Ciberseguridad en la Marina Mercante

Trabajo Fin de Grado
Grado en Ingeniería Radioelectrónica Naval
Julio de 2023

Autor:
Adrián Rodríguez Machado

Tutores:
Prof. Dr. José Agustín González Almeida
Dra. Amanda Peña Navarro

Escuela Politécnica Superior de Ingeniería
Sección Náutica, Máquinas y Radioelectrónica Naval
Universidad de La Laguna

D/Dª. José Agustín González Almeida, Profesor de la UD de Marina Civil, perteneciente al Departamento de Ingeniería Civil, Náutica y Marítima de la Universidad de La Laguna:

Expone que:

D. **Adrián Rodríguez Machado**, ha realizado bajo mi dirección el trabajo fin de grado titulado: **Ciberseguridad en la Marina Mercante**.

Revisado dicho trabajo, estimo reúne los requisitos para ser juzgado por el tribunal que sea designado para su lectura.

Para que conste y surta los efectos oportunos, expido y firmo el presente documento.

En Santa Cruz de Tenerife a 20 de julio de 2023.

Fdo.: José Agustín González Almeida.

Director del trabajo.

Rodríguez Machado, A. (2023). *Ciberseguridad en la Marina Mercante*. Trabajo de Fin de Grado. Universidad de La Laguna.

RESUMEN

Este trabajo de investigación se centra en el estudio de la ciberseguridad marítima, respaldado por la creciente cantidad de ataques reportados en los últimos años. Las investigaciones previas han revelado un aumento significativo en los casos de ataques y han destacado la falta de actualizaciones en los sistemas específicos de los buques, el uso de contraseñas por defecto y la insuficiente preparación de las tripulaciones para abordar estos problemas.

El objetivo general de este estudio es adquirir conocimientos en el campo de la ciberseguridad marítima y crear conciencia sobre esta problemática. Se exponen diversas técnicas utilizadas para comprometer la seguridad de los buques, junto con la falta de preparación de los marinos, quienes operan estos sistemas críticos. Los objetivos específicos de este trabajo incluyen la formación personal en ciberseguridad marítima y la posibilidad de continuar investigando en este campo para futuros estudios. En cuanto al texto, se busca presentar un trabajo que exponga los aspectos principales de los sistemas más relevantes.

El diseño de investigación utilizado se basa en una metodología de bola de nieve, comenzando con la búsqueda inicial de "ciberseguridad en la marina mercante" y desarrollando el tema a partir de ahí. Se han utilizado herramientas como el buscador académico de Google y se han consultado las publicaciones de las principales organizaciones internacionales de marina mercante, como la IMO. Los datos recopilados se analizaron mediante la comparación de diversas publicaciones relacionadas, con el objetivo de establecer puntos comunes y generar un texto claro que explique los aspectos principales de cada apartado. En relación con la legislación, se citan literalmente los artículos que regulan la ciberseguridad por parte de los diferentes organismos.

En conclusión, este trabajo bibliográfico sobre ciberseguridad marítima destaca la necesidad de abordar los desafíos existentes en la protección de los sistemas de la marina mercante. Resalta la importancia de la formación y la concienciación para mejorar la preparación de los marinos y garantizar la seguridad en la navegación marítima en el contexto de las amenazas cibernéticas actuales.

Palabras claves: [Hacking, ciberseguridad, piratas informáticos, marina mercante, IMO].

Rodríguez Machado, A. (2023). *Ciberseguridad en la Marina Mercante*. Trabajo de Fin de Grado. Universidad de La Laguna.

ABSTRACT

This university research paper focuses on the study of maritime cybersecurity, driven by the increasing number of reported attacks in recent years. Previous research has revealed a significant rise in attack cases and highlighted the lack of updates in specific ship systems, the use of default passwords, and the insufficient preparedness of crews to address these issues.

The overall objective of this study is to acquire knowledge in the field of maritime cybersecurity and raise awareness about this problem. Various techniques used to compromise the security of ships, coupled with the inadequate preparedness of seafarers who operate these critical systems, are explored. The specific objectives of this work include personal education in maritime cybersecurity and the possibility of further research in this field for future studies. Regarding the text, the aim is to present a comprehensive overview of the key aspects of the most relevant systems.

The research design employed follows a snowball methodology, starting with the initial search for "maritime cybersecurity" and developing the topic from there. Tools such as the academic search engine of Google and publications from major international maritime organizations like the IMO were utilized. Data collected was analyzed by comparing various related publications to establish commonalities and generate a clear text that explains the main points of each section. In terms of legislation, specific articles regulating cybersecurity from different organizations are cited verbatim.

In conclusion, this bibliographic work on maritime cybersecurity emphasizes the need to address the existing challenges in protecting merchant shipping systems. The importance of education and awareness is highlighted to enhance seafarers' preparedness and ensure safety in maritime navigation amidst current cyber threats.

Keywords: [Hacking, cibersafety, hackers, merchant marine, IMO].

AGRADECIMIENTOS

"Quiero expresar mi profundo agradecimiento a mi familia, a la Prof. Dr. Amanda Peña Navarro, al coordinador Prof. Dr. José Agustín González Almeida y a mis compañeros en los buques donde he navegado. Su apoyo y contribución han sido fundamentales para el éxito de este trabajo. Estoy sinceramente agradecido por su inestimable ayuda y guía."

Índice del TFG

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. Introducción

El avance de las tecnologías y la conectividad ha permitido una mayor interconexión en diversos dispositivos como smartphones, portátiles, relojes inteligentes y auriculares, que tienen la capacidad de reproducir, grabar y distribuir contenido multimedia. En el ámbito de la industria marítima, estos avances tecnológicos tienen un impacto significativo, ya que se pueden localizar buques con precisión mediante sistemas de posicionamiento como el GPS, y monitorear su estado, tripulantes, destinos, carga y velocidad. Además, los propios sistemas de los buques, como los sistemas SCADA y las centrales contra incendios, han sido modernizados para garantizar un control eficiente. Sin embargo, todos estos sistemas, que son ejecutados por ordenadores, son susceptibles de ser vulnerados, lo que da lugar al problema de la ciberseguridad.

La ciberseguridad se define como la práctica de proteger los sistemas críticos y la información sensible de los ataques digitales. Esto implica salvaguardar los sistemas y las aplicaciones en red contra amenazas tanto internas como externas. Los ataques cibernéticos pueden tener diversas formas, desde los clásicos ataques informáticos a los sistemas del Internet de las cosas (IoT), hasta ataques basados en ingeniería social.

El tema de la ciberseguridad en el sector marítimo es de gran relevancia, y es necesario analizarlo desde diferentes perspectivas. Se abordarán en profundidad los tipos de ataques y las formas de actuación de los atacantes. Sin embargo, antes de entrar en detalle, es fundamental examinar las publicaciones y regulaciones de organizaciones como la Organización Marítima Internacional (IMO) y otras entidades legislativas relacionadas con la marina mercante. Estas publicaciones y regulaciones buscan mitigar, mejorar y regular la ciberseguridad en la industria marítima.

2. Organizaciones y gobiernos. Sobre la ciberseguridad marítima.

Si se plantea qué conocimiento y previsión tiene y ha tenido la comunidad internacional marítima sobre los ciberataques y la ciberseguridad aplicada al sector marítimo, se puede observar que las leyes, regulaciones y códigos no han sido ni tan rápidos, ni tan efectivos como los atacantes.

2.1. IMO

Dentro del marco de estudio, es relevante mencionar la resolución "MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems (SMS)" (IMO Maritime Safety Committee, 2017), publicada por el Comité de Seguridad Marítima de la Organización Marítima Internacional (IMO) en junio de 2017, durante su nonagésima octava sesión. Esta resolución, de una página, insta a las administraciones a garantizar que los riesgos asociados a los ciberataques en la navegación sean abordados adecuadamente en los manuales de gestión de seguridad existentes, tal como se define en el Código Internacional de Gestión de la Seguridad Operacional del Buque y la Prevención de la Contaminación (IGS). Se estableció una fecha límite para la primera verificación anual del Documento de Conformidad de la empresa después del 1 de enero de 2021.

Estas resoluciones son aplicables al estudio que se está llevando a cabo y proporcionan una base importante para comprender y analizar la ciberseguridad en el sector marítimo.

2.1.1. Resolución “MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems (SMS)”.

La resolución MSC.428(98) destaca la importancia de la ciberseguridad en los sistemas informáticos, una preocupación expresada no solo por las administraciones, sino también por las sociedades de clasificación, fabricantes de equipos, armadores, proveedores de servicios y puertos. Estas entidades resaltan la necesidad de regular y capacitar a profesionales que puedan comprender estas amenazas y preparar al resto de los trabajadores y marinos para prevenir posibles ataques informáticos que puedan poner en riesgo la seguridad y la operatividad de los buques y los sistemas informáticos en puertos y buques.

La resolución MSC.428(98) también menciona la necesidad de realizar posibles modificaciones en la resolución "*A.741(18) Código internacional de gestión de la seguridad operacional del buque y la prevención de la contaminación (Código Internacional de Gestión de la Seguridad CGS)"* (Boletín Oficial del Estado, BOE, 1993). Esta resolución, adoptada por

la Asamblea de la IMO, estableció el uso del Código ISM (Código Internacional de Gestión de la Seguridad) el 4 de noviembre de 1993. Se plantea la necesidad de modificar este código para incluir la seguridad informática como consideración y cómo debe ser agregada en los manuales de gestión de las navieras.

En respuesta a estas preocupaciones, la IMO publicó el documento "*MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management*" (IMO, 2017), el 5 de julio de 2017. Este documento de seis páginas proporciona las primeras recomendaciones en ciberseguridad. Estas directrices se basan en una revisión anterior publicada el 1 de junio de 2016, titulada "*MSC.1/Circ.1526, Interim Guidelines On Maritime Cyber Risk Management*" (IMO, 2016), donde se comenzó a elaborar y estudiar estas directrices. Es importante destacar que esta última resolución ha reemplazado por completo a la resolución "MSC-FAL.1/Circ.3" mencionada al principio del párrafo.

2.1.2. Resolución “MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management”

La resolución "MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management" se divide en cuatro apartados.

En la introducción, se plantea la importancia de la ciberseguridad, las recomendaciones en materia de ciberseguridad, la seguridad a bordo y las responsabilidades de los armadores y navieros en relación con la digitalización de los buques y la flota.

El primer apartado, denominado "general", proporciona el contexto necesario para comprender la importancia de la ciberseguridad en la marina mercante y los campos de aplicación del documento. Este apartado se divide en dos subapartados. El primero, denominado "background", ofrece un primer acercamiento a los posibles sistemas que podrían verse comprometidos por un ciberataque, como los sistemas de gobierno, carga, propulsión, comunicaciones y seguridad de carga y pasajeros. También se mencionan aspectos como la distinción entre OT (Operation Technology) e IT (Information Technology), los perfiles de los atacantes, la gestión de ciberataques y las complicaciones asociadas con la actualización y la longevidad de los sistemas.

El segundo subapartado del apartado "general" se centra en las aplicaciones del documento y a qué industria va dirigido. Se destaca que el texto se enfoca en el sector marítimo, incluyendo puertos, buques y organismos gubernamentales relacionados con la marina mercante. Además, se enfatiza que la responsabilidad legislativa recae en los gobiernos donde el buque esté abanderado y en las sociedades de clasificación.

El siguiente apartado, "Elements of cyber risk management", presenta una lista de pasos a seguir en caso de ser objetivo de un ciberataque y el enfoque que se debe tomar. Se define la gestión de la ciberseguridad como el proceso de identificar, analizar, evaluar y comunicar un riesgo cibernético, y se mencionan los enfoques y el marco de gestión de riesgos para un ciberataque.

El último apartado, "best practices for implementation of cyber risk management", presenta guías elaboradas y publicadas por otras organizaciones, como "*The Guidelines on Cyber Security Onboard Ships*" (Baltic and International Maritime Council, BIMCO, 2020), publicada por BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF e IUMI, y el estándar "*ISO/IEC 27001*" (International Organization for Standardization, ISO, 2022) sobre sistemas de gestión de seguridad de la información publicado por ISO y IEC. Estas publicaciones ofrecen un enfoque más completo y técnico sobre la ciberseguridad.

En resumen, la resolución "MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management" plantea la importancia de la ciberseguridad en los buques y establece pautas iniciales desde la perspectiva de la IMO. Aunque el documento no profundiza en detalles técnicos, proporciona las bases para incorporar la ciberseguridad en los manuales de gestión de las navieras.

2.2. Europa

La ciberseguridad marítima es crítica en Europa debido a la creciente dependencia tecnológica en la industria marítima. La Comisión Europea ha establecido la Directiva NIS y el RGPD para abordar este problema. La EMSA ha publicado un marco de ciberseguridad marítima para mejorar la resiliencia cibernética. Otras iniciativas importantes incluyen la colaboración con la OTAN y el Fondo Europeo de Defensa. La Unión Europea trabaja activamente en la protección de sistemas y datos críticos en la industria marítima.

2.2.1. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, publicada el 6 de julio de 2016, establece medidas para garantizar un alto nivel de seguridad de las redes y sistemas de información en la Unión Europea. En el sector del transporte marítimo, se aplican requisitos de seguridad a todas las operaciones, incluyendo sistemas de radio,

telecomunicaciones, sistemas informáticos y redes. Los Estados miembros deben considerar los códigos y directrices internacionales existentes para identificar a los operadores marítimos de manera coherente. Esta directiva será reemplazada por la Directiva (UE) 2022/2555, que entrará en vigor el 18 de octubre de 2024 y busca garantizar un alto nivel común de ciberseguridad en toda la Unión Europea. . (El Parlamento Europeo y El Consejo de La Unión Europea, 2016, pág. L 194/2), (El Parlamento Europeo y El Consejo de La Unión Europea, 2016, pág. L 194/3), (Parlamento Europeo y El Consejo de La Unión Europea, 2022, pág. L 333/142 Artículo 44).

2.2.2. Directiva (UE) 2022/2555 del parlamento europeo y del consejo el 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)

La directiva establece los deberes de los Estados miembros en materia de ciberseguridad, incluyendo la gestión de datos, privacidad, sanciones por mal uso y el intercambio de información y asistencia en materia de ciberterrorismo y ciberseguridad entre los Estados miembros.

En el sector del transporte marítimo, se considera como un subsector de alta criticidad dentro del sector de transporte. La directiva obliga a las navieras, armadores y puertos a implementar políticas sólidas de tratamiento de datos para operar en los puertos europeos y garantizar la seguridad de la Unión Europea. A partir de un momento no especificado, las navieras deberán contar con un certificado de calidad en ciberseguridad y tratamiento de datos, como por ejemplo la certificación de Bureau Veritas en materia de ciberseguridad.

En general, esta directiva establece un marco para las políticas de ciberseguridad de los países miembros, estableciendo obligaciones tanto en infraestructuras como en políticas. Sin embargo, se deja la responsabilidad a los gobiernos de cada país para asegurar que el sector privado se prepare para cumplir con los requisitos de la directiva.

Tabla 1 "sección de la tabla del anexo 1 "Sectores de alta Criticidad", en el documento "directiva (UE) 2022/2555" (Parlamento Europeo y El Consejo de La Unión Europea, 2022, pág. Anexo I)

Sector	Subsector	Tipo de entidad
2. Transporte	a) Transporte aéreo	— Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.º 300/2008 utilizadas con fines comerciales
		— Entidades gestoras de aeropuertos, tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo ([6]); aeropuertos, tal como se definen en el artículo 2, punto 1, de dicha Directiva, en particular los aeropuertos de la red básica enumerados en el anexo II, sección 2, del Reglamento (UE) n.º 1315/2013 del Parlamento Europeo y del Consejo ([7]); y entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos
		— Operadores de control de la gestión del tráfico que prestan servicios de control del tránsito aéreo, tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.º 549/2004 del Parlamento Europeo y del Consejo ([8])
	b) Transporte por ferrocarril	— Administradores de infraestructuras, tal como se definen en el artículo 3, punto 2, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo ([9])
		— Empresas ferroviarias, tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio, tal como se definen en el artículo 3, punto 12 de dicha Directiva
	c) Transporte marítimo y fluvial	— Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo ([10]), sin incluir los buques particulares explotados por esas empresas
		— Organismos gestores de los puertos, tal como se definen en el artículo 3, punto 1, de la Directiva 2005/65/CE del Parlamento Europeo y del Consejo ([11]), incluidas sus instalaciones portuarias, tal como se definen en el artículo 2, punto 11, del Reglamento (CE) n.º 725/2004, y entidades que operan obras y equipos que se encuentran en los puertos
		— Operadores de servicios de tráfico de buques (STB), tal como se definen en el artículo 3, letra o), de la Directiva 2002/59/CE del Parlamento Europeo y del Consejo ([12])
	d) Transporte por carretera	— Autoridades viarias, tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión ([13]) responsables del control de la gestión del tráfico, excluidas las entidades públicas para las cuales la gestión del tráfico o la explotación de sistemas de transporte inteligentes sea una parte no esencial de su actividad general
		— Operadores de sistemas de transporte inteligentes, tal como se definen en el artículo 4, punto 1, de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo ([14])

2.3. Ciberseguridad en España.

El 5 de diciembre de 2013 el Consejo de Seguridad Nacional aprobó la Estrategia de Ciberseguridad Nacional, junto con la Estrategia de seguridad Marítima. Ambos documentos confieren el fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional a futuro en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas.

De estos documentos nacen, o se reforman, diversos organismos nacionales con el fin de, o bien proteger el ciberespacio nacional tanto privado como público, la ciberdefensa del estado o la formación y consultoría de nuevos profesionales.

2.3.1. Documento de Estrategia de ciberseguridad Nacional de 2013.

El documento emitido desde la presidencia del gobierno se define como "*el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas*" (Presidencia del Gobierno, Gobierno de España, 2013, pág. 3).

El documento se compone de 5 capítulos:

El primero, “Ciberespacio y su seguridad” define el ciberespacio como un sitio global y dinámico compuesto por las infraestructuras TIC. También las características de los ciberataques comunes, su bajo coste, la ubicuidad y fácil ejecución, su efectividad e impacto, y el reducido riesgo para el atacante. Además, identifica como riesgos y amenazas un amplio espectro proveniente de: individuos aislados, hacktivistas, amenazas internas, delincuentes, terroristas, estados extranjeros que se suman a los problemas causados por causas técnicas o fenómenos naturales.

El segundo capítulo, “Propósito y principios rectores de la ciberseguridad en España” presenta la hoja de ruta del estado español en materia de ciberseguridad integrando a las administraciones públicas, sector privado y los ciudadanos todo esto bajo cuatro principios rectores: el liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional.

El tercer capítulo “Objetivos de la ciberseguridad”, define un objetivo global y seis objetivos específicos. Este primer objetivo de “*lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques*” (Presidencia del Gobierno, Gobierno de España, 2013, pág. 21) los otros 6 objetivos de refieren a:

Tabla 2 "Objetivos especificos de la ciberseguridad" (Instituto Español de Estudios Estratégicos, IEEE, 2013, pág. 6 tabla nº1)

Ámbito	Objetivo
Administraciones Públicas	garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por éstas poseen el adecuado nivel de seguridad y resiliencia
Empresas e infraestructuras críticas	impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular
Ámbito judicial y policial	potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio
Sensibilización	concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio

Capacitación	alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad
Colaboración internacional	contribuir a la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo

El cuarto capítulo "Líneas de acción de la ciberseguridad Nacional", se centra en definir las líneas de actuación que deben tomarse para alcanzar los objetivos señalados en el anterior capítulo.

El quinto y último capítulo," la ciberseguridad en el Sistema de Seguridad Nacional", establece la estructura de los diferentes organismos a cargo de la ciberseguridad nacional los cuales deben dar una respuesta conjunta y adecuada para preservar la ciberseguridad.

Esta estructura se compone de 3 partes bajo la dirección del presidente del Gobierno: a) el Consejo de Seguridad Nacional; b) el Comité Especializado de Ciberseguridad; c) el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

En resumen, este documento articula la defensa de la ciberseguridad en España, presentando una hoja de ruta y generando nuevos comités especializados en la ciberseguridad.

2.3.2. Documento de Estrategia de Seguridad Marítima Nacional de 2013 aplicado a la marina mercante.

"*La Estrategia de Seguridad Marítima Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2013 y las adapta a las exigencias especiales del ámbito marítimo, en línea con otros instrumentos estratégicos en el ámbito internacional*" (Presidencia del Gobierno, Gobierno de España, 2013, pág. 3).

