cibernéticos Marítimos " nace del trabajo de investigación "NIVEL DE CONOCIMIENTO DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS EN LA TRIPULACIÓN DE LA FLOTA DE LA EMPRESA NAVIERA "ELCANO,S.A ", LIMA-2020"con el propósito de familiarizar y concientizar a la tripulación sobre los riesgos cibernéticos a los que estamos expuestos como marinos mercantes, brindándoles los conocimientos teóricos ,recomendaciones ,y acciones para que puedas saber a que te enfrentas .Cabe resaltar la importancia de este tema ,ya que es de gran impacto en la seguridad de la compañía, el buque y la tripulación.
Recuerda que la mejor defensa eres tu ,informándote y concientizándote puedes ser par-

ANTECEDENTES

ATAQUES CIBERNÉTICOS MARÍTIMOS

-ATAQUE A MAERSK !

-Malware NotPeya de 2017

-Reinstalación de "4,000 nuevos servidores, 45,000 nuevas PC y 2,500 aplicaciones.

-GPS PIRATEADO DE UN YATE

-Señal GPS pirateado en el Mar Mediterráneo.

-Convencieron al oficial de cambiar de rumbo ,llevándolos hacia el peligro

-20 BUQUES CON SEÑAL GPS DIFERENTE

-Colocaron a todos los buques en territorio ruso

-Diferencia de 100 millas en el Mar Negro

-PUERTO DE SAN DIEGO

-Ataque de Rasomware.

-Perjudico sus sistemas de TI

-2018

-PUERTO DE AMBERES

-Los narcotraficantes reclutaron hackers para violar los sistemas de TI que controlaban el movimiento y la ubicación de los contenedores


Internet y sus sistemas de intranet fueron cerra-
BW Group which commands
USD 2.0 bn LNG fleet & USD 2.1 bn LPG fleet
came under attack in July 2017
COSCO interrumpio sus acciones de descarga
LISTA CRONOLOGICA DE ATAQUES Y
2010
2011
2012
2013
2014
2016
2017
2018
Drilling rig infected with malware
Pirate Cyber Attack
GPS jamming /spoofing
Hacking of cargo tracking system
ISO 27001/27002
IEC 62443
U.S. Port hacker attack
Bulk carrier SWB shuts down – ransomeware
January
BIMCO Cyber security guideline
February
ABS Guidance note
LR Guidance note
September
DNV-GL guideline
Major shipping company infected by ransomeware
July
IMO guidelines Maritime cyber risk management
"Prepare for the unknown"
May
EU GDPR
July
DNV-GL class notation

¿Qué es lo primero que debo saber ?

CIBERESPACIO

Para comprender los riesgos cibernéticos, se debe identificar el ciberespacio, el cual se puede definir como "un conjunto de redes y sistemas de comunicación que están interconectados, directa o indirectamente" (Pastor, Pérez, Arnáiz, y Taboso, 2009). El ciberespacio en el ámbito marítimo es, por lo tanto, el entorno que engloba los componentes tecnológicos, es decir, las vulnerabilidades inherentes a su empleo y las amenazas que pueden afectarlos, como los factores humanos ya que son estos los que ca-

RIESGOS CIBERNÉTICOS MARÍTIMOS

La ciberseguridad marítima es un tema en rápido crecimiento dentro de la industria naviera, debido a las continuas innovaciones y avances tecnológicos, que resultan en una desconexión del sector para adecuarse a las nuevas exigencias informáticas, causando vulnerabilidades y amenazas en los equipos a bordo, por lo que la Organización Marítima Internacional y otros organismos involucrados al ámbito marítimo identifican que estos problemas deben ser reconocidos y se deben coordinar esfuerzos para mitigar y evitar que

En este sentido el Comité de Facilitación y el Comité de Seguridad Marítima (MSC-FAL) de la Organización Marítima Internacional (OMI) señala que:

> El riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posible, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas. (MSC-FAL, 2017, p.1)

IMO
INTERNATIONAL MARITIME ORGANIZATION

Bajo esta primicia las empresas navieras deben adoptar todos los mecanismos disponibles para prevenir cualquier circunstancia que coloque en peligro a los tripulantes por un ataque cibernético, ante ello "los interesados deberían tomar las medidas necesarias para salvaguardar el transporte marítimo de las amenazas y vulnerabilidad actuales y emergentes relacionadas con la digitalización, la integración y automatización de los procedimientos y sistemas del transporte marítimo" (MSC-FAL, 2017, p.1).

