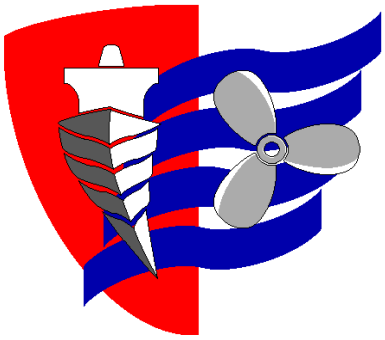
ESCUELA TÉCNICA SUPERIOR DE NÁUTICA

UNIVERSIDAD DE CANTABRIA



Trabajo Fin de Grado

METODOLOGÍA PARA UNA CIBERSEGURIDAD RESILIENTE EN UN BUQUE CIVIL

METHODOLOGY FOR A RESILIENT CIBERSECURITY IN A MERCHANT SHIP

Para acceder al Título de Grado en

INGENIERÍA NÁUTICA Y TRANSPORTE MARÍTIMO

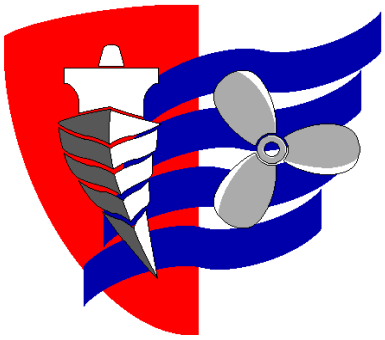
Autor: Dr. Josu Ruiz Godia

Director: Dr. Ernesto Madariaga Domínguez
Universidad de Cantabria

Marzo 2021

ESCUELA TÉCNICA SUPERIOR DE NÁUTICA

UNIVERSIDAD DE CANTABRIA



Trabajo Fin de Grado

METODOLOGÍA PARA UNA CIBERSEGURIDAD RESILIENTE EN UN BUQUE CIVIL

METHODOLOGY FOR A RESILIENT CIBERSECURITY IN A MERCHANT SHIP

Para acceder al Título de Grado en

INGENIERÍA NÁUTICA Y TRANSPORTE MARÍTIMO

Marzo 2021

ÍNDICE

RESUMEN

Este estudio, desarrolla una metodología para analizar y evaluar los ciberriesgos de un buque civil. Proponemos un plan de contingencia, medidas de defensa y de recuperación de los sistemas involucrados en un incidente de ciberseguridad. La amenaza al sector marítimo no es ficción, ya existen diversos incidentes y las consecuencias de un ataque podrían ser catastróficas. En los últimos años, se han multiplicado los episodios de ataques a equipos, redes a nivel mundial y la ciberseguridad es de la máxima importancia para los estados, los cuales publican y actualizan leyes para intentar frenar estas actividades que tanto perjudican a todos los sectores.

Debemos de proveernos de las mejores soluciones tecnológicas de seguridad que tengamos al alcance y realizar una monitorización continua, lo que nos dará a conocer en todo momento, qué protecciones tenemos y cuáles son los riesgos potenciales a los que nos enfrentamos. El incremento, ya imparable, del uso de la tecnología en la nube para controlar los sistemas de a bordo, tanto desde el propio buque como desde tierra por la compañía naviera, añade un escenario complejo que agrava la situación de defensa frente a posibles amenazas.

Las empresas marítimas, han de tener sistemas informáticos rígidos aplicando múltiples capas de medidas de protección y han de establecer un riguroso control de los usuarios y de los permisos de acceso a los sistemas.

PALABRAS CLAVE

Seguridad Marítima, Ciberseguridad Marítima, DAFO, Terrorismo Marítimo, Hackers, Malware, Sistema de Seguridad Nacional, Plan de Contingencia.

ABSTRACT

This academic study develops a methodology to analyze and evaluate the cyber risks of a motor merchant. We propose a contingency plan, defense measures and recovery of the systems involved in a cybersecurity incident. The threat to the maritime sector is not fiction, there are already several incidents and the consequences of an attack could be catastrophic. In recent years, episodes of attacks on computers and networks have multiplied worldwide and cybersecurity is of the utmost importance for states, which publish and update laws to try to stop these activities that are so damaging to all sectors.

We must provide ourselves with the best technological security solutions available to us and carry out continuous monitoring, which will let us know at all times what protections we have and what are the potential risks we face. The already unstoppable increase in the use of cloud technology to control on-board systems, both from the ship itself and from the shore by the shipping company, adds a complex scenario that aggravates the defense situation against possible threats.

Maritime companies, must have rigid computer systems applying multiple layers of protection measures and must establish rigorous control of users and access permits to the systems.

KEYWORDS

Maritime Safety, Maritime Cibersecurity, DAFO, Terrorism, Hackers, Malware, National Security System, Contingency Plan.

CAPÍTULO I: INTRODUCCIÓN

1.1. INTRODUCCIÓN

Este trabajo forma parte del Convenio entre el Ministerio de Defensa y la Universidad de Cantabria (Ministerio de Defensa, 2019), en concreto con la Escuela Técnica Superior de Náutica, para la investigación de los protocolos de Seguridad Marítima.

Se va a desarrollar una metodología para garantizar la seguridad informática a bordo de un buque civil. Este objetivo se alcanzará mediante la realización de una identificación y posterior evaluación de los Ciberriesgos. En las últimas décadas se ha impuesto, como base del análisis de la seguridad informática, el desarrollo de metodologías que la garanticen, mediante la realización de la identificación y posterior evaluación de los ciberriesgos. Este trabajo conserva la misma filosofía.

La amenaza al sector marítimo no es ficción y las consecuencias de un ataque podrían ser catastróficas. Podemos imaginar buques con todo tipo de cargas peligrosas navegando con los sistemas de carta electrónica hackeados o su señal del Sistema Global de Posicionamiento (GPS), con una posición alterada, un buque con la máquina parada en medio de un temporal por un ataque al sistema de propulsión, etc.

En los últimos años se han multiplicado los episodios de ataques a equipos y redes a nivel mundial y la ciberseguridad es de la máxima importancia para los Estados. Debemos de proveernos de las mejores soluciones tecnológicas de seguridad que tengamos al alcance y realizar una monitorización continua lo que nos dará a conocer, en todo momento, qué protecciones tenemos y cuáles son los riesgos potenciales a los que nos enfrentamos.

La globalización y la conexión total a nivel planetario de las redes, via cable o via radio donde una persona desde el lugar mas remoto o desde un país donde no exista control o tratados de seguridad, puede llegar a acceder a un equipo en la otra parte del mundo con un interés maligno y realizar un ataque.

Una de las características mas llamativas de esta temática es su dinamismo,

tanto en lo referente a los conocimientos previos, como en lo referente a los conocimientos actuales y futuros, muy cambiantes y diversos. Esta característica hace que sea difícil proponer medidas y asegurar una protección duradera, mas aun con el interés que hay en digitalizarlo todo. Queremos que todo se realice muy rápido, que todo sea controlable y no vemos lo que dejamos en el camino, muchas deficiencias de seguridad.

El teletrabajo y guardar los datos en “la nube” (Cloud Computing) aumentan el riesgo, la digitalización nos rodea, cada vez está mas cerca, antes era ciencia ficción, pero ahora podemos controlar las luces de casa, el termostato y hasta los electrodomésticos tienen conexión a internet. El incremento, ya imparable, del uso de la tecnología en la nube para controlar los sistemas de a bordo, tanto desde el propio buque como desde tierra por la compañía naviera, añade un escenario complejo que agrava la situación de defensa frente a posibles amenazas.

La llegada de Internet ha supuesto que se usen masivamente las redes también en los buques. Es el desarrollo, sin precedentes, de la Industria 4.0 lo que va a permitir tanto grandes mejoras como amenazas. El futuro se mueve hacia una industria marítima mas automatizada, integrada e interdependiente y, sin duda, con un aumento del riesgo.

La Organización Marítima Internacional (OMI), también ha sido objeto de un ataque informático en el año 2020. Se detectó la intrusión de ciberdelincuentes en su página web y sufrieron una interrupción de su servicio provocado por un sofisticado ciberataque. Los técnicos informáticos bloquearon los sistemas clave para evitar mayores daños por el ataque. Aún en el mes de febrero de 2021 la Web de la OMI está con problemas de acceso y la Web Global Integrated Shipping Information System (GISIS), la mayor parte de las veces se queda bloqueada.

En España existe un Sistema de Seguridad Nacional integrado por un Consejo de Seguridad Nacional del que depende, entre otros, el Consejo Nacional de Seguridad Marítima. Hasta hace pocos años, los ataques cibernéticos se

centraban en la industria y el objetivo estaba mas centrado en recopilar datos de patentes, producción o financieros.

Este interés ha cambiado en los últimos años y a eso hay que acompañarlo con unos ataques mucho mas sofisticados que se centran en dañar a las empresas y tomar el control de sus sistemas. Los atacantes buscan empresas financieras, compañías aéreas, energéticas, etc.

Las empresas deben de proveerse de sistemas rígidos, donde la clave pasa por la aplicación de múltiples capas de medidas de protección (capas, anillos de seguridad, para retrasar el ataque y su efectividad). Hay que realizar un estudio y un inventario detallado de todos los sistemas que pueden verse afectados y acompañarlo con una evaluación de riesgos de ataque informático en todos ellos así como con una guía de buen uso estableciendo un control de los usuarios y los permisos de acceso.

CAPÍTULO II: OBJETIVO Y METODOLOGÍA

2.1. OBJETIVO FUNDAMENTAL

Este Trabajo Fin de Grado titulado "METODOLOGÍA PARA UNA CIBERSEGURIDAD RESILIENTE EN UN BUQUE CIVIL", tiene por objetivo fundamental el desarrollar una metodología que garantice la seguridad informática a bordo de un buque civil. Este objetivo se alcanzará mediante la realización de una identificación y posterior evaluación de los ciberriesgos de un buque civil con independencia de su zona de navegación.

2.2. OBJETIVO METODOLÓGICO

Para alcanzar el Objetivo Fundamental de este Trabajo Fin de Grado, en Ingeniería Náutica y Transporte Marítimo, es necesario establecer una metodología que desarrolle como ensayo académico y se establezca un análisis crítico una metodología de trabajo para erradicar las ciberamenazas en un buque civil. Por Objetivo Metodológico, por consiguiente de este Trabajo Fin de Grado, se ha basado en:

- Realizar un análisis de Fortalezas, Oportunidades, Debilidades, Amenazas (DAFO/CAME), para analizar la implantación de las medidas de protección encaminadas a mejorar la ciberseguridad a bordo y poder de ese modo auditarla.

- Desarrollar una metodología para realizar una identificación y posterior evaluación de los ciberriesgos del buque respecto a la seguridad informática mediante la norma ISO 27001 *Information Security Management.*

- Diseñar un modelo de medidas de protección del buque frente a los riesgos informáticos actuales que implemente controles sencillos y seguros, así como desarrollar medidas de detección.

- Establecer planes de contingencia.

- Responder y Recuperarse de los incidentes de ciberseguridad del buque civil, con los conocimientos y destrezas que desarrollé cuando realicé el Máster en Ciberseguridad, en la Universidad Americana de Europa (UNADE), en el año

2018.

- A su vez, como herramientas mecánicas, este Trabajo Fin de Grado, se ha realizado, tras la consulta bibliográfica de:

1. Documentos de la Organización Marítima Internacional (OMI): la Resolución MSC.428(98) del 2017, *Maritime Cyber Risk Management in Safety Management Systems* y la MSC-FAL.1/Circ.3 *Guidelines on Maritime cyber risk management, Directrices sobre la gestión de los riesgos cibernéticos marítimos* (MSC-FAL.1/Circ.3) (Organización Marítima Internacional, 2017).

2. Normas ISO, especialmente la citada ISO 27001. Esta Norma especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones (ISO/IEC 27000, 2018).

3. Directrices como las de la organización *Baltic and International Maritime Council* (BIMCO) (BIMCO, 2016) o de la *U.S. National Institute of Standards and Technology* (NIST framework) *Framework for improving critical infrastructure Cybersecurity* (National Institute of Standars and Technology, 2018) o la *Digital Container Shipping Association (DCSA) DCSA Implementation Guide for Cyber Security on Vessels* (DCSA, 2020).

4. Páginas web relativas a la ciberseguridad marítima.

5. Revistas científicas de alto impacto, a las que está suscrita la Universidad de Cantabria.

6. Publicaciones del Ministerio de Transporte, Movilidad y Agenda Urbana, etc.

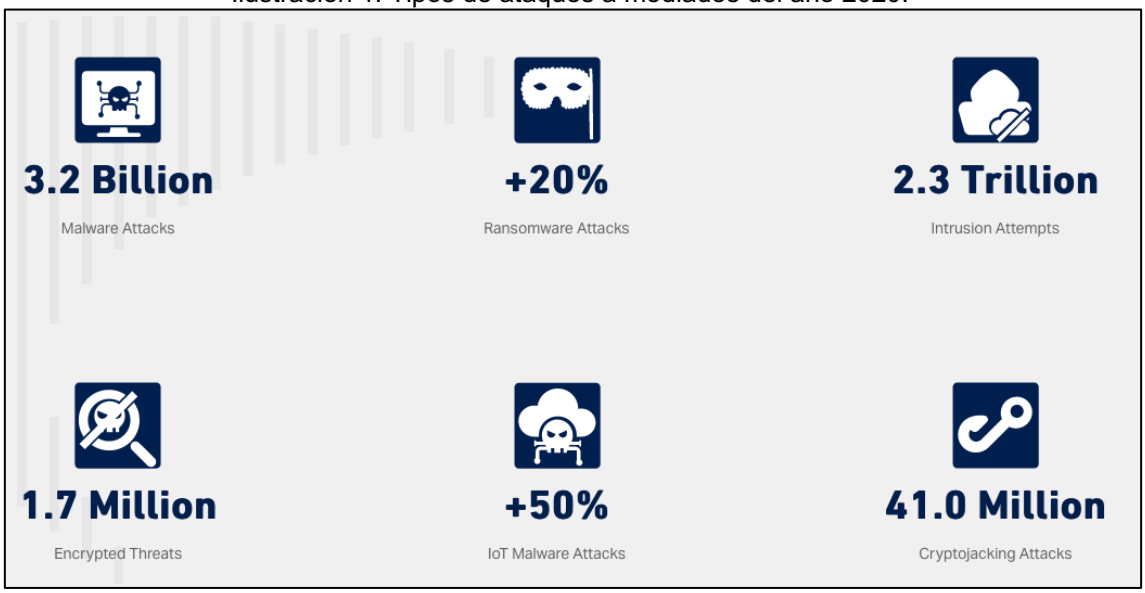
CAPÍTULO III: EVOLUCIÓN DE LOS CIBERATAQUES AL TRANSPORTE MARÍTIMO

3.1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

La seguridad informática nos lleva a pensar en una tarea que no es de nuestro interés, que depende de los profesionales informáticos y que nosotros somos simplemente unos espectadores. Sabemos que no es un contexto sencillo y que está lleno de códigos extraños e inaccesibles para las personas que no tienen formación alguna en la materia. Esto nos descarga de esa responsabilidad, nos hace pasivos y este es uno de los peligros mas comunes.

En los últimos años se han multiplicado los episodios de ataques a equipos y redes a nivel mundial y la ciberseguridad es de la máxima importancia para los Estados.

Ilustración 1: Tipos de ataques a mediados del año 2020.

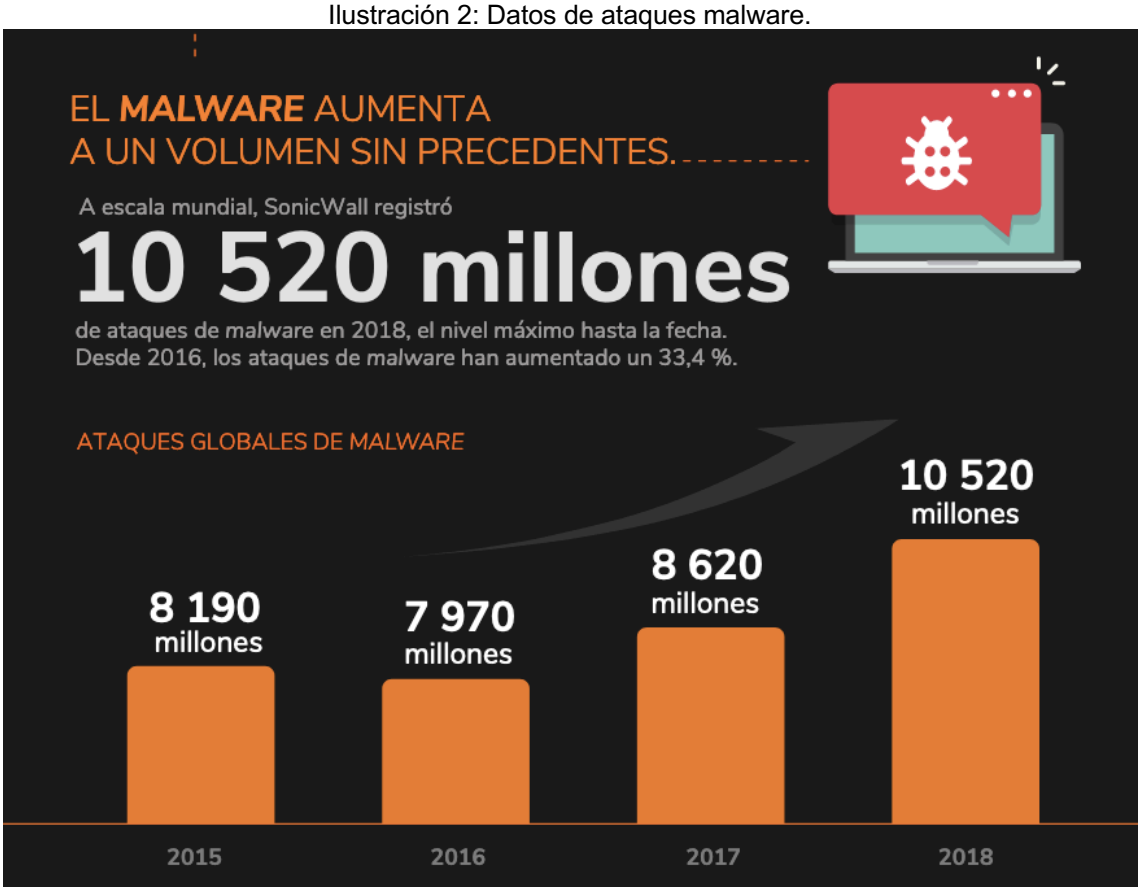


Fuente: (Sonicwall, 2021).