El Documento de Estrategia de Seguridad Marítima Nacional de 2013 aborda la ciberseguridad como un desafío en el ámbito marítimo. Reconoce que el uso cada vez más extendido de las tecnologías de la información y comunicaciones (TIC) en el sector marítimo aumenta la probabilidad de ciberataques contra elementos esenciales para sus operaciones. (Presidencia del Gobierno, Gobierno de España, 2013, pág. 28)

El documento establece una serie de acciones para mejorar la ciberseguridad en el sector marítimo nacional:

- Establecimiento de actuaciones concretas en el marco de la ciberseguridad para mejorar los estándares de seguridad marítima.
- Adopción de un enfoque integral de la ciberseguridad, incluyendo la evaluación de riesgos y amenazas cibernéticas específicas para el ámbito marítimo y la identificación de activos críticos del sector.
- Apoyo a acciones dirigidas a prevenir, defender, detectar, analizar, recuperar y responder coordinadamente a las ciberamenazas en el espacio marítimo, con el objetivo de limitar los efectos negativos de un ciberataque.
- Incorporación de aspectos de seguridad cibernética en las redes de telecomunicaciones y sistemas de información marítima, así como el desarrollo y aplicación de tecnologías específicas para fortalecer las estructuras de seguridad, la capacidad de vigilancia, prevención y respuesta en dichos sistemas.
- Fomento del intercambio de información, la cooperación y la colaboración público-privada tanto a nivel nacional como internacional, junto con el desarrollo de estándares y mejores prácticas en ciberseguridad en el ámbito marítimo.
- Creación de un marco de conocimientos específicos sobre ciberseguridad dirigido a los profesionales del ámbito marítimo, así como acciones de concienciación y sensibilización en este campo. (Presidencia del Gobierno, Gobierno de España, 2013, pág. 40)

En resumen, el documento destaca la necesidad de abordar la ciberseguridad de manera específica en el sector marítimo, involucrando la preparación del personal, la legislación internacional, el compromiso del sector privado y el intercambio de información y colaboración entre los países y partes interesadas.

2.3.3. Plan Nacional de Ciberseguridad Español.

El Plan Nacional de Ciberseguridad de España es una herramienta integral que aborda la protección de sistemas y redes informáticas en diversos sectores, incluido el marítimo. Para garantizar la ciberseguridad en el ámbito marítimo, se establecen medidas específicas para proteger los sistemas y redes informáticas de los buques, puertos y terminales marítimos. (Bolentín Oficial del Estado, BOE, 2015). (Ministerio de la presidencia, relaciones con las cortes y memoria democrática., 2022)

“La Ley de Seguridad Nacional tiene por objeto regular los principios básicos, órganos superiores y autoridades y los componentes fundamentales de la Seguridad Nacional; el

Sistema de Seguridad Nacional, su dirección, organización y coordinación; la gestión de crisis y la contribución de recursos a la Seguridad Nacional". (Departamento de Seguridad Nacional Española, s.f.)

Estas medidas incluyen la identificación y evaluación de riesgos cibernéticos, la protección de sistemas y redes, la implementación de sistemas de monitorización y detección de amenazas, la formación especializada del personal, la elaboración de planes de contingencia y la promoción de la cooperación y colaboración entre las diferentes autoridades y empresas del sector.

El objetivo principal es prevenir posibles ciberataques que puedan comprometer la seguridad marítima, la navegación, el comercio internacional y la protección medioambiental. Al fortalecer la ciberseguridad en el ámbito marítimo, se busca garantizar la integridad y disponibilidad de los sistemas y redes informáticas, así como la protección de la información sensible y crítica.

Además, el plan promueve la concienciación y educación en ciberseguridad, tanto para el personal involucrado en el sector marítimo como para los usuarios y el personal a bordo de los buques. Se busca fomentar las mejores prácticas de seguridad y garantizar que todos los actores relevantes estén preparados y capacitados para hacer frente a posibles incidentes de ciberseguridad.

En resumen, el Plan Nacional de Ciberseguridad de España aborda específicamente la ciberseguridad en el ámbito marítimo, estableciendo medidas y estrategias para proteger los sistemas y redes informáticas de los buques, puertos y terminales marítimos, así como promoviendo la concienciación y colaboración entre los diferentes actores involucrados en el sector marítimo.

2.3.4. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información se promulgó en respuesta a la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, que busca establecer un alto nivel común de ciberseguridad entre los países miembros de la Unión Europea. Este real decreto tiene como objetivo regular la seguridad de las redes y sistemas de información utilizados para la provisión de servicios esenciales y servicios digitales, así como establecer un sistema de notificación de incidentes. (Boletín Oficial del Estado, BOE, 2018, pág. 7)

El ámbito de aplicación de esta normativa abarca tanto al sector público como al privado, y establece obligaciones para los prestadores de servicios digitales, proveedores de servicios de confianza y operadores de infraestructuras críticas. Algunas de las medidas establecidas en este real decreto son las siguientes:

- Creación de un Centro de Respuesta a Incidentes de Seguridad de la Información de la Administración General del Estado (CERT): Este centro tiene la responsabilidad de coordinar la respuesta a los incidentes de seguridad informática a nivel estatal.
- Obligación de notificación de incidentes: Los prestadores de servicios digitales deben informar a las autoridades competentes sobre cualquier incidente de seguridad que afecte a la confidencialidad, integridad o disponibilidad de los servicios que prestan.
- Marco de certificación para proveedores de servicios de confianza: Se establece un marco de certificación que garantiza la seguridad y confiabilidad de los proveedores de servicios de confianza.
- Medidas de seguridad para operadores de infraestructuras críticas: Los operadores de infraestructuras críticas deben adoptar medidas de seguridad específicas para proteger su infraestructura y garantizar la continuidad de los servicios esenciales que prestan.
- Marco de cooperación y colaboración: Se crea un marco de cooperación y colaboración entre las diferentes autoridades competentes en materia de seguridad de la información.

En resumen, este real decreto tiene como objetivo principal garantizar la seguridad de las redes y sistemas de información utilizados en la prestación de servicios esenciales y digitales, así como proteger la información que circula a través de ellos. Estas medidas son fundamentales para el correcto funcionamiento de la economía y la sociedad en la actualidad, y se enmarcan en los esfuerzos de la Unión Europea por establecer un alto nivel de ciberseguridad en todos sus países miembros.

2.3.5. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

El Real Decreto 43/2021, de 26 de enero, tiene como objetivo principal desarrollar y complementar el marco normativo establecido por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Este nuevo decreto establece medidas adicionales para fortalecer la seguridad de las redes y sistemas de información utilizados en la prestación de servicios digitales, así como la protección de la

información que se transmite a través de ellos. (Boletín Oficial del Estado, BOE, 2021, pág. 8189 Sec. I.)

Entre las principales medidas establecidas en el Real Decreto 43/2021 se incluyen:

- Criterios y requisitos para la certificación de proveedores de servicios de confianza: Se definen los criterios y requisitos que deben cumplir los proveedores de servicios de confianza para obtener la certificación que garantice su seguridad y fiabilidad.
- Responsable de seguridad de la información: Los prestadores de servicios digitales tienen la obligación de designar a una persona responsable de la seguridad de la información.
- Sistema de notificación de incidentes de seguridad informática: Se establece un sistema que permite la rápida y eficaz comunicación de los incidentes de seguridad entre los prestadores de servicios digitales y las autoridades competentes.
- Catálogo de infraestructuras críticas: Se crea un catálogo que identifica las infraestructuras críticas que deben ser protegidas mediante medidas específicas de seguridad.
- Evaluaciones periódicas y planes de contingencia: Los operadores de infraestructuras críticas tienen la obligación de realizar evaluaciones periódicas de la seguridad de su infraestructura y elaborar planes de contingencia para hacer frente a posibles incidentes.
- Registro de incidentes de seguridad informática: Se establece un registro que permite llevar un registro de los incidentes de seguridad ocurridos, facilitando su análisis para mejorar la prevención y respuesta ante futuros incidentes.

En resumen, el Real Decreto 43/2021 complementa y desarrolla el marco normativo establecido por el Real Decreto-ley 12/2018. Su objetivo es fortalecer la seguridad de las redes y sistemas de información en España, estableciendo medidas adicionales para garantizar la fiabilidad y protección de la información. Aunque no hace referencia explícita al sector marítimo, los operadores en este ámbito deben tener en cuenta las medidas de seguridad establecidas en ambos decretos para proteger sus sistemas de información y la información que se transmite a través de ellos.

2.3.6. Equipos de respuesta a incidentes de seguridad informática del estado español.

Actualmente se encuentran 3 centros de respuesta en el panorama nacional.

- CCN-CERT, del Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia (CNI), para el ámbito del sector público y de la Administración pública.
- ESPDEF-CERT, del Mando Conjunto del Ciberespacio, para el ámbito de Defensa.
- INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, para el resto de los casos, fundamentalmente para el ámbito empresarial privado.

2.3.7. Legislación marítima aplicada a la Marina Mercante al amparo del estado español.

En el ámbito de la Marina Mercante, como operador de servicios esenciales, se aplican una serie de requerimientos y obligaciones de seguridad en cumplimiento de la legislación marítima amparada por el estado español. A partir de enero de 2021, estas entidades deben aprobar políticas de seguridad de redes y sistemas de información que contemplen los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, políticas de recuperación, pentesting, reevaluación periódica y la segregación de tareas.

Las políticas de seguridad abarcan diferentes aspectos, que incluyen, al menos, los siguientes ítems:

- Análisis y gestión de riesgos.
- Gestión de riesgos de terceros o proveedores.
- Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
- Gestión del personal y profesionalidad.
- Adquisición de productos o servicios de seguridad.
- Detección y gestión de incidentes.
- Planes de recuperación y aseguramiento de la continuidad de las operaciones.
- Mejora continua.
- Interconexión de sistemas.
- Registro de la actividad de los usuarios.

Estas medidas adoptadas se formalizan en un documento llamado "Declaración de aplicabilidad de medidas de seguridad" que es suscrito por el responsable de seguridad de la información designado y se incluye en la política de seguridad aprobada por la dirección de la organización. (Pereira, 2022, págs. 260, 261)

En cuanto a la declaración de aplicabilidad, conocida como Statement of Applicability (SoA) en inglés, es el documento que establece la relación de medidas de seguridad aplicables al sistema de información correspondiente, de acuerdo con su categoría, y que se encuentran recogidas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, que lo regula. (Centro Criptológico Nacional, CCN, 2023)

En resumen, tanto la Organización Marítima Internacional (IMO), el Parlamento Europeo como los propios estados están legislando para establecer altos estándares de seguridad en el sector marítimo. El objetivo es proporcionar un marco garantista tanto para el sector público como privado, asegurando una correcta gestión de los datos y, en caso de accidentes o ataques, garantizando una respuesta conjunta a través de las autoridades en la lucha contra los ciberdelitos o el ciberterrorismo. Esto ofrece a las empresas un marco de acción para la gestión de su ciberespacio.

3. Hacking.

La digitalización, integración y automatización en el transporte marítimo han creado amenazas y vulnerabilidades que deben abordarse. Los sistemas críticos y vulnerables incluyen el puente de mando, la gestión de carga, la propulsión y el control de acceso. Es necesario proteger los sistemas técnicos y de información para evitar riesgos en el transporte marítimo. Las amenazas cibernéticas seguirán aumentando, por lo que es importante tomar medidas para proteger los sistemas y procedimientos críticos.

3.1. Breve historia del hacking.

"Hacker: Persona que se deleita en tener un conocimiento íntimo del funcionamiento interno de un sistema, ordenador o red de ordenadores en particular. El término es mal empleado usualmente en un contexto peyorativo, donde "Cracker" sería el término correcto" (RFC Series (ISSN 2070-1721), 1996, pág. 23).

Podemos definir a un Hacker como un investigador, un individuo que estudia y explora los límites de una tecnología con el afán de evolucionar esa tecnología, descubrir nuevas funciones o errores del sistema, con el fin del mero conocimiento o el reconocimiento académico.

La historia del hacking se remonta a principios del siglo XX, cuando el inventor Gugliermo Marconi fue interceptado por el mago Nevil Maskelyne durante un experimento con telégrafos inalámbricos. Aunque Marconi denunció a Maskelyne por interferir en su comunicación, el mago logró exponer las vulnerabilidades del sistema y contribuyó al avance de la tecnología al obligar a tomar medidas de seguridad. (Hipertextual, 2011) Otros ejemplos destacados de hackers incluyen a los científicos que descifraron el código de la máquina Enigma utilizada por los nazis durante la Segunda Guerra Mundial. (Karpersky daily, 2015). Estos hackers desempeñaron un papel fundamental en el desarrollo tecnológico al buscar los límites y fallos de los sistemas. Sin embargo, es importante destacar que algunos hackers actúan de manera ilegal con el fin de obtener beneficios económicos o realizar actividades ilícitas. Aunque estas acciones son condenables, existe una distinción entre los hackers que notifican los errores y contribuyen a mejorar la seguridad y aquellos que los explotan de manera perjudicial. El descubrimiento de vulnerabilidades y su divulgación responsable son necesarios para el avance de la tecnología y la protección de los datos.

3.1.1. Breve historia del Hacking en la Marina mercante.

La historia del hacking en la marina mercante es relativamente corta debido al uso reciente de tecnología informática en el sector. Sin embargo, ha habido casos significativos de ciberataques en los últimos años. En la década de 1990, se produjo uno de los primeros ciberataques conocidos en la industria marítima cuando el grupo de hackers "Los Piratas del Mar Egeo" accedió al sistema informático de la naviera griega Piraeus, intentando extorsionar a la compañía. En la década de 2000, los ciberataques se volvieron más sofisticados y frecuentes. Por ejemplo, en 2001, el virus "Nimda" afectó los sistemas de la naviera Maersk, causando interrupciones y pérdida de datos. (TechTarget Security, 2021) En 2007, el ataque informático contra Estonia afectó la capacidad del país para coordinar operaciones portuarias (BBC news, 2017). En 2017, el ransomware NotPetya impactó a la naviera Maersk, causando daños económicos significativos y perturbando sus operaciones. Estos incidentes han llevado a la industria marítima a tomar medidas para mejorar su seguridad informática y protegerse de futuros ciberataques. En el trabajo, "*A Retrospective Analysis of Maritime Cyber Security Incidents*" (P.H. Meland, K. Bernsmed, E. Wille, Ø.J. Rødseth, & D.A. Nesheim, 2021) se registran 46 ataques informáticos a la industria marítima, desde el 2010 hasta el 2020.

3.2. Ataques informáticos. Definiciones y alcance

Los sistemas informáticos y de control en los buques son cruciales para su operatividad, pero también representan desafíos significativos. Además de los problemas mecánicos, climáticos y errores humanos, los fallos en los ordenadores y sistemas informáticos son una preocupación importante para la tripulación. En algunos casos, estos fallos pueden dejar inutilizados buques de gran tamaño.

La salud de los sistemas de control es un factor de riesgo adicional para los buques, junto con la corrosión, las vibraciones y el desgaste. Las actualizaciones, contraseñas y el control de acceso de los sistemas informáticos, como los sistemas de gestión, los ordenadores convencionales, los sistemas de control, los PLC (Controladores Lógicos Programables) y los sistemas SCADA, son aspectos críticos a tener en cuenta.

Tradicionalmente, los ordenadores asociados a los sistemas de control se encontraban en una red privada local, limitando su comunicación a otros dispositivos y al exterior, excepto en casos de mantenimiento programado donde la conexión se realizaba de manera local. Sin embargo, en los buques más modernos, esta configuración ha cambiado. Algunos buques cuentan con sistemas de asistencia remota en sus motores principales, lo que permite a los operarios de la marca constructora del motor monitorizar y modificar los parámetros desde cualquier parte del mundo.

Estos sistemas interconectados se agrupan en diferentes categorías, que se detallarán en el siguiente subapartado.

3.2.1. Definiciones de los conjuntos de sistemas principales.

La diferencia entre los sistemas de IT y OT en el ámbito marítimo es similar a otros campos. Los sistemas de IT se centran en la comunicación, navegación, seguridad cibernética, gestión de la tripulación y sistemas de información de gestión empresarial. Por otro lado, los sistemas de OT se ocupan de la producción y operación a bordo, como el control del motor, la gestión de la energía, la navegación y la estabilidad del buque.

La interconexión entre los sistemas de IT y OT en un buque se está volviendo más común para mejorar la eficiencia operativa, pero también presenta desafíos de seguridad y gestión de riesgos. Es importante tener en cuenta que los sistemas de OT tienen requisitos específicos de seguridad, confiabilidad y resistencia que a menudo difieren de los requisitos de IT.

En cuanto a los ataques cibernéticos, la mayoría se dirigen hacia los sistemas de IT, como el robo de datos o los ataques de denegación de servicio, ya que son más fáciles de realizar y monetizar. Sin embargo, los sistemas de OT son objetivos de alto nivel y suelen estar relacionados con terrorismo o ciberguerra, ya que controlan las operaciones y maquinaria industriales.

Un ejemplo destacado de un ataque a los sistemas de OT es el virus Stuxnet, que afectó a la maquinaria iraní utilizada en el programa nuclear del país. Este malware destruyó o alteró los valores de las centrifugadoras de uranio, retrasando significativamente el proyecto nuclear iraní. (Kaspersky Daily , 2014)

En el ámbito marítimo, el accidente del buque Ever Given en el canal de Suez también plantea la posibilidad de un ataque a los sistemas de OT. Aunque aún no se ha proporcionado un informe completo del incidente, algunos análisis sugieren que podría haber habido anomalías en el sistema de navegación que comprometieron la ruta del buque. (Safety4Sea, 2021)

En resumen, la diferenciación entre los sistemas de IT y OT en el ámbito marítimo es relevante para comprender los diferentes enfoques y desafíos asociados a cada uno. Los sistemas de OT en el sector marítimo pueden ser objetivos de alto nivel en ataques cibernéticos y su seguridad es fundamental para garantizar la operación segura y eficiente de los buques.

3.2.2. Amplitud o intencionalidad de los ciberataques.

Es correcto distinguir entre ataques no dirigidos y ataques dirigidos en el ámbito de la ciberseguridad. Los ataques no dirigidos son más comunes y se llevan a cabo sin un objetivo específico, buscando vulnerabilidades en sistemas y redes para explotarlas. Estos ataques suelen ser menos sofisticados y pueden afectar a una amplia gama de usuarios, dispositivos o empresas en la industria marítima.

Por otro lado, los ataques dirigidos son más selectivos y están diseñados para atacar a un individuo, colectivo o entidad específica. Estos ataques suelen ser más sofisticados y pueden involucrar técnicas de ingeniería social y múltiples etapas para lograr su objetivo. En el ámbito marítimo, estos ataques podrían dirigirse a una compañía naviera en particular, un buque específico o una operación específica.

Es importante reconocer que los ataques dirigidos pueden representar un mayor peligro y tener consecuencias más graves para la seguridad y la operación de los sistemas marítimos. Por lo tanto, es esencial que las empresas marítimas implementen medidas de seguridad cibernética adecuadas para protegerse contra ambos tipos de ataques.

Algunas de estas medidas pueden incluir la implementación de firewalls para proteger las redes, sistemas de detección de intrusiones para identificar actividad sospechosa, actualizaciones regulares de software y sistemas de seguridad, y la capacitación de la tripulación en prácticas de seguridad cibernética para estar alerta ante posibles ataques.

Es fundamental estar preparados y tomar medidas proactivas para proteger los sistemas y datos en el entorno marítimo, ya que los ciberataques pueden tener impactos significativos en la seguridad, operatividad y reputación de las empresas y buques involucrados.

3.3. Definiciones y perfiles de los atacantes

Existen varios perfiles de ciberatacantes con diferentes motivaciones y niveles de habilidad. Algunos de los perfiles comunes son los hacktivistas, ciberdelincuentes, espías cibernéticos, hackers éticos, script kiddies y hackers patrocinados por el estado.

Los hacktivistas buscan promover causas políticas o sociales a través de ataques cibernéticos, mientras que los ciberdelincuentes buscan obtener ganancias financieras. Los espías cibernéticos recopilan información para agencias gubernamentales, los hackers éticos trabajan para mejorar la seguridad, los script-kiddies son aficionados con habilidades limitadas y los hackers patrocinados por el estado realizan ataques en nombre de gobiernos. Es importante comprender estos perfiles para prevenir y mitigar los ciberataques.

3.4. Técnicas y ataques más comunes.

Dentro del mundo hacking se emplean diversas herramientas con el fin de aprovechar las vulnerabilidades de los sistemas, ya sea de los propios dispositivos como de los operadores de estos sistemas.

3.4.1. Malware, Software malicioso.

El malware, o software malicioso, es un término general que engloba diferentes tipos de software diseñados para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario.

- Ransomware: Es un tipo de malware que restringe el acceso a archivos o sistemas y exige el pago de un rescate para restaurar el acceso. Se propaga a través de correos electrónicos de phishing, descargas de software malicioso o vulnerabilidades de seguridad.
- Fileless Malware: Es un tipo de malware que no deja rastros en el sistema de archivos y reside en la memoria del sistema. Se propaga a través de correos electrónicos de phishing, descargas de software malicioso o vulnerabilidades de seguridad.
- Spyware: Es un tipo de malware diseñado para recopilar información personal o confidencial sin el conocimiento o consentimiento del usuario. Se instala a través de descargas de programas gratuitos o mediante la apertura de correos electrónicos o enlaces infectados.
- Adware: Es un software que muestra anuncios no deseados en dispositivos con el objetivo de generar ingresos para sus creadores. Se instala a través de descargas de programas gratuitos o mediante la apertura de correos electrónicos o enlaces infectados.
- Troyanos: También conocidos como "caballos de Troya", son programas maliciosos que se disfrazan como software legítimo para engañar al usuario y obtener acceso no autorizado al sistema. Se propagan a través de archivos adjuntos de correo electrónico o enlaces de descarga.
- Gusanos: Son programas maliciosos que se propagan automáticamente a través de redes de computadoras aprovechando vulnerabilidades en el sistema operativo o aplicaciones instaladas. No requieren la interacción del usuario para replicarse.
- Rootkits: Son conjuntos de software diseñados para ocultar la presencia de otros programas maliciosos en un sistema. Permiten el acceso no autorizado y persistente al sistema, proporcionando control remoto al atacante.