Los factores de ***vulnerabilidad*** más comunes del sector marítimo incluyen situaciones en las que un barco es atacado por terroristas en una forma de acto político, o piratas/grupos criminales que secuestran la carga. Detrás de estos secuestros de carga, los motivos varían de ser un acto político a la generación de fondos. Los contenedores son usados como método de transporte en diferentes delitos transnacionales, como el contrabando de drogas, armas en-

TIPOS DE AMENAZAS

La complejidad de los sistemas y las partes interesadas involucradas en la operación marítima requieren que cada empresa considere las amenazas desde diferentes perspectivas, de acuerdo con el servicio prestado y las vulnerabilidades del sistema. Sin embargo, de acuerdo a la Boyes, Isbell y Luck (2016), las amenazas presentadas en la industria marítima se pueden clasificar en dos elementos principales: las amenazas direc-

AMENAZAS DIRECTAS

- **HACKTIVISMO O GRUPO ACTIVISTA**

- **COMPETIDOR INDUSTRIAL DE ESPIONAJE**

- **IMPULSADO POR EL GOBIERNO O PATROCINADO POR EL ESTADO.**

- **TERRORISMO**

AMENAZAS DIRECTAS NO INTENCIONALES

AMENAZA INTERNA O POR NATURALEZA

Pueden ser errores de empleados o proveedores de servicios. Los empleados internos pueden comprometer los sistemas de la industria marítima por negligencia, descuido, ignorancia o simplemente error humano, abriendo accidentalmente correos electrónicos maliciosos, utilizando medios extraíbles infectados o accediendo a sitios web y redes sociales falsas.

Estos actos no intencionales exponen los sistemas o datos confidenciales a amenazas, poniendo la seguridad de las empresas en diferentes niveles de riesgo dependiendo del acceso que tengan a los sistemas (Boyes, *et. al.*, 2016).

Se reconoce que este tipo de amenaza representa una falta de capacitación y conciencia de los tripulantes, representando el máximo riesgo para las empresas. Además, "por naturaleza" puede describirse como un error en un sistema, software o aplicación derivado de una mala instalación o fabricación, que no proporciona las medidas de seguridad necesarias para mantener el sistema seguro (NEP&I, 2017).

MALWARE

¿Qué es ?

Es un software maliciosos diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.. Los tipos de malware incluyen spyware (software espía), adware (software publicitario), phishing, virus, troyanos, gusanos, rootkits, ransomware y secuestradores del navegador. El 77 % de los ataques perpetrados en el mundo marítimo es por este medio.

¿De donde proviene ?

Frecuentemente, el malware accede a su dispositivo a través de Internet y del correo electrónico, aunque también puede conseguir acceder a través de sitios web hackeados, demos de juegos, archivos de música, barras de herramientas, software, suscripciones gratuitas o cualquier otra cosa que descargue de Internet en un dispositivo que no esté protegido con software antimalwa-

- Navegar por Internet sin actualizar los programas de antivirus o anti-malwares,
- Navegar en redes poco seguras,
- Descargar programas y softwares de fuentes desconocidas,
- Abrir archivos con extensiones desconocidas

¿Cómo prevenir ?

La forma más efectiva de prevenir *malware* es la instalación de programas que los detecten como, por ejemplo, antivirus, anti-*malware* o anti-*spywares*, que puedan escanear el computador regularmente, prevenir ataques y mantener una protección actua-

¿Cómo saber si mi computador esta infectado ?

- Procesamiento lento
- Ejecuta procesos desconocidos
- Interrumpe su conexión a Internet
- Aparecen ventanas con mensajes de advertencia
- Se comporta de manera extraña
- Formas de contagio de malwares
- Abrir archivos desconocidos enviados por correo electrónico

RANSONWARE

¿ Qué Hace?

Restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado ransomware como WannaCry, Petya, Cerber, Cryptolocker y Locky .

¿ Cómo evitarlo?

-Asegúrese de que todo el software de su equipo está actualizado, incluyendo su sistema operativo, su navegador y cualquier complemento de barra de herramientas que utilice.
-Asegúrese de que su software antivirus y su protección cortafuegos están actualizados

¿ Quién lo crea?

Lo crean estafadores con un gran conocimiento en programación informática. Puede entrar en su PC mediante un adjunto de correo electrónico o a través de su navegador si visita una página web infectada con este tipo de malware. También puede acceder a su PC a través

¿ Cómo reconocerlo?

PHISHING

¿ Qué es ?

El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que los tripulantes revelen información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

¿Cómo Funciona ?

Los mensajes de phishing parecen provenir de organizaciones legítimas como PayPal, UPS, una agencia gubernamental o su banco. Sin embargo, en realidad se trata de imitaciones. Los correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa,

embaucándolo para que facilite información sobre su cuenta, lo que puede

¿Cómo lo evito ?