En la primera mitad del año 2020, se produjeron millones de ataques de todo tipo, como se muestra en la Ilustración 1. Sigue llamando la atención el incremento imparable anual de los ataques.

Desde el año 2015 al año 2018 se registró un aumento del malware del 33.4%. En la Ilustración 2, se muestran datos relativos a los millones de ataques de malware. De estos números, mas de 206 millones fueron ataques de ransomware, la mitad en Estados Unidos. Una empresa cualquiera, a nivel global, puede sufrir una media de 25.000 ataques de malware anuales.

Ilustración 2: Datos de ataques malware.



Fuente: (Sonicwall, 2021).

Organismos como la Organización Marítima Internacional (OMI), están alerta desde hace años y están desarrollando documentación que ayude a adoptar una posición de defensa ante esta amenaza que parece se va a convertir en un gran problema durante los próximos años, debido al incremento del uso de las tecnologías en los buques (Fabra, 2002).

España, por su parte, tiene definidos unas estrategias de seguridad nacional que son llevados a cabo desde el Departamento de Seguridad Nacional (DSN).

3.2. ARQUITECTURA DE DATOS Y CIBERSEGURIDAD

La cuestión referente a la seguridad informática recae en toda la sociedad, aunque no lo parezca. Es imposible que sepamos mucho de todo lo que nos rodea pero es nuestro deber, por nuestro bien y el de la sociedad, que adquiramos conocimientos básicos y concienciarnos. No debemos relajarnos y tampoco, esto es muy habitual, “tirar la toalla”, pensando que al fin y al cabo un

buen hacker va a poder traspasar las medidas que pongamos y dejará nuestro intento en nada. Aquí aparece un término crucial que forma parte del título de este trabajo: resiliencia. Debemos asumir que es imposible frenar al 100% los riesgos y ataques cibernéticos y el poder adoptar una actitud resiliente frente a las vulnerabilidades es imprescindible, para ser capaz de gestionar el riesgo existente y superarlo con un mínimo impacto. Esta actitud nos provee de una serie de pautas y medidas que reducirán al mínimo los riesgos y será muy difícil que nos veamos afectados. Hay que proveerse de las soluciones tecnológicas de seguridad y realizar una monitorización continua lo que nos dará a conocer, en todo momento, qué protecciones tenemos y cuáles son los riesgos potenciales a los que nos enfrentamos. Además, crearemos una verdadera cultura de la seguridad (Håvold, 2010) entre la tripulación.

3.2.1. DEFINICIÓN DE CIBERSEGURIDAD

Podemos definir la Ciberseguridad tal y como la describe la Unión Internacional de Telecomunicaciones (UIT): *"… el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno."*

La definición recoge las redes interconectadas y su hardware, incluyendo las bases de datos y servicios. El Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos (NIST), reconoce en su definición de ciberseguridad la existencia de un espacio no físico como es el ciberespacio que requiere de habilidades que aseguren su protección.

3.2.2. LA SEGURIDAD INFORMÁTICA

La seguridad en la información de caracteriza por tres dimensiones (ISO/IEC 27000, 2018):

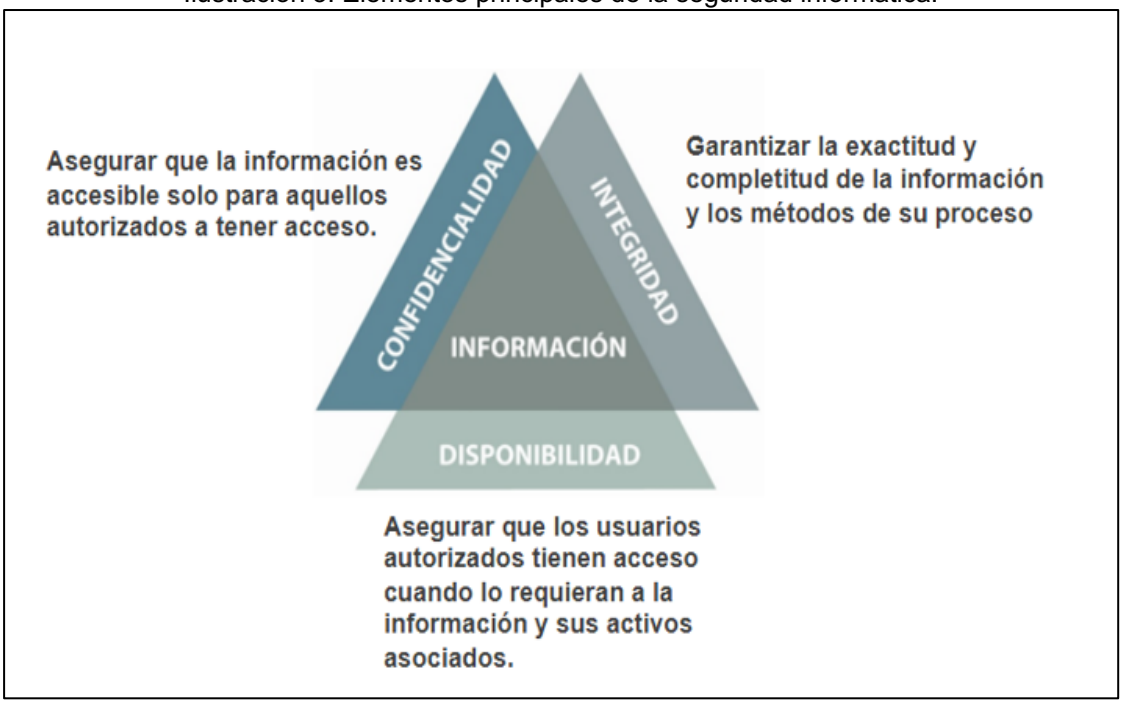
- **Confidencialidad**. Solo debe acceder a la información quien tiene permiso.

- **Integridad**. La información no es manipulada.

- **Disponibilidad**. La información debe estar siempre disponible.

En la Ilustración 3, se muestra un resumen de lo explicado.

Ilustración 3: Elementos principales de la seguridad informática.



Fuente: (Lisot, 2021).

Los riesgos de seguridad de la información son aquellos que se derivan de la pérdida de confidencialidad, integridad o disponibilidad de los sistemas de información.

Estos son los conceptos clave de la seguridad informática: amenaza, riesgo y vulnerabilidad.

- **Amenaza**. Cualquier acontecimiento el que no podemos evitar que suceda y que representa un riesgo para el sistema.

- **Riesgo**: El resultado de la probabilidad de que una amenaza se materialice asociado al impacto negativo que puede tener en nuestra organización o vida diaria.

- **Vulnerabilidad**: Una fragilidad en nuestro sistema que permite que una

amenaza puede materializarse.

A continuación, en la Ilustración 4, podemos ver la relación del riesgo con el resto de los conceptos clave de la seguridad informática.

Ilustración 4: Composición del Riesgo.

Fuente: (INCIBE, 2021).

3.2.3. EL COMIENZO DE LA CIBERSEGURIDAD

La ciberseguridad nació con el mundo digital y aquellos virus iniciales que nos sorprendían, no hace tantos años a todos, fueron el motor de la evolución de la ciberseguridad hasta lo que conocemos hoy en día. Además, para nuestra sorpresa, seguramente no será igual en el futuro, dado que su capacidad de cambio es muy rápida y tenemos la necesidad de adaptarnos mas velozmente que los que intentan quebrarla o fracasaremos en nuestro intento de proteger la

información.

La ciberseguridad ha existido desde esos inicios del mundo digital, no pueden convivir por separado, siempre ha habido y habrá un vinculo entre ambos y es lo normal, es como poner una puerta en una casa y no añadirle una cerradura.

En un mundo ideal será así, pero no en nuestro mundo actual, cada vez mas digitalizado y cada vez con mas amenazas. La globalización y la conexión total a nivel planetario de las redes, donde una persona desde el lugar mas remoto o desde un país donde no exista control o tratados de seguridad, puede llegar a acceder a un equipo en la otra parte del mundo con un interés maligno. Esto ha sido heredado de otros ámbitos, la seguridad ha ido unida a las actividades humanas, como es lógico, sobre todo para preservar la vida. La evolución de la seguridad nos ha llevado a la seguridad jurídica, laboral, etc.

Hemos vivido esta preocupación desde los inicios de la seguridad de la información, en los años 1970 y 1980, donde nos preocupaban las copias de seguridad para superar los fallos en los medios de almacenamiento, mas frágiles que los actuales, o los primeros virus que tenían capacidad de replicarse y se transmitían por aquellos Compact Disk (CD), o a través de los primeros Universal Serial Bus (USB). Ya entonces, las primeras vulnerabilidades nos sorprendieron a todos. En esta época apareció *Creeper*, el primer malware y llegaba a los ordenadores a través de la Agencia de Proyectos de Investigación Avanzados (ARPANET, la antecesora de Internet). A la vez llegaban los primeros antivirus, el primero fue *Reaper*, que no dejaba de ser otro virus que buscaba al virus *Creeper* para eliminarlo.

Entraron en las empresas los Firewall, también llamado Cortafuegos, para prevenir y proteger a nuestra red interna de intrusiones de otras redes. Estos aparatos ya se quedaron para siempre y comenzamos a sufrir entonces el envío masivo de emails (esto nos dura por desgracia). Hoy en día, sigue siendo una de las formas mas eficaces de vulnerar una empresa. Ya desde el año 1980, se utilizó la Ingeniería Social para evadir sistemas protegidos desde su interior, es decir, los propios empleados facilitan las contraseñas a los hackers

que les llaman con cualquier motivación, por ejemplo, argumentando que llaman del Departamento de Informática, basándose en que todo el mundo quiere ayudar y en la propia confianza humana hacia los demás.

Empezamos ya entonces a ver nuevas palabras que no iban a desaparecer nunca y que iban a formar parte de nuestro vocabulario informático habitual, podemos ver un resumen de las mas importantes en el epígrafe 3.2.6. de este Capítulo.

3.2.4. EVOLUCIÓN DE LA CIBERSEGURIDAD

Una de las características mas llamativas de esta temática es su dinamismo, tanto en lo referente a los conocimientos previos, como en lo referente a los conocimientos actuales y futuros, muy cambiantes y diversos. Esta característica hace que sea difícil proponer medidas y asegurar una protección duradera, mas aun con el interés que hay en digitalizarlo todo, incluso planteando, no en un futuro muy lejano, que haya buques no tripulados (Lloyd's, 2016). Estos buques son considerados como drones autónomos, tripulados desde tierra de manera remota. La empresa Rolls-Royce ya está trabajando en estos prototipos y la tecnología es su elemento principal.

Evidentemente esto tiene todo el sentido, es una especie de "carrera" hacia lo desconocido, donde unos intentan protegerse y otros intentan encontrar una opción en esa protección y entrar en los sistemas para obtener algún beneficio, sea económico, estratégico, espionaje, etc.

Diariamente se encuentran miles de carencias de los programas informáticos y en los componentes electrónicos (vulnerabilidades) y desde hace algunos años los fabricantes de dicho software las publican haciendo mas fácil el camino a los atacantes. El objetivo de dichas publicaciones es que los usuarios finales tomen acciones, principalmente la de actualizar dichos sistemas (parches), o de protegerse mientras se encuentra una solución. Esto es aprovechado por los hackers para entrar en los sistemas que no han realizado cambios, no han instalado esos parches o actualizaciones. Al final, es una carrera, larga y dura,

pero sobre todo una carrera donde no podemos mirar atrás ni a los lados, hay que mirar hacia delante y correr mas que los perseguidores, los atacantes.

Los gobiernos son lentos en publicar Leyes que penalicen en la medida justa estos actos pero se van mentalizando y van desarrollando normativa acorde a una realidad que, al menos en el sector marítimo, es de grandísima importancia para las vidas humanas, el medioambiente, la economía, la estrategia, etc. Este es un sector donde un acto terrorista puede ser muy visible y de grandes efectos destructivos.

Existen varios incidentes que han llamado la atención en los últimos años y que han despertado a las Autoridades para que den ese paso adelante, tan esperado.

En el año 2010, durante el traslado de una plataforma petrolífera (Crawford, 2019) la estructura se escoró produciendo una serie de heridos. Después de la investigación se pudo demostrar que fue un ataque producido por virus informáticos en los ordenadores y sistemas de control de la plataforma.

En ese mismo año los ciberataques se sofisticaron muchísimo y eran muy difíciles de detectar, los virus se ocultaban en cualquier lugar, sobre todo en los emails con archivos adjuntos donde al hacer clic, en una imagen o en una supuesta factura que nos enviaba un proveedor. Ya entonces caíamos en la trampa y el dispositivo se infectaba y, lo que es peor, se infectaban los equipos de la red, el servidor y se replicaba a nuestros contactos que recibían nuestro email y lo abrían confiados. Los actuales malares, mucho mas sofisticados, no son detectados por los antivirus.

En el año 2011, el Gobierno de España publicaba la primera Estrategia de Española de Seguridad (EES), donde no se puede leer con claridad la diferencia entre prevención, protección y contaminación. Parece que estemos leyendo un texto marítimo, traspuesto al ordenamiento jurídico español anterior al año 1990. La EES, recordada por su deficiente aproximación hacia la dimensión estratégica de la mar (Curt García, 2018), se corrigió en el año 2013,

con la nueva ESN-2013 que ya trataba lo marítimo en mejor modo (Gobiemo, 2012). La última publicación del 2017 (ESN-2017) hace un detenido análisis del tema marítimo (Gobierno de España, 2017). Existe un entorno de colaboración virtual, con la herramienta llamada SEGMAR (Sistema de Información Nacional para compartir información de Seguridad Marítima) que conecta a los centros operativos nacionales de seguridad marítima. Se celebra periódicamente una Conferencia de Centros Operativos de Seguridad Marítima y se ha implementado una Célula de Información y Análisis de Riesgos y Amenazas a la Seguridad Marítima (CIARA).

A finales del 2017, surgieron virus muy peligrosos, con tecnología filtrada de la industria militar. Recordaremos al virus WannaCry o el NotPeyta que afectaron a miles de ordenadores causando pérdidas de 300 millones de dólares (Crawford, 2019).

En el 2018, el Secretario General de la Organización de Naciones Unidas (ONU), Antonio Guterrez, hablaba ya de "*Episodios de guerra cibernética entre Estados*" (Crawford, 2019). Uno de los mayores problemas es que no hay un esquema reglamentario para estos ataques, no está claro si se puede aplicar la Convención de Ginebra o el Derecho Internacional. A esto le sumamos que el 90% del transporte mundial se realiza por mar por lo que la seguridad de este sector es clave para la estabilidad mundial. La ingeniería tradicional se ha centrado en la seguridad a bordo de los buques, como la duplicidad de los sistemas y las comunicaciones, pero no se han considerado estrategias relacionadas con la ciberseguridad. La Organización del Tratado del Atlántico Norte (OTAN), afirma que "*los países tienen justificación legal para usar la fuerza militar contra todo aquel que ayude a un país enemigo a lanzar un ciberataque"*.

La OMI, adoptó la resolución MSC.428(98), sobre la *Gestión de los Riesgos Cibernéticos Marítimos* en los Sistemas de Gestión de la Seguridad donde se considera que un proceso de auditoría SMS aprobado debe incluir la gestión de los ciberriesgos de acuerdo con los objetivos y los requerimientos funcionales del Código Internacional de Gestión (ISM) (Organización Marítima

Internacional, 2017). Debe de asegurarse que los ciberriesgos quedan registrados en el SMS, no mas allá de la primera verificación anual del documento de la compañía Document of Compliance (DoC), después del 1 de enero del 2021.

Aproximadamente, en la actualidad, hay unos 50.000 buques mercantes operando internacionalmente (Alcaide and Llave, 2020) transportando todo tipo de cargas. Estos buques operan asimismo en infraestructuras críticas para poder ejecutar sus trabajos con normalidad (puertos, plataformas, refinerías, etc.). El gran aumento del transporte de contenedores en los últimos años ha llevado a un crecimiento de las actividades ilícitas en los mismos. La Comisión Europea (Consejo de la UE, 2004) define a éstas infraestructuras críticas (CI), como esenciales para el mantenimiento de las funciones sociales vitales (Alcaide and Llave, 2020) y el Estado de España, en el Real Decreto 704/2011 (Ministerio del Interior, 2011) ya establece medidas para la protección de dichas infraestructuras y en el año 2013, establece una Estrategia de Ciberseguridad Nacional (Gobiemo, 2013).

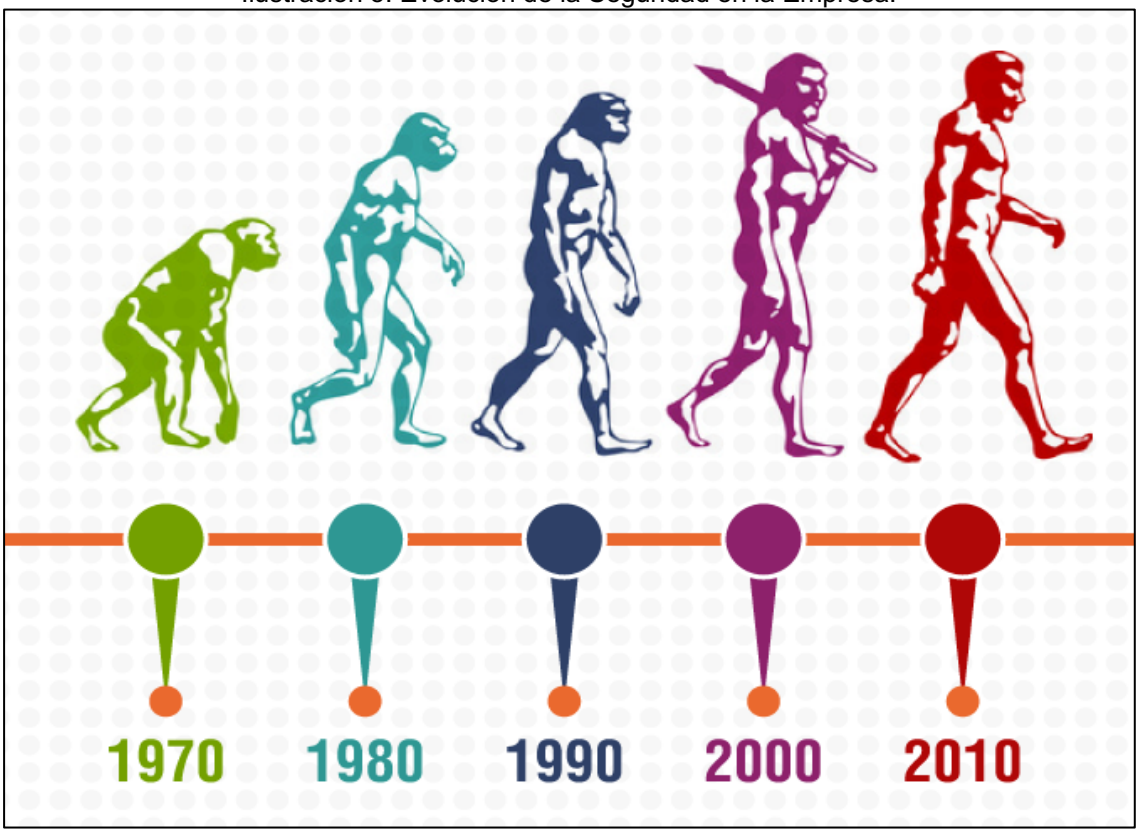
La Ilustración 5, muestra una comparativa de la seguridad con la evolución del ser humano, desde sus orígenes hasta la actualidad. La evolución de la seguridad, como se puede comprobar a simple vista, ha sido realizada en tan solo 40 años. Es muy significativa ya que nos da una idea de los grandes avances en la informática en un plazo relativamente corto.