- Malware móvil: Es aquel diseñado para infectar dispositivos móviles, como smartphones o tabletas. Realiza actividades maliciosas como robo de información, acceso a cuentas bancarias y descarga de más malware.
- Exploits: Son técnicas o códigos maliciosos que aprovechan vulnerabilidades en el software o sistema operativo para ejecutar código no autorizado en un sistema informático.
- Scareware: Es una técnica que intenta asustar a los usuarios para que compren software o servicios de seguridad falsos o innecesarios. Se presenta como un programa de seguridad legítimo que detecta amenazas inexistentes.
- Keyloggers: Son programas o hardware que registran y monitorean todas las pulsaciones de teclas en un teclado. Pueden ser utilizados de manera legítima o malintencionada para robar información confidencial como contraseñas y datos personales.

Estos diferentes tipos de malware se propagan a través de diferentes medios, como correos electrónicos de phishing, descargas de software malicioso, enlaces infectados o aprovechando vulnerabilidades en sistemas operativos y programas. Para protegerse, es importante tener precaución al descargar archivos o hacer clic en enlaces, instalar software solo desde fuentes confiables y mantener los sistemas actualizados con las últimas actualizaciones de seguridad.

3.4.2. Ataques de denegación de servicio, DoS y DDoS

Los ataques DoS (Denegación de Servicio) y DDoS (Denegación de Servicio Distribuida) funcionan de manera similar, pero difieren en la forma en que se generan y distribuyen los ataques. En ambos casos, el objetivo es abrumar un servidor o red con tráfico malicioso, lo que resulta en la interrupción del servicio para los usuarios legítimos.

- En un ataque DoS, un solo dispositivo, como una computadora o un servidor, envía una gran cantidad de tráfico a una dirección IP específica, sobrecargando el servidor o la red y dejando fuera de servicio el servicio en cuestión. Los atacantes suelen utilizar técnicas como el envío de paquetes mal formados o paquetes de gran tamaño, o inundar el servidor con solicitudes que parecen legítimas pero que en realidad son falsas.
- En un ataque DDoS, en cambio, se utilizan múltiples dispositivos, a menudo comprometidos y controlados por un atacante, para enviar tráfico simultáneamente a

una dirección IP específica, sobrecargando el servidor o red. Los atacantes pueden utilizar botnets, que son redes de dispositivos comprometidos que son controlados a distancia para llevar a cabo el ataque.

La principal diferencia entre un ataque DoS y un ataque DDoS es que en el primero, un solo dispositivo está generando tráfico malicioso, mientras que, en el segundo, múltiples dispositivos trabajan juntos para sobrecargar el servicio o red objetivo.

En general, los ataques DoS y DDoS pueden ser difíciles de detectar y prevenir, ya que los atacantes pueden utilizar una amplia variedad de técnicas y herramientas para generar tráfico malicioso.

3.4.3. Phishing, suplantación de la identidad.

El phishing es un ataque informático que tiene como objetivo engañar a los usuarios para obtener información personal o confidencial. Los atacantes utilizan diversos métodos para lograr esto, como el envío de correos electrónicos falsos o la creación de sitios web falsos que se asemejan a los legítimos.

- El spear phishing es una variante del phishing que se dirige a individuos o grupos específicos. Los atacantes realizan una investigación exhaustiva sobre sus objetivos y envían correos electrónicos o mensajes personalizados que parecen provenir de fuentes confiables. Estos mensajes suelen contener información personalizada para hacerlos más convincentes, como nombres de colegas o detalles de proyectos en los que están involucrados.
- El whaling es una forma más sofisticada de phishing que se dirige a altos ejecutivos y líderes de empresas. Los atacantes realizan investigaciones detalladas para crear mensajes altamente personalizados y convincentes que parecen provenir de fuentes confiables. Estos mensajes a menudo incluyen información confidencial sobre la empresa o el objetivo y pueden solicitar acciones como transferir fondos o proporcionar información de inicio de sesión.
- El SMiShing es un tipo de ataque de phishing que utiliza mensajes de texto en lugar de correos electrónicos. Los mensajes de texto parecen provenir de fuentes legítimas y a menudo incluyen enlaces maliciosos o números de teléfono que los destinatarios deben llamar para proporcionar información. Los atacantes utilizan técnicas de ingeniería social para hacer que los mensajes sean urgentes y persuadir a las víctimas a tomar medidas rápidas.

- El vishing es un ataque de phishing que se realiza a través de llamadas telefónicas. Los atacantes se hacen pasar por empresas legítimas y solicitan información personal o financiera durante la llamada. Pueden utilizar tecnología de manipulación de identidad de llamadas para hacer que la llamada parezca provenir de una fuente confiable y pueden utilizar tácticas de miedo o coerción para persuadir a las víctimas.

Estos ataques de phishing son efectivos porque a menudo parecen legítimos y se hacen pasar por empresas o servicios confiables. Los usuarios deben estar atentos y tomar precauciones, como verificar la autenticidad de los correos electrónicos y mensajes, evitar hacer clic en enlaces sospechosos o proporcionar información confidencial a través de llamadas telefónicas o mensajes de texto no verificados. Además, las organizaciones deben educar a sus empleados sobre estos ataques e implementar medidas de seguridad, como filtros de correo electrónico y autenticación de dos factores, para protegerse contra el phishing.

3.4.4. Spoofing

El Spoofing es un tipo de ataque informático en el que se falsifica o suplanta la identidad de un remitente o un dispositivo con el objetivo de engañar a la víctima haciéndole creer que la información es legítima. Este tipo de ataque se utiliza en diferentes escenarios, como phishing, spam, fraude y ataques de denegación de servicio distribuido (DDoS).

En el Spoofing, los atacantes pueden falsificar información como direcciones IP, nombres de dominio, números de teléfono, direcciones de correo electrónico o identificadores de sesión para hacer que el receptor crea que la información proviene de una fuente confiable. Por ejemplo, un atacante puede suplantar la dirección de correo electrónico de una persona conocida y enviar un correo electrónico con un enlace malicioso o un archivo adjunto infectado.

El Spoofing también se utiliza en ataques de phishing, donde los atacantes engañan a los usuarios haciéndoles creer que están interactuando con un sitio web o servicio legítimo. En este caso, los atacantes falsifican la dirección del sitio web para que parezca la legítima, lo que lleva a los usuarios a ingresar información personal o financiera confidencial.

Existen diferentes formas de Spoofing, entre las más comunes se encuentran:

- Domain Spoofing: En este caso, se utiliza un dominio o página web falsa para engañar a los usuarios y hacerles creer que están interactuando con un sitio web legítimo.

- Email Spoofing: Se envían correos electrónicos suplantando la identidad corporativa o personal de una persona o entidad. Los atacantes falsifican la dirección de correo electrónico para que parezca provenir de una fuente confiable y persuadir a los destinatarios a realizar acciones no deseadas.
- ARP Spoofing: Es un tipo de Spoofing que se utiliza para interceptar el tráfico de red en una red local. Los atacantes falsifican las respuestas ARP (Protocolo de Resolución de Direcciones) para hacer que un dispositivo crea que la dirección MAC del atacante es la dirección MAC de otro dispositivo en la red. Esto les permite interceptar y modificar el tráfico de red, lo que puede incluir información confidencial como contraseñas y datos financieros.
- El ARP Spoofing, también conocido como "envenenamiento ARP", es comúnmente utilizado por los atacantes en redes locales no seguras. Para protegerse contra este tipo de Spoofing, se pueden utilizar herramientas como ARPWatch, que alertan a los usuarios cuando se detectan respuestas ARP falsificadas. Es importante estar atento a los posibles indicios de Spoofing y tomar medidas para protegerse contra estos ataques, como verificar la autenticidad de los sitios web y correos electrónicos, y utilizar técnicas de autenticación seguras.

3.4.5. Identity-Based Attacks

Los ataques de identidad, también conocidos como "Identity-Based Attacks", se enfocan en comprometer la identidad de un usuario legítimo para obtener acceso no autorizado a sistemas y datos. Estos ataques pueden llevarse a cabo mediante ingeniería social, suplantación de identidad, phishing, malware y otras técnicas.

Algunos de los ataques de identidad más comunes son:

- Kerberoasting: Este ataque se aprovecha de una debilidad en el protocolo de autenticación de Kerberos en Windows para extraer las credenciales de usuario de un servidor de Active Directory. Luego, el atacante utiliza esas credenciales para acceder a otros recursos de la red.
- Man-in-the-Middle (MITM) attack: En este tipo de ataque, un atacante intercepta y manipula la comunicación entre dos partes que creen estar comunicándose directamente. El atacante puede ver, modificar o suplantar los datos transmitidos y robar información confidencial.

- Silver Ticket Attack: Este ataque explota una debilidad en el protocolo de autenticación de Kerberos para generar un ticket de servicio "Silver Ticket" que proporciona acceso no autorizado a otros recursos en la red.
- Credential Stuffing: En este ataque, un atacante utiliza combinaciones de nombres de usuario y contraseñas robadas de un sitio web comprometido para intentar acceder a otras cuentas de usuarios en diferentes sitios web. Esto tiene éxito cuando los usuarios reutilizan las mismas credenciales en múltiples sitios.
- Password Spraying: En este tipo de ataque, el atacante intenta iniciar sesión en una cuenta con una lista de contraseñas comunes o adivinadas, en lugar de probar muchas combinaciones de nombres de usuario y contraseñas.
- Brute Force Attacks: En este ataque, el atacante intenta descubrir una contraseña o clave de cifrado realizando múltiples intentos automáticos y repetitivos utilizando diferentes combinaciones de caracteres.

Estos ataques de identidad pueden comprometer la seguridad y la privacidad de los usuarios y los sistemas. Por lo tanto, es importante utilizar medidas de seguridad, como contraseñas fuertes, autenticación de dos factores y educación sobre los riesgos asociados con la ingeniería social y el phishing.

3.4.6. Ataques de inyección de código.

Los ataques de inyección de código, también conocidos como "code injection", son un tipo de ataque cibernético en el que un atacante aprovecha una vulnerabilidad en un sistema para insertar y ejecutar código malicioso en una aplicación web o base de datos. Estos ataques pueden ser de diferentes tipos, incluyendo la inyección de SQL, la inyección de comandos y la inyección de scripts, entre otros.

Los ataques de inyección de código permiten a los atacantes robar, modificar o eliminar datos de la aplicación o base de datos. También pueden tomar el control del sistema y utilizarlo para llevar a cabo otros ataques adicionales.

Para prevenir los ataques de inyección de código, es importante seguir prácticas de seguridad como validar y filtrar los datos de entrada, limitar los permisos de acceso a la aplicación o base de datos, y mantener actualizado el software para corregir las vulnerabilidades conocidas. Además, es fundamental educar a los desarrolladores y usuarios sobre las mejores prácticas de seguridad en línea.

Existen tres tipos principales de ataques de inyección de código:

- Inyección SQL: En este tipo de ataque, el atacante aprovecha una vulnerabilidad en una aplicación web para insertar código SQL malicioso en una consulta de base de datos. Esto sucede cuando las aplicaciones web no validan adecuadamente los datos de entrada, permitiendo al atacante introducir código SQL en las consultas de la base de datos. Los ataques de inyección SQL pueden conducir al robo, modificación o eliminación de datos, así como al control del sistema.
- Cross-Site Scripting (XSS): Este tipo de ataque ocurre cuando un atacante explota una vulnerabilidad en una aplicación web para insertar código malicioso, generalmente JavaScript, en una página web que será vista por otros usuarios. Los ataques de XSS se producen cuando las aplicaciones web no validan adecuadamente los datos de entrada y permiten que el código malicioso se ejecute en el navegador web de los usuarios. Esto puede permitir al atacante robar información, realizar acciones en nombre del usuario o tomar el control de su sesión. Los ataques de XSS se dividen en tres categorías: Reflejado, Almacenado y DOM-Based, dependiendo de cómo se inserte y ejecute el código malicioso.
- Malvertising: Este término se refiere a anuncios publicitarios maliciosos que se utilizan para propagar malware o redirigir a los usuarios a sitios web maliciosos. Los atacantes se aprovechan de las redes publicitarias de terceros para mostrar anuncios infectados

en sitios web legítimos. Estos anuncios pueden contener código malicioso que descarga y ejecuta malware en los dispositivos de los usuarios, o pueden utilizar técnicas de phishing para engañar a los usuarios y obtener información confidencial.

Al implementar medidas de seguridad adecuadas y estar al tanto de estas técnicas de ataque, se puede reducir significativamente el riesgo de sufrir un ataque de inyección de código.

3.4.7. Supply Chain Attacks

Los ataques de Supply Chain Attacks (SCA) son un tipo de ataque cibernético que tiene como objetivo explotar vulnerabilidades en la cadena de suministro de una organización, en lugar de atacar directamente a la organización en sí. En este tipo de ataque, los atacantes infiltran software o hardware malicioso en la cadena de suministro de una organización a través de proveedores de terceros, socios comerciales, distribuidores o fabricantes, con el fin de infiltrarse en la red de la organización o robar información valiosa.

Los ataques de Supply Chain Attacks pueden tener una amplia gama de objetivos, desde la extracción de información confidencial y propiedad intelectual, hasta la instalación de puertas traseras para el acceso no autorizado a la red de la organización, hasta el secuestro de sistemas para el pago de rescates.

Este tipo de ataques son muy peligrosos y difíciles de detectar, ya que el software o hardware malicioso se integra en los productos o servicios legítimos suministrados por los proveedores de terceros. Para prevenir los ataques de Supply Chain Attacks, es importante realizar una evaluación de riesgos de la cadena de suministro y asegurarse de que los proveedores de terceros y socios comerciales sigan las mejores prácticas de seguridad. También es importante implementar medidas de seguridad sólidas en la red de la organización, como la autenticación multifactor y la encriptación de datos, para limitar el daño en caso de un ataque exitoso.

3.4.8. Amenazas Internas

Las amenazas internas en ciberseguridad se refieren a cualquier actividad maliciosa que se origina desde dentro de una organización, ya sea intencional o no intencional, que compromete la seguridad de los sistemas, la información y los recursos de la organización.

Estas amenazas pueden ser causadas por empleados, contratistas, socios comerciales o cualquier otra persona con acceso a los sistemas de la organización.

Las amenazas internas pueden ser intencionales, como el robo de información confidencial, la venta de información a terceros, la destrucción de datos, el sabotaje de los sistemas, la extorsión o el ransomware. Estas amenazas son generalmente causadas por empleados descontentos, ex empleados, contratistas o socios comerciales malintencionados.

También hay amenazas internas no intencionales, que pueden ser causadas por errores humanos, descuido o falta de capacitación. Estas amenazas pueden incluir la pérdida accidental de información confidencial, la eliminación accidental de archivos importantes, el uso de contraseñas débiles, la apertura de correos electrónicos no deseados o el clic en enlaces maliciosos.

Para prevenir las amenazas internas, es importante implementar medidas de seguridad sólidas, como la implementación de políticas y procedimientos de seguridad claros, la educación y capacitación del personal en buenas prácticas de seguridad, el monitoreo y la auditoría de los sistemas, el control de acceso y los controles de seguridad física. También es importante llevar a cabo revisiones regulares de seguridad y evaluaciones de riesgos para identificar vulnerabilidades potenciales y tomar medidas para mitigarlas.

3.4.9. DNS Tunneling

El DNS tunneling es una técnica utilizada por los ciberdelincuentes para evadir los controles de seguridad y exfiltrar datos de una red a través del protocolo DNS (Domain Name System). El DNS es utilizado comúnmente por los dispositivos en la red para resolver nombres de dominio en direcciones IP, permitiendo que los dispositivos se comuniquen entre sí y accedan a Internet.

En un ataque de DNS tunneling, el atacante utiliza un software malicioso para enviar información codificada en un paquete de consulta DNS, que se envía a un servidor DNS comprometido. El servidor DNS interpreta el paquete de consulta como una solicitud legítima y reenvía la información al atacante a través del protocolo DNS, que puede ser descodificada y utilizada por el atacante para robar información confidencial, como contraseñas, credenciales de inicio de sesión y otra información valiosa.

El DNS tunneling es difícil de detectar porque el tráfico DNS es comúnmente permitido en las redes, lo que significa que los paquetes de datos pueden pasar fácilmente los controles

de seguridad. Además, los atacantes pueden utilizar métodos de codificación y ocultamiento para disfrazar los datos exfiltrados como tráfico DNS legítimo.

Para prevenir los ataques de DNS tunneling, es importante implementar medidas de seguridad sólidas, como el monitoreo y la auditoría del tráfico DNS, la implementación de políticas de seguridad claras, la educación y capacitación de los empleados en buenas prácticas de seguridad, y el uso de herramientas de detección y prevención de amenazas.

3.4.10. IoT-Based Attacks

Los IoT-Based Attacks son ataques que se dirigen específicamente a dispositivos conectados a Internet de las cosas (IoT, por sus siglas en inglés). Los dispositivos IoT son aquellos que se conectan a internet para intercambiar datos y realizar tareas sin necesidad de intervención humana. Esto incluye una amplia gama de dispositivos, desde termostatos inteligentes hasta cámaras de seguridad, desde electrodomésticos hasta automóviles conectados.

Los IoT-Based Attacks pueden tomar muchas formas diferentes, pero generalmente tienen como objetivo tomar el control de un dispositivo IoT para causar daño o para utilizarlo como parte de una red más grande de dispositivos comprometidos, conocida como botnet. Los ataques pueden ser perpetrados mediante el uso de vulnerabilidades en el software de los dispositivos IoT, como contraseñas débiles, software desactualizado o puertos abiertos no seguros.

Los IoT-Based Attacks pueden tener consecuencias graves, como la interrupción de servicios, el robo de datos o la propagación de malware. Es importante que los fabricantes de dispositivos IoT y los usuarios tomen medidas para asegurar los dispositivos y protegerlos contra los ataques.

3.5. Ataques de ingeniería social en Marina mercante.

Los ataques de ingeniería social en el ámbito de la marina mercante pueden tener consecuencias graves, ya que involucran la manipulación psicológica de las personas para obtener información confidencial o realizar acciones perjudiciales. (Verizon, 2022) Algunos ejemplos de ataques de ingeniería social en la marina mercante son: (Crowdstrike, 2021)

- Phishing: Los atacantes envían correos electrónicos falsos que se hacen pasar por entidades legítimas, como empresas navieras o autoridades marítimas, con el objetivo

de engañar a las víctimas para que revelen información confidencial o realicen acciones no deseadas, como instalar programas maliciosos.

- Whaling: Similar al phishing, pero dirigido a directivos de alto nivel en la marina mercante, como capitanes, jefes de flota o jefes de máquinas. Los atacantes se hacen pasar por estas personas importantes y solicitan información confidencial o acciones que puedan comprometer la seguridad de la organización.
- Baiting: Los estafadores utilizan falsas promesas o incentivos para atraer a las personas y persuadirlas para que revelen información personal o instalen malware en el sistema. Por ejemplo, pueden ofrecer premios o descuentos a cambio de información confidencial.
- Diversion Theft: Este tipo de ataque se origina fuera de Internet y se basa en engañar a los mensajeros o personal de la marina mercante para que realicen acciones incorrectas, como entregar paquetes en el lugar equivocado o a la persona equivocada. Esto puede resultar en el robo de información confidencial o la manipulación de pedidos y envíos.
- Business Email Compromise: Los atacantes se hacen pasar por ejecutivos de confianza y autorizados dentro de la organización y solicitan a los empleados que realicen transferencias bancarias u otras tareas financieras. Mediante la suplantación de identidad, los estafadores engañan a las víctimas y logran que realicen acciones no autorizadas.
- Smishing / SMS-phishing: Los atacantes utilizan mensajes SMS para engañar a las personas y hacer que hagan clic en enlaces maliciosos o descarguen contenido peligroso en sus dispositivos móviles. Este tipo de ataque se está volviendo más común a medida que las personas pasan más tiempo en sus teléfonos móviles.
- Quid Pro Quo: Los atacantes ofrecen un servicio deseable a cambio de información confidencial. Por ejemplo, pueden hacerse pasar por técnicos de soporte informático y solicitar credenciales de inicio de sesión bajo el pretexto de resolver problemas técnicos.
- Pretexting: Los atacantes crean escenarios plausibles y se hacen pasar por personas de autoridad o interés para convencer a las víctimas de que compartan información valiosa y confidencial. Utilizan la persuasión y la manipulación para obtener datos personales y acceder a cuentas y sistemas.
- Honeytrap: Este ataque se dirige a personas que buscan relaciones en línea a través de sitios de citas o redes sociales. Los atacantes crean perfiles falsos y establecen relaciones de confianza con las víctimas para obtener dinero, información personal o instalar malware.