- No responda a enlaces en correos electrónicos no solicitados, Facebook o mensajes de texto (celular)
- No abra archivos adjuntos de correos electrónicos no solicitados.
- Proteja sus contraseñas y no las revele a nadie.
- No proporcione información confidencial a nadie por teléfono, en persona o a través del correo electrónico.
- Mantenga actualizado su navegador y aplique los parches de seguridad.
- Introduce tus datos confidenciales sólo en sitios web seguros. Para que un sitio se pueda considerar como 'seguro', el primer paso -aunque no el único- es que empiece por "https://", lo que implica que sigue el protocolo de transferencia de hipertexto, y que el navegador muestre el icono de un candado cerrado.

SPEAR-PHISHING

A diferencia de los correos electrónicos de phishing normales, los de spear-phishing están muy personalizados. El objetivo final es el mismo, engañar al destinatario para que haga clic en un enlace URL o un archivo adjunto malicioso pero en este caso, el mensaje contiene el nombre, la empresa o el cargo de la víctima, o se mencionan a sus compañeros de trabajo y contactos. Estos detalles personales hacen mucho más probable que el usuario abra o ejecute el contenido malicioso. Además, dada la proliferación de redes sociales y sitios web para hacer contactos profesionales, a los ciberdelincuentes les resulta relativamente sencillo reunir la información personal necesaria

¿Cómo reconocerlo ?

Pueden aparecer iconos nuevos o no identificados en la barra de tareas en la parte inferior de su pantalla, y las búsquedas pueden provocar que se le redirija a un motor de búsqueda diferente. Aparecen mensajes de error aleatorios cuando realiza operaciones que antes funciona-

SPYWARE

Es un tipo de malware difícil de detectar. Recopila información sobre sus hábitos y su historial de navegación o información personal (como números de tarjetas de crédito) y a menudo utiliza Internet para enviar esta información a terceros sin su conocimiento. Los keyloggers son un tipo de spyware que monitoriza sus pulsaciones en el teclado

¿Cómo evitarlo ?

-Asegúrese de que su navegador, su sistema operativo y su software tienen las actualizaciones y los parches de seguridad más recientes.
-Establezca niveles más altos de seguridad y privacidad en su navegador.
-Extreme las precauciones si frecuenta sitios de intercambio de archivos.
-No haga clic en las ventanas emergentes de publici-

¿De donde provienen ?

Está incluido dentro de otro software o en descargas de sitios de intercambio de archivos (por ejemplo, sitios donde descarga música o películas gratis) o se instala cuando abre un adjunto de un correo electrónico. Debido a la naturaleza secreta del spyware, la mayoría de la gente ni siquiera sabe

EQUIPOS Y SISTEMAS VULNERABLES

Los barcos utilizan cada vez más sistemas que dependen de la digitalización, la integración y la automatización, los cuales requieren una gestión del riesgo cibernético a bordo. A medida que la tecnología continúa desarrollándose, la tecnología de la información (TI) y la tecnología operativa (OT) a bordo de los bu-

TECNOLOGIA DE LA

la TI cubre los aspectos de tecnologías para el procesamiento de la información, incluidas las tecnologías de software, hardware y comunicación

TECNOLOGIA OPERATIVA

Los sistemas de OT controlan el mundo físico y los sistemas de TI administran los datos. OT es un hardware y software que monitorea / controla directamente

Information technology

- IT Networks
- Emails
- Administration, acc… crew lists, …
- PMS
- Stores req…
- Electro… nuals
- El… certificates
- …nts to work
- Charter party, notice of readiness, bill of lading..