Dicha ilustración 5, ha sido creada por el Instituto Nacional de Ciberseguridad, órgano dependiente del Ministerio de Asuntos Económicos y Transformación Digital, encargado de desarrollar la ciberseguridad y de la confianza digital de los ciudadanos, actualmente una referencia en España sobre ciberseguridad.

Hay bastantes incidentes y esto va en aumento. Es muy importante tomárselo muy en serio, cualquier incidente es ya un aviso de lo que puede ser una catástrofe (Lloyd's, 2018). Los ataques cibernéticos vulneran las políticas establecidas en Europa por lo que se puede afirmar sin lugar a dudas que es el actual talón de Aquiles de nuestra sociedad (Machin Nieva and Gazapo

Manuel, 2016).

Ilustración 5: Evolución de la Seguridad en la Empresa.



Fuente: (INCIBE, 2021).

Desde los atentados terroristas a las Torres Gemelas en nueva York (USA) en el año 2001, se tomó este rumbo de almacenar en la nube la información para no depender solamente de servidores locales que pueden sufrir un daño irreparable, en caso de destrucción. Se perdieron muchos datos informáticos de bancos y aseguradoras y los técnicos pudieron comprobar que solamente se salvaron los datos que estaban en tránsito. Ese fue el inicio del Cloud Computing, el almacenamiento en la nube. La próxima pregunta es: *¿Quién asegura que nuestros datos se mantienen íntegros en la nube?*

3.2.5. ESTADO ACTUAL DE LA CIBERSEGURIDAD

El teletrabajo y guardar los datos en “la nube” (Cloud Computing) aumentan el riesgo, la digitalización nos rodea, cada vez esta mas cerca, antes era ciencia ficción, pero ahora podemos controlar las luces de casa, el termostato y los electrodomésticos tienen conexión a internet.

La tecnología 5G, la quinta generación de tecnologías de telefonía móvil ya está funcionando, ampliando su cobertura. Se estima que en el año 2025, haya conectados, con esta tecnología, 1700 millones de usuarios en el mundo. Esto va a venir muy relacionado con el desarrollo del internet de las cosas (IoT), que interconectará digitalmente objetos cotidianos con internet. Aunque parezca mentira, habrá mas cosas conectadas a internet que personas. Si los objetos cotidianos tuvieran incorporados etiquetas de radio podrían ser identificados y gestionados por otros equipos de la misma manera que si lo fuesen por seres humanos. La ampliación de dispositivos va, lógicamente, relacionada con el crecimiento de las amenazas. Se define entonces una nueva puerta de entrada para los ciberdelincuentes, para acceder a los hogares y a las empresas, donde también existirán multitud de dispositivos de este tipo. Una brecha de seguridad en un dispositivo IoT es posible y en los próximos años parece ser que pueda convertirse en la opción mas sencilla de los atacantes para entrar en un sistema.

En el 2018, un 59% de las empresas de Estados Unidos y Reino Unido habían experimentado brechas de seguridad via proveedores o clientes (Alcaide and Llave, 2020). En una encuesta de BIMCO, ya en el año 2016, el 21% de las empresas habían sufrido algún tipo de ciberataque y, de éstas, un 70% respondía a malware y un 20% a robo de credenciales. El costo anual para la economía mundial se estimó, para el año 2019, en dos trillones de dólares.

Actualmente se están generando nuevos motores basados en la Inteligencia Artificial (IA). Esto supondrá un gran avance ante los ataques ya que se pueden analizar una gran cantidad de datos y relacionarlos al instante para detectar comportamientos anómalos. La IA se está aplicando con un uso ofensivo en la ciberseguridad, no sin preocupación, ya que tiene capacidad de evolucionar y tomar decisiones, incluso sin ser supervisada por los humanos.

También se hace necesario citar la privacidad de las personas. Ya hoy en día juega un papel muy importante, mas que nunca, y es una de las mayores preocupaciones. Todos tenemos en nuestros dispositivos, que están conectados las 24 horas del día a Internet, fotos, vídeos, documentos

personales e información privada y a eso hay que añadir que tenemos una copia total o parcial de dicha información en la nube (Cloud Computing). Todo está en la nube y cada vez nos vamos dejando llevar por este sistema, ya que descargamos de esta gran tarea de almacenamiento a los dispositivos. Es muy cómodo, si perdemos o se nos estropea el dispositivo, en un plazo muy corto de tiempo, lo tenemos funcionando al 100%, con el mismo contenido, software y datos que el dispositivo anterior. Si un criminal accede a estos datos podría pedirnos un rescate económico a cambio de no borrarlos, hacerlos públicos, no realizar operaciones bancarias en nuestro nombre, etc

A eso podemos añadir diversos estudios que han demostrado que los equipos informáticos, tanto estén conectados a la red como si no, transmiten nuestros datos a servidores que generan perfiles y que son utilizados por empresas para su beneficio, y lo que es mas curioso, si cabe, cuando aceptamos los contratos en portales y páginas web, muy conocidos, nos encontramos que, como usuarios, aceptamos el uso de nuestros datos por parte de dichas empresas.

El coronavirus ha agravado los ciberataques en la industria marítima debido a un crecimiento de los ataques de tipo ransomware. Se han constatado ataques a los puertos de Amberes, Barcelona y hasta a la Guardia Costera de los EE.UU. Principalmente se ha debido al aumento de las conexiones remotas por la imposibilidad de acceder físicamente al buque, por las cuarentenas, y por las restricciones de viaje.

El 30 de noviembre es el Día Mundial de la Ciberseguridad y la primera vez que se celebró fue en el año 1988.

3.2.6. TÉRMINOS EMPLEADOS EN CIBERSEGURIDAD.

Los términos mas comunes usados en ciberseguridad son, como ya hemos podido comprobar, términos complejos. Por este motivo, a continuación, explicamos los más relevantes:

Adware: Cualquier programa que muestra publicidad de forma automática al usuario durante su instalación o su uso, y así genera beneficios a sus

creadores. Aunque se asocia al malware o software malicioso, no lo es forzosamente. Puede ser un medio legítimo usado por los desarrolladores de software que lo implementan en sus programas y que desaparece cuando se adquiere la versión completa del programa. Si recopila información sobre el ordenador donde se ha instalado, entonces sí se considera malware. Un sinónimo sería malvertising (Arévalo and Moscoso, 2017).

Amenaza: La amenaza en ciberseguridad se considera una circunstancia desfavorable que acontece cuando tiene consecuencias negativas sobre los activos provocando su falta de disponibilidad, funcionamiento incorrecto o pérdida de valor. Puede tener causas naturales, ser accidental o intencionada. Si sucede a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovecha su existencia, en ocasiones, deriva en un incidente de seguridad (DCSA, 2020).

Antivirus: Se trata de un programa informático diseñado para detectar, bloquear y eliminar código malicioso (virus, caballos de troya, gusanos, etc.). De este modo protege, no siempre, a los equipos de otros programas peligrosos conocidos como malware. Estos programas maliciosos son responsables de la infección del ordenador en una de cada cinco ocasiones (Lloyd's, 2016).

Autenticación: Con este procedimiento se comprueba que alguien es quién dice ser cuando accede al ordenador o a un servicio online, en Internet. De esta manera se pretende establecer una comunicación segura (Curt García, 2018).

Botnet: Hace referencia a un conjunto de ordenadores que se llaman bots y que los controla de forma remota un ciberdelincuente. Los pueden utilizar para realizar diversos tipos de delitos, como el envío de *spam*. Los botnets se caracterizan por tener un servidor central (C&C, de sus siglas en inglés Command & Control), al que se conectan los bots para enviar información y recibir comandos (Curt García, 2018; Lloyd's, 2018).

Cookie: Con este término se hace referencia a un pequeño fichero que almacena información enviada por un sitio web y que se queda guardado en el equipo del usuario. De este modo, dicho sitio web puede consultar la actividad previa del mismo. Así, permiten llevar un control de los usuarios o recabar información sobre sus hábitos de navegación. Hay que tener cuidado con las cookies porque pueden implicar un ataque contra la privacidad del usuario (Lloyd's, 2016).

Gusano (Worm): Es un programa malicioso o malware, que tiene como característica principal su alto grado de "dispersabilidad", es decir, que se propaga con una gran rapidez (Alcaide and Llave, 2020).

HTTPS: Es el "Protocolo seguro de transferencia de hipertexto" y es más conocido por sus siglas HTTPS, del inglés *Hypertext Transfer Protocol Secure*. Se trata de un protocolo de red basado en el HTTP, a secas, es decir en el "Protocolo de Transferencia de Hipertexto", pero como indica su "S" final está destinado a la transferencia segura de datos de hipertexto. Sería la versión segura de HTTP. Debe aparecer en páginas webs donde se vayan a realizar operaciones monetarias y para ello el usuario debe de fijarte en la URL, donde tiene que aparecer con la "S" (Machin Nieva and Gazapo Manuel, 2016).

Malware: Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un dispositivo. Esta palabra nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, caballos de troya, backdoors, spyware, etc. Lo que une a todos estos programas es su carácter dañino (Enrique *et al.*, 2019).

Phishing: El phishing es una práctica que los ciberdelincuentes emplean para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito y datos bancarios, haciéndose pasar por una comunicación confiable y legítima (DCSA, 2020).

Zombie: Es el nombre que se da a los ordenadores controlados de manera

remota por un ciberdelicuente, tras haberlos infectados con un *malware*. El atacante remoto generalmente utiliza el ordenador zombie para efectuar actividades ilícitas a través de internet, como el envío de comunicaciones electrónicas no deseadas, así como la propagación de otro malware (Crawford, 2019).

3.3. ORIGEN DE LOS CIBERATAQUES

Las motivaciones de los ataques pueden ser muy variadas. En la Ilustración 6, podemos ver un resumen de los tipos principales según la BIMCO.

Ilustración 6: Identificación de actores potenciales.

Actores	Motivaciones
Intrusos accidentales	Sin motivo malicioso o mala suerte o por falta de conocimiento.
Activistas	Venganza, atención en los medios, daño en la reputación.
Criminales	Interés económico, espionaje.
Oportunistas	Reto informático, reputación social, interés económico.
Terroristas	Ideología, espionaje, interés económico.

Fuente: (BIMCO, 2016).

3.4. CLASIFICACIÓN DE LOS ATAQUES

Los ataques informáticos, o también denominados ciberataques, pueden ser de dos tipos, los ataques no dirigidos y los ataques dirigidos.

Los ataques no dirigidos, son los menos peligrosos. Se usan herramientas disponibles en Internet para localizar, descubrir y explotar vulnerabilidades de su objetivo, en este caso el buque civil. Este tipo de ataque se produce cuando el atacante busca en la red sistemas desprotegidos al azar y puede dar con cualquier sistema. Son típicas las siguientes herramientas y técnicas usadas para descubrir posibles victimas:

- **Malware**: es un tipo de software malicioso que esta diseñado para acceder o dañar un ordenador sin que el propietario lo sepa. Hay varios tipos de malware: troyanos, ransomware, spyware, virus y gusanos. El ransomware, muy conocido en los últimos años, es capaz de encriptar los datos de un sistema de almacenamiento, desde el propio disco duro del ordenador hasta un servidor,

hasta que el usuario no pague un rescate, que suele ser económico. El malware también es capaz de aprovecharse de los "bugs" o fallos del código del software así como de otro tipo de vulnerabilidades de los sistemas o fallos en el hardware, para poder aprovechar, de manera remota, esa ventaja y acceder a los sistemas. La mayor parte de las veces el malware es introducido en los sistemas con un archivo adjunto en un correo electrónico o al visitar una pagina web maliciosa (Crawford, 2019).

- **Water holing**: donde se establece una pagina web falsa muy parecida a una conocida por los empleados y donde se procede a reenviarlos a una web maliciosa, aprovechándose de la confianza del usuario por la pagina principal (Arévalo and Moscoso, 2017).

- **Scanning**: búsqueda por Internet de vulnerabilidades al azar que pueden ser aprovechadas (BIMCO, 2016).

- **Typosquatting:** también llamado falsa Uniform Resource Locator (URL). Se centra en los errores que cometen los usuarios al escribir mal una dirección web donde son redirigidos a una web maliciosa (Machin Nieva and Gazapo Manuel, 2016).

Los ataques dirigidos son mas sofisticados y utilizan técnicas que se crean específicamente para atacar un objetivo concreto, en nuestro caso, el buque civil. Se utilizan técnicas como las siguientes:

- **Ingeniería Social:** se usan técnicas de contacto con las victimas a través de redes sociales o incluso llamadas telefónicas suplantando a personas del Departamento de Informática, por ejemplo, para obtener claves de acceso (Machin Nieva and Gazapo Manuel, 2016).

- **Fuerza Bruta:** se hacen multitud de intentos con diferentes contraseñas generadas y donde se espera tener suerte y entrar al sistema. Por ese motivo es muy importante tener contraseñas complejas (Alcaide and Llave, 2020).

- **Relleno de credenciales:** técnica que utiliza nombres de usuario y

contraseñas ya usadas anteriormente en el sistema para intentar adivinar otras existentes (Curt García, 2018).

- **Denegación de servicio (DoS):** tipo de ataque muy común actualmente que se basa en enviar miles de peticiones a un servidor de manera que su gran tarea lo bloquea y lo hace lento dejando sin servicio a los usuarios (Machin Nieva and Gazapo Manuel, 2016).

- **Phising:** a través de emails atractivos o engañosos se piden datos de los usuarios para después acceder a las redes. Esta técnica también es muy actual. Estos emails pueden también contener archivos adjuntos que nos llevan a una web maliciosa (National Institute of Standars and Technology, 2018).

- **Spear phising:** es muy parecida a la técnica de phising pero los emails son personalizados y dirigidos al usuario. Se envía software malicioso o enlaces que llevan a web maliciosas (BIMCO, 2016).

- **Suplantación de la cadena de suministro:** esta técnica es muy peligrosa ya que la confianza en el proveedor hace que se puedan introducir en el sistema software que ha sido enviado, en teoría, por un tercero de confianza (BIMCO, 2016).

Los ataques siempre siguen unos métodos para su implantación en los sistemas. Cronológicamente puede que transcurran meses o años desde que se inicia la investigación del objetivo hasta que se consigue penetrar en el sistema.

Por su parte, la Oficina Gubernamental para la Ciencia del Reino Unido ha identificado tres categorías de ciberataques en relación a los objetivos (Crawford, 2019):

- Ataques a los activos de la empresa.

- Ataques a los sistemas de información.

- Ataques al GPS o sistemas de navegación.

3.5. OBJETIVOS DE LOS ATAQUES CIBERNÉTICOS

El objetivo de los ataques cibernéticos es el acceso a la información, la protección de los sistemas de control y gestión (Ministerio de Defensa, 2019), los accesos no autorizados, la manipulación etc. Deben ser evitados, controlados y llevados a un riesgo aceptable. Pueden darse, como ejemplo, una serie de incidentes como los siguientes:

- Vulneración del sistema de Cartas Electrónicas Electronic Chart Display and Information System (ECDIS). Ya en el año 2014, se demostró que podía accederse a este sistema (Crawford, 2019). El Grupo NCC, (Grupo de Expertos a Nivel Mundial que ofrecen servicios de Ciberseguridad) detectó varias debilidades de seguridad en el sistema. Los atacantes podrían haber tenido la capacidad de interactuar con la red a bordo solo a través de la inserción de un dispositivo USB o a través de una descarga de internet.

- El sistema Automatic Identification System (AIS**),** se utiliza para evitar colisiones entre buques. Se ha demostrado también que el sistema tiene debilidades y pueden verse alterados los datos como identidad, tipo, posición, etc. (Crawford, 2019). Un atacante con una radio Very High Frecuency (VHF), puede utilizar las debilidades en el sistema. En el año 2013, la empresa Trend Micro pudo demostrar la facilidad con la que se pueden crear buques fantasmas en cualquier ubicación del mundo siendo reconocidos por el resto de los buques como naves reales o activar una alerta de colisión falsa. También se podrían enviar partes meteorológicos falsos haciendo que un buque desviara su trayectoria.

- Fallo del sistema durante una actualización del software debido a un dispositivo de memoria USB, infectado, o fallos en el software de los sistemas.

- Introducción de Malware en los sistemas informáticos desde las cuentas de correo de la tripulación.

Ilustración 7: Logotipo de la NGA.

Fuente: (National Geospatial Agency, 2021).

- Manipulación o pérdida del sensor externo de datos, que es crítico para el funcionamiento del buque, incluyendo el Sistema Global de Navegación por Satélite (GNSS), o el Sistema de Posicionamiento Global (GPS). El sistema GNSS, de utilidad pública, es mas vulnerable debido a que no está encriptado. No hay que olvidar, que el GPS, es un canal abierto de una la Agencia de Inteligencia National Geospatial-Intelligence Agency (NGA), el la Ilustración 7 podemos ver su logotipo. De hecho el sistema de posicionamiento GPS es un canal abierto que en más del 75% de los datos lleva un error para que no se pueda utilizar maliciosamente. El canal milimétrico de posicionamiento, que es de uso militar, se llama Precise Positioning Service (PPS), está encriptado y solamente es accesible a usuarios militares autorizados.

- Accesos no autorizados a las redes internas del buque por terceros.