4. Hacking en la marina mercante.

El entorno marítimo ha experimentado cambios significativos en las últimas décadas. En particular, el Sistema de Socorro y Seguridad Marítimos (SMSSM) se ha integrado en el Convenio para la Seguridad de la Vida Humana en el Mar (SOLAS) y ha incorporado tecnologías avanzadas, como la llamada selectiva digital (DSC) y el sistema satelital Cospas-Sarsat. Incluso las embarcaciones de recreo están adoptando cada vez más estas nuevas tecnologías.

No obstante, la evolución más notable en los buques se encuentra en sus sistemas de información, que regulan casi todos los aspectos de la vida en el mar. Es común encontrar sistemas de automatización y navegación basados en controladores lógicos programables (PLC), sistemas de supervisión y adquisición de datos (SCADA) para monitoreo, y computadoras tradicionales para la gestión de pasajeros o carga, por ejemplo. Al igual que otros sistemas automatizados, los sistemas de información a bordo de los buques no están exentos de los riesgos de ciberseguridad que ahora se consideran en todas las evaluaciones de riesgos empresariales.

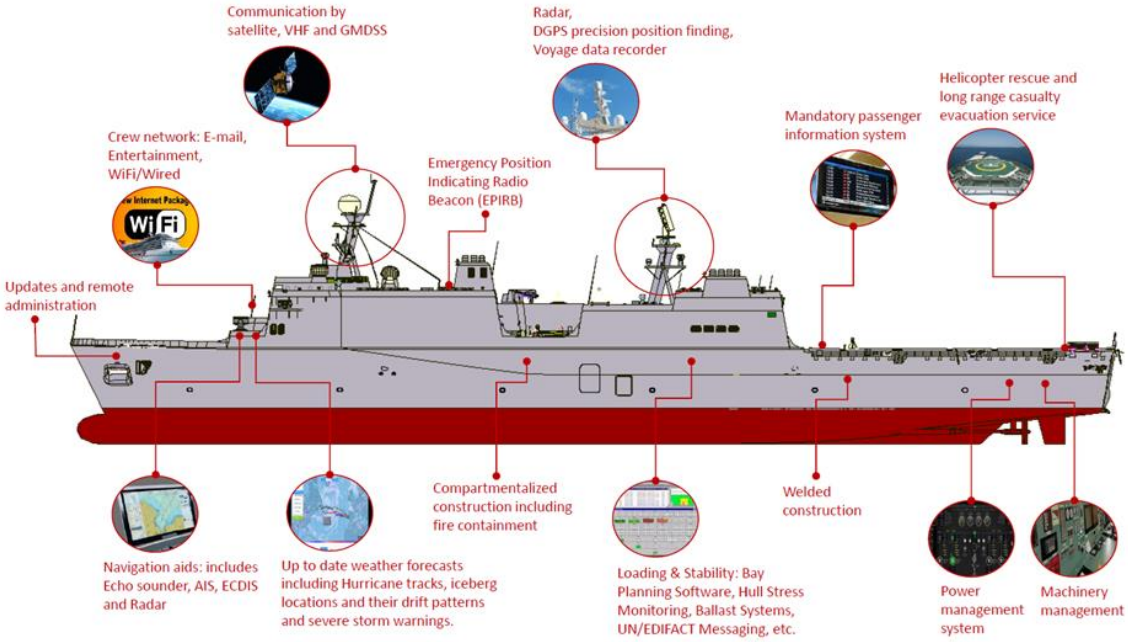
El sistema de información de un buque generalmente se divide en tecnología de la información (TI), tecnología operativa (TO) y sistemas de comunicaciones (SC). La TI se encarga principalmente de proporcionar información de alto nivel y facilitar la gestión del buque y sus operaciones (pasajeros, carga, tripulación, etc.). La TI en los buques es similar a la de las empresas tradicionales, aunque puede estar desconectada de una red de datos mientras está en el mar y alejada de proveedores. La TI utiliza datos de diversas fuentes, como registros de pasajeros, y también se relaciona con la TO. Por otro lado, la TO está conectada al mundo físico a través de sensores y puede interactuar con él de diversas formas. En los buques, esto se refleja, por ejemplo, en el sistema de navegación que utiliza datos de ubicación GPS, velocidad y dirección del viento, caudal de agua, capacidad de los tanques de combustible, potencia de los motores, entre otros. La comunicación entre TI y TO se realiza a través de redes especializadas (como Profibus) o mediante la conexión manual de medios extraíbles.

4.1. Equipos electrónicos principales y debilidades informáticas en un buque.

Los buques modernos están equipados con una compleja variedad de equipos que hacen que la navegación sea mucho más segura, eficiente y reactiva. Sin embargo, muchos de estos

equipos son susceptibles de sufrir un ataque informático. En la figura se muestra un esquema de los equipos principales del buque, tanto de la navegación y comunicaciones como de la máquina del buque.

Ilustración 1 "Sistemas automáticos en los buques modernos" (Akpan, Bendiab, Shiaeles , Karamperidis, & Michaloliakos , 2022, pág. 124)



Sistemas de navegación, RADAR, AIS (Automatic Identification Systems), sistemas de comunicación, sistemas de control de los equipos auxiliares, así como los motores principales, generadores, variadores de frecuencia, etc.

Dentro de los sistemas de navegación se incluye la carta electrónica o ECDIS (Electronic Chart Display and Information System), el sistema GPS (Global Positioning System) y el GNSS (Global Navigation Satellite System). El GPS y GNSS son piezas clave para la navegación autónoma del barco junto con el piloto automático y otros recursos, los cuales pueden calcular la posición relativa del buque y tomar decisiones respecto a esa información.

En el sistema AIS (Automatic Identification Systems) las señales AIS se transmiten desde los buques a través de frecuencias de radio VHF. En las pantallas de navegación de las embarcaciones y puertos equipadas para recibir información AIS aparece un icono que indica la ubicación y rumbo del buque transmisor además de un conjunto de especificaciones e identificaciones del buque. Se utiliza para el seguimiento y la asistencia del tráfico de buques y para notificar a las autoridades portuarias y marítimas la ubicación del buque. También es

muy útil para la investigación de accidentes, operaciones de búsqueda y rescate, y previsión meteorológica.

La carta electrónica o EGDIS es un sistema integrado para la navegación, el cual combina datos de diferentes fuentes (AIS, RADAR, GPS...) para mostrarlos en una interfaz gráfica sobre una carta náutica digital.

El RADAR (RAdio Detecting And Raging) es también un elemento indispensable en la navegación moderna, ya que muestra lo que rodea al buque, así como los objetos físicos que se encuentran en el rumbo.

Con el fin de garantizar las tasas de transmisión de datos y comunicación de alta velocidad a lo largo de las operaciones navales la mayoría de los barcos y buques modernos están equipados con el Terminal de Muy Pequeña Apertura de sus siglas en inglés VSAT.

Actúa como estación terrestre para que el satélite transmita y reciba datos desde la antena. El transceptor se monta por encima de la cubierta para alinearse con la vista del satélite, y la unidad de control se encuentra debajo de la cubierta y sirve de interfaz del ordenador.

El VSAT ofrece una variedad de servicios de comunicación y seguridad como ECDIS, AIS, teléfono, Internet, manipulación de la carga, integración inalámbrica, bienestar de la tripulación y previsión meteorológica. Opera en diferentes frecuencias, formas y tamaños. Normalmente, las frecuencias de operación son banda C y banda Ku y trabaja con Red en Estrella (Hub privado), Punto-a-Punto (Hub privado personalizado) capaz de soportar una gran cantidad de lugares y Sistemas Mesh, los cuales son regularmente más pequeños que los sistemas en estrella (entre 5 y 30 sitios generalmente).

La industria naval moderna también está viendo un aumento en la demanda de sistemas automatizados de videovigilancia inteligente para supervisar las operaciones de transporte o navegación, especialmente en las grandes áreas de almacenamiento, los generadores y los grandes buques.

Además, la industria naval depende en gran medida de los sistemas de control industrial, ICS (Industrial Control Systems) y las redes de IT (Information Tecnology) Los ICSs ayudan a recoger y agregar rápidamente datos de seguridad y operativos de todos los sistemas de control y sistemas de automatización del buque. Sensores, alertas y seguridades de todo tipo, tanto en la máquina principal, como los sistemas auxiliares. Lo que permite a la tripulación planificar trabajos, mantenimientos y decisiones con la mayor cantidad de información posible.

El Sistema Mundial de Socorro Marítimo (SMSSM), el sistema de control de la propulsión, los sistemas de puente integrados IBS (Integrated Bridge Systems), la gestión de la maquinaria y los sistemas de control de la energía son otros elementos clave de los sistemas de

automatización a bordo de un buque que desempeñan un cada vez más importante a la hora de facilitar el funcionamiento fluido, seguro y eficiente del buque.

A medida que aumenta la complejidad, digitalización y automatización de los sistemas en la industria marítima, esta se enfrenta cada vez a nuevos problemas relacionados con la protección y seguridad de los datos.

Podemos dividir los sistemas susceptibles a un ataque informático en dos grupos, los sistemas de ayuda a la navegación y GMDSS y por otro lado los sistemas de control industrial, sistemas auxiliares, propulsión del buque y los protocolos de conexión entre sistemas.

4.2. Sistemas de ayuda a la navegación y GMDSS.

En función del tipo de buque y las aguas que navega, se requiere de unos equipos obligatorios para llevar a cabo la navegación de forma segura, en la siguiente tabla se hace un listado de los sistemas obligatorios para los buques convencionales.

Tabla 3 "Sistemas de ayuda a la navegación y GMDSS y su uso"

Sistemas	Uso
Automatic Identification System (AIS)	- Seguimiento y asistencia al tráfico marítimo. - Evitar una colisión. - Notificar a los puertos y a las autoridades marítimas la ubicación del buque. - Calcular la distancia entre el buque y los demás buques. - Garantizar la seguridad marítima vigilando el tráfico. - Investigación de accidentes y operaciones de búsqueda y salvamento. COMPAS- SARSAT
GPS y GNSS	- Muestra la posición del barco. - Muestra la velocidad del buque. - Muestra la ruta y la hora.
Carta electrónica (Electronic Chart Display Information System, ECDIS)	- Recoge y combina datos de los sensores electrónicos de navegación. - Muestra la posición del buque en tiempo real.
Very Small Aperture Terminal (VSAT)	- Utiliza una red de satélites para enviar y recibir datos - Ofrece diversos servicios de comunicación y seguridad
Radar	- Proporciona información sobre el entorno del buque - Detección de la posición y la velocidad de los objetos
Circuito cerrado de televisión, CCTV (Video Surveillance System, VSS)	- Supervisar las operaciones de transporte en bodegas - Supervisar las operaciones de transporte en zonas críticas del buque. - Información e imagen en las maniobras del buque. - Gestión de la zona de pasaje.

Global Maritime Distress System (GMDSS)	- Difusión de mensajes de socorro relacionados con cuestiones de seguridad - Envío y recepción de alertas críticas de seguridad
NAVTEX	- Transmisión y recepción automatizada de información sobre seguridad marítima. - Recibir / difundir radioavisos náuticos
VDR “caja negra”	- Recopilar y conservar datos en caso de un accidente o desastre
INMARSAT - C	- Télex, fax, datos o correo electrónico
RADIOS GMDSS	- Comunicación entre buques y autoridades - Llamada selectiva digital. - Comunicación en emergencias.
EPIRB	- Ayuda a los servicios de búsqueda y salvamento en caso de emergencia en el mar. - Transmite la situación del accidente
IT Network Systems	- Utilizado para procesos internos/externos de envío, recepción y almacenamiento de datos. - Gestión de los documentos del buque. Ordenadores del puente - Utilizado para el bienestar de la tripulación. - Utilizado para dispositivos personales de la tripulación (Bring your own device, BYOD)

4.3. Control industrial, sistemas auxiliares, gobierno, propulsión del buque, protocolos de conexión entre sistemas y redes.

Para llevar a cabo la navegación del buque se requieren un conjunto de sistemas que deben interconectarse entre sí. Desde el control del timón en el puente se envía la señal que debe actuar los sistemas mecánicos que realizan cambios físicos en el buque, ya sea cambiando el paso de la hélice, cayendo el timón a una banda y actuando las hélices de proa en buques convencionales, o en casos como los catamaranes, reduciendo las revoluciones de los motores principales y modificando la dirección de jets gracias a los sistemas hidráulicos. Estas acciones se llevan a cabo a gracias a sistemas de control que se componen de autómatas, variadores de frecuencia, PLCs y sensores y que requieren de protocolos de comunicación para que las señales de control sean procesadas y se puedan realizar las maniobras correspondientes.

En un buque convencional los sistemas del puente y la máquina se encuentran interconectados en una red que transfiere esos datos.

Ilustración 2 "Layout de conexiones entre sensores, sistemas de navegación y máquina" (Hyra, 2019, pág. 54)

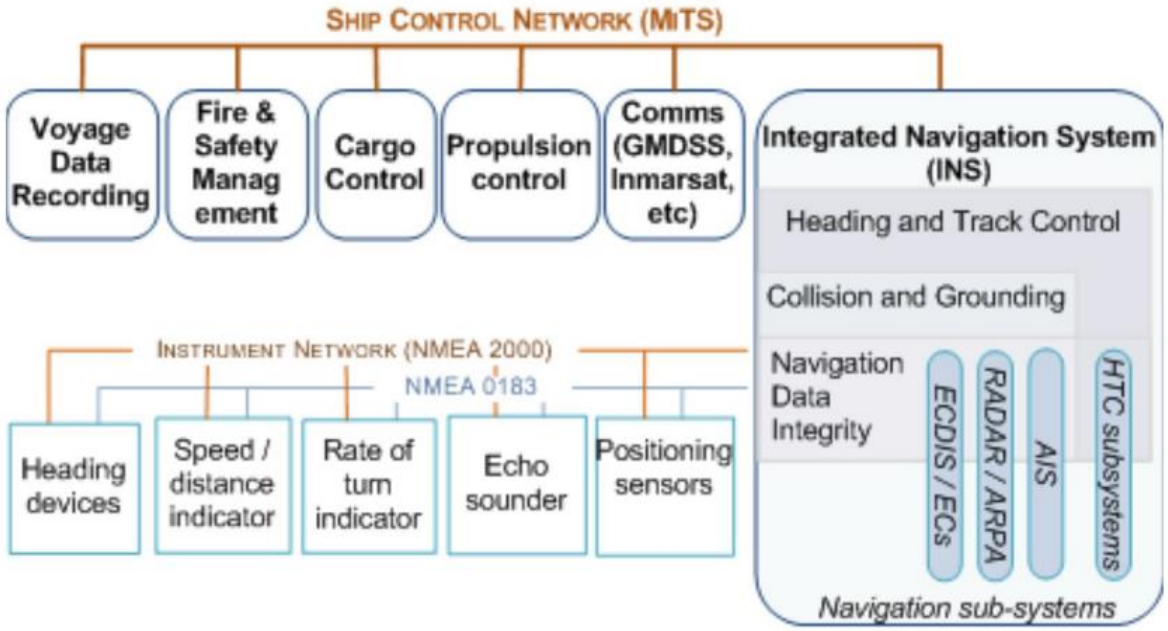
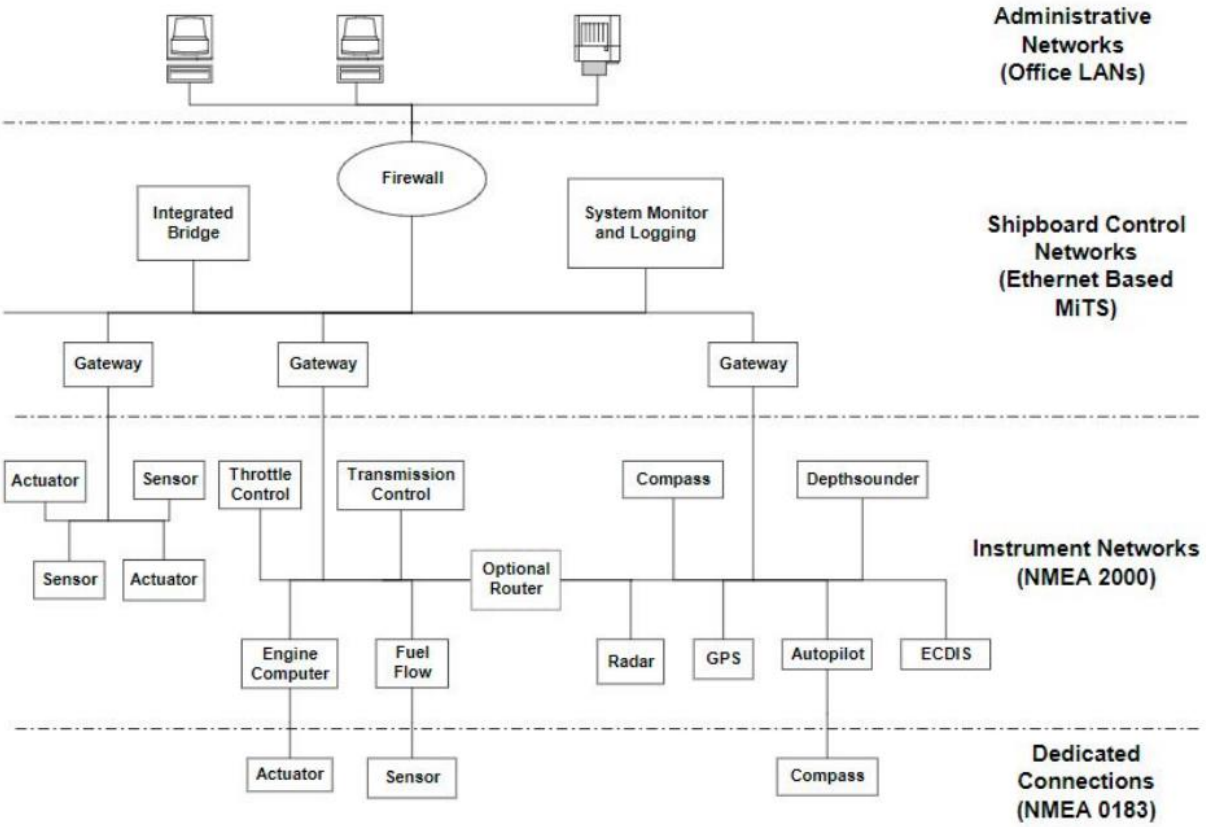


Ilustración 3 "Otra aproximación a la distribución de las redes del buque" (Hyra, 2019, pág. 55)



El conjunto de los sistemas de control y protocolos principales se presentan en la tabla a continuación.

Tabla 4 "Control industrial, sistemas auxiliares, gobierno, propulsión del buque, protocolos de conexión entre sistemas y redes y su uso."

Sistemas	Uso
Global Industrial Control Systems (ICSs)	- Ayudar a reducir los errores humanos - Aumentar la productividad de los recursos - Prolongar la vida útil de los equipos - Controlar y supervisar los parámetros a bordo de un buque
Sistemas de propulsión y gestión de maquinaria y control de potencia	- Supervisar y regular la maquinaria de a bordo - Supervisar y regular la propulsión - Supervisar y regular el gobierno
Redes de Area Local, LAN	- Conjunto de ordenadores interconectados - Permite el traspaso de información y control entre dispositivos.
Estándar Ethernet	- Elemento de conexión entre los diferentes sistemas de control del buque.
CAN BUS	- Protocolo de conexión en motores. - Simplifica y reduce la cantidad de conexiones en los motores.
Protocolos NMEA	- Protocolo de conexión entre diferentes dispositivos y sistemas del buque.
SCADA/RTU	- Sistema que controla y monitoriza los procesos industriales. - El conjunto de diferentes elementos como PLC, sensores, electroválvulas y motores forman el sistema SCADA.
PLC	-Unidad de control electrónico compleja más simple.
HMI	- Visualizar los datos de los sistemas de control. - Gestión de las alarmas en sistemas de control. - Enviar señales de control a los diferentes sistemas del buque.

5. Ciberataques a los sistemas GMDSS, gestión y de ayuda a la navegación del buque.

Todos los avances informáticos también abren un abanico de posibles ataques por parte de hackers o en el peor de los casos piratas informáticos, que podrían causar fallos catastróficos. Poco a poco, los ataques informáticos y problemas ocasionados en los buques han dado lugar a que se vaya aumentado la investigación e interés en este ámbito. En estos últimos años la cantidad de ataques no solo es mayor en cantidad sino también en escala.

Ataques de todo tipo, desde controlar remotamente el rumbo del buque, interrumpir las operaciones en puerto, hasta el robo de información valiosa o el encriptado de la misma. De hecho, la mayoría de los sistemas informáticos de los buques modernos son inseguros y vulnerables a los ataques porque se consideran menos críticos para la seguridad y el rendimiento. En este apartado veremos varios ciberataques a los buques modernos basándonos en las tecnologías y sistemas mencionados.

5.1. AIS (Automatic Identification System).

El Sistema de Identificación Automática (AIS, por sus siglas en inglés) es un sistema de comunicaciones que se utiliza en la industria marítima para el intercambio automático de información entre buques, satélites y estaciones terrestres.