Finance and reputation

Operation technology

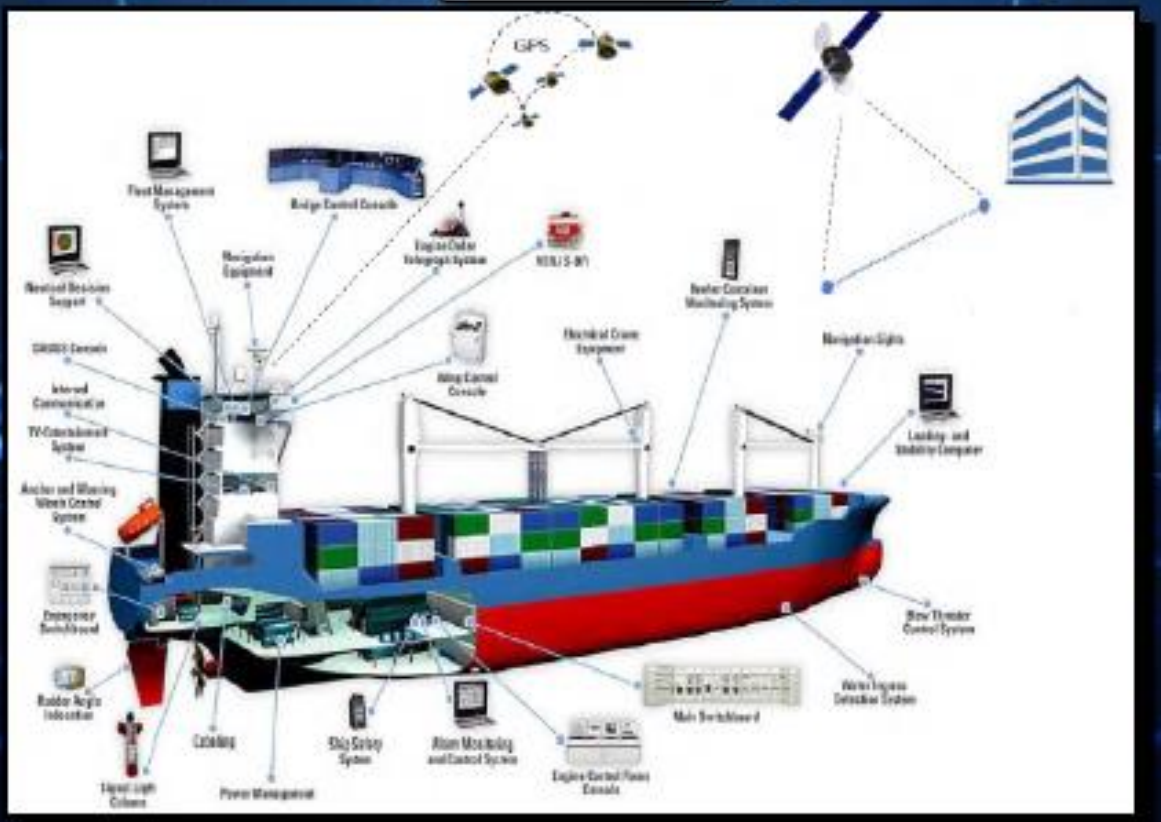
- PLC (Programmable Logic … ers)
- SCADA *(supervisory c… d data acquisition)*
- On-board mea… t and control
- ECDIS
- GPS
- R… support for engines
- …loggers
- …ngine & Cargo control
- Dynamic positioning, …

Life, Property and Environment

Por su parte MSC-FAL (2017), señalan que:

Las tecnologías cibernéticas se han convertido en esenciales para el funcionamiento y la gestión de los numerosos sistemas cruciales para la seguridad y la protección del transporte marítimo, y la protección del medio marino. En algunos casos, estos sistemas han de cumplir las normas internacionales y las prescripciones de las Administraciones de abanderamiento. No obstante, la vulnerabilidad generada por el acceso, la interconexión o el establecimiento de redes entre estos sistemas puede dar lugar a riesgos cibernéticos que deberían abordarse. (p. 1)

- LOS SISTEMAS DE PUENTE
- LOS SISTEMAS DE MANIPULACION Y GESTION DE LA CARGA
- LOS SISTEMAS DE PROPULSION Y GESTION DE LAS MAQUINAS
- LOS SISTEMAS DE COMUNICACION
- LOS SISTEMAS ADMINISTRATIVOS Y DE BIENESTAR DE LA TRIPULACION
- LOS SISTEMAS DE CONTROL DE ACCESO
- LOS SISTEMAS DE SERVICIO A LOS PASAJEROS
- LAS REDES PUBLICAS PARA LOS PASAJEROS



AIS

Sistema de identificación automática. El AIS opera mediante coordenadas GPS e intercambia datos sobre la posición de un barco, el rumbo e información primordial con la de otros barcos cercanos en alta mar y en la costa. El equipo de amenazas con visión de futuro de Trend Micro, pudo recrear una frecuencia VHF en AIS que simulaba un "barco falso" en un puerto y alertó a las embarcaciones cercanas que estaban en curso de colisión con otra embarcación. Además, expuso una lista completa de habilidades de "falsificación" de AIS, incluyen-

-Rumbo falso, velocidad, bandera y nombre del barco
-Alertas meteorológicas falsas que causan desviaciones del plan original del movimiento previsto
-Falsificación como autoridad de aplicación de la ley marítima (USCG)
-Plataformas de rescate falsas
-Situaciones de hombre al agua.
-Demasiados ecos de AIS que conduce a informes dobles y datos fal-