- Accesos remotos no autorizados desde tierra usando la comunicación de control remoto de los sistemas.

Ilustración 8: Yate White Rose of Drax.

Fuente: (Vesselfinder, 2021).

3.5.1. CASOS DE CIBERATAQUES

Los casos de ciberataques marítimos no son tan ruidosos en los medios de comunicación como los que se formulan contra empresas (Roach, 2004), sin embargo, constituyen una constante en el tiempo. Los casos más destacados, han sido:

White Rose of Drax: En el año 2013, un equipo de investigación de la Universidad de Texas-Austin demostró como un potencial atacante podría tomar el control remoto de un buque a través de la manipulación de su GPS, se aprecia en la Ilustración 8, el M/Y White Rose of Drax.

Mediante la transmisión de señales falsas de GPS, el equipo de investigación fue capaz de dominar lentamente las señales del GPS del yate obteniendo el control de su sistema de navegación. El yate alteró su rumbo, pero en la pantalla del radar solo se apreciaba una línea recta (Crawford, 2019).

Ataque a Maersk: En el año 2017, la empresa marítima Maersk, sufrió un ataque informático tipo ransomware impidiendo el acceso a sus usuarios (Crawford, 2019) y causando unas pérdidas de unos 250 millones de dólares.

Durante los 10 días posteriores al ataque los empleados solo pudieron gestionar un 20% de las demandas de transporte y la compañía tuvo que reemplazar 45.000 ordenadores, 4.000 servidores e instalar 2.500 aplicaciones.

En la Ilustración 9 podemos ver un buque contenedor de la empresa Maersk.

Ilustración 9: Buque de la compañía naviera Maersk.

Fuente: (Camara Maritima del Ecuador, 2021).

Ataque a plataformas petrolíferas: En el año 2010, durante un traslado de una plataforma desde Corea del Sur a Brasil la estructura se escoró hacia una banda produciendo una serie de heridos en la tripulación. La investigación confirmó que se trataba de una plaga de virus en los ordenadores y los sistemas de control de la plataforma.

Otro ciberataque en 2012, a la plataforma Noble Regina, mientras se estaba construyendo, resultó en una escora de 17º, lo que ocasionó un accidente afectando a sus 89 trabajadores (Crawford, 2019).

A continuación, en la Ilustración 10 podemos ver una foto de la plataforma

citada.

Ilustración 10: Plataforma petrolífera Noble Regina.

Fuente: (The New Paper, 2021).

Ataque a una compañía naviera iraní: En agosto del 2011, piratas informáticos penetraron en los servidores de IRISL, la mayor compañía naviera iraní. Se dañaron datos de tarifas, números de carga, fechas de entrega y lugares. Hubo un gran descontrol sobre la ubicación de un gran número de contenedores y se entregaron muchos de éstos en lugares equivocados o se perdieron (Machin Nieva and Gazapo Manuel, 2016). En la Ilustración 11 se puede ver un buque de la compañía naviera iraní.

Ataque a los sistemas aduaneros y/o portuarios: En el año 2012, piratas informáticos pusieron en peligro el sistema de carga que controlaba el Servicio de Aduanas y Protección Fronteriza de Australia. Los ciberdelincuentes querían saber qué contenedores estaban bajo sospecha por la policía o las autoridades aduaneras. Con esta información sabrían si necesitaban abandonar contenedores con carga de contrabando (Enrique *et al.*, 2019).

Entre 2011 y 2013 el puerto de Amberes sufrió ataques parecidos y necesitó dos años para poder recuperarse (Crawford, 2019).

Ilustración 11: Buque de la compañía naviera IRISL.

Fuente: (Tehran Times, 2021).

3.6. LA CIBERSEGURIDAD Y LA ORGANIZACIÓN MARÍTIMA INTERNACIONAL

La Organización Marítima Internacional (OMI) también ha sido objeto de un ataque informático en el año 2020. Se detectó la intrusión de ciberdelincuentes en su página web y sufrieron una interrupción de su servicio provocado por un sofisticado ciberataque. Los técnicos informáticos bloquearon los sistemas clave para evitar mayores daños por el ataque.

Desde 2016, el Comité de Seguridad Marítima de la OMI, aprobó la guía de gestión de ciberriesgos marítimos reconociendo este tipo de amenazas en el ámbito marítimo y su posible impacto en las naves y sus tripulaciones. La OMI, consideró necesaria la incorporación en la gestión de riesgos de las compañías y buques los riesgos de la ciberseguridad.

La aproximación a la gestión de los riesgos de la OMI, propone un enfoque basado en la implementación y mantenimiento de cinco elementos: **identificación, protección, detección, respuesta y recuperación.**

Además, plantea la adopción de ciertas buenas prácticas tales como:
- Marco de ciberseguridad del Instituto de Ingeniería y Tecnología del Reino Unido.

- Estándar de seguridad en tecnologías de la información ISO 27001.

- Guía de la ciberseguridad a bordo de los buques del Consejo Marítimo Internacional y del Báltico (BIMCO).

3.7. MEDIOS DE LUCHA CONTRA LOS CIBERATAQUES

En España existe un Sistema de Seguridad Nacional integrado por un Consejo de Seguridad Nacional del que depende, entre otros, el Consejo Nacional de Seguridad Marítima.

El Sistema de Seguridad Nacional: El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones. En el Sistema se integran los componentes fundamentales, siguiendo los mecanismos de enlace y coordinación que determine el Consejo de Seguridad Nacional, actuando bajo sus propias estructuras y procedimientos. En función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada (Curt García, 2018).

En materia de Seguridad Marítima, el Consejo Nacional de Seguridad Marítima en calidad de órgano colegiado de apoyo al Consejo de Seguridad Nacional, en el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional en el ámbito de la seguridad marítima, centró sus trabajos en desarrollar el Plan de Acción de la Estrategia Nacional de Seguridad Marítima, así como en estudiar y analizar la mejor fórmula para fomentar la cooperación en las operaciones de seguridad marítima (Barroilhet Acevedo, 2004), establecer medidas para afrontar la ciberseguridad en el espacio marítimo, elaborar de forma bimestral un análisis de amenazas y riesgos en el ámbito marítimo y desarrollar el Plan

integral de seguridad marítima en el estrecho de Gibraltar. La Ilustración 12 muestra el organigrama de dicho sistema de seguridad nacional.

Ilustración 12: Sistema de Seguridad Nacional de España.

Fuente: (Departamento de Seguridad Nacional, 2021).

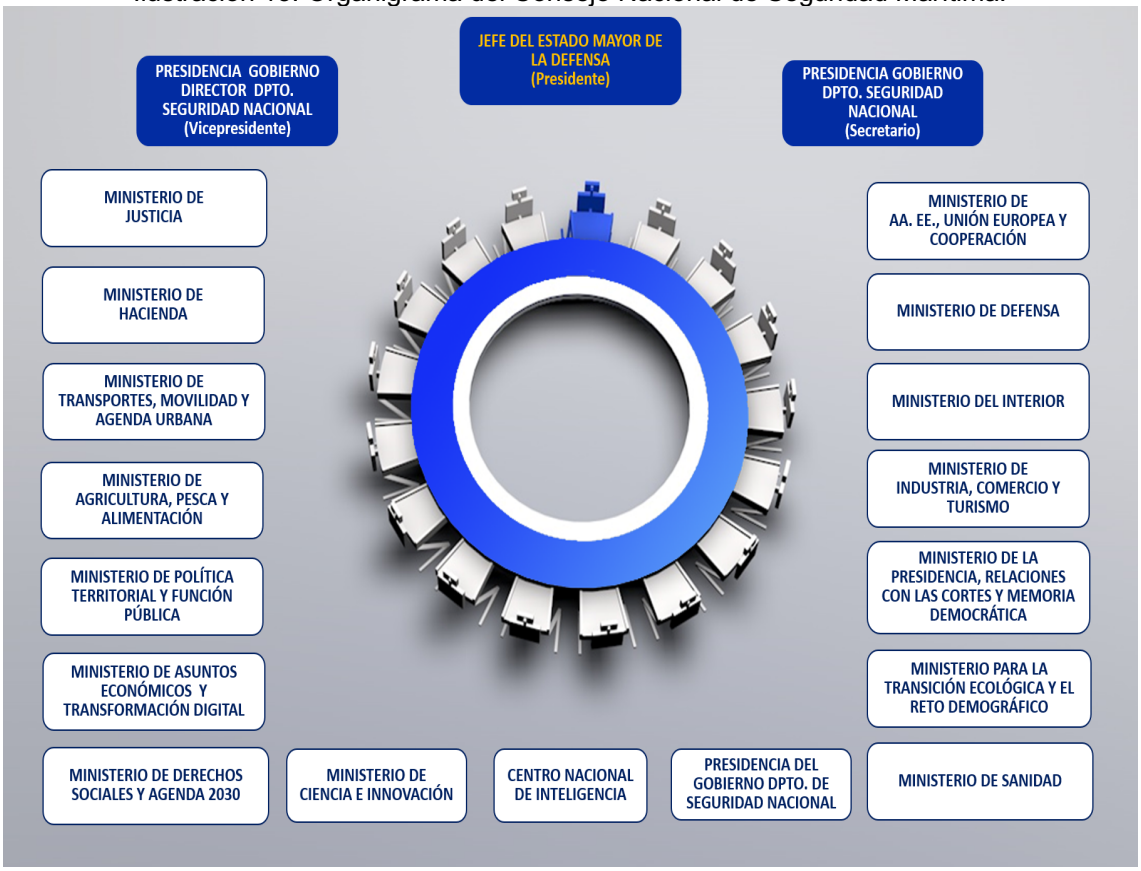
La composición de este Consejo refleja el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de seguridad marítima, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad. En el Consejo pueden participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria.

El Consejo Nacional de Seguridad Marítima, podemos ver su organigrama en la

Ilustración 13, ejerce las siguientes funciones:

- Apoyar la toma de decisiones del Consejo de Seguridad Nacional en materia de seguridad marítima mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

Ilustración 13: Organigrama del Consejo Nacional de Seguridad Marítima.



Fuente: (Departamento de Seguridad Nacional, 2021).

- Reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas, con competencias relacionadas con el ámbito de la seguridad marítima, así como entre los sectores público y privado.

- Contribuir a la elaboración de propuestas normativas en el ámbito de la seguridad marítima para su consideración por el Consejo de Seguridad Nacional.

- Prestar apoyo al Consejo de Seguridad Nacional en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional del año 2013 en lo relacionado con la seguridad marítima y promover e impulsar sus revisiones.

- Verificar el grado de cumplimiento de la Estrategia de Seguridad Marítima Nacional e informar al Consejo de Seguridad Nacional.

- Impulsar los estudios necesarios y hacer propuestas para que la Estrategia de Seguridad Marítima Nacional evolucione armónicamente con respecto a la Política Marítima Integrada, la futura Estrategia Europea de Seguridad Marítima y otras estrategias con dimensión internacional.

- Realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la seguridad marítima y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes. Los riesgos y las amenazas a la seguridad marítima se muestran, en un formato gráfico, en la Ilustración 14.

Ilustración 14:Riesgos y Amenazas a la Seguridad Marítima.

Fuente: (Departamento de Seguridad Nacional, 2021).

- Contribuir a la disponibilidad de los recursos existentes y realizar los estudios y análisis sobre los medios y capacidades de las distintas Administraciones Públicas y Agencias implicadas, con la finalidad de catalogar las medidas de respuesta eficaz en consonancia con los medios disponibles y las misiones a realizar, todo ello en coordinación con los órganos y autoridades directamente competentes y de acuerdo con las competencias de las diferentes Administraciones Públicas implicadas en el ámbito de la seguridad marítima.

- Facilitar la coordinación operativa entre los órganos y autoridades competentes cuando las situaciones que afecten a la seguridad marítima lo precisen y mientras no actúe el Comité Especializado de Situación.

- Todas aquellas otras funciones que le encomiende el Consejo de Seguridad Nacional.

El Centro Criptológico Nacional (CCN-CERT): El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN) adscrito al Centro Nacional de Inteligencia (CNI). Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre (Gobiemo, 2012).

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes. Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el Art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin. De acuerdo con esta normativa y la

Ley 40/2015 de Régimen Jurídico del Sector Público, es competencia del CCN-CERT, la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT, en coordinación con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

Este organismo publica unas guías con el fin de mejorar el grado de ciberseguridad de las organizaciones. Son periódicamente actualizadas y completadas con otras nuevas en función de las amenazas y vulnerabilidades detectadas. Podemos ver su logotipo en la Ilustración 15.

Ilustración 15: Logotipo del CNPIC.

Fuente: (CNPIC, 2021).

La Oficina Nacional de Seguridad, que depende del Centro Nacional de Inteligencia: La Oficina Nacional de Seguridad (ONS), se creó en 1983 dentro del Centro Nacional de Inteligencia (CNI), como órgano de trabajo de su Director para auxiliarle en el cumplimiento de sus cometidos relacionados con la protección de la información clasificada (Gobiemo, 2012).

Grupo de Delitos Telemáticos de la Guardia Civil: El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet.

Su origen se remonta al año 1996, cuando se constituyó el Grupo de Delitos Informáticos (GDI), para atender a las pocas denuncias que había entonces por los llamados delitos informáticos.

Su buen hacer y el crecimiento exponencial de usuarios de la red, propiciaron el crecimiento del grupo, que pasó a llamarse Departamento de Delitos de Alta Tecnología (DDAT), asumiendo como nueva competencia el fraude en el sector de las telecomunicaciones.

Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información, o contra éstos, lo que se conoce popularmente como el cibercrimen. El departamento cambia de nombre por el actual, Grupo de Delitos Telemáticos (GDT). Estos cambios se acompañaron de la creación de los Equipos de Investigación Tecnológica (EDITE's), en cada una de las provincias de España.

El esfuerzo principal del GDT, y de los EDITE's, ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías, consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia.

Cabe destacar en el trabajo del GDT, su presencia continuada en seminarios y conferencias internacionales, lo que le ha permitido crear con una red de contactos policiales a nivel internacional, esencial en la resolución de determinadas investigaciones.

Actualmente es miembro y participa activamente en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen, y en Grupo de Europol.

Instituto Nacional de Ciberseguridad (INCIBE): El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio

de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional.

La misión de INCIBE, es por tanto reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos, en general. Vemos su logotipo en la Ilustración 16.

Ilustración 16: Logotipo del INCIBE.

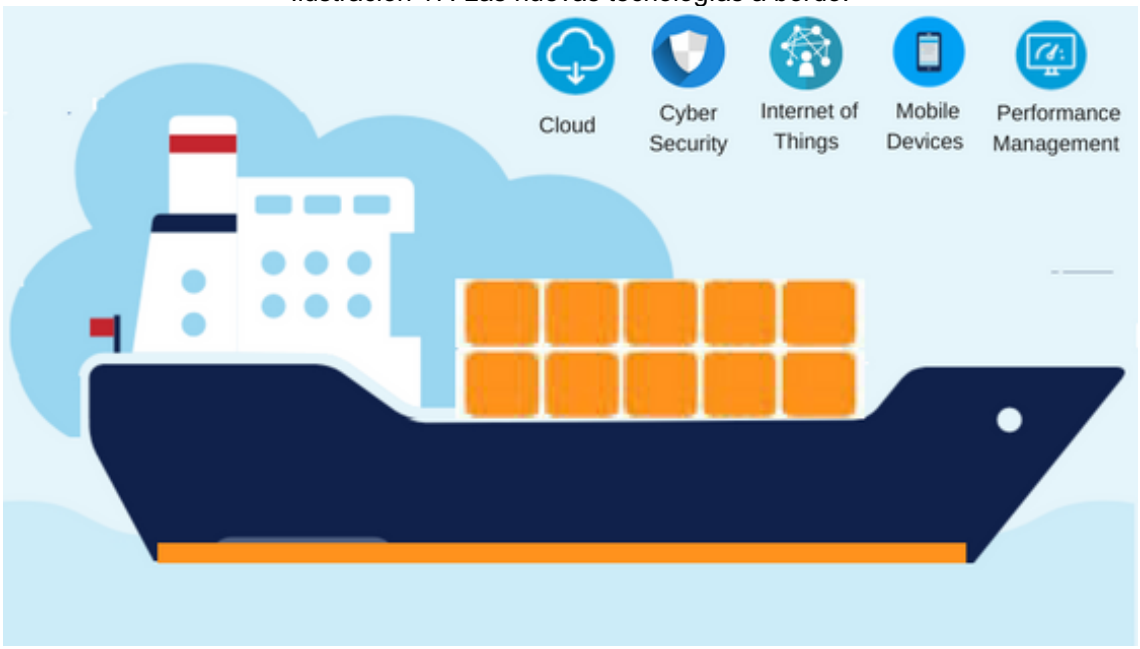
Fuente: (INCIBE, 2021).

CAPÍTULO IV: METODOLOGÍA PARA UNA CIBERSEGURIDAD RESILIENTE EN UN BUQUE CIVIL

4.1. METODOLOGÍA PARA UNA CIBERSEGURIDAD RESILIENTE A BORDO DE UN BUQUE CIVIL

La industria marítima tiene unas peculiaridades, como todos sabemos, especiales, y por ese motivo la ciberseguridad ha de considerarse desde otros puntos de vista, desde unos escenarios mas diversos y únicos, donde la distancia es cada vez menor, gracias a la tecnología, pero aun es una diferencia importante. Tenemos ya, desde hace unos pocos años, nuevas tecnologías en los buques, lo mismo que en tierra, como se muestra en la Ilustración 17.

Ilustración 17: Las nuevas tecnologías a bordo.



Fuente: (SHM Group, 2021).

De crucial interés en un sector donde la seguridad de las personas, el buque, el entorno medioambiental, la compañía naviera y la carga tienen gran importancia, la ciberseguridad es clave, y sus efectos potenciales negativos pueden ser devastadores. Podemos imaginar un buque petrolero donde sus sistemas se vean alterados y se produzca una colisión con otro buque de las mismas características.

Deben implantarse por esos motivos, medidas en varios niveles de la compañía naviera donde se definan las responsabilidades de cada trabajador y se puedan asimismo implantar procedimientos y formación que aseguraran, en

caso de darse un incidente, la continuidad de las operaciones normales. A esto habrá que añadir un plan de contingencia que será regularmente probado. Es totalmente recomendable que esto sea aceptado, cumplido y respetado desde la parte directiva de la empresa y los altos cargos deberán involucrarse si quieren llegar a buen puerto.