"*Su objetivo es ayudar a identificar buques, ayudar en el seguimiento de objetivos, ayudar en operaciones de búsqueda y salvamento, simplificar el intercambio de información y proporcionar información adicional para ayudar al conocimiento de la situación*" (Organización Marítima Internacional (OMI), A 29/Res.1106).

Originalmente se desarrolló como una herramienta para evitar colisiones que permitía a los buques comerciales detectarse unos a otros con mayor claridad en todas las condiciones y mejorar la calidad de la información de que disponía el capitán sobre el entorno que le rodeaba. Para ello, el AIS transmite continuamente la identidad, posición, velocidad y rumbo de un buque, junto con otra información pertinente, a todos los demás buques equipados con AIS que se encuentren dentro de su radio de acción. Combinado con una estación costera, este sistema también ofrece a las autoridades portuarias y a los organismos de seguridad marítima la posibilidad de gestionar el tráfico marítimo y reducir los peligros de la navegación marítima.

5.1.1. Buques que emplean AIS.

"*La regla V/19.2.4 del Convenio para la Seguridad de la Vida Humana en el Mar (SOLAS) de la OMI exige que todos los buques de 300 GT o más que realicen viajes internacionales y todos los buques de pasaje, independientemente de su tamaño, lleven a bordo un sistema AIS*." (NATO Shipping Centre, 2021)

5.1.2. Señal AIS y tipos de AIS.

El AIS transmite en 2 frecuencias dedicadas de VHF, AIS 1: 161,975 MHz- canal 87B Simplex para la comunicación de buque a buque. AIS 2 162,025 MHz – canal 88B, dúplex para la comunicación puerto a buque.

Existen 2 tipos de AIS, de clase A, obligatorios para los buques comerciales con un desplazamiento bruto superior a 300 toneladas y en todos los buques de pasajeros, y clase B dirigidos para los buques fuera de SOLAS, principalmente los buques de recreo.

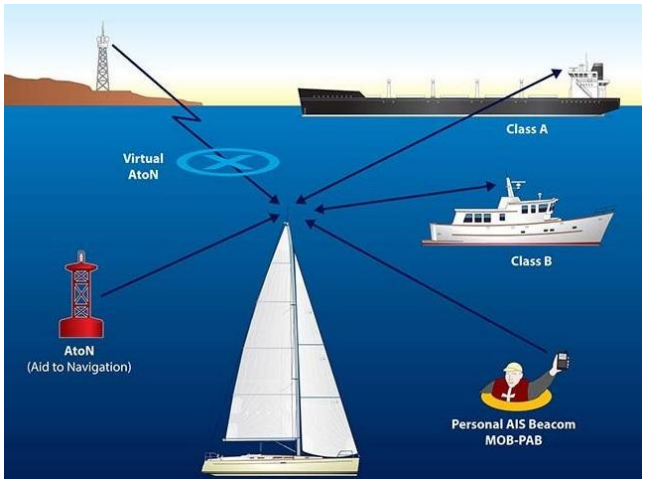


Ilustración 4 "Sistemas AIS" (NATO Shipping Centre, 2021)

5.1.3. Información del mensaje AIS.

El sistema consiste en una serie de equipos instalados en los buques y en las estaciones terrestres que reciben y transmiten información sobre la posición, velocidad, rumbo y otros datos relevantes de los buques que se encuentran en su área de cobertura. Los datos se transmiten en tiempo real y se muestran en una pantalla de radar o en un sistema de visualización de mapas en las estaciones receptoras.

Además de la información de posición y movimiento del buque, el AIS también transmite información sobre su identidad, nombre, tipo, tamaño, carga, puerto de origen y destino, y otros datos relevantes. Esta información puede ser utilizada por otros buques cercanos, estaciones terrestres, autoridades portuarias y servicios de tráfico marítimo para mejorar la seguridad y la eficiencia en la navegación.

Así los datos transmitidos se dividen en dos tipos: Información estática e información dinámica.

- La información estática se transmite automáticamente cada 6 minutos o bajo demanda y esta trasmite el numero IMO del buque, el número MMSI de estación de radio, nombre del buque y distintivo de llamada, tipo de buque, eslora y manga del buque y la situación de la antena AIS en el buque.
- La información dinámica, se transmite en función de la velocidad y situación del buque, envía los datos de posición con el índice de precisión, la relación de tiempo de la posición en UTC y el rumbo COG.

"El AIS no puede desconectarse, salvo contadas excepciones. Según las directrices de la OMI recogidas en la Resolución A. 917(22), el AIS debe estar siempre en funcionamiento cuando los buques estén navegando o fondeados. La tripulación de un buque en circunstancias singulares puede apagar su emisión AIS por diversas razones legítimas, pero este comportamiento puede indicar que un buque está ocultando su localización e identidad para encubrir actividades ilegales" (NATO Shipping Centre, 2021).

5.1.4. Arquitectura AIS.

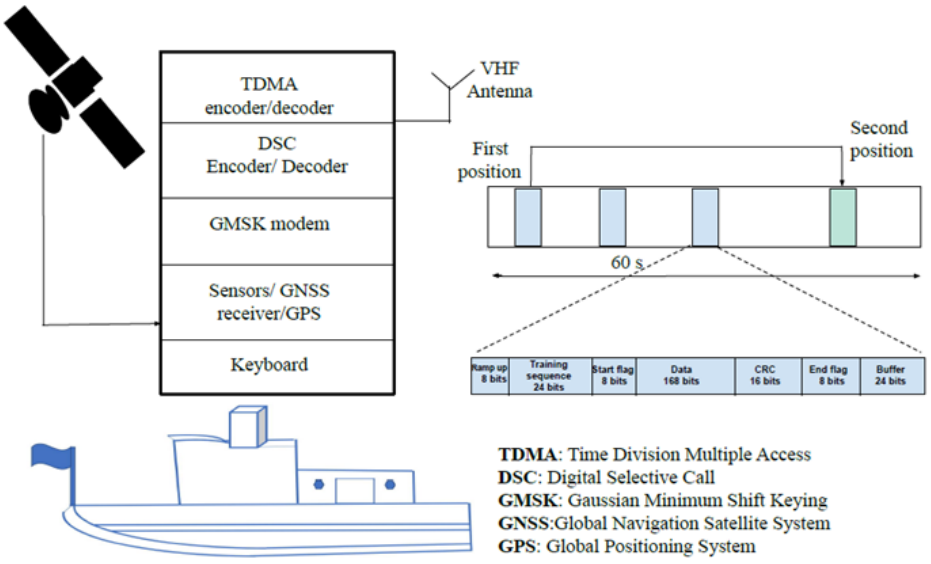


Ilustración 5 "Arquitectura simplificada de AIS clase A." (Mohamed , y otros, 2021, pág. 14)

La arquitectura AIS se compone de lo siguiente, principalmente:

- Time-division Multiple Access (TDMA): Protocolo por el cual la comunicación entre buques para el sistema AIS comparte la misma frecuencia.
  La información transmitida, sentencia, se divide en compartimentos de tiempo, huecos, cada uno contiene información como, por ejemplo, la localización del buque y su identidad. Se presenta un caso en la figura, la duración de la sentencia es de 60 segundos y esta subdividida en 2250 huecos.
- Llamada selectiva digital (LSD, en inglés: DSC): la organización Internacional de Telecomunicaciones, se sus siglas en ingles ITU (International Telecommunications Union) obliga a poseer a bordo un equipo con las funciones necesarias para el uso de DCS. Este sistema de socorro permite emitir alertas a las autoridades más cercanas en cualquier parte del mundo y recibir llamadas de socorro de otros buques. Un fallo en el sistema de DSC podría tener graves consecuencias.
- Gaussian Minimum Shift Keying (GMSK): La modulación GMSK se caracteriza por su alta eficiencia espectral y baja interferencia entre canales.
- Sistema Global de Navegación por Satélite (GNSS): Un GNSS proporciona la localización de un buque mediante satélites en red y es operado por el AIS.

5.1.5. Análisis de vulnerabilidades al sistema AIS.

El AIS proporciona datos estáticos, dinámicos y relacionados con el viaje, de acuerdo con el Convenio sobre la Seguridad de la Vida Humana en el Mar (SOLAS). Los tipos de datos del AIS se detallan en la figura; por tanto, los mapeos de la arquitectura del buque y las señales transmitidas son esenciales para la identificación de sus vulnerabilidades. Una estrategia exitosa para explotar las vulnerabilidades dentro del AIS y para definir ataques de impacto en el buque se basa en lo siguiente:

- Identificar las vulnerabilidades: Para realizar un ataque a un buque se puede recopilar información relacionada y donde podrían estar los principales factores para realizar el ciberataque. Si el buque tiene varios años desde su botadura y no ha actualizado sus sistemas o redes, estas podrían tener problemas endémicos conocidos de esas versiones.
- Obtener información sobre la infraestructura. Muchos buques tienen perfiles completos en internet, con planos y sistemas instalados en las zonas críticas

- Mapear la infraestructura informática. Para atacar al sistema AIS no es estrictamente necesario comprometer solo la recepción o transmisión de las señales AIS, se puede comprometer el sistema que interconecta los diversos componentes para que el AIS se muestre en los monitores de los RADAR o EGDIS. Los protocolos de conexión NMEA son un punto de partida para realizar un ataque al AIS.

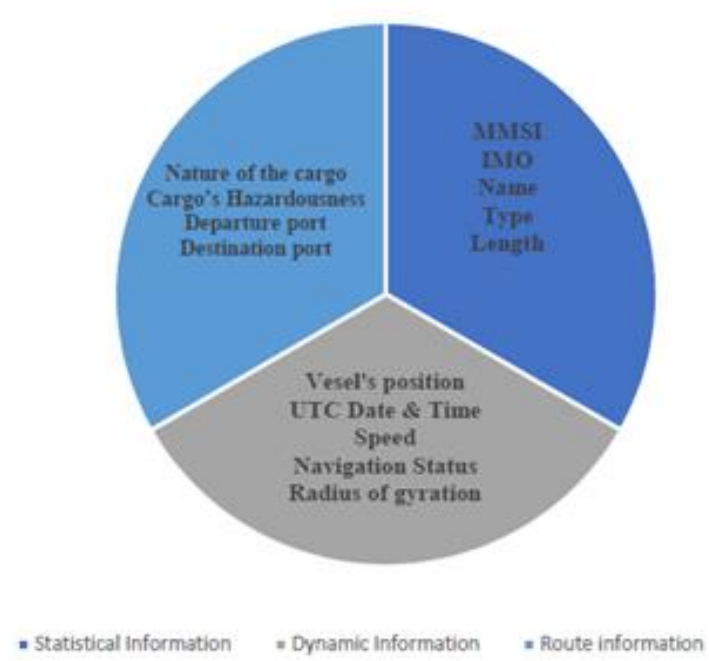


Ilustración 6 "Datos AIS" (Mohamed , y otros, 2021, pág. 13)

Los sistemas AIS se comunican por aire sin ningún tipo de autenticación ni comprobación de integridad, lo que permite a los piratas informáticos utilizarlo para difundir mensajes falsos. La radio controlada por software es utilizada por los atacantes para instigar señales falsas de "hombre en el agua", o haciendo que un barco pueda pasar desapercibido, o transmitir informes meteorológicos falsos. Estos hechos son preocupantes ya que, confiar en datos o reportes que pueden ser inexactos, o falsos, puede desembocar en malas decisiones y a resultados desastrosos.

Los datos AIS también son de libre acceso al público a través de sitios web como Vessel Finder Limited (https://www.vesselfinder.com/) y Marine Traffic. En este contexto, la OMI critica la divulgación de información sobre los buques y sus itinerarios porque esta información puede ser muy útil en caso de ataque dirigido. (Akpan, Bendiab, Shiaeles , Karamperidis, & Michaloliakos , 2022)

5.1.6. Resumen de amenazas al sistema AIS.

Los ataques al sistema AIS pueden ser divididos en 3 grupos, spoofing, hijacking y denegación de servicio. Y a su vez si pueden realizarse por radiofrecuencia (RF) o por software (SW). Se presenta una tabla a continuación con las categorías, ataques principales y su medio de ataque.

Tabla 5 "Sumario de amenazas" (Balduzzi, Pasta, & Wilhoit, 2014)

Categoría	Amenaza	SW	RF
Spoofing	Buques	X	X
	Ayudas a la Navegación	X	X
	SARs	X	X
	Colisiones (CPA)		X
	Radiobalizas de socorro		X
	Previsión meteorológica		X
Hijacking	Hijacking	X	X
Denegación de servicio	Slot Starvation		X
	Frequency Hopping		X
	Timing Attack		X

5.1.7. Spoofing de AIS.

El spoofing de AIS consiste en simular, copiar o suplantar una señal AIS con el objetivo de difundir esa información maliciosa a los buques del entorno o al objetivo. Dentro de esta técnica se encuentran varios tipos de señales que pueden ser copiadas y transmitidas con el objetivo malicioso del atacante. Las señales que se pueden simular son:

- El “Ship Spoofing” consiste en la creación de un buque válido e inexistente, es decir, una falsificación. Este proceso implica asignar información estática y dinámica al buque ficticio. La información estática incluye elementos como el nombre del buque, identificadores (como el MMSI e indicativo de llamada), pabellón, tipo de buque, tipo de carga, fabricante y dimensiones. Por otro lado, la información dinámica se refiere al estado del buque (por ejemplo, en navegación o fondeado), posición, velocidad,

rumbo y destino. Cabe mencionar que también se pueden suplantar aeronaves que participan en operaciones de búsqueda y salvamento (SAR), las cuales están equipadas con transpondedores AIS de clase B, de acuerdo con las regulaciones establecidas. Esta amenaza brinda al atacante una amplia gama de escenarios maliciosos. Por ejemplo, podrían introducir un buque ficticio en la jurisdicción de una nación adversaria o hacer que un cargamento portador de armas nucleares navegue por aguas pertenecientes a una nación desnuclearizada. Además, la falsificación de buques representa un problema para los sistemas automatizados encargados de realizar la identificación e inferencia de datos a partir de la información AIS recopilada. Estos sistemas son utilizados, por ejemplo, para detectar buques que derraman petróleo en alta mar o para predecir el comercio marítimo. Un atacante podría falsificar dicha información con el objetivo de inculpar a otro buque o entidad.

- Spoofing a las ayudas a la navegación, en inglés "spoofing AtoNs", implica la generación de información falsa con el propósito de inducir a un buque objetivo a llevar a cabo maniobras erróneas. Este tipo de ataques pueden adoptar varias formas, como la colocación de boyas adicionales o modificadas estratégicamente en la entrada de un puerto, con el fin de perturbar el seguimiento y la navegación precisa de los buques. Otro ejemplo de este tipo de ataques es la instalación de boyas falsas que, de manera maliciosa, pueden llevar a un buque a navegar en aguas de poca profundidad, lo que puede resultar en daños materiales o poner en peligro la seguridad de las personas a bordo. Dado el gran número y la diversidad de ayudas a la navegación existentes, se generan múltiples escenarios posibles para llevar a cabo este tipo de ataques. Es importante reconocer la importancia de salvaguardar la integridad y la confiabilidad de las ayudas a la navegación, así como implementar medidas de seguridad efectivas para mitigar el riesgo de posibles ataques de “spoofing AtoNs”.

Una de las aplicaciones primordiales del Sistema de Identificación Automática (AIS, por sus siglas en inglés) es la prevención de colisiones entre buques, lo cual ha sido implementado de manera efectiva como medida para reducir el riesgo de colisiones, especialmente en áreas marítimas donde no se cuenta con vigilancia por parte de las autoridades portuarias.El sistema AIS permite una respuesta automática una vez que se detecta una posible colisión entre buques. Esta funcionalidad, conocida como Punto Más Cercano de Aproximación (CPA, por sus siglas en inglés), consiste en calcular la distancia mínima entre dos buques, al menos uno de los cuales se encuentra en movimiento. Gracias al CPA, es posible configurar un buque para que active una alerta tanto visual en la consola del capitán como acústica a través de una sirena, y realice cambios en su rumbo con el fin de evitar una colisión. Sin embargo, existe una amenaza latente que radica en la posibilidad de

engañar a un buque que se encuentra en curso de colisión con otro buque objetivo. Este engaño desencadena una alerta de colisión en el sistema CPA del buque que está siendo víctima de la suplantación, lo que podría llevar a que el buque modifique su rumbo y se dirija hacia una roca o quede varado durante marea baja.

Además de su función para evitar colisiones, el Sistema de Identificación Automática (AIS) tiene una amplia utilización en operaciones de búsqueda y salvamento marítimo. En estas situaciones, los transpondedores de búsqueda y salvamento (SART) desempeñan un papel crucial. Estos dispositivos, que son autónomos y herméticos, están diseñados específicamente para casos de emergencia con el propósito de facilitar la detección y localización de embarcaciones y personas en peligro, como en casos de hombres al agua.

Un AIS-SART se activa automáticamente al entrar en contacto con el agua y emite una señal de socorro mediante radio, seguida de la transmisión de la posición GPS, lo cual ayuda a localizar a los supervivientes. Sin embargo, se ha identificado una amenaza que involucra la generación de una falsa baliza de socorro para un hombre al agua, en coordenadas elegidas por el atacante.

Según las especificaciones del protocolo, los transpondedores AIS están obligados a generar una alerta al recibir un mensaje de este tipo. En este escenario, el atacante, por ejemplo, un pirata marítimo, activa una alerta SART con el fin de inducir a su víctima a navegar hacia un espacio marítimo hostil controlado por el atacante. Es importante tener en cuenta que, por ley, una embarcación está obligada a unirse a una operación de rescate una vez que recibe un mensaje de búsqueda y salvamento.

Spoofing de partes meteorológicos, la difusión de previsiones meteorológicas falsas a través del sistema AIS. Este tipo de engaño puede tener repercusiones significativas en la seguridad marítima y la toma de decisiones de los buques que dependen de las previsiones meteorológicas para planificar sus rutas y actividades. Al proporcionar información falsa sobre las condiciones meteorológicas, los atacantes pueden inducir a los buques a tomar decisiones erróneas, exponiéndolos a riesgos innecesarios, como tormentas, vientos fuertes o marejadas

5.1.8. Hijacking de AIS.

El hijacking (secuestro) del Sistema de Identificación Automática (AIS) se refiere a la manipulación de la información transmitida por las estaciones AIS existentes, alterando datos como la carga, la velocidad, la ubicación y la bandera del buque real. Este tipo de ataque tiene

la intención de generar información engañosa y distorsionada sobre la situación y las características de un buque.

Un ejemplo de este tipo de ataque es la modificación maliciosa de la información proporcionada por las ayudas a la navegación instaladas en los puertos por las autoridades para asistir y supervisar a los buques. En la variante de ataque de software, el atacante intercepta y monitoriza la comunicación (ataque de "hombre en el medio") y sustituye la información AIS de manera arbitraria. En la versión de ataque de radiofrecuencia, el atacante reemplaza el mensaje AIS original con una señal falsa de mayor potencia. En ambos casos, el receptor recibe una versión modificada del mensaje AIS original de la víctima, manipulada por el atacante.

Estos ataques de secuestro de AIS pueden tener consecuencias graves en términos de seguridad marítima y toma de decisiones por parte de los operadores. La información falsa transmitida puede dar lugar a malentendidos, riesgos de colisión, desvíos no deseados de rutas, o incluso puede ser utilizado para llevar a cabo acciones ilícitas o actos de piratería.

Para contrarrestar esta amenaza, es fundamental implementar medidas de seguridad y autenticación sólidas para proteger la integridad y la confiabilidad de los mensajes AIS. Además, es crucial educar y capacitar a los operadores y autoridades marítimas sobre las posibles vulnerabilidades y técnicas de ataque, para que puedan tomar medidas preventivas y estar alerta ante cualquier actividad sospechosa en el sistema AIS.

5.1.9. Denegación de servicio de AIS.

Estos ataques solo pueden ser realizados en el espectro de radiofrecuencia, donde se transmitirían señales al resto de sistemas AIS alrededor del atacante.

- Slot Starvation: Este ataque que consiste en suplantar a la autoridad marítima para reservar todo el "espacio de direcciones de transmisión AIS", con el fin de impedir que todas las estaciones dentro de la cobertura se comuniquen. Esto incluye y ayudas a la navegación, así como las pasarelas AIS utilizadas en la monitorización del rastreo. Como resultado, el atacante puede inutilizar los sistemas AIS a gran escala.
- Frecuency Hopping o “Salto de frecuencias”: El atacante haciéndose pasar por una autoridad marítima y emitiendo órdenes a uno o varios transpondedores AIS para que cambien sus frecuencias de funcionamiento. Según las especificaciones del protocolo, la estación receptora debe mantener la información y los cambios de frecuencia

persistirán incluso si el sistema se reinicia. Además, este tipo de operación puede estar vinculado a una región geográfica específica, lo que permite al atacante "programar" un buque objetivo para que cambie su frecuencia al ingresar a una región elegida por el atacante, lo que resulta en la inutilización del sistema AIS.