LOS EQUIPOS DE PUENTE MAS

ECDIS

Sistema Electrónico de Información de Visualización de Cartas .).Es el principal medio de navegación. El sistema ECDIS proporciona cartas digitales electrónicas que permiten al oficial de puente (OOD) navegar adecuadamente.Hay diferentes sensores que están conectados al ECDIS como : AIS, GPS, Radar ,los cuales son considerados los mas propensos a los ataques cibernéticos marítimos .El Ecdis al recibir la información de cartas más actualizada requiere que los sistemas ECDIS establezcan una conexión a través de redes de Internet no seguras a bordo de los barcos, lo que podría poner en riesgo la integridad de los datos de navegación de un barco (OCIA, 2016).

En enero de 2014, NCC Groups, desempeñó el papel de un pirata informático que intentaba acceder al ICS de un barco. Después de someterse a pruebas, "se encontraron varias debilidades de seguridad, incluida la capacidad de leer, descargar, reemplazar o eliminar cualquier archivo almacenado en la computadora que aloja

PROTOCOLOS DE SEGUIRDAD

La seguridad marítima puede verse como el conjunto de medidas preventivas proyectadas para proteger al sector marítimo mundial y para reducir el efecto de peligro, daño,

En este sentido el Comité de Facilitación de la OMI (FAL) y el Comité de Seguridad Marítima (MSC) definieron las Directrices de la OMI sobre la gestión del riesgo cibernético marítimo en MSC-FAL.1 / Circ.319. Ambos reconocieron la necesidad urgente de crear conciencia sobre las amenazas y vulnerabilidades del riesgo cibernético y proporcionar recomendaciones de alto nivel sobre cómo gestionar este hecho actual y emergente, incluyendo las áreas principales que apoyan la gestión eficaz del riesgo cibernético (identificar, proteger, detectar, responder y

OMI ORGANIZACIÓN MARÍTIMA INTERNACIONAL

¿Qué medidas se pueden tomar ?

El Plan de seguridad del buque SSP y el Manual de gestión de seguridad SMM pueden ser los documentos apropiados para incluir referencias a políticas y controles de ciberseguridad marítima,

- Capacitación y conocimiento de capitanes , oficiales, ingenieros y tripulación sobre riesgos y controles de ciberseguridad .
- Medidas de seguridad preventivas implantadas en el barco y en tierra para mitigar los riesgos en los sistemas de TI a un nivel aceptable .
- Política para el uso de medios almacenamiento extraíbles como memorias USB, Unidades externas ,CD Y DVD
- Política de seguridad de acceso a internet que indica restricciones aplicables según las operaciones que se realicen en el barco .
- Política y controles de acceso a la red para la tripulación y las redes inalámbricas WIFI.
- Política y controles de acceso a la red para la tripulación y las redes inalámbricas WIFI.
- Controles de acceso físicos y lógicos a los diversos sistemas de barcos en función de su nivel de sensibilidad .
- Análisis de riesgos de los sistemas informáticos de TI.

Plan de Contingencia para sistemas informáticos de tecnología de la información.

Politica y procedimientos para actualizar y mantener los sistemas de información y navegación.

Criterios de autorización para conexiones remotas desde la oficina de la compañía para el monitoreo y manteni-

¿Qué encontraremos en el ISM?

Los manuales, procedimientos y listas de verificación de seguridad cibernética deben tener su propia identidad y la documentación de respaldo debe incorporarse en un Manual de seguridad cibernética del buque (MCSEC), el mismo podría derivarse del SSP y SMM como en

La existencia de un plan de contingencia para los sistemas de navegación ECDIS debe estar en el SMM. En caso de que haya una contingencia, los detalles del Plan de Contingencia de los Sistemas de TI, incluido el ECDIS, deben

El control de acceso físico a diferentes áreas del barco debe indicarse en el SSP. Los controles de acceso lógico para los sistemas de TI en las diferentes áreas físicas se deben encontrar en el MCSEC

Cuando las lecturas de posición del barco en ECDIS no corresponden con las lecturas anteriores de ECDIS o las correcciones visuales actuales que sugieren un mal funcionamiento del sistema o una intercepción deliberada. Además de seguir los procedimientos recomendados por SMM para la navegación segura del barco, se debe consultar el procedimiento de gestión de incidentes cibernéticos MCSEC para evaluar el posible ciberincidente


ANTE LOS RIESGOS CIBERNÉTICOS
LA MEJOR DEFENSA ERES TÚ!