Los incidentes de ciberseguridad pueden afectar gravemente a una compañía naviera, desde lo mas sencillo que pudiera simplemente dañar la reputación de esta hasta hechos donde haya pérdidas de vidas humanas o desastres medioambientales.

La compañía naviera deberá de hacerse una serie de preguntas iniciales para centrar sus objetivos de protección a un nivel de riesgo aceptable. Este tipo de cuestiones se basan en conocer los riesgos, los impactos potenciales de un ciberincidente, las responsabilidades, los controles existentes y las protecciones de los sistemas, las buenas practicas, la formación, etc. Establecerá entonces, basándose en la cadena de mando, responsabilidades de cada trabajador de la compañía. Por ultimo, y no menos importante, es imprescindible que la relación con terceros sea muy controlada, asegurándose la madurez de sus procedimientos en los sistemas informáticos.

4.2. METODOLOGÍA PARA UNA CIBERSEGURIDAD RESILIENTE A BORDO DE UN BUQUE CIVIL

La realización de dicha metodología se basa en varias fases, tal y como se puede comprobar en la Ilustración 18.

Ilustración 18: Fases para la realización de la metodología.

Fase	Metodología
1	Análisis DAFO/CAME.
2	Identificación y evaluación de los ciberriesgos.
3	Diseño de medidas de protección.
4	Establecimiento de planes de contingencia.
5	Respuesta y recuperación de los incidentes.

Fuente: Elaboración propia.

4.2.1. FASE 1. ANÁLISIS DAFO/CAME

El análisis DAFO/CAME es una herramienta que nos ayuda a analizar las variables internas y externas de una empresa o proyecto. Este estudio interno y externo de la empresa tiene como objetivo determinar su situación real dentro del mercado.

El nombre, que en realidad es una sigla, responde a la unión de la primera letra de las palabras Debilidades-Fortalezas-Amenazas-Oportunidades.

Cuando hacemos este análisis para un proyecto, se convierte en una forma poderosa de evaluarlo ya que esta herramienta va a ayudarnos a planificarlo estratégicamente y analizaremos las fortalezas, las debilidades, las amenazas y las oportunidades.

Es un punto de partida, en forma de matriz, que nos permite saber en que situación se encuentra el proyecto.

Los componentes que pertenecen al análisis interno del proyecto son:
- **Debilidades**. Los puntos débiles que tiene nuestro proyecto, que lo limitan.

- **Fortalezas**. Los puntos fuertes que tiene nuestro proyecto.

Los componentes que pertenecen al análisis externo, que no dependen directamente del proyecto, pero que lo afectan:
- **Amenazas**. Factores externos que nos repercuten negativamente.

- Oportunidades. Factores externos que nos aportan una ventaja, una fortaleza.

Esto, normalmente, se representa en un cuadro como muestra la Ilustración 19, en forma de matriz ya que así se puede ver de una forma gráfica y de un solo vistazo podemos observar los factores internos y los factores externos.

Ilustración 19: Gráfico del análisis DAFO.

Fuente: (Marketing SGM, 2021).

En lo referente a la ciberseguridad a bordo de un buque civil, tenemos que estudiar todos los componentes que nos afectan y situarlos en uno de estos grupos de análisis.

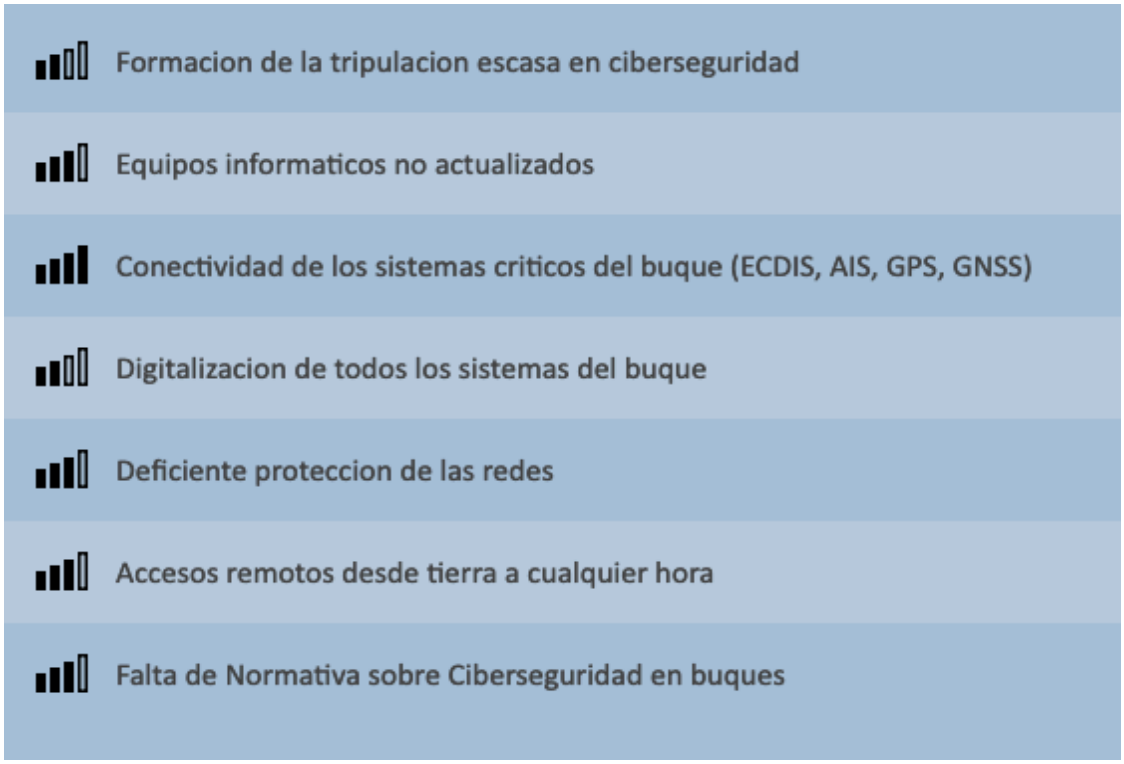
A continuación se muestran los cuadros DAFO, del proyecto, como un resumen gráfico, como se aprecia en las Ilustraciones de la 20 a la 23. Se pueden ver, a la izquierda de cada factor, una escala gráfica de uno a cuatro, que representa la importancia de dicho factor. Esta escala nos indica, de menor a mayor, el nivel de importancia.

Por ejemplo, respecto al análisis de los factores de las debilidades, no tiene la misma importancia la formación de la tripulación que la conectividad a sistemas críticos del buque.

Las debilidades, resumidas en la Ilustración 20, son un punto mejorable, es decir, nos preguntaremos que es lo que tenemos que mejorar en el proyecto. En nuestro caso, son de importancia aquellos factores que son mejorables y son el objetivo de los posibles atacantes.

Las amenazas son un punto mejorable. Nos preguntaremos cuales son los obstáculos del proyecto, las dificultades que lo complican o empeoran.

Ilustración 20: Análisis DAFO sobre las Debilidades.



Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

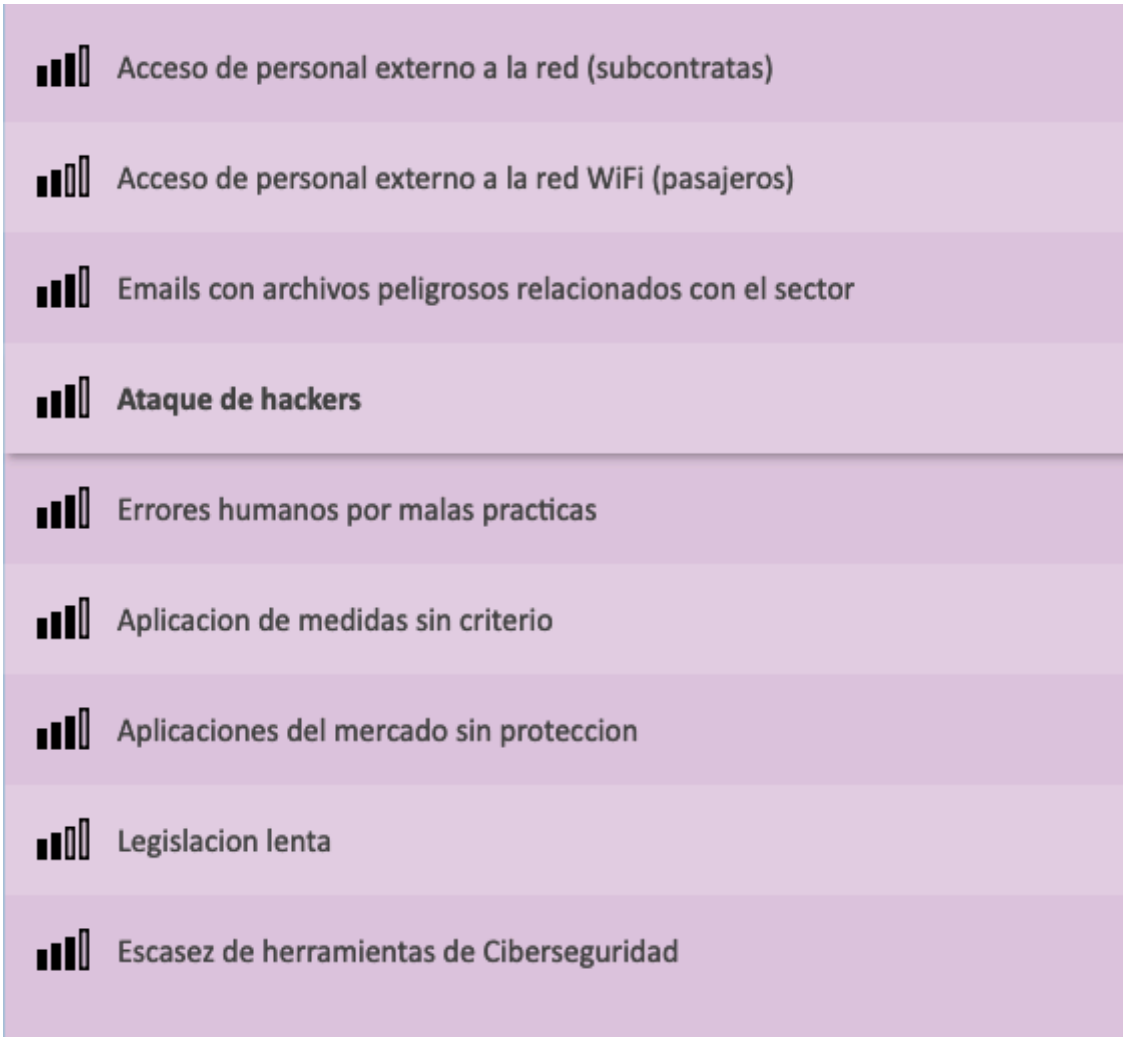
La ciberseguridad a bordo debe ser profundamente analizada y periódicamente actualizada y las amenazas tienen que ser conocidas siempre que se tengan datos, de ahí la importancia de la comunicación de los incidentes por todas las empresas del sector. De esa manera, podemos blindarnos frente a las nuevas amenazas.

De nuevo, en una escala de importancia de menor a mayor, podemos ver en la Ilustración 21 una relación de amenazas conocidas. Muchas de estas amenazas pueden ser eliminadas o minimizadas con unas simples medidas de protección.

En lo referente a las Fortalezas, anotaremos lo que estamos haciendo bien, lo que refuerza y hace mas sólido al proyecto. También están representadas por importancia, de modo gráfico, como ya se ha explicado.

Las fortalezas en ciberseguridad son nuestra ventaja frente a los atacantes. Se trata de que esta relación de factores sea lo mas amplia posible y que tengan el peso suficiente para servir de medida fuerte de protección.

Ilustración 21: Análisis DAFO sobre las Amenazas.



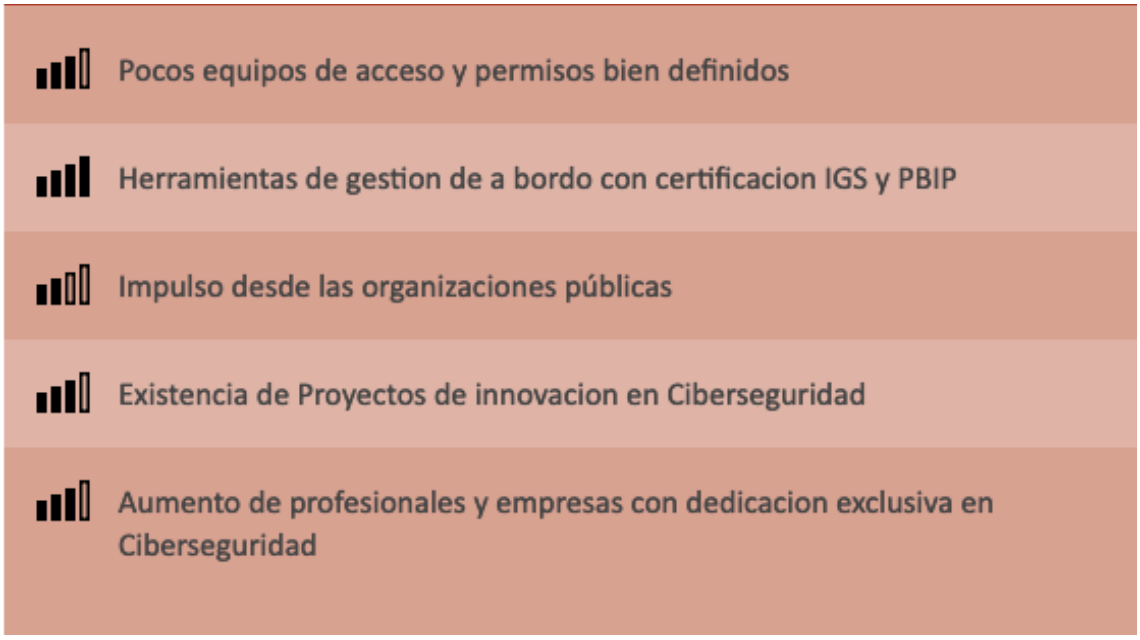
Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

A medida que eliminamos amenazas vamos aumentando las fortalezas, es decir, podemos tomar medidas para convertir una amenaza en una fortaleza llevando a cabo una serie de medidas de protección en los sistemas y de eso modo minimizar los riesgos, convertirnos en usuarios resilientes.

Nos preguntaremos cuales son nuestros objetivos, nuestras metas, lo que empuja positivamente al proyecto, que es lo que marca o define las Oportunidades, que se han resumido en la Ilustración 23.

En ciberseguridad no podemos restarles importancia a las oportunidades ya que son elementos que tenemos a nuestro alcance, de fácil aplicación y que nos resultan en ventajas rápidamente.

Ilustración 22: Análisis DAFO sobre las Fortalezas.



Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

Estas oportunidades, normalmente, se basan en experiencias positivas de otros usuarios o en el uso de tecnología de última generación como barrera de lucha frente a las amenazas.

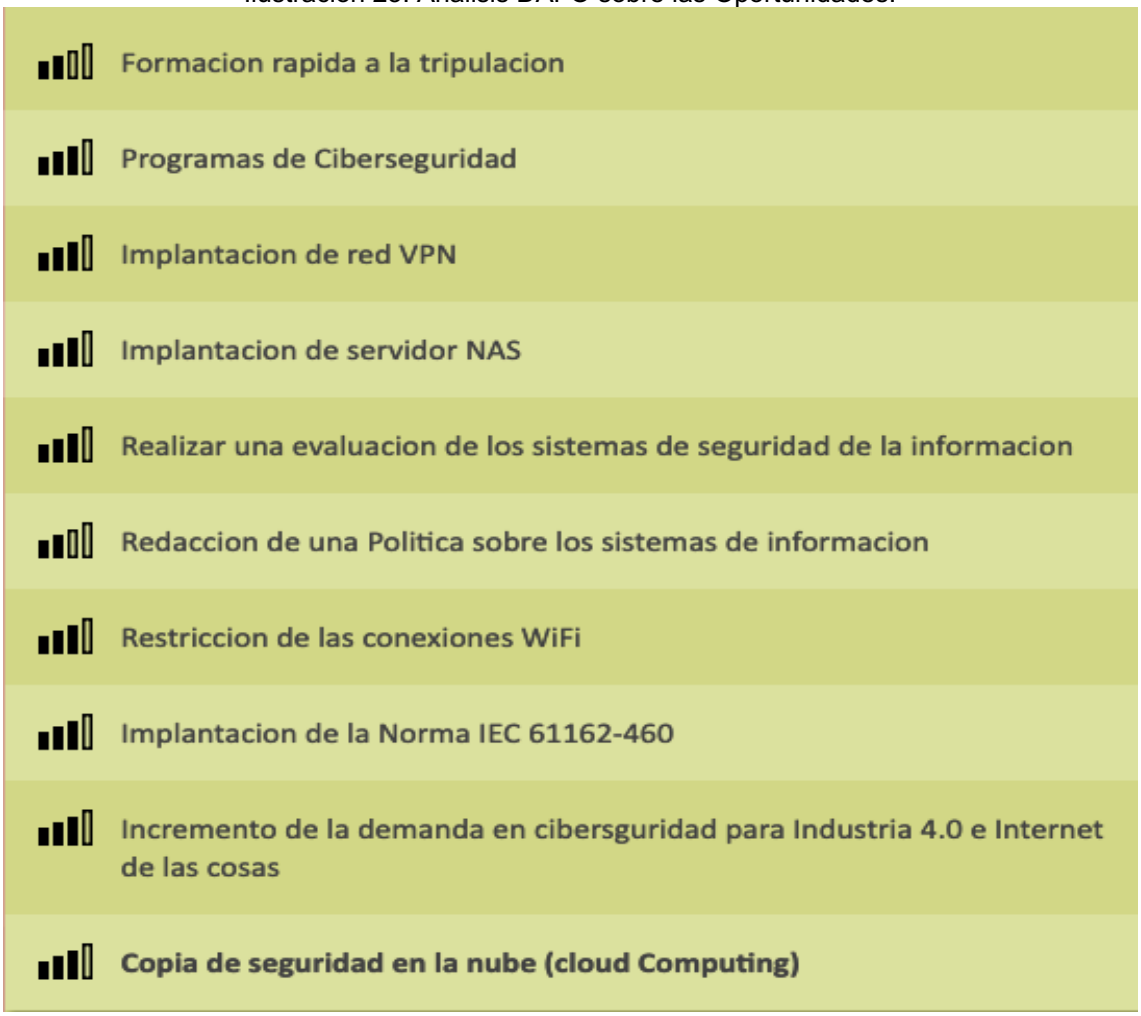
La inversión en tecnología para la lucha contra los atacantes es rentable, siempre, basta con pensar las consecuencias que va a tener para los activos de la empresa no poder disponer de los mismos o la pérdida o robo de la información, entre otras consecuencias graves.