Es importante destacar que, en el caso de dispositivos de clase B, la normativa AIS impide el reinicio manual del transpondedor y no notifica al usuario sobre el cambio de frecuencia. Esto puede llevar a que el buque objetivo permanezca inconsciente de la manipulación y siga transmitiendo información en una frecuencia alterada y potencialmente inaccesible para otros receptores AIS legítimos.

Este tipo de ataque puede tener graves implicaciones en la seguridad marítima, ya que puede afectar la capacidad de seguimiento y supervisión de los buques y dificultar la detección de posibles colisiones, operaciones de búsqueda y salvamento, y el intercambio de información vital entre las autoridades y los buques.

- Timing Attack, ataque de sincronización: el usuario malicioso ordena al transpondedor o transpondedores AIS que retrasen su tiempo de transmisión. El atacante, con sólo renovar la orden, puede impedir que el transpondedor o transpondedores sigan comunicando su posición. Esto hace que, por ejemplo, un buque desaparezca de los radares habilitados para AIS. Inversamente, el atacante puede sobrecargar (es decir, inundar) el tráfico marítimo, incluidos los servicios de tráfico de buques y embarcaciones, solicitando a las estaciones existentes que envíen actualizaciones a un ritmo muy elevado.

5.1.10. Estrategias de mitigación para los sistemas AIS.

La detección de anomalías es una estrategia que implica aplicar técnicas de detección de patrones inusuales en los datos AIS recopilados, tanto de proveedores en línea como de servicios de tráfico marítimo. El objetivo es identificar actividades sospechosas, como cambios inesperados en las rutas de los buques o información estática inusual. Además, los datos AIS pueden correlacionarse con información satelital para detectar discrepancias, como inconsistencias en las dimensiones de un buque. Si bien la detección de anomalías puede ser efectiva en sistemas de recolección de datos, no parece ser una solución completa para los transpondedores a bordo de los buques, ya que aún pueden ser vulnerables a amenazas específicas de RF, como la interrupción de la disponibilidad de la señal y la suplantación de dispositivos SART.

Una forma complementaria de mitigación es adoptar un esquema de infraestructura de clave pública (PKI, por sus siglas en inglés) basado en el protocolo AIS utilizado en las comunicaciones por radiofrecuencia (RF). Se sugiere el uso de X.509, que es un estándar ampliamente reconocido para PKI. En este enfoque, los certificados digitales son emitidos por autoridades marítimas nacionales oficiales que actúan como autoridades de certificación y se configuran en los transpondedores simultáneamente con los identificadores de las estaciones, como el MMSI y el indicativo de llamada. X.509 proporciona autenticación en los mensajes intercambiados entre estaciones, como entre buques y las autoridades portuarias. Los certificados se gestionan de dos formas: aquellos pertenecientes a estaciones destacadas, como las estaciones de seguimiento de tráfico (STB), se cargan previamente a través de instalaciones en tierra, por ejemplo, cuando un buque ingresa a un puerto; los certificados genéricos y aquellos previamente desconocidos para una estación se intercambian con estaciones cercanas (es decir, buques en navegación) a solicitud, durante la fase de conocimiento mutuo entre dos buques. Los buques con acceso a Internet vía satélite pueden recuperar los certificados de servicios en línea.

La implementación de un esquema PKI basado en X.509 en el protocolo AIS fortalece la autenticación y la confidencialidad de las comunicaciones entre las estaciones, ayudando a prevenir ataques de suplantación y mejorando la seguridad del sistema. Sin embargo, es importante destacar que este enfoque requiere una gestión adecuada de los certificados y la cooperación entre las autoridades marítimas nacionales para asegurar la emisión y distribución segura de los certificados digitales.

En resumen, la detección de anomalías en los datos AIS y la implementación de un esquema PKI basado en X.509 son enfoques complementarios que pueden fortalecer la seguridad y la confiabilidad del sistema AIS, tanto en la detección de actividades sospechosas como en la autenticación de las comunicaciones entre las estaciones marítimas. (Balduzzi, Pasta, & Wilhoit, 2014)

5.2. GPS (Global Position System).

El GPS y las tecnologías relacionadas con la navegación son vitales en el sector marítimo tal y como lo concebimos, así, son objetivos específicos de varios ciberataques que pretenden explotar fallos de diseño para desestabilizar los servicios de los que dependen estas tecnologías.

Estos ataques suponen un riesgo alto, ya que además de las violaciones de los protocolos de datos dando como resultado el mal funcionamiento de los equipos vinculados al GPS, estos ataques pueden acabar con daños materiales o víctimas humanas, como el

caso donde un grupo de estudiantes tomaron el control de un yate de 80 millones de dólares y cambiaron su rumbo sin que ninguna alarma ni advertencia avisara a la tripulación.

En otra ocasión en Corea del Sur, la interferencia de la señal GPS afectó a la recepción de señal de más de 1000 aviones y más de 700 barcos durante una semana.

"Dichos ciberataques pueden clasificarse como de dificultad media a dificultad alta y son el resultado de los diseños y normas de los sistemas GPS y de navegación. Según, los sistemas de comunicación por satélite (SATCOM), incluidos los que conectan los buques a través de Internet entre sí y con el continente, contienen un gran número de vulnerabilidades y agujeros de seguridad críticos, como dispositivos que utilizan protocolos no seguros o incluso no documentados, cuentas configuradas de fábrica, la posibilidad de explotar la función de restablecimiento de contraseña y puertas traseras". (P.H. Meland, K. Bernsmed, E. Wille, Ø.J. Rødseth, & D.A. Nesheim, 2021)

Los ataques a los sistemas GPS se pueden dividir en dos grupos, ataques de jamming, saturar la frecuencia en la que se transmiten las señales gps interfiriendo en su transmisión o bien ataques de spoofing donde un atacante simula ser un emisor GPS y modifica los valores GPS para crear una disrupción en el rumbo de la nave.

5.3. GNSS (Global Navigation Satellite System).

El uso de variables de posición y tiempo está cada vez más extendido en sistemas y procesos que requieren automatización, ejecución en tiempo real, rastreo de activos, sincronización de operaciones o control remoto. Aunque la precisión y la exactitud son esenciales, no son suficientes por sí solas. También se debe garantizar la integridad, disponibilidad y, en algunos casos, la confidencialidad de los datos.

Entre las tecnologías disponibles para el geoposicionamiento y la cronometría se encuentran las redes Wi-Fi y las torres GSM (Global System for Mobile). Sin embargo, los sistemas Global Navigation Satellite System (GNSS) son considerados como la tecnología por excelencia, y los más conocidos y de cobertura global son el Galileo (europeo), GLONASS (ruso), BeiDou (chino) y GPS (americano).

Uno de los sistemas más interconectados es el GNSS. Como resultado de esto, buques autónomos que dependen de las comunicaciones mejoradas con los satelites para comunicarse con el centro de control podrían falsear tanto la información recibida como la enviada, estando estos datos muy vulnerables a un ciberataque, por ejemplo, un "man-in-the-middle", "DoS" o modificaciones en los paquetes de datos. Además, las señales de baja

potencia de los satélites son especialmente vulnerables a los ataques de “jamming” y “spoofing” siendo estos ataques de gran impacto y bajo esfuerzo.

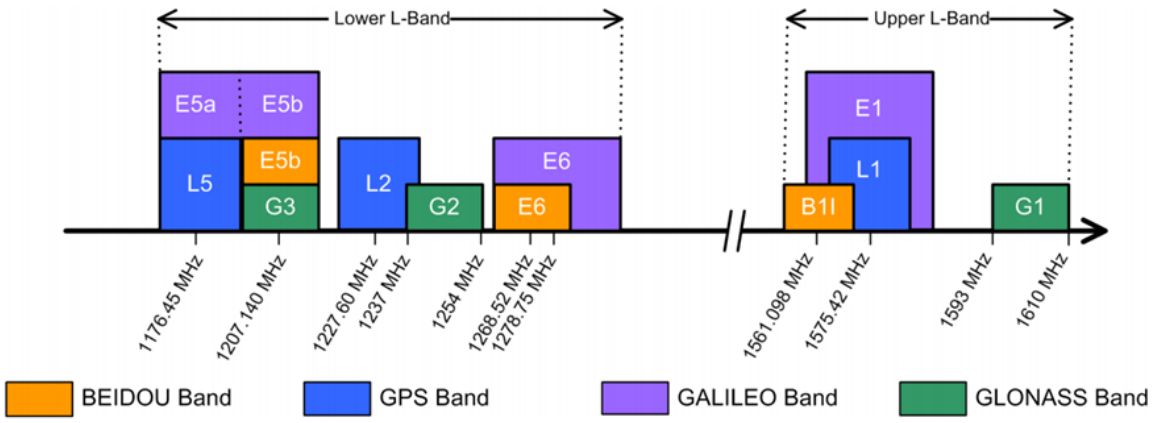
Adicionalmente, la grandísima importancia de la posición por satélite puede llevar al mal funcionamiento de otros sistemas interconectados, como pueda ser el AIS, sistemas de posicionamiento dinámico o el ECDIS. (INCIBE, Instituto Nacional de Ciberseguridad, 2020)

5.3.1. El sistema GNSS y su señal.

Cada sistema GNSS opera con un conjunto característico de bandas de frecuencia, mediante las cuales se transmite información por radiodifusión. Cada señal de RF (Radio Frequency) que lleva información viaja desde el segmento espacial hasta el segmento de usuario. En conjunto con el segmento de control, estos tres segmentos forman la segmentación de todo GNSS:

- Segmento espacial: formado por la constelación de satélites que pertenecen a cada sistema GNSS. Esta constelación es la que genera los datos que serán procesados por los receptores.
- Segmento de control: integrado por una red de estaciones terrestres que se encargan de supervisar y corregir los datos transmitidos desde el segmento espacial.
- Segmento de usuario: compuesto por los equipos receptores, que calculan las variables de posición y tiempo a partir de los datos recibidos. Este segmento es el que posibilita la compatibilidad entre los distintos sistemas GNSS.

Ilustración 7 "BEIDOU, GALILEO, GLONASS & GPS bandas de frecuencia." (ROHDE & SCHWARZ, pág. 6)

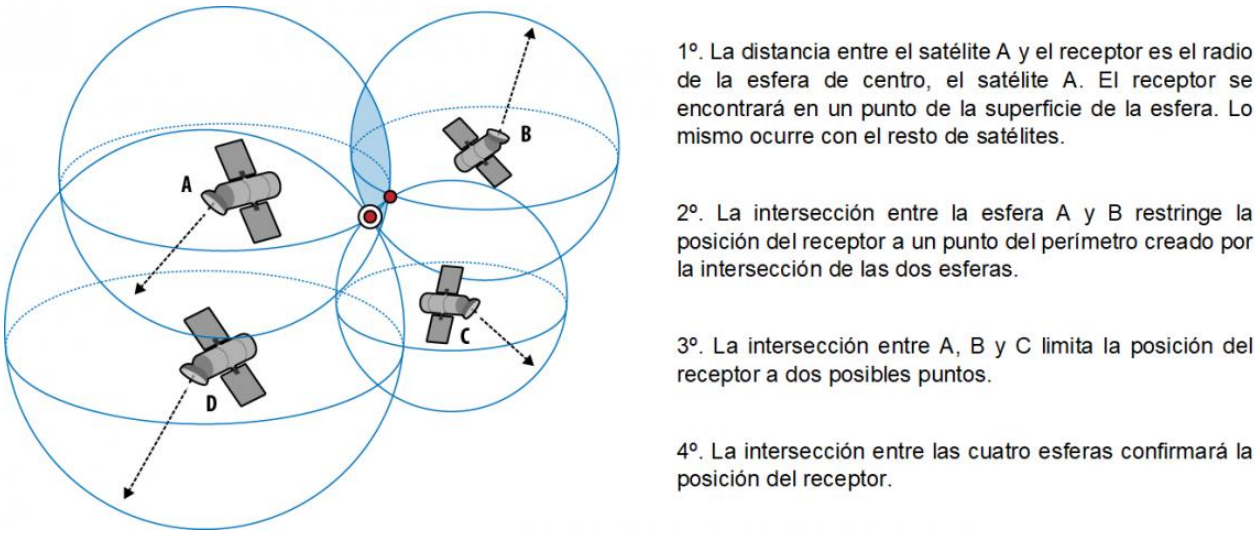


La señal GNSS que el hardware o software del receptor debe procesar está compuesta por:

- Una señal portadora analógica de frecuencia UHF (Ultra High Frequency), con la que el receptor debe estar sintonizado y sincronizado para recibir y procesar correctamente los datos.
- Un código digital PRN (PseudoRandom Noise), que identifica a cada satélite y determina si el servicio de posicionamiento es para uso civil o militar. Por ejemplo, los códigos C/A (civil) y P (militar) del GPS.
- Un mensaje de navegación digital que incluye dos tipos de paquetes de datos: el almanaque y las efemérides. El almanaque contiene parámetros orbitales e información temporal, mientras que las efemérides proporcionan datos precisos sobre la posición del satélite.

Tanto el envío de las señales desde los satélites como el proceso de adquisición de señal por parte de los receptores activos son periódicos. La sincronización de la transmisión se logra gracias a los relojes en los satélites y los receptores. Cuando la señal es sintonizada por el receptor, mide el tiempo que tarda la onda en llegar y, conociendo la velocidad de propagación en el vacío, calcula su distancia al satélite. Con los datos de cuatro satélites, el receptor puede calcular su posición 3D (latitud, longitud y altitud) mediante trilateración.

Ilustración 8 "Cálculo de la posición usando la trilateración." (O'REILLY, 2022)



5.3.2. Vulnerabilidades y amenazas del GNSS.

Toda señal transmitida por un satélite GNSS es vulnerable debido a que es una onda de radiofrecuencia. Además, cuando la señal llega a la superficie terrestre, su potencia disminuye, lo que la hace más vulnerable a múltiples amenazas, tanto intencionadas como no intencionadas. Estas amenazas incluyen:

- Condiciones del entorno, que afectan la dirección y el tiempo de propagación de la onda de RF y sus características. Esto puede impedir que el receptor sintonice la señal correctamente. Las condiciones del entorno incluyen la composición de la atmósfera, los fenómenos de refracción y reflexión, la propagación multicamino y la línea de mira entre el satélite y el receptor.
- Errores del sistema emisor, como fallos en los relojes a bordo de los satélites o el envío de datos incorrectos.
- Errores del sistema receptor, que pueden ser el resultado de un mal funcionamiento o una mala calidad del hardware del equipo. Esto puede introducir ruido en la señal a procesar o puede deberse a un fallo en el reloj, lo que resulta en una mala sincronización.
- Factores humanos, como la dependencia de un único GNSS, la falta de capacitación para su uso y el no reconocimiento de un mal funcionamiento. Estos factores también pueden contribuir al procesamiento de información incorrecta.
- Interferencias, que abarcan todas las transmisiones de RF no deseadas que se superponen a la banda de frecuencia de un GNSS. Las interferencias no intencionadas incluyen las Comunicaciones inalámbricas de Banda Ultra Ancha (UWB), el Servicio Móvil por Satélite (MSS) e incluso otros GNSS. Las interferencias intencionadas incluyen las técnicas de jamming y spoofing.

5.3.3. Jamming de GNSS.

El jamming es una técnica de interferencia intencionada que consiste en emitir señales de RF con características específicas y mayor potencia que la señal objetivo. El objetivo es bloquear total o parcialmente la recepción de la señal objetivo.

Además, existe otro tipo de jamming llamado meaconing. En este caso, el proceso consiste en sintonizar señales GNSS reales, grabarlas y luego retransmitirlas con un cierto retardo y mayor potencia para confundir al receptor. Este método no controla las variables de tiempo y posición que el receptor calcula. Aunque existe una cierta probabilidad de que se den casos contrarios, como se verá en la sección de spoofing.

Es importante destacar que el equipo inhibidor o jammer no trabaja de forma selectiva, lo que puede tener efectos colaterales en otros sistemas, como en el control de tráfico aéreo (ATC). El uso de estos dispositivos está prohibido salvo autorización, aunque su comercialización es legal. Existen muchos tipos de jammers con diferentes precios y tamaños.

Los jammers de potencia inferior a 100W son los más peligrosos porque son difíciles de detectar. Un inhibidor pequeño y económico de 1W puede cubrir 20 km2. Los PPD (Personal Privacy Devices) y los equipos SDR (Software Defined Radio) transmisores son ejemplos de estos dispositivos.

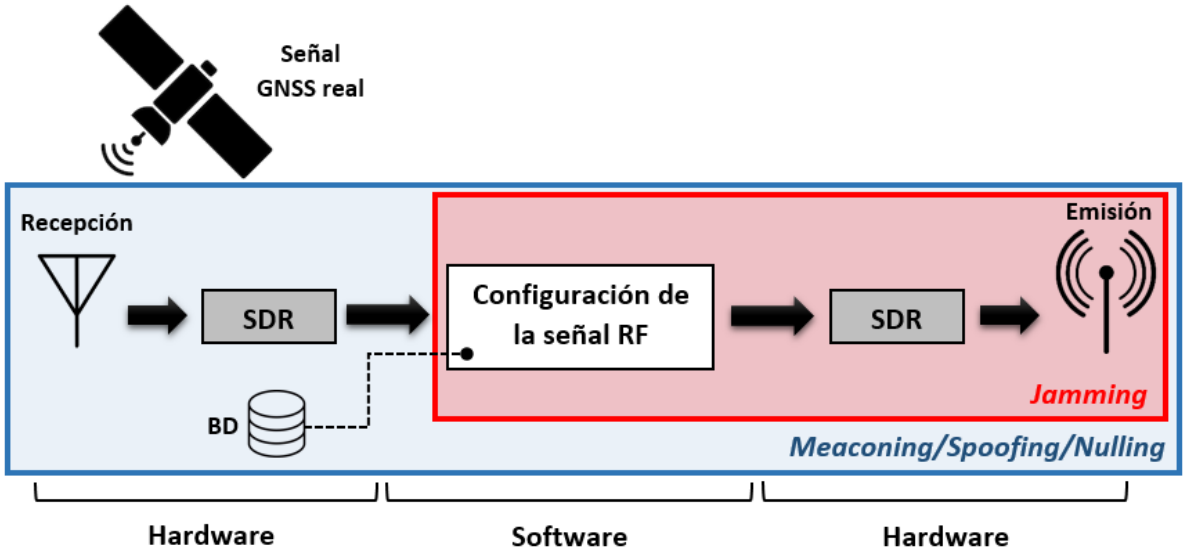


Ilustración 9 "Diagrama de bloques para las operaciones jamming y spoofing usando bloques SDR como Front-End." ((INCIBE), 2020)

5.3.4. Spoofing de GNSS.

El spoofing es una técnica de interferencia intencionada en la que se suplanta la señal GNSS con una señal falsa de mayor potencia. Esto hace que el receptor GNSS sintonice la señal falsa en lugar de la real, lo que resulta en una posición calculada incorrecta o en una variable temporal errónea. El spoofer es el equipo utilizado para realizar este ciberataque, que es ilegal.

Existen varias técnicas para lograr el objetivo del spoofing. La primera técnica consiste en simular una señal GNSS falsa mediante el uso de bases de datos en línea relativas a almanaque, efemérides y códigos PRN en un software simulador. Si la señal falsa es la primera que sintoniza el receptor objetivo, tras activar su periodo de adquisición, esta técnica tiene éxito. En caso contrario, el jamming se utiliza como etapa previa.

Otra técnica es generar una señal GNSS análoga y sincronizada con la señal real, lo que implica un proceso gradual de alineación y desalineación entre las señales real y falsa en

tiempo, forma y potencia. Para lograrlo, el spoofer debe tener capacidad de recepción y emisión y conocer la forma de la señal real.

La técnica de nulling implica que el spoofer emita dos señales por cada señal GNSS real a suplantar. Una de ellas es la señal real pero desfasada 180º, lo que anula la señal emitida por el satélite. La otra señal es la falsa, de mayor potencia.

Finalmente, el meaconing es una técnica de jamming que puede resultar en el procesamiento correcto de una señal falsa por parte del receptor GNSS, incluso si este es de tipo militar, lo que puede llevar a la obtención de una posición falsa.

5.3.5. Estrategias de mitigación para GNSS.

Ambas amenazas pueden ser enfrentadas mediante la opción de incrementar la potencia de la señal real mediante repetidores para hacerla más fuerte. Sin embargo, esta solución no es suficiente.

A continuación, se presentan soluciones para el jamming:

- Detectores de jamming: son dispositivos que detectan a un jammer activo cercano mediante algoritmos de procesado de señal que identifican alteraciones en la onda recibida, como picos de frecuencia.
- Antenas anti-jamming: también conocidas como CRPA (Control Reception Pattern Antenna), son matrices de antenas receptoras con capacidad para modificar sus patrones de recepción. De esta manera, se puede reducir la interferencia en la dirección en la que se recibe y crear un espacio nulo para evitar el jamming. También permiten detectar la dirección origen de la interferencia y proporcionar una ganancia adicional de recepción de las señales reales.
- Equipos inerciales: consiste en acoplar a un receptor GNSS una unidad de medida inercial IMU (Inertial Measurement Unit). De esta forma, ante la pérdida de señal, el receptor realizará sus cálculos en base a los últimos datos calculados y a los proporcionados por la IMU.
- Filtros notch o de rechazo de banda adaptativos para eliminar la región del espectro de frecuencia afectado por la interferencia. Han de implementarse antes del ADC (Analog-to-Digital Converter) del receptor.