La copia de seguridad en la nube sea, seguramente, una de las medidas mas fáciles de aplicar y mas eficaces para tener la información fuera del alcance de los atacantes y como respaldo en caso de que consigan los mismos llegar a la información y la encripten, por ejemplo.

Las conexiones VPN son otra medida muy efectiva.

Este primer análisis nos ayudará a ver el proyecto de forma neutral, visualizarlo desde nuevas perspectivas, buscar soluciones a problemas, tomar decisiones según los datos obtenidos, localizar puntos débiles, detectar amenazas y oportunidades, valorar otras estrategias, etc.

Ilustración 23: Análisis DAFO sobre las Oportunidades.



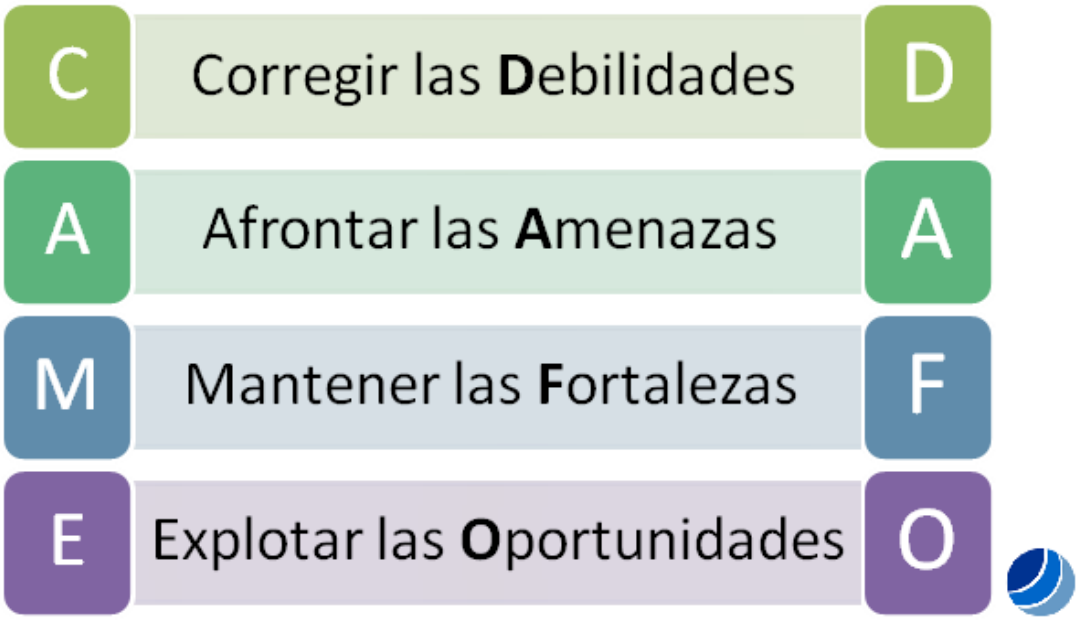
Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

Una vez realizado el DAFO, debemos trazar estrategias y entonces se comienza con el análisis CAME. Esto nos va a permitir definir acciones para tomar medidas frente a lo que muestra el análisis DAFO. Vamos entonces a tratar de convertir las debilidades en fortalezas y las amenazas en oportunidades.

Esto debe de estar vivo, es decir, debe de repetirse periódicamente porque surgen nuevos factores. Tendremos entonces una matriz como el mostrado en la Ilustración 24.

Existen diferentes tipos de estrategias dependiendo de lo que se vaya combinando. Al referirnos a la ciberseguridad, las estrategias se tomarán, como es lógico, con el objetivo de proteger la información.

Ilustración 24: Gráfico del análisis CAME.



Fuente: (Calidad Total, 2021).

Las claves imprescindibles para el análisis son las siguientes y los resultados son mostrados en las Ilustraciones 25 a la 28.

- **Corregir las debilidades**. La clave es reorientar, hay que conocer bien las debilidades y entonces corregirlas, o eliminarlas, con el objetivo de convertirlas en oportunidades. Es una estrategia de cambio o reorientación.

- **Afrontar las amenazas**. En este caso seguiremos una estrategia de supervivencia. Hay que conocerlas y enfrentarse a ellas. El objetivo es que no se conviertan en debilidades, por eso hay que minimizar las debilidades.

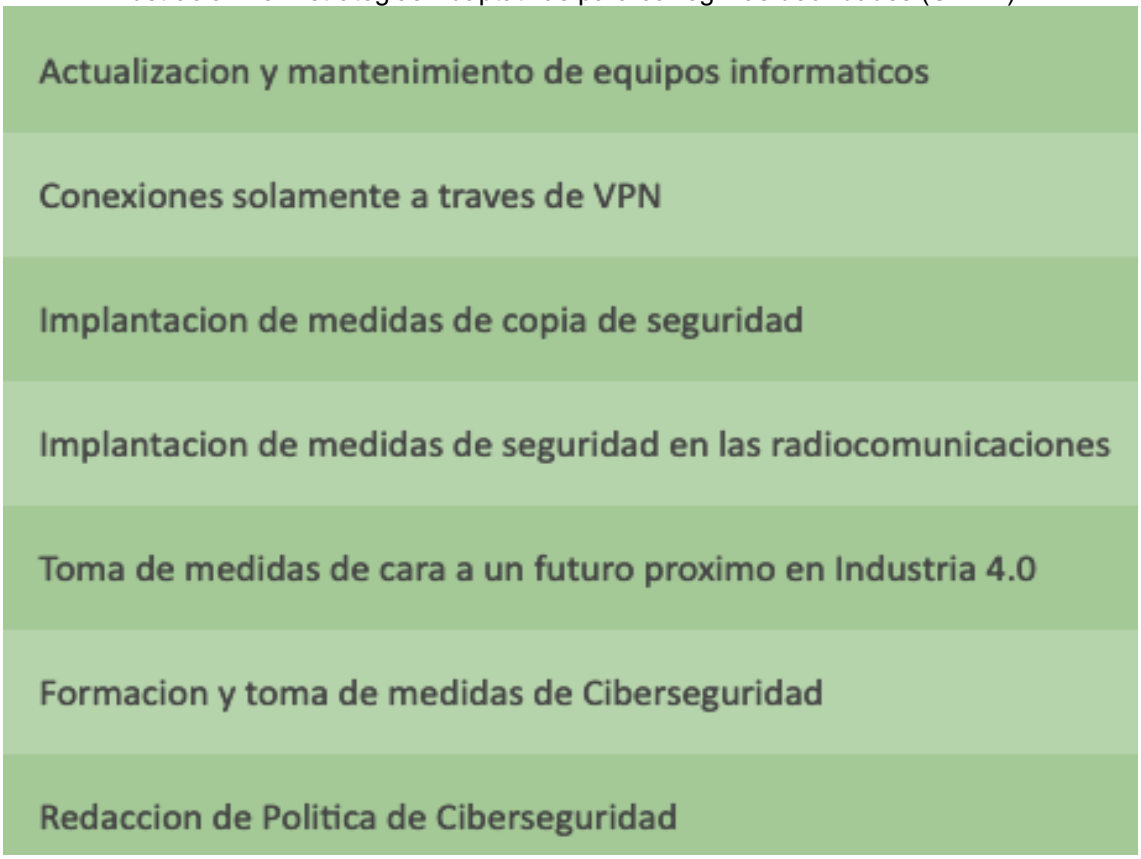
- **Mantener las fortalezas**. Con una estrategia defensiva, para evitar perderlas, ya que son el peso de nuestra ventaja y sigan siendo nuestro punto fuerte. Utilizaremos las fortalezas para disminuir las amenazas.

- **Explotar las oportunidades y convertirlas en fortalezas**. Con una estrategia ofensiva, consiste en utilizar las fortalezas para aprovechar las oportunidades.

Comenzamos **corrigiendo las debilidades**, para corregirlas. Esto también se puede denominar Estrategia Adaptativa. En lo referente a la ciberseguridad, se

tomarán las medidas necesarias para protegernos de aquellas debilidades analizadas mediante acciones encaminadas a mejorarlas o incluso mitigarlas.

Ilustración 25: Estrategias Adaptativas para corregir las debilidades (CAME).



Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

Seguimos a continuación, **afrontando las amenazas,** con una estrategia de supervivencia. Esto nos permitirá dejar los sistemas con un perfil de riesgo menor y de ese modo tener mas garantías de cara a un posible ataque.

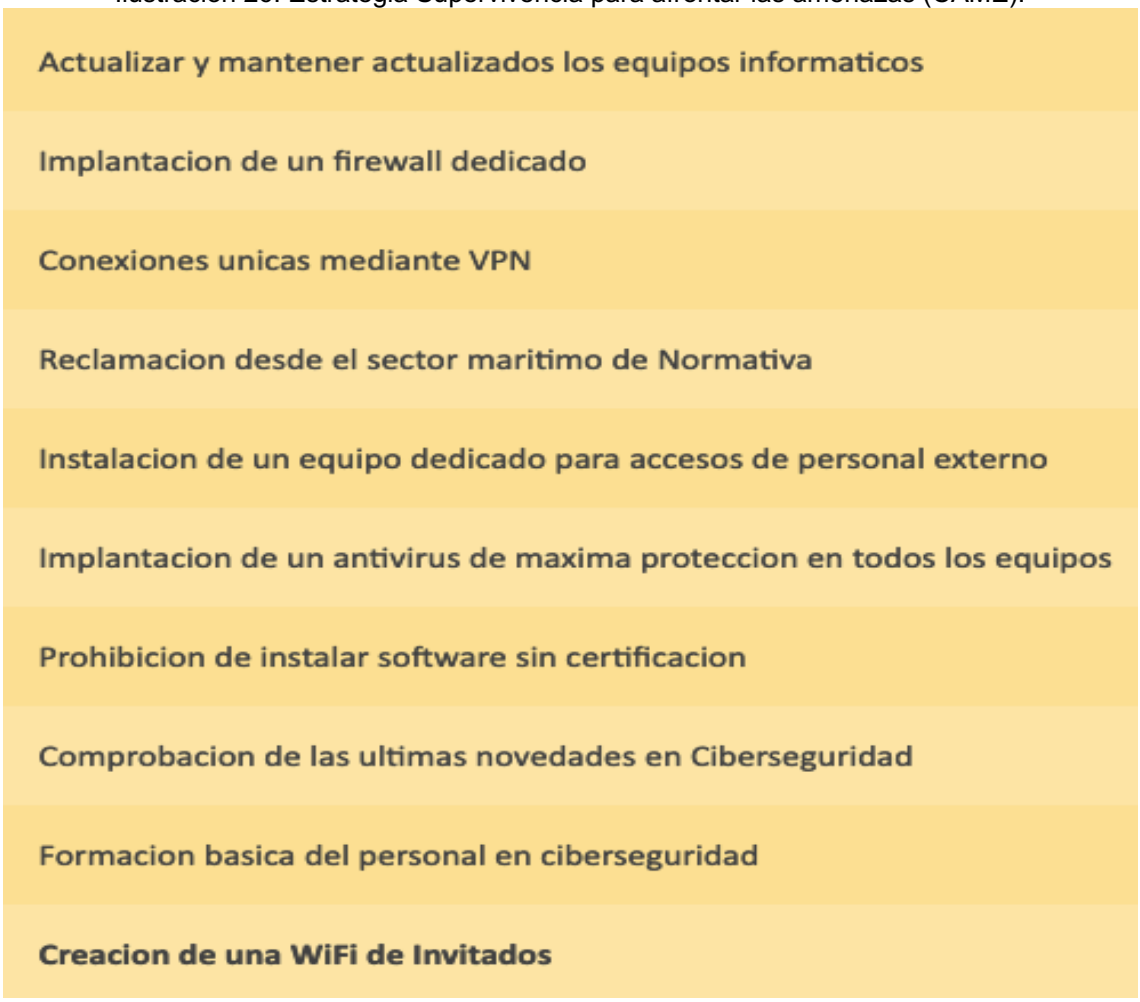
A continuación y por último, se muestra el cuadro que identifica a **mantener las fortalezas**, con una estrategia defensiva.

La ciberseguridad en este punto se basa en darle peso a las fortalezas del sistema para que no pierdan esa capacidad de protección frente a los atacantes.

Y finalmente se muestra el cuadro que se refiere a **Explotar las oportunidades y convertirlas en fortalezas** con una estrategia ofensiva.

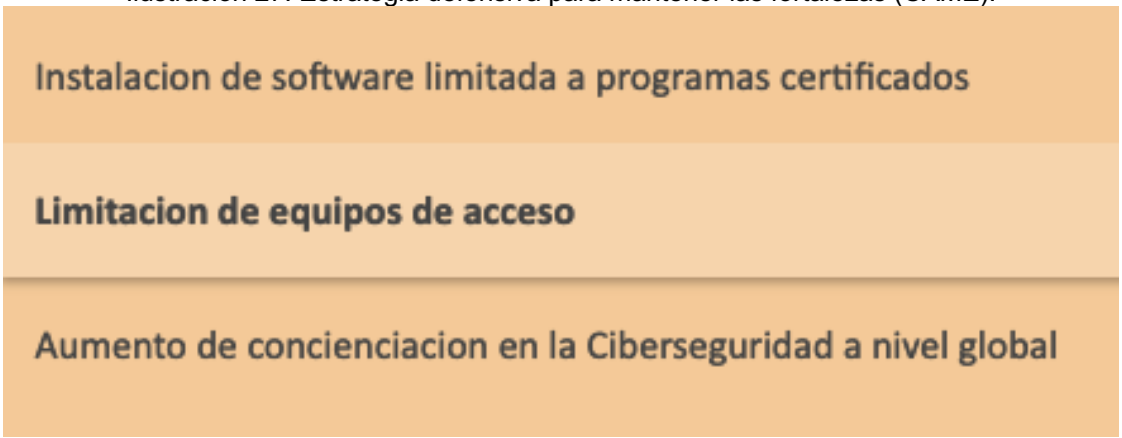
Son medidas de fácil implantación ya que, en muchos casos, nos referiremos a herramientas comerciales que tienen su experiencia demostrada en la protección.

Ilustración 26: Estrategia Supervivencia para afrontar las amenazas (CAME).



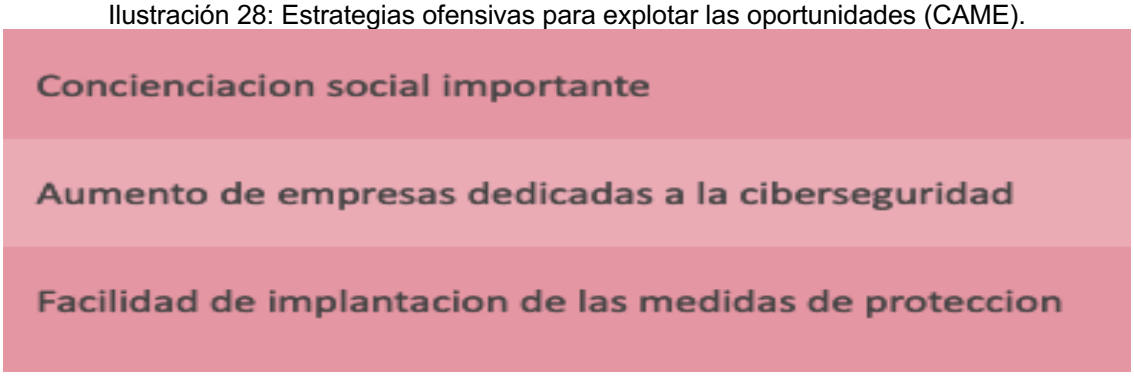
Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

Ilustración 27: Estrategia defensiva para mantener las fortalezas (CAME).



Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

Ilustración 28: Estrategias ofensivas para explotar las oportunidades (CAME).



Fuente: (Ministerio de Industria Comercio y Turismo, 2021).

4.2.2. FASE 2. IDENTIFICACIÓN Y EVALUACIÓN DE LOS CIBERRIESGOS

Para llevar a cabo una aproximación de la gestión de los ciberriesgos se hace necesario basarnos en varias etapas:

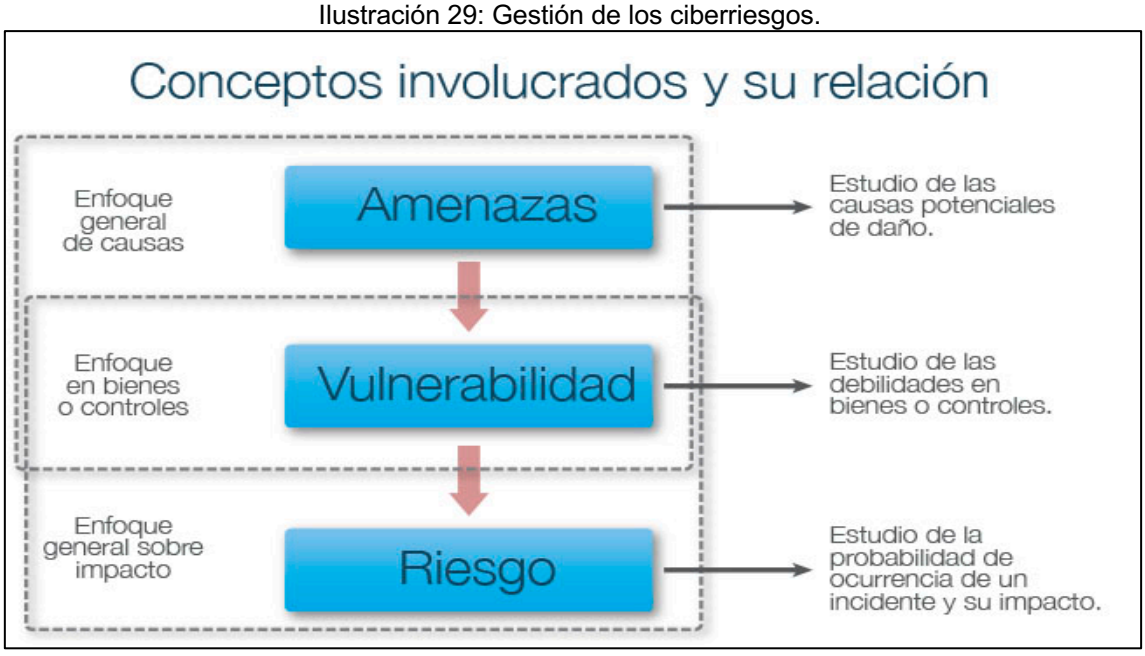
- Etapa 1. Identificar las amenazas.

- Etapa 2. Identificar las vulnerabilidades.

- Etapa 3. Calcular la probabilidad, evaluar el impacto y el riesgo.

Se puede ver la relación de las tres etapas en la Ilustración 29, a modo de resumen.

Ilustración 29: Gestión de los ciberriesgos.



Fuente: (Magazcitum, 2021).

Este programa de etapas corresponde a una filosofía basada en:

Identificar → Proteger → Detectar → Responder → Recuperar

4.2.2.1. ETAPA 1. IDENTIFICAR LAS AMENAZAS

Para identificar correctamente las amenazas tenemos que conocer a los posibles actores potenciales que puedan tener interés en entrar en los sistemas. Hay que tener en cuenta las posibles motivaciones y los posibles objetivos de los delincuentes informáticos. Puede ser un tripulante, desde dentro de la organización, o un hacker externo, o incluso un proveedor, o un cliente.

Podemos dividir estos actores en los siguientes grupos y motivaciones, ver Ilustración 30, ya mostrada en el capítulo anterior:

Ilustración 30: Identificación de actores potenciales.

Actores	Motivaciones
Intrusos accidentales	Sin motivo malicioso o mala suerte o por falta de conocimiento.
Activistas	Venganza, atención en los medios, daño en la reputación.
Criminales	Interés económico, espionaje.
Oportunistas	Reto informático, reputación social, interés económico.
Terroristas	Ideología, espionaje, interés económico.

Fuente: (BIMCO, 2016).

Hay una serie de hitos comunes a los ciberataques, que son cronológicos, como muestra la Ilustración 31, (National Institute of Standars and Technology, 2018). Son los pasos que un atacante va realizando a medida que accede a los sistemas y va saltando las seguridades, por diversos motivos, hasta llegar a su objetivo.

En la mayoría de los casos poder realizar ataques conlleva meses o años de trabajo y en algunas ocasiones, incluso es habitual acabar abandonando porque no se puede completar alguna parte, o porque la empresa ha realizado mejoras en sus sistemas que impide que los atacantes puedan avanzar en sus

objetivos. También pueden acabar siendo detectados por los técnicos informáticos lo que hace que aborten el plan de ataque.

Ilustración 31: Hitos de los ciberataques.

Etapas
Reconocimiento e investigación.
Preparación.
Distribución.
Explotación.
Instalación.
Comando y control.
Acciones sobre los objetivos.

Fuente: (National Institute of Standars and Technology, 2018).

Reconocimiento e Investigación: Actualmente es lo mas utilizado para saber de una compañía es su pagina web y sobre todo sus páginas en las redes sociales así como los foros técnicos, publicaciones, etc. Cualquier dato que la organización tiene en abierto, sin proteger. Cualquier dato vale para ir formando un perfil de objetivo y definir los procedimientos del ataque. En esta fase también se procede a analizar las vulnerabilidades de los sistemas con programas que monitorizan y escuchan los puertos (sniffers, rastreadores). Con los datos recogidos, el atacante valora que métodos de ataque podría utilizar y valora también la probabilidad de éxito. Esta es una parte de la concienciación de los empleados de la empresa ya que, en muchas ocasiones, se les envía correos electrónicos solicitando información y no se dan cuenta de estos indicios de reconocimiento.

Preparación: Se prepara el ataque de forma específica sobre un objetivo. Suele ser habitual que el atacante suplante la identidad de algún empleado y envíe un correo electrónico para recabar mas datos. Vuelve a ser indispensable la concienciación con la ciberseguridad de los usuarios, como ya se ha comentado.

Distribución: Se produce la transmisión del ataque. Cuando el usuario abre el documento infectado que había adjunto al correo electrónico (phising). La primera línea de defensa es identificar estos incidentes y aprender. Como se

puede comprobar, con una formación y concienciación de las personas se pueden detener los ataques en una etapa muy temprana.

Explotación: Aquí se detona el ataque comprometiendo al equipo infectado y la red a la que pertenezca. Entran en juego las vulnerabilidades y los sistemas no actualizados con los últimos parches, así como los antivirus sin actualizar.

Instalación: El atacante instala el malware en la víctima. Si hay robo de credenciales es mas sencillo y puede introducirse en los sistemas como si se tratara de un usuario mas. Dependiendo de los permisos de dicho usuario, podrá acceder a mas o menos recursos.

Comando y control: El atacante ya tiene el control del sistema en el que podrá realizar acciones maliciosas dirigidas desde un servidor central conocido como C&C (Command and Control), pudiendo robar credenciales, capturar pantallas, extraer documentación confidencial, instalar programas, conocer la red, información importante y sensible como manifiestos, listas de tripulación y pasajeros, etc.

Acciones sobre los objetivos: Fase final donde el atacante se hace con los datos e intenta expandir su acción maliciosa hacia mas objetivos.

4.2.2.2. ETAPA 2. IDENTIFICAR LAS VULNERABILIDADES

Existen una serie de vulnerabilidades que son comunes a los sistemas en buques civiles como se muestra en la Ilustración 32.

Tenemos que añadir, además de las citadas, varias vulnerabilidades como las siguientes:

- Interface de comunicación Buque-Tierra. Cada día son mas los buques que integran sistemas modernos en los que la comunicación con tierra es mayor y donde se intercambian muchos datos con la compañía naviera con el objetivo de controlar sistemas, como los motores, el mantenimiento y los diagnósticos remotos, el seguimiento de containers y la carga, el viaje, etc. Estos datos proporcionan muchas ventajas y mejoras pero añaden vulnerabilidades (AI,

Marítimo and Crawford, 2019).

Ilustración 32: Relación de Vulnerabilidades.

Vulnerabilidades en buques civiles
Sistemas operativos obsoletos o no soportados.
Software sin los parches actualizados.
Software antivirus y antimalware desactualizado o no existente.
Configuraciones de seguridad no adecuadas en usuarios y redes o uso de Contraseñas del fabricante por defecto.
Redes sin mantenimiento ni segmentadas.
Firewalls no existentes o mal configurados.
Sistemas críticos siempre conectados a tierra.
Accesos inadecuados de terceros.
Tripulación no formada de manera adecuada.
Falta de planes de contingencia o procedimientos.

Fuente: (BIMCO, 2016).

- Visitas al buque. Los terceros pueden visitar los buques como tradicionalmente o hacer conexiones remotas. Algunos agentes o prácticos llevan consigo dispositivos que requieren conectarse a las redes del buque y en algunas ocasiones imprimir documentos. Esto debe de segregarse de la red.

- Mantenimiento del software. Los sistemas requieren de actualizaciones y normalmente se hace por empresas autorizadas desde tierra o a bordo. Esto requiere de la máxima confianza y el máximo nivel de seguridad por las graves implicaciones, como es de suponer (Gobiemo, 2013). Los proveedores deben de informar antes de proceder a la actualización del procedimiento a seguir y del contenido de la actualización.

La identificación de las vulnerabilidades se centrará en analizar aplicaciones y sistemas para encontrar amenazas potenciales.

El objetivo de este análisis va a ser identificar las vulnerabilidades que puedan comprometer al sistema y se produzca una perdida de confidencialidad, integridad y disponibilidad de los datos (CIA), que veremos seguido, en la denominada Etapa 3. La siguiente Ilustración 33, resume los sistemas de a

bordo.

Ilustración 33: Sistemas a bordo.

Sistemas a bordo de un buque civil
Sistemas de control de la carga.
Sistemas del puente como el GPS, ECDIS, AIS, GMDSS, Radar, etc.
Sistemas de manejo de la propulsión, maquinaria y energía.
Sistemas de control de acceso de la tripulación (CCTV).
Sistemas de acceso de pasajeros.
Redes WiFi para los pasajeros.
Sistemas administrativos y de la tripulación.
Sistemas de comunicación como la comunicación por satélite, WiFi, Voz sobre IP (VOIP), comunicaciones integradas a bordo, sistemas de alarmas, etc.

Fuente: (BIMCO, 2016).

4.2.2.3. ETAPA 3. CALCULAR LA PROBABILIDAD, EVALUAR EL IMPACTO Y EL RIESGO

La **probabilidad** es el producto de la amenaza y la vulnerabilidad.

En el documento SMS de la compañía se incluirá una matriz de riesgos que será medida en una escala de probabilidad de uno a cinco que se calculará así tal y como se muestra en la siguiente Ilustración 34.

Ilustración 34: Niveles de Probabilidad.

Nivel	Probabilidad
Nivel 1	Muy improbable, nunca se ha citado el caso.
Nivel 2	Muy raro y como resultado de una serie de sucesos desafortunados.
Nivel 3	Suceso que ha ocurrido en la compañía, pero en un contexto de un fallo en un equipo y errores humanos.
Nivel 4	Ocurre en alguna ocasión en la compañía.
Nivel 5	Ocurre frecuentemente en la compañía.

Fuente: (BIMCO, 2016).

El modelo CIA (Confidencialidad, Integridad y Disponibilidad) proporciona un método para evaluar el **impacto** de lo que significa la perdida de esos tres parámetros. El SMS de la compañía deberá de contener una matriz de cálculo del impacto en una escala también de uno a cinco, mostrado en la siguiente Ilustración 35.

Ilustración 35: Niveles de Impacto.

Nivel	Impacto
Nivel 1	Sin efectos en la salud, medioambientales, finanzas o en la reputación de la compañía.
Nivel 2	Efecto muy pequeño en la salud, medioambientales, finanzas o en la reputación de la compañía.
Nivel 3	Algunos efectos en la salud, medioambientales, finanzas o en la reputación de la compañía.
Nivel 4	Efectos mayores en la salud, medioambientales, finanzas o en la reputación de la compañía.
Nivel 5	Efectos fatales en la salud, medioambientales, finanzas o en la reputación de la compañía.

Fuente: (BIMCO, 2016).

Otros sistemas calculan el impacto en tres escalas: bajo, medio y alto.

La evaluación del **riesgo** se realiza en 4 partes:

- Análisis previo de las actividades: Esta parte comprende una toma de datos compleja donde han de conocerse de manera profunda todos los sistemas. Se revisará toda la documentación de los sistemas, se identificará los principales proveedores del equipamiento critico, se identificarán los aspectos de ciberseguridad con terceros, se revisará con detalle los programas de mantenimiento y se establecerán contratos sobre las empresas que mantienen los equipos y sistemas.

- Análisis del buque: Se deberá de analizar al detalle sistema a sistema en el buque. Cada conexión es un punto de vulnerabilidad.

En esta parte se calculará un riesgo inicial en cada sistema. Esto dará como resultado un número que se calcula con la formula siguiente (Arévalo and Moscoso, 2017):

Riesgo = probabilidad x impacto

Si el riesgo inicial es mayor que el criterio aceptado por la compañía deberán de realizarse una serie de mejoras hasta que el riesgo sea aceptable. Eso se denomina mitigación del riesgo. Por ejemplo, el sistema ECDIS tiene una probabilidad de nivel 4 porque puede ocurrir por motivos como: introducción de un USB en un equipo, ordenador usado de manera inadecuada, conexión a la

red por una impresora compartida, actualización del sistema de cartas sin control, etc.

El impacto es de nivel 5, debido al riesgo de una catástrofe por abordaje o varada.

El producto quedaría:

Riesgo = 4 x 5 = 20

El riesgo inicial no es aceptado por lo que se toman medidas de mitigación del riesgo:

- Se establecen contraseñas mas seguras, se aísla un equipo para imprimir, se restringe el uso del ECDIS, se elimina la opción del uso del puerto USB.

Esto hace que la probabilidad descienda hasta uno y, a pesar de que el impacto sea el mismo, la probabilidad hace que el resultado sea menor:

Riesgo = 1 x 5 = 5 → **ACEPTABLE**

Ilustración 36: Barrera de defensa principal.

Barrera de defensa principal
Seguridad física del buque de acuerdo con el plan de seguridad (SSP).
Protección de las redes.
Detección de intrusos (IDS).
Uso de firewall. Ver ilustración 38.
Pruebas periódicas de vulnerabilidad.
Software aprobado.
Control de accesos.
Controles de configuraciones y cambios.
Procedimientos adecuados sobre uso de dispositivos externos y contraseñas.
Advertencias a la tripulación sobre ciberseguridad.
Comprensión y familiarización de los procedimientos y respuesta a incidentes.
Redactar guías de buen uso de los sistemas y difundirlas en las formaciones a la tripulación.
Copias de seguridad en servidor espejo y en la nube. En caso de ataque o caída del servidor principal se puede restaurar el sistema en minutos. En caso de encriptación de los datos se pueden restablecer desde la nube.
Cubrir las posibles vulnerabilidades entre sistemas.

Fuente: (BIMCO, 2016).

4.2.3. FASE 3. DISEÑO DE UN MODELO DE MEDIDAS DE PROTECCIÓN

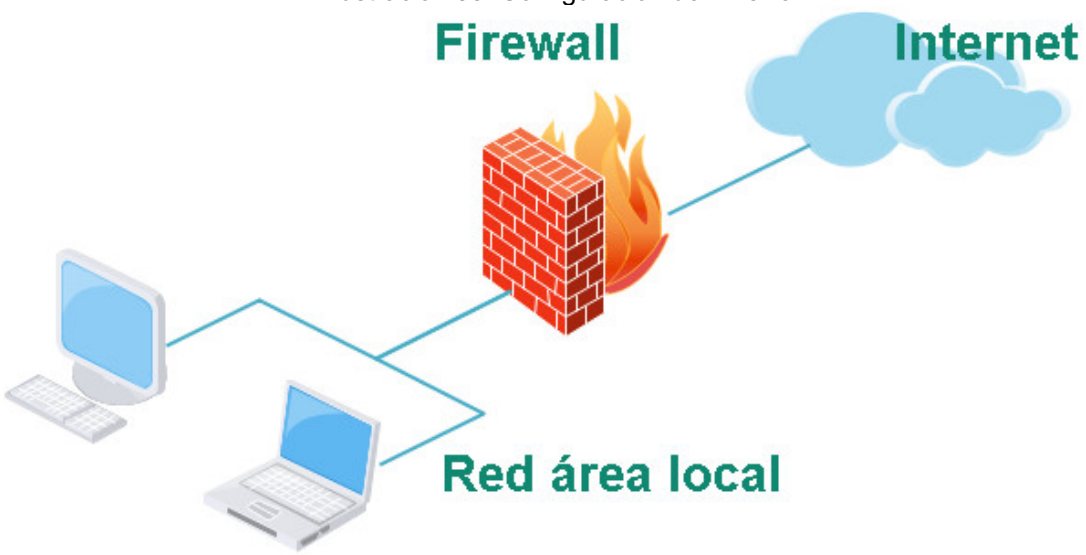
La defensa es la clave en este tipo de desarrollo. Es importante crear una serie múltiple de capas de medidas de protección que harán que las probabilidades de que pueda detectarse un incidente de ciberseguridad sean mayores y además se optimizan los recursos para poder proteger la confidencialidad, integridad y disponibilidad de los datos en los sistemas. En la Ilustración 36, se muestran las barreras principales.

Ilustración 37: Barreras de defensa prácticas y de bajo coste.

Barrera de defensa prácticas y de bajo coste
Limitación y control de los puertos de comunicación, protocolos y servicios.
Configuración de los dispositivos de redes como firewalls, Routers y Switches.
Segregación de los sistemas con firewalls.
La seguridad física suele ser la mas simple y barata, separar sistemas.
Comunicaciones de radio y satélite protegidas.
Acceso a redes WiFi con contraseñas seguras y encriptados. Sistemas IPS.
Uso de redes Virtual Private Network (VPN).
Uso de configuración segura de software y hardware.
Protección del correo electrónico y del navegador de paginas web.
Revisión periódica de parches del software.

Fuente: (BIMCO, 2016).

Ilustración 38: Configuración del Firewall.



Fuente: (Ciberinteligencia, 2021).

Las siguientes medidas, Ilustración 37, son mas prácticas y de bajo coste, fácilmente aplicables por la poca inversión necesaria, así como su rapidez de

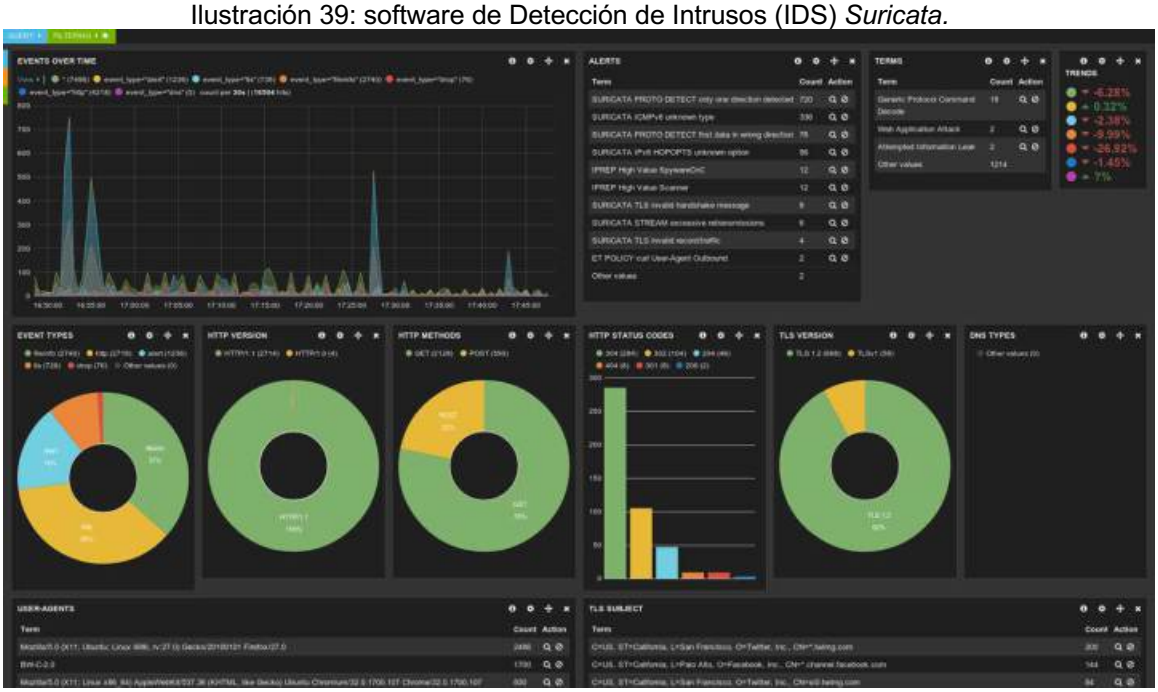
implantación.