En cuanto a las soluciones al spoofing, se encuentran:

- Algoritmos de procesado de señal: buscan cambios bruscos en las características de la señal recibida, como la amplitud, fase o potencia, o también comprueban la función de autocorrelación de la misma. Esta técnica solo permite la detección en el momento inicial del ataque spoofing, después de esto, es inservible.
- Monitorización del espectro radioeléctrico: para detectar señales duplicadas.
- Matriz de antenas receptoras: detecta la señal falsa por su ángulo de llegada.
- Cifrado: esta solución está presente para servicios militares o bajo autorización, quedando excluida del uso civil. El cifrado puede ser simétrico o asimétrico y puede hacerse a nivel de señal o a nivel de datos. Los códigos de cifrado y los algoritmos utilizados son secretos y sin ellos es imposible lograr el spoofing. Además, los receptores compatibles con esta solución deben integrar los algoritmos clasificados, disponer del repositorio de claves pertinente y estar certificados para su uso militar.
    - A nivel de señal únicamente se cifra el código PRN. Es el caso del código P(Y) del GPS, que resulta de cifrar el código P mediante un código W.
    - A nivel de datos únicamente se cifra el mensaje, no el PRN. Con ello, el receptor podrá hacer un seguimiento de la señal, pero nunca sabrá lo que dice el mensaje y, por tanto, no calculará la posición falseada. Es el caso del OS-NMA de Galileo.
- Uso de un servidor de datos PRN: este método permite verificar la transmisión a partir de históricos de datos PRN almacenados sin que el receptor los tenga en su memoria interna, con lo que se ofrece seguridad a receptores simples.
  ((INCIBE), 2020)

El uso masivo de receptores GNSS ha dado lugar a una amenaza constante de técnicas de jamming y spoofing, que evolucionan a la par que la tecnología. Esto ha llevado al desarrollo de equipos más pequeños y baratos con estrategias de ataque más sofisticadas.

Además, hasta ahora, las transmisiones GNSS para uso civil carecen de protección contra jamming y spoofing, mientras que las militares sí la tienen. Para los usos autorizados, aún no existe una política reguladora.

Las técnicas de jamming y spoofing pueden utilizarse para atacar o defender, como en la protección de espacios aéreos restringidos contra drones.

Para hacer frente a estas ciberamenazas, se están desarrollando nuevas estrategias, como las nuevas generaciones de sistemas (como el GPS III), el uso de sistemas complementarios (como los sistemas de aumentación SBAS) o el desarrollo de nuevos receptores (como GUARD, el diseño universal anti-spoofing GNSS).

5.4. Carta electrónica ECDIS (Electronic Chart Display Information System).

"*El Sistema de Información y Visualización de (ECDIS) se considera una tecnología operativa fundamental para la planificación de viajes y se acepta como con las cartas de papel actualizadas (cumple con la normativa de la OMI y el transporte obligatorio), y desempeña un papel central en la seguridad de la navegación y el transporte marítimo (IMO MSC.1/Circ.1503/Rev.1 2017).”* (Svilicic, Brčić, Žuškin, & Kalebić, 2019)

El ECDIS (Sistema Electrónico de Visualización e Información de Cartas de Navegación) se compone principalmente de un software instalado en un ordenador personal estándar con un sistema operativo convencional preinstalado. El software ECDIS ha sido diseñado de manera flexible para adaptarse al sistema operativo subyacente. Esta flexibilidad permite abordar los desafíos de interconexión y control que surgen al utilizar diferentes activos tecnológicos y equipos informáticos convencionales. Si bien existen regulaciones y políticas marítimas que rigen el mantenimiento del software ECDIS (por ejemplo, IMO MSC.1/Circ.1503/Rev.1 2017, IMO 2010), la responsabilidad de implementar las disposiciones adecuadas recae en los armadores y proveedores de hardware y software subyacentes. Estos proveedores de hardware subyacentes son seleccionados y respaldados por los armadores, en colaboración con los fabricantes de equipos ECDIS.

El programa suele estar instalado y usarse en ordenadores antiguos, los cuales no tienen actualizaciones de seguridad. Los mapas son directamente descargados desde internet o introducidos a mano vía un USB, ambos capaces de comprometer el sistema fácilmente. Varios autores investigaros el software de ECDIS y descubrieron varios fallos o brechas de seguridad que podrían permitir a un atacante borrar, reinstalar archivos en el sistema, así como inyectar código malicioso. Como resultado modificar las lecturas de los sensores y sistemas externos comprometiendo el funcionamiento del ECDIS y causando abordajes.

5.4.1. Funcionamiento y estructura ECDIS.

De acuerdo con los requisitos de cumplimiento a bordo, el sistema ECDIS debe estar homologado, con cartas náuticas electrónicas actualizadas (en inglés Electronic Navigational Charts, ENCs), el software ECDIS actualizado e instalado con un sistema de respaldo

adecuado (OMI MSC.1/Circ.1503/Rev.1 2017, OMI MSC.282(86) 2009, OMI 2017, OMI 2018). Según las normas de rendimiento de la OMI, el sistema consta de tres sensores obligatorios (posición, rumbo y velocidad) que están conectados directamente al ECDIS. Además, el ECDIS permite agregar sensores adicionales relativos a el entorno de navegación y la seguridad del buque. La actualización regular de las cartas electrónicas también garantiza un rendimiento fiable del ECDIS y representa un requisito básico para una navegación segura. Las cartas electrónicas se actualizan habitualmente con dispositivos de almacenamiento portátiles, como un pendrive y muy raramente a través de una conexión a Internet.

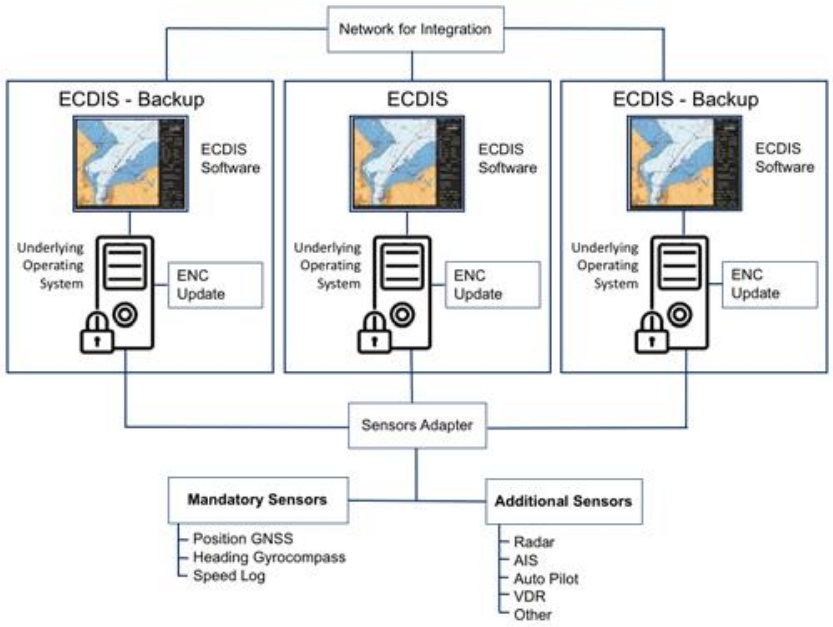


Ilustración 10 "Configuración típica de un sistema ECDIS con back up" (Svilicic, Brčić, Žuškin, & Kalebić, 2019, pág. 232)

El sistema de backup del ECDIS está regulado por las normas OMI para garantizar navegación segura en caso de fallo del ECDIS (OMI SOLAS 2014, IMO MSC.232(82) 2006, IMO MSC.282(86) 2009). La función de un sistema de backup ECDIS es permitir asumir con seguridad las funciones del ECDIS, así como garantizar una navegación segura el resto del viaje.

5.4.2. Vulnerabilidades principales de ECDIS.

Al funcionar el software de ECDIS en un ordenador con sistemas operativos antiguos donde no suelen recibir actualizaciones, los ordenadores que ejecutan el programa son susceptibles de ser atacados con inyección de código malicioso o con vulnerabilidades endémicas de esos sistemas operativos lo que puede llevar a sufrir ataques de malware como

el ransomware, que podrían cifrar el ordenador que aloja el programa y dejarlo fuera de servicio.

"*La vulnerabilidad crítica detectada está relacionada con la versión vulnerable de Server Message Block (SMB) versión 1, alertando de que se requiere la instalación inmediata de un conjunto de parches de seguridad liberados por el proveedor es necesaria (Microsoft, 2018). La vulnerabilidad del servicio SMB es particularmente interesante para la industria marítima debido a uno de los incidentes de ciberseguridad marítima más reconocidos, el ataque NotPetya a la empresa de transporte de contenedores Maersk (CERT.be, 2018). NotPetya es un programa malicioso de ransomware que se propagó rápidamente por todo el mundo utilizando vulnerabilidades en el protocolo SMB v1 (US-CERT, 2018)*". (Svilicic, Brčić, Žuškin, & Kalebić, 2019, pág. 233)

Además de los problemas endémicos de los sistemas que alojan el software, las cartas electrónicas empleadas para actualizar los ECDIS son susceptibles a inyecciones de código a través del servidor "Apache" donde están alojadas.

También vulnerabilidades de cruces de directorios, lo que permite tras inyectar código malicioso en el propio archivo de la carta electrónica e introducir esta carta en el sistema ECDIS, robar información del dispositivo, como datos de la red, números de serie o contraseñas.

Por último, inyecciones de código de HTTP. Lo cual permite al atacante dar órdenes al sistema ECDIS para borrar, cambiar o alterar archivos en la memoria de ECDIS o incluso modificaciones de los valores de los sensores, para confundir al sistema e introducir variaciones en la ruta, enmascarar áreas restringidas a la navegación entre otras.

"*Traspaso de directorios: Se descubrió que ECDIS ejecutaba un servidor Web Apache local que era vulnerable a un ataque transversal de directorio. Esta debilidad permitía a NCC navegar, listar y descargar cualquiera de los archivos almacenados en la máquina Windows 7.*

Métodos HTTP peligrosos: El servidor web Apache de ECDIS que se ejecutaba en el puerto TCP 50000 permitía los métodos HTTP PUT y DELETE. Esta vulnerabilidad permitía subir, borrar o reemplazar cualquier archivo localizado en el sistema ECDIS Windows 7.

Software de servidor web Apache obsoleto: El sistema ECDIS ejecutaba un software de servidor web Apache obsoleto que tenía múltiples vulnerabilidades y debilidades asociadas con él, tales como la vulnerabilidad de cruce de directorio y denegación de servicio. Además, se descubrió que se utilizaba la versión 2.0 de Apache Xerces, que también presentaba numerosas vulnerabilidades." (NCC GROUP, 2014)

5.4.3. Estrategias de mitigación de las ciber-amenazas en ECDIS.

El uso de lectores de metadatos, que comprueben la autoría de las cartas electrónicas, así como quien ha modificado el contenido de la misma es una práctica recomendable antes de cada actualización de cartas electrónicas. Además de eso, mantener los ordenadores donde corren los ECDIS, con antivirus y los cortafuegos actualizados es una buena práctica que puede prevenir que aquellas cartas que no cuenten con firma digital sean reconocidas por el sistema. También exigir a los fabricantes actualizaciones completas de todo el sistema, tanto del software ECDIS como de la propia máquina.

Por último, es recomendable cerrar los puertos virtuales que estarían dedicados a la actualización remota o monitoreo desde la empresa que fabrica el dispositivo, ya que cualquier puerto abierto podría ser una puerta de entrada para un atacante, donde podría hacerse pasar además por fabricante y posiblemente teniendo permisos de administrador en el sistema.

5.5. VSAT (Very Small Aperture Terminal).

5.5.1. Estructura de los VSAT.

La tecnología VSAT (Very Small Aperture Terminal) se utiliza en el ámbito marítimo para proporcionar comunicaciones bidireccionales por satélite, incluyendo servicios de internet, datos y telefonía. En el mercado marítimo, las soluciones VSAT suelen ser suministradas como un paquete completo que incluye el segmento de espacio satelital, equipos y servicios de telefonía e internet.

Históricamente, los servicios VSAT en el ámbito marítimo han utilizado bandas de frecuencia Ku y C para el mercado comercial, utilizando satélites en órbita geoestacionaria (GEO). Dado que los buques están en constante movimiento y los satélites están en ubicaciones fijas en el espacio, se requieren antenas VSAT estabilizadas con capacidad de seguimiento. Estas antenas suelen tener un diámetro de hasta 2,4 metros y suelen estar ocultas dentro de una cúpula. La velocidad de transmisión de datos en los sistemas VSAT marítimos suele variar entre 64 Kbps y 8 Mbps, aunque también pueden ofrecerse velocidades más bajas o más altas.

Un sistema remoto de VSAT marítimo consta típicamente de dos partes:

- Una antena y un transceptor ubicados en la parte exterior del buque, generalmente dentro de una cúpula. En el sector marítimo, esto se conoce como la "unidad sobre cubierta" (Above Deck Unit, ADU).

- Una unidad interior que interactúa con la unidad exterior y controla la antena. En el sector marítimo, esto se conoce como la "unidad bajo cubierta" (Below Deck Unit, BDU).

Estas dos partes trabajan en conjunto para proporcionar una conectividad confiable a bordo de los buques, permitiendo comunicaciones satelitales bidireccionales para diversas aplicaciones, como acceso a internet, transferencia de datos y servicios telefónicos.

5.5.2. Frecuencias de los VSAT.

Existen tres bandas de radiofrecuencia VSAT en las que operan los satélites de comunicaciones y militares. Estas bandas de frecuencia determinan la calidad del enlace y la zona de cobertura:

- *"La banda C se utiliza principalmente para comunicaciones de voz y datos, así como para backhauling. Debido a su menor potencia, requiere una antena más grande que la banda Ku, normalmente de 2,4 m para uso marítimo. Sin embargo, debido a su menor rango de frecuencias, funciona mejor en condiciones meteorológicas adversas en tierra. Además, la banda C suele tener grandes haces y permite dar cobertura "mundial" con sólo tres satélites.*
- *La banda Ku se utiliza normalmente para el acceso directo del consumidor al hogar, aplicaciones de educación a distancia, conectividad minorista y empresarial, además de marítima. El tamaño de las antenas es mucho menor que en la banda C, ya que la mayor frecuencia permite obtener una mayor ganancia con antenas más pequeñas. Las redes en esta banda son más vulnerables a la lluvia, sobre todo en zonas tropicales.*
- *La banda Ka se utiliza principalmente para la banda ancha bidireccional y las redes militares. Las antenas parabólicas de la banda Ka pueden ser mucho más pequeñas y suelen tener un diámetro de entre 60 cm y 1,2 metros (de 2' a 4'). La potencia de transmisión es mucho mayor que en las bandas C, X o Ku. Debido a las frecuencias más altas de esta banda, es más vulnerable a la calidad de la señal."*
  (MARLINK, 2019)

5.5.3. Estrategias de mitigación de los ciberataques en VSAT.

Con el uso generalizado de VSAT en la industria marítima moderna, algunos aspectos de la red VSAT, como la transmisión transparente y la apertura, deben mejorarse para contrarrestar las amenazas a la seguridad, especialmente el acceso no autorizado y los

ataques de interceptación. En 2014, IOActive probó varios VSAT de diferentes proveedores y concluyó que, dado que utilizaban la transmisión en texto plano sin autenticación, cifrado, seguridad o verificación de la información personal, todos los dispositivos probados eran vulnerables en los niveles de implementación. Como resultado de la débil protección, los atacantes pueden enviar señales falsas o código malicioso al dispositivo para inutilizarlo o comprometer el sistema, impidiendo que el barco navegue con seguridad.

El riesgo real es que las interfaces de red VSAT pueden encontrarse en Internet utilizando herramientas como el Shodan Ship Tracker. Esto puede revelar información valiosa y sensible, como nombres de marcas, códigos de productos y otros datos que podrían utilizarse en ciberataques. La información estándar suele estar disponible en los sitios web de los proveedores, y muchos terminales siguen utilizando la misma configuración de fábrica, incluidos el nombre de usuario y la contraseña del servidor. Un atacante puede alterar las coordenadas y la configuración del GPS, así como descargar software malicioso si encuentra una interfaz VSAT abierta, y esto permite seguir pirateando la red y proporcionar acceso a los sistemas de gestión críticos.

5.6. RADAR (RAdio Detection And Ranging).

El radar marino es un sistema de ayuda a la navegación que se utiliza de manera obligatoria en los buques. Su principal función es la identificación, seguimiento y posicionamiento de buques, incluyendo el propio buque, con el propósito de cumplir con las regulaciones COLREG (Reglas de Navegación Marítima para Prevenir Abordajes) y garantizar una navegación segura de un punto a otro.

5.6.1. Bandas de frecuencia en los sistemas RADAR.

El radar marino se divide en dos bandas de frecuencia: la banda X, que opera a una frecuencia de 10 GHz, y la banda S, que opera a una frecuencia de 3 GHz. La banda X, al tener una frecuencia más alta, proporciona una imagen más clara y una mejor resolución en general. Por otro lado, la banda S se utiliza especialmente en condiciones de lluvia o niebla, así como para la identificación y seguimiento de objetivos.

El uso del radar marino es esencial para la seguridad marítima, ya que permite a los navegantes detectar otros buques y objetos en el entorno, lo que ayuda a prevenir colisiones y garantizar una navegación segura en todo momento. Además, el radar marino también proporciona información sobre la distancia, la velocidad relativa y la dirección de los buques

cercanos, lo que ayuda en la toma de decisiones para evitar abordajes y mantener el cumplimiento de las regulaciones marítimas.

5.6.2. Amenazas al sistema RADAR.

Aunque las señales de radar son más difíciles de interrumpir que las de los satélites, siguen siendo susceptibles a las interferencias y a los ataques DDoS (Distributed Denial of Service). Por consiguiente, los RADAR son susceptibles a técnicas de jamming donde un atacante que genera una señal idéntica a la empleada por el sistema RADAR, dirige esa señal al buque objetivo, a razón de apantallar parte del muestreo, o bien generando una zona de sombra como la que se podría generar por de una chimenea que se encuentra por encima del nivel del radar o, al contrario, dejando una zona de la muestra completamente en blanco con el objetivo de esconder otros buques u obstáculos.

En el caso de un ciberataque el radar puede proporcionar información falsa sobre los objetos cercanos debido a los falsos ecos causados por ondas de radar externas. Esta información incorrecta puede provocar abordajes.

Es importante tener en cuenta que mientras el radar y otras frecuencias del espectro electromagnético son susceptibles a la interferencia basada en el ruido o a los ataques de suplantación más avanzados, los mecanismos para lograr el mismo efecto varían significativamente entre los sistemas

5.7. CCTV ó VSS (Video Sulveillance Systems).

Los sistemas de videovigilancia tienen un papel fundamental en la navegación, operatividad y seguridad de los buques. Estos sistemas se emplean mayoritariamente para monitorizar, controlar y realizar tanto operaciones críticas de un buque, como puede ser el atraque en puerto, como controlar zonas críticas como las salas de máquinas o proteger a la tripulación de polizones o piratas.

Sin embargo, los sistemas de CCTV se han visto comprometidos por sus vulnerabilidades.

5.7.1. Buffer overflow en sistemas de CCTV

Los investigadores de Bitdefender descubrieron que dos modelos de cámaras de CCTV (PrivacyPC, Craig Heffner, s.f.), utilizadas en los barcos modernos, son vulnerables a

fallos de desbordamiento de búfer. Al explotar esta vulnerabilidad, los investigadores pudieron rastrear las actividades de la cámara pirateada y sobrescribir las contraseñas.

"*El buffer overflow o desbordamiento de buffer, es un problema de seguridad de la memoria en donde el software/programa no considera o no verifica sus límites de almacenamiento. Entonces, la memoria del programa recibe una cantidad de datos mayor a la que realmente puede procesar de acuerdo a cómo fue desarrollado. Además de desembocar en problemas de funcionamiento de dicho programa o que, simplemente, se detenga inesperadamente."* (REDES ZONE, Lorena Fernández, 2020)

Estos fallos de desbordamiento pueden dar lugar a vulnerabilidades y fallos que pueden ser aprovechados por ciberdelincuentes. Estas debilidades en la seguridad pueden permitir la ejecución de código malicioso y dar lugar a diversos tipos de ataques.

Si el sistema presenta una vulnerabilidad que permite la ejecución remota de código, un atacante podría aprovecharla para ejecutar malware en el sistema comprometido. Esto podría permitir al atacante llevar a cabo ataques adicionales, como ataques de denegación de servicio distribuido (DDoS) para bloquear el servicio, inyecciones SQL para comprometer bases de datos, ataques de phishing si se obtienen datos personales de los usuarios, o incluso filtraciones de datos sensibles de la red de cámaras del buque.

5.7.2. Estrategias de mitigación en sistemas de CCTV

Contraseñas sólidas, redes securizadas y pentesting del sistema de forma continuada son las directrices principales para proteger los sistemas de circuito cerrado de televisión cuando estos funcionan bajo una estructura de red ethernet.