Las medidas de protección deben de incluirse en un procedimiento en el que la tripulación tenga una formación periódica y esto debe de extenderse al personal de tierra que visita el buque. Lo ideal es acompañarlo con simulacros. Deben conocerse los riesgos relativos al uso de emails y como manejarlos de manera segura, el uso de internet, la geolocalización de la tripulación, el uso de los dispositivos personales, el mantenimiento del software, las contraseñas, la detección de actividades sospechosas, etc.

Una parte muy importante, que no debe de olvidarse, en la defensa es la capacidad de poder detectar intrusos, así como infecciones. Existen sistemas de detección de intrusos Intrusion Detection Systems (IDS), ver Ilustración 39, que son recomendables tener activos y que forman parte de una opción del firewall, que debe ser activada.

En cuanto a la detección de infecciones es clave la adquisición de software de escaneo que detecte el malware y los virus. Este software debe ser actualizado por toda la tripulación periódicamente.

Ilustración 39: software de Detección de Intrusos (IDS) *Suricata.*



Fuente: (Ciberinteligencia, 2021).

4.2.4. FASE 4. PLANES DE CONTINGENCIA

Una pérdida en los sistemas de a bordo puede provocar un desastre tan grande que incluso peligre la vida de las personas, el medioambiente, la integridad del buque o la continuidad de la compañía. Es esencial que se tomen medidas inmediatamente para proteger todo lo anterior. Estas medidas estarán dentro de un plan de respuesta que incluirá una investigación de lo ocurrido.

La seguridad 100% no existe. Debemos estar preparados. Es un Plan de Contingencia y de Continuidad del Negocio, además de los peligros añadidos, ya comentados, por ser a bordo de un buque civil, con cargas diversas.

Inicialmente será importante buscar sistemas alternativos que sustituyan a los afectados como modo de operar, sin esperar mas tiempo.
Puede ocurrir que varios sistemas se vean afectados a la vez.

La Ilustración 40, a modo de resumen, muestra una lista de sistemas afectados.

Ilustración 40: Lista de Sistemas afectados.

Lista de Sistemas afectados
Pérdida de disponibilidad de las cartas electrónicas o la navegación electrónica.
Pérdida de la disponibilidad de los datos de sistema GNSS.
Pérdida de la conectividad con tierra incluyendo en sistema GMDSS.
Pérdida de la disponibilidad de los sistemas de control de propulsión, sistemas auxiliares y otros sistemas críticos.
Denegación de servicio (DoS) o fallo en los datos por ransomware.

Fuente: (BIMCO, 2016).

El plan de contingencia debe ser entrenado y revisado por la tripulación de manera periódica. Consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan los datos y los sistemas.

Estos planes deben ser diseñados con mucho cuidado. Se aconseja que se hagan simulacros antes de ponerlos en marcha para probar su efectividad y ajustar detalles de su implementación. Organismos con el citado INCIBE tienen planes ya generados que pueden servir de guía inicial (Instituto Nacional de Cibersegidad INCIBE, 2017).

En algunas ocasiones, se podrá decidir aislarse de las comunicaciones con tierra con el objetivo de proteger la seguridad de la operación del buque. Esto puede ser tan sencillo como quitar un cable o desconectar un firewall.

4.2.5. FASE 5. RESPUESTA Y RECUPERACIÓN TRAS UN INCIDENTE DE CIBERSEGURIDAD

Los ciberincidentes requieren de una respuesta rápida y activa para recuperar los sistemas y volver a la normalidad lo antes posible. Solamente así podremos decir que han tenido éxito. Se debe de priorizar en una detección y una respuesta ágil. Los tres siguientes conceptos son determinantes: velocidad de detección (cuánto tiempo se tarda en detectar el incidente), tiempo de recuperación/restauración a la actividad normal (cuánto se tarda en volver a la actividad normal) y tiempo de respuesta (cuánto se tarda en identificar y movilizarse). El objetivo es asegurarnos de que todos los tripulantes con responsabilidad conozcan y apliquen un procedimiento rápido y eficaz para actuar ante cualquier incidente.

Esto se organiza con un plan de respuesta a incidentes de seguridad. Este plan contiene un conjunto de instrucciones diseñadas para ayudar a las empresas a detectar, responder y recuperarse de los incidentes de seguridad en la red.

La mayoría de este tipo de planes se centran en la detección de malware, robo de datos (phising) y en las interrupciones del servicio (DoS). Un ataque cibernético podría ir mas allá de modo que es recomendable añadir mas variables al plan.

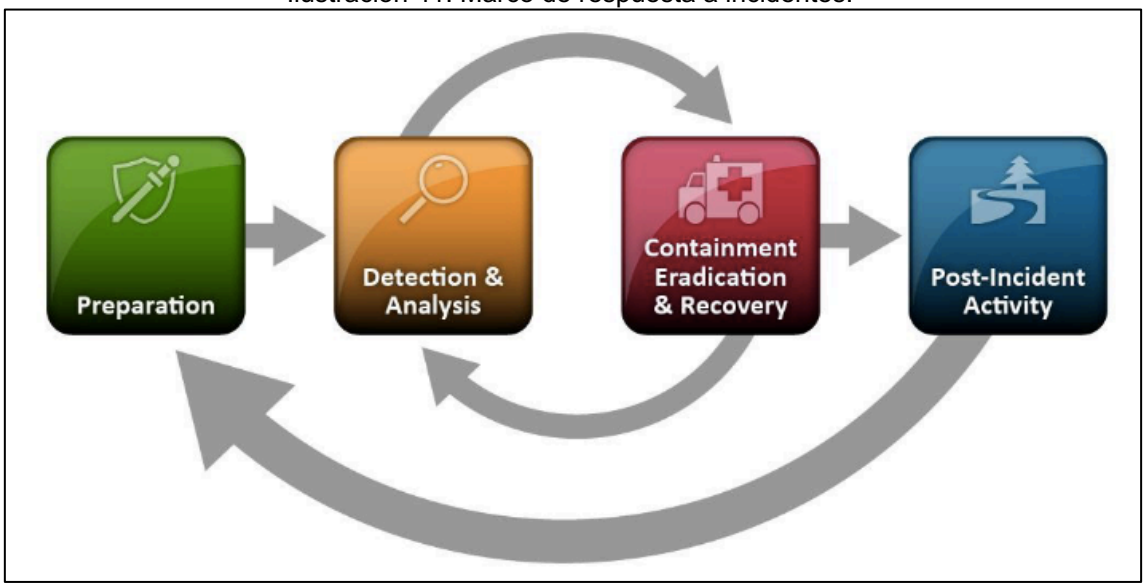
Existen marcos de respuesta a incidentes, por ejemplo, de la organización

NIST (Cichonski, 2012) que proporciona pautas generales sobre cómo responder a un incidente. Se muestra el gráfico de respuesta en la Ilustración 41.

Cualquier empresa que tenga activos digitales (ordenadores, servidores, datos en la nube, etc.) tiene el potencial de recibir un ataque cibernético. La mayoría solo se dan cuenta después de haber recibido el ataque.

Es necesario nombrar un equipo responsable para la gestión y, sobre todo, tener el máximo apoyo desde la Dirección de la empresa.

Ilustración 41: Marco de respuesta a incidentes.



Fuente: (National Institute of Standars and Technology, 2018).

Para poder organizar dicho plan se han definido cuatro fases, basadas en las indicaciones del NIST:

Preparación: Se determinan cuales son los sistemas críticos del buque y su localización, se asegura una copia (back-up) correcta y se aplica el procedimiento de respuesta al incidente. En este paso se prepara, por adelantado, un plan sólido de respuesta que ayude a evitar las brechas de seguridad. Aquí se nombra al equipo responsable y se establecen las estrategias así como se realizan los simulacros. Es imprescindible determinar la ubicación exacta de todos los activos.

Detección y análisis: Una vez detectada la amenaza hay que determinar la causa del incidente para ver cómo se puede contener. Lo ideal en esta fase es realizar una monitorización de la trayectoria del ataque, Se hace necesario saber que sistemas se han visto afectados y como, se extiende lo anterior a los datos y se analiza si queda alguna amenaza pendiente en otros sistemas. Se hace necesario en este momento notificar y documentar el incidente. Dependiendo de los datos recogidos se priorizará la respuesta.

Contención y erradicación: Hay que verificar si las reglas del firewall han sido modificadas, verificar que el antivirus y el anti-malware están actualizados, hacer una imagen del disco de los sistemas afectados y hay que considerar hacer una copia de la RAM para su análisis forense posterior. Es el momento de la contención.

Recuperación: Recuperar los sistemas y datos, investigar el incidente y prevenir que pueda volver a ocurrir. El procedimiento debe ser actualizado cada cierto tiempo y con mas razón después de un incidente donde habrá mucho aprendido.

CONCLUSIONES

Primera:

Los ciberataques al sector marítimo son una realidad. Se ha registrado que del año 2015 al año 2018, un aumento de la criticidad en términos de motivación de la amenaza, la competencia técnica de los atacantes y complejidad de estos. Esto ha significado, pérdidas económicas muy cuantiosas.

Segunda:

Establecer una evaluación con el DAFO (Debilidades-Amenazas-Fortalezas-Oportunidades), permite disponer en todo momento de una perspectiva real de la situación de la ciberseguridad en el buque civil. El plan de seguridad informática ha de ser revisado periódicamente, lo que contribuirá a la mejora del plan de protección y del plan de contingencias.

Tercera:

Se recomienda la aplicación de múltiples capas como medidas de protección (capas, anillos de seguridad, para retrasar el ataque y su efectividad). Hay que realizar un estudio y un inventario detallado de todos los sistemas del buque que pueden verse afectados y acompañarlo con una evaluación de riesgos de ataque informático en todos ellos, así como con una guía de buen uso estableciendo un control de los usuarios y de los permisos de acceso.

Cuarta:

Es imprescindible la formación continua e innovadora de la tripulación y el establecimiento de una filosofía clara de mentalización en la compañía en todos los niveles. Esto debe de incluir simulacros para tener muy claro las tareas a ejecutar en caso de un incidente y consecuentemente en función de auditorias internas y externas.

Quinta:

Se recomienda el uso de IA (Inteligencia Artificial) unido a la máxima colaboración entre gobiernos y empresas, para luchar conjuntamente contra los ciberataques. Se ha demostrado, que es la mejor herramienta disponible junto con el monitoreo y la detección, para proteger y proporcionar alertas tempranas compartidas.

BIBLIOGRAFÍA

Al, C., Marítimo, T. and Crawford, J. C. (2019) 'Amenza Real O Ciencia Ficción ?', pp. 15–23.

Alcaide, J. I. and Llave, R. G. (2020) 'Critical infrastructures cybersecurity and the maritime sector', in *Transportation Research Procedia*, p. 8. doi: 10.1016/j.trpro.2020.03.058.

Arévalo, F. M. and Moscoso, I. P. C. S. A. (2017) 'Agile Methodology for Computer Risk Management', *Killkana Técnica*, pp. 31–42. doi: 10.26871/killkana.

Barroilhet Acevedo, C. (2004) 'El Código Internacional para la Protección de los Buques e Instalaciones Portuarias: orígenes del Código PBIP.', *Revista de Derecho de la Universidad Católica de Valparaíso*, XXV, pp. 33–48.

BIMCO (2016) 'The Guidelines on Cyber Security onboard Ships', *BIMCO*, p. 36. Available at: www.bimco.org.

Calidad Total (2021) *Página Web Blog Calidad Total*. Available at: http://ctcalidad.blogspot.com/2016/10/analisis-came-trabajando.html.

Camara Maritima del Ecuador (2021) *Página Web Camara Marítima del Ecuador*.

Ciberinteligencia (2021) *Página Web Ciberinteligencia*. Available at: https://ciberinteligencia.wordpress.com/2018/10/08/introduccion-a-la-ciberseguridad-i/.

Cichonski, P. (2012) 'Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology', *NIST Special Publication*, 800–61, p. 79. Available at: http://dx.doi.org/10.6028/NIST.SP.800-61r2%5Cnhttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

CNPIC (2021) *Página Web CNPIC*. Available at: https://www.csirt.es/index.php/es/miembros/cnpic.

Consejo de la UE (2004) *Reglamento (CE) No 725/2004 del Parlamento*

europeo del Consejo de 31 de marzo de 2004 relativo a la mejora de la protección de los buques y las instalaciones portuarias.

Crawford, J. C. (2019) 'Ciberataque al transporte maritimo, Amenza Real O Ciencia Ficción ?', *REVISMAR*, pp. 15–23.

Curt García, L. (2018) 'La estrategia de seguridad marítima nacional ante su próxima revisión: avances y opciones de mejora', *Instituto Español de Estudios Estratégicos*, p. 20. Available at: http://www.funciva.org/uploads/ficheros_documentos/1372756446_la_nueva_estrategia_nacional_de_se.

DCSA (2020) 'Implementation Guide forCyber Security on Vessels 1.0', *DCSA*, p. 110.

Departamento de Seguridad Nacional (2021) *Página Web Departamento de Seguridad Nacional*. Available at: https://www.dsn.gob.es/.

Enrique, L. *et al.* (2019) 'Ciberseguridad en la automatización a bordo a través de sistemas digitales integrados en redes internas y externas', *Grupo COMISMAR*, pp. 14–17.

Fabra, U. P. (2002) 'El análisis crítico del discurso y el pensamiento social Teun Van Dijk y Athenea Digital', *Athenea Digital* -, 1(Primavera), pp. 1–7.

Gobiemo, E. (2012) *Estrategia de Seguridad nacional ESN-2013*.

Gobiemo, E. (2013) *Estrategia de Ciberseguridad Nacional*. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf.

Gobierno de España (2017) *Estrategia de Seguridad Nacional.ESN-2017*. doi: 10.1111/j.1467-9868.2008.00700.x.

Håvold, J. I. (2010) 'Culture in maritime safety', *Maritime Policy and Management*, 27(1), pp. 79–88. doi: 10.1080/030888300286716.

INCIBE (2021) *Página Web INCIBE*. Available at: https://www.incibe.es/proyectos-europeos/sic-spain.

Instituto Nacional de Cibersegidad INCIBE (2017) 'Plan de Contingencia y de continuidad del negocio', *Plan de Contingencia y Continuidad de Negocio*, pp. 1–31. Available at: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf.

ISO/IEC 27000 (2018) 'International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and', *ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA*, 34(19), pp. 45–55. Available at: http://www.worldcat.org/title/service-operation/oclc/254028066&referer=brief_results%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf%0Ahttp://k504.kh.

Lisot (2021) *Página Web Lisot*. Available at: https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/.

Lloyd's (2016) 'Cyber-enabled ships', *Lloyd´s Register*, p. 20.

Lloyd's (2018) 'Cyber security ? You ' re right , it ' s a hot topic .', *Lloyd´s Register*, p. 3.

Machin Nieva, N. e. and Gazapo Manuel, M. gazapo. lapayese@hotmail. co. (2016) 'La Ciberseguridada como factor critico en la seguridad de la UE.', *UNISCI Discussion Papers*, (42), pp. 47–68. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=119225869&lang=es&site=eds-live&custid=ns021105&authtype=ip,sso.

Magazcitum (2021) *Página Web Magazcitum*. Available at: https://www.magazcitum.com.mx/?p=2193.

Marketing SGM (2021) *Página Web Marketing SGM*. Available at: https://www.marketingsgm.es/analisis-dafo-todo-lo-que-necesitas-saber/.

Ministerio de Defensa (2019) *Convenio entre el Ministerio de Defensa y la*

Universidad de Cantabria para la investigación de los protocolos de Seguridad Marítima. España: BOE.

Ministerio de Industria Comercio y Turismo (2021) *Herramienta DAFO*. Available at: https://dafo.ipyme.org/Home#.

Ministerio del Interior (2011) *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*, *Boe*. Available at: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849.

National Geospatial Agency (2021) *Página Web National Geospatial Agency*. Available at: https://www.nga.mil/.

National Institute of Standars and Technology (2018) 'Framework for improving critical infrastructure cybersecurity', *Proceedings of the Annual ISA Analysis Division Symposium*, pp. 9–25.

Organización Marítima Internacional (2017) 'Directrices sobre la gestión de los riesgos cibernéticos marítimos', *Documento OMI*, MSC-FAL. 1(0), p. 7. Available at: http://www.imo.org/es/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3 - Directrices Sobre La Gestión De Los Riesgos Cibernéticos Marítimos (Secretaría) (1).pdf.

Roach, J. A. (2004) 'Initiatives to enhance maritime security at sea', *Marine Policy*, 28(1), pp. 41–66. doi: 10.1016/j.marpol.2003.10.010.

SHM Group (2021) *Página Web SHM Group*. Available at: https://medium.com/@sayali02ii/7-technology-trends-that-are-shaping-the-shipping-industry-26b417a1bcfb.

Sonicwall (2021) *Página Web Sonicwall*. Available at: https://www.sonicwall.com/.

Tehran Times (2021) *Página Web Tehran Times*. Available at: https://www.tehrantimes.com/news/437368/IRISL-ranks-14th-among-world-s-top-100-shipping-lines.

The New Paper (2021) *Página Web The new paper*. Available at: https://www.tnp.sg/news/singapore/firm-fined-400k-over-oil-rig-incident.

Varios autores (2010) '" Memoria histórica " , Amenaza para la paz en Europa', *ECR Grupo*, p. 161.

Vesselfinder (2021) *Página Web Vesselfinder*. Available at: https://www.vesselfinder.com/es/vessels/WHITE-ROSE-OF-DRACHS-IMO-1008140-MMSI-235862000.

AVISO DE RESPONSABILIDAD

Este documento es el resultado del Trabajo Fin de Máster de un alumno, siendo su autor responsable de su contenido.

Se trata por tanto de un trabajo académico que puede contener errores detectados por el tribunal y que pueden no haber sido corregidos por el autor en la presente edición.

Debido a dicha orientación académica no debe hacerse un uso profesional de su contenido.

Este tipo de trabajos, junto con su defensa, pueden haber obtenido una nota que oscila entre cinco y 10 puntos, por lo que la calidad y el número de errores que puedan contener difieren en gran medida entre unos trabajos y otros.

La Universidad de Cantabria, la Escuela Técnica Superior de Náutica, los miembros del Tribunal de Trabajos Fin de Máster, así como el profesor/a director no son responsables del contenido último de este Trabajo.