En cuanto al problema del buffer overflow se traslada a los proveedores y desarrolladores de los equipos donde estos deben emplear estándares de desarrollo de código seguro.

Es importante destacar que el desarrollo seguro de software es fundamental para prevenir este tipo de fallos y mitigar los riesgos de seguridad. Las buenas prácticas de seguridad, como el uso de técnicas de codificación segura, la validación adecuada de entradas de usuario, la gestión correcta de permisos y privilegios, y la implementación de mecanismos de autenticación y cifrado adecuados, son fundamentales para reducir la superficie de ataque y proteger los sistemas y los datos de los usuarios. (Bugeja, Jönsson, & Jacobsson, 2018)

Además, es esencial que los desarrolladores y las organizaciones realicen pruebas de seguridad y evaluaciones periódicas para identificar y corregir posibles vulnerabilidades en

sus sistemas y aplicaciones. La seguridad debe ser considerada desde las etapas iniciales del desarrollo de software y debe ser una preocupación continua a lo largo del ciclo de vida del producto para garantizar la protección de los usuarios y la integridad de los datos.

5.8. NAVTEX y los avisos a navegantes.

NAVTEX (del inglés NAVigational TEXt Messages) es un sistema utilizado para la transmisión y recepción automatizada de información sobre seguridad marítima. Su objetivo principal es difundir radioavisos náuticos y proporcionar información crítica para la navegación segura de los buques en el mar.

NAVTEX utiliza la telegrafía de impresión directa de banda estrecha para enviar mensajes a los receptores NAVTEX instalados en los buques. Estos mensajes contienen información relevante, como el estado del tiempo, alertas meteorológicas, datos de mareas, zonas de navegación restringida y otros avisos importantes para la seguridad marítima.

El sistema NAVTEX forma parte del Sistema Mundial de Socorro y Seguridad Marítima (SMSSM) y se utiliza en todo el mundo para proporcionar información actualizada y urgente a los navegantes. Al ser un servicio automatizado, los buques equipados con receptores NAVTEX pueden recibir y procesar la información de manera rápida y eficiente, lo que contribuye a mejorar la seguridad en el entorno marítimo.

5.8.1. Señal y frecuencia de transmisión NAVTEX.

Los coordinadores NAVTEX son responsables de supervisar los mensajes transmitidos por cada estación, asegurándose de que se ajusten a la información contenida en cada mensaje y a la cobertura geográfica requerida. Esto permite a los usuarios decidir si desean recibir mensajes únicamente del transmisor que cubre la zona marítima en la que se encuentra su buque, o si prefieren recibir mensajes de varios transmisores según corresponda.

El servicio NAVTEX utiliza una frecuencia única y se organiza de manera que las transmisiones de las estaciones designadas dentro de cada zona NAVAREA/METAREA se realicen de forma sincronizada para evitar interferencias mutuas.

Esta señal tiene un rango de hasta 400 millas náuticas.

Los mensajes NAVTEX se transmiten mediante modulación binaria por desplazamiento de frecuencia (BFSK) a 100 bits/s y un desplazamiento de frecuencia de 170

Hz. Los caracteres se codifican utilizando el juego de caracteres CCIR 476 de 7 bits, que permite una detección básica de errores. La corrección de errores hacia delante (FEC) se consigue repitiendo cada carácter tras un retardo de 3 caracteres, es decir, ...ABCDE... se convierte en ...A.B.CADBEC.D.E... Es el mismo formato que el formato SITOR-B. (Frisnit Navtex Decoder, s.f.)

El Navtex internacional se refiere a la transmisión coordinada y recepción automática de información sobre seguridad marítima en la frecuencia de 518 kHz, utilizando la telegrafía de impresión directa de banda estrecha en inglés.

Por otro lado, el Navtex nacional se utiliza para la transmisión y recepción de información sobre seguridad marítima en frecuencias distintas a la de 518 kHz (490 kHz en el territorio nacional) y en los idiomas determinados por las Administraciones correspondientes. El servicio NAVTEX permite que los buques equipados con receptores especializados reciban de manera automática los radioavisos náuticos y meteorológicos, así como cualquier información urgente relacionada con la seguridad marítima, presentándolos visualmente o imprimiéndolos. (Salvamento Maritimo , 2021)

5.8.2. Amenazas al sistema NAVTEX.

El sistema Navtex es vulnerable a ataques de jamming o de denegación de servicio, donde un atacante puede bloquear la frecuencia de transmisión de una zona específica.

La tripulación puede ser víctima de un ataque de phishing, donde un atacante envía mensajes o partes falsos para alentar a decisiones erróneas por parte de la tripulación que podrían poner en peligro el buque o desembocar en pérdidas económicas.

5.8.3. Estrategias de mitigación en el sistema NAVTEX.

En ambos casos, donde o bien el sistema este comprometido por un ataque de jamming o se tengan sospechas de que el parte recibido pueda ser falso, se recomienda cambiar de frecuencias de nacional a internacional, o viceversa, con el objetivo de contrastar la información o en el caso del jamming de descartar una avería del dispositivo y cerciorarse de que el buque es víctima de un ciberataque.

Además de esto es recomendable revisar los avisos a navegantes por internet, ya que estos se publican semanalmente, lo que puede garantizar que la información recibida es fidedigna. (Instituto Hidrográfico de la Marina, s.f.)

5.9. VDR “caja negra”.

La "caja negra" marítima, (voyage data recorder, VDR), consta de dos componentes principales: una unidad de recopilación de datos y una unidad de almacenamiento protegida. El sistema se encuentra a bordo de la embarcación, mientras que una cápsula protectora está montada en cubierta y contiene una memoria de estado sólido de alta capacidad.

La cápsula está diseñada para resistir diversas condiciones adversas, como incendios, presión en aguas profundas, impactos y penetración.

La unidad de recopilación de datos registra de manera continua una duración de 12 horas de la actividad a bordo, incluyendo información como la fecha y hora, la posición del buque, la velocidad, el rumbo, el audio del puente, las comunicaciones VHF relacionadas con las operaciones, la información del radar que muestra la imagen en tiempo real, la profundidad bajo la quilla, el ángulo del timón, las órdenes y respuestas del motor, el estado de apertura del casco, el estado de las puertas estancas y los cortafuegos, el control de la tensión del casco, y la velocidad y dirección del viento.

5.9.1. Ataques dirigidos vía USB al sistema de VDR.

Una investigación por la universidad de Plymouth en Reino Unido, (Harish, Tam, & Jones, 2022) planteó un escenario donde un sistema de VDR es vulnerado teniendo acceso puntual al buque o bien gracias a un ataque dirigido. Gracias a un dispositivo USB denominado Rubber Ducky. USB Rubber Ducky fue creado por una empresa de ciberseguridad, Hak5. La herramienta ganó popularidad en la comunidad de seguridad debido a sus propiedades, como la facilidad de uso y potentes capacidades. Cuando se conecta físicamente, el Rubber Ducky inyecta pulsaciones de teclas en el ordenador al que está conectado. Los usuarios pueden especificar las combinaciones de teclas que desean utilizando un lenguaje de programación llamado Ducky Script. El script se escribe en un archivo de texto y luego se transfiere a una tarjeta Secure Digital (SD) formateada con la tabla de asignación de archivos (FAT). Este dispositivo puede transmitir los datos robados vía WIFI, almacenarlos en la memoria o realizar inyecciones de código.

En el experimento, los investigadores prepararon un programa por el cual con solo introducir el USB en el ordenador de VDR, el programa robaba los datos del sistema, como números de serie, sistema operativo y datos guardados en la VDR como audio o rutas por las que ha navegado el buque.

Tras realizar el robo de los datos de la VDR, el programa dejó un script latente el cual tras 24 horas cifraba los datos de la VDR y la dejaba inutilizada. Los investigadores aclaran

en el artículo que el script podría también modificar los datos de la caja negra en vez de cifrarlos.

Tras el robo de datos el análisis del sistema desveló que ese sistema en particular de VDR era susceptible a una vulnerabilidad de Eternal Blue. "*El PC de la VDR ejecutaba el sistema operativo de Windows Embedded Standard 7 y un análisis Nmap (Network Mapper) descubrió que los puertos 139 y 445 estaban abiertos. Se descubrió que el PC VDR era vulnerable al exploit Eternal Blue, que aprovecha una vulnerabilidad de ejecución remota de código en servidores Microsoft SMBv1 con la entrada de vulnerabilidad CVE-2017-0143 en la base de datos Common Vulnerabilities and Exposures (CVE) [26]. Esta vulnerabilidad tiene una puntuación CVSS (Common Vulnerability Scoring System) de 8,1 (ALTA) y el famoso ataque WannaCry utilizó este exploit para propagar su infección*." (Harish, Tam, & Jones, 2022, pág. 78)

En resumen, el propio sistema operativo es vulnerable a malware de alto riesgo por emplear sistemas operativos obsoletos.

5.9.2. Estrategias de mitigación en los sistemas de VDR.

"*La ciberseguridad de los equipos marítimos está en pañales, y existe poca bibliografía sobre los registradores de datos de viaje y aún menos investigación sobre su seguridad. Gran parte de la bibliografía disponible son informes de accidentes en los que se han visto implicados RDT, publicados por organizaciones como la MAIB. Otros artículos analizan la investigación desde un punto de vista forense digital y sugieren formas de mejorar la seguridad de los datos de las grabadoras de datos de viaje, como el artículo sobre el naufragio del Costa Concordia* (Piccinelli & Gubian, 2013)*. La integridad y la disponibilidad de los datos son propiedades críticas de la tríada Confidencialidad, Integridad y Disponibilidad (CIA) para dispositivos como las grabadoras de datos de viaje. Un estudio de* (Seong & Gwan-Hyung , 2019) *desarrolló un algoritmo de registro de datos basado en hash, en el que la hora y la fecha del mensaje se utilizan para generar una clave de autenticación y una función hash se utiliza para generar una clave que, combinada con el mensaje original, puede utilizarse para comprobar la integridad del mensaje. La investigación para mejorar el Módulo de Alarma Remota (RAM) conectado a la VDR sería buena para alertar a la tripulación y a la gente del puente si algo va mal en el sistema* (Jonggu , Bokjin, Deokhwan , & Hangsoeb , 2009)*. Es necesario mejorar la seguridad de los VDR tanto desde el punto de vista técnico como normativo, a tenor de la escasa investigación realizada en este ámbito. En los próximos años, los VDR estarán más conectados, lo que permitirá nuevos vectores de ataque, como el acceso Wi-Fi y una mala configuración de la red, ampliando la superficie de ataque. El cifrado de los*

datos críticos y el despliegue de métodos de control de acceso ayudarían a proteger en cierta medida la confidencialidad de las pruebas. También debe restringirse el uso de los puertos USB, además de señalar cuándo se conecta un dispositivo USB al sistema." (Harish, Tam, & Jones, 2022, pág. 78)

5.10. INMARSAT- C.

Este sistema de comunicación marítima ofrece servicios de shore-to-ship, de ship-to-shore y de ship-to-ship. Su capacidad de almacenamiento y transmisión permite utilizarlo para télex, fax, datos o correo electrónico. Es una pieza clave del Sistema Mundial de Socorro y Seguridad Marítimos (SMSSM).

El Convenio Internacional para la Seguridad de la Vida Humana en el Mar (SOLAS) obliga a todos los buques mercantes de más de 300 toneladas de arqueo bruto (TRB) a llevar equipos conformes con el SMSSM.

5.10.1. Señal y frecuencia de transmisión INMARSAT-C,

El servicio funciona mediante un transceptor Inmarsat-C o un minitransceptor C de menor potencia. Los datos se transfieren entre MES y LES a una velocidad de 600 bits/segundo. Las frecuencias de transmisión (TX) son 1626,5MHz -1645,5MHz y las de recepción (RX) son 1530,0MHz - 1545,0MHz.

5.11. Radios GMDSS.

La herramienta de comunicación más empleada en los buques son las radios. Estos equipos vienen descritos por las reglas y regulaciones del Sistema Mundial de Socorro y Seguridad Marítimos (de sus siglas en inglés GMDSS). Estos equipos vienen con unos requerimientos en cuanto a frecuencias de trabajo y en función de las aguas por las que navega el buque. Podemos encontrar equipos de frecuencia media (MF), alta frecuencia (HF) o muy alta frecuencia (VHF). Todas las especificaciones de estos equipos vienen definidas en el código SOLAS en su capítulo 4, "Radiocomunicaciones" (SOLAS Cap. 4º, s.f.)

En nuestro caso se empleará un equipo de VHF para explicar las frecuencias y las vulnerabilidades del equipo, el cual es obligatorio para todos los buques, independientemente de las aguas en las que navegue.

5.11.1. Señal y frecuencia de transmisión VHF GMDSS,

Los equipos de VHF (very high frecuency) trabajan con ondas métricas en la banda de frecuencias entre los 30 y los 300 Megahercios (MHz). La banda de frecuencias reservada para las comunicaciones marítimas está entre los 156 y los 174 MHz.

"*Regla 7 Equipo radioeléctrico - Generalidades 1. Todo buque ira provisto de: .1 una instalación radioeléctrica de ondas métricas que pueda transmitir y recibir; .1.1 mediante LSD (llamada selectiva digital) en la frecuencia de 156,525 MHz. (canal 70). Será posible iniciar la transmisión de las alertas de socorro en el canal 70 en el puesto desde que se gobierne normalmente en buque; y .1.2 mediante radiotelefonía en las frecuencias de 156,300 MHz. (canal 6), 156,650 MHz. (canal 13) y 156,800 Mhz. (canal 16);"* (IMO, International Maritime Organization, 1976)

Varias de estas frecuencias tienen ciertos usos específicos y escuchas permanentes. El gobierno español mantiene un listado en línea de las diferentes frecuencias de escucha en los diferentes sistemas en función de la zona de navegación. (Ministerio de Transportes, Movilidad y Agenda Urbana. , s.f.) (Escuela PdR, s.f.)

5.11.2. Jamming de señal a los equipos de VHF, HF y MF.

La interferencia de RF es el concepto utilizado para interrumpir la transmisión de una determinada estación de radio o satélite. Como resultado de la interferencia de señales de radiofrecuencia, la señal inalámbrica deseada no puede recibirse o descodificarse correctamente en la estación receptora inalámbrica.

Las condiciones para generar una señal de jamming son; La frecuencia y la modulación de la señal del atacante debe ser igual a la frecuencia de recepción del equipo que se quiere atacar y la señal del atacante debe ser más potente que las señales que recibiría normalmente el dispositivo comprometido

En esencia un circuito LC con la suficiente ganancia es capaz de inhibir la recepción de señal de un sistema de radiocomunicaciones.

5.11.3. Ataques de spoofing en llamada selectiva digital, LSD.

En el siguiente trabajo, (Forsberg, 2022) se describe el procedimiento para simular una señal de emergencia LSD de "hombre al agua" y transmitirla como falsa información. El experimento concluye con la recepción de un mensaje en VHF falso, el cual en un caso real podría llevar a una mala toma de decisiones, desviando un buque de su ruta y llevando este a aguas poco profundas donde podría encallar.

El método utilizado en el experimento consistió en crear un script python para generar mensajes según la especificación DSC y luego enviarlos por radio con un SDR, a saber, un HackRf.

5.11.2. Estrategias de mitigación en sistemas de Radio de GMDSS.

- Cifrado en mensajes de emergencia. Las transmisiones realizadas a través de radios HF pueden contar con protección mediante diversas opciones, como DES (Data Encryption Standard) 56 y AES (Advanced Encryption Standard) 256. Estas opciones de encriptación aseguran que las comunicaciones sean codificadas utilizando algoritmos indescifrables. Para lograr esto, se utiliza una clave única que solo el sistema del destinatario posee, lo que garantiza que el mensaje solo esté disponible y comprensible para el receptor adecuado. Para cualquier otra persona que intercepte la transmisión, el contenido será ininteligible.
- Llamadas seguras. Esta opción ofrece una conexión segura mediante un PIN de cuatro dígitos en cada radio. La comunicación en una red de este tipo puede ser punto a punto o punto a multipunto, permitiendo llamadas de grupo. Siguiendo un enfoque similar a los sistemas militares de salto de frecuencia, utiliza un canal asignado específico y puede cambiar de frecuencia, o "saltar", entre 4 y 15 veces por segundo, según la elección del usuario.
- Salto de frecuencias Este método utiliza un conjunto de frecuencias de emisión que cambian rápidamente tanto en el extremo emisor como en el receptor. Este patrón de "saltos" sólo es perceptible para las unidades preconfiguradas para comunicarse entre sí. (Airport Technology, 2022)

5.12. Radiobaliza de emergencia (Emergency Position Indicating Radio Beacon, EPIRB).

Dispositivo para alertar a los servicios de búsqueda y salvamento en caso de emergencia en el mar. Se trata de un equipo de rastreo que transmite una señal en una banda específica para localizar un bote salvavidas, una balsa salvavidas, un buque o personas en peligro.

5.12.1. Tipos de EPIRB.

- COSPAS-SARSAT- Las EPIRBS del sistema COSPAS-SARSAT funcionan en las bandas de 406,025 MHz y 121,5 MHz y son aplicables a todas las zonas marítimas.
- INMARSAT E- La banda de 1,6 GHz es en la que funciona esta EPIRB. Son aplicables para las zonas marítimas A1, A2 y A3.
- VHF CH 70- Funciona en la banda de 156.525 MHz y sólo es aplicable en la zona A1.

Estas EPIRB tienen una distinción en categorías en función de su encendido, donde las EPIRB de categoría I pueden activarse manual o automáticamente, mientras que las de categoría II sólo manualmente. Sin embargo, ambos dispositivos transmiten una frecuencia de 406MHz.

Por último, las EPIRB se pueden diferenciar si están equipadas con un sistema de GNSS o no. En el caso de estar equipadas con un GNSS los datos de posición son mucho más precisos, facilitando los trabajos de búsqueda y rescate. (Salvamento Maritimo , 2017)

5.12.2. Funcionamiento y señal de la EPIRB.

El dispositivo contiene dos radiotransmisores, uno de 5 vatios y otro de 0,25 vatios, cada uno de los cuales funciona a 406 MHz, la frecuencia internacional estándar que suele utilizarse para las señales de socorro. El radiotransmisor de 5 vatios está sincronizado con un satélite meteorológico GOES que gira alrededor de la Tierra en una órbita geosíncrona.

El COSPAS-SARSAT es un sistema internacional de búsqueda y salvamento por satélite fundado por Estados Unidos, Rusia, Canadá y Francia para detectar radiobalizas de emergencia.

Una EPIRB transmite señales al satélite. La señal consiste en un número de identificación cifrado (todo en código digital) que contiene información como la identificación del barco, la fecha del suceso, la naturaleza del incidente, los contactos de emergencia y la posición.

El UIN es un número de identificación único programado en fábrica en cada baliza. El número UIN consiste en una serie de 15 dígitos de letras y números que conforman la identidad única de la baliza. El UIN figura en una etiqueta blanca en el exterior de la baliza. El UIN también se denomina Hex ID.

El Terminal Local de Usuario (unidades receptoras de satélite o estaciones terrestres) calcula la posición del siniestro utilizando el desplazamiento Doppler (que es el cambio de frecuencia o longitud de onda de una onda, u otros eventos periódicos, para un observador que se mueve con respecto a su fuente).

El satélite transmite el mensaje digital a los servicios de emergencia, MRCC (Mission Rescue Co-Ordination Centre). Además, el MRCC es responsable de las operaciones SAR y supervisa la ejecución de la misión de rescate. (Marine In Sight, 2022)

5.12.3. Ciberseguridad en los sistemas EPIRB.

Los sistemas EPIRB son vulnerables a ataques de spoofing, phishing de señal y de DoS (denegación de servicio). La publicación, (Costin, Khandker, Turtiainen, & Hämäläinen, 2023) explica los diferentes ataques y hace especial hincapié en los ataques de spoofing donde se encuentran:

- Ataques básicos de spoofing, donde el atacante puede falsificar (parcial o totalmente) cualquier mensaje COSPAS-SARSAT válido y de aspecto legítimo. mensajes COSPAS-SARSAT. El receptor no puede detectar que se está produciendo dicha suplantación sin disponer de otro medio de verificación.
- Close-to-target Mimicry Spoofing: El atacante puede desplegar un dispositivo de suplantación cerca del objetivo, por ejemplo, utilizando un dron cerca del objetivo o incluso introducir en objetivo el transmisor falso. Emplearemos como ejemplo un buque. Debido a la posición del dron "close-to-target", cuando se emite una señal falsa COSPAS-SARSAT es difícil/imposible que el Centro de Coordinación SAR sepa que la que la señal ha sido falsificada y no proviene del buque al que se realiza el ataque. Desde el punto de vista del el Centro de Coordinación SAR, la alerta falsa esta geo-posicionada exactamente sobre el buque y que debería ser tratada como una señal de socorro real, desencadenando así la toda la cadena de eventos, comandos y acciones de la operación de salvamento. Este ataque es aún más difícil de detectar en condiciones meteorológicas adversas y de baja visibilidad.
- Overwhelming Spoofing: El atacante satura todo el sistema COSPAS-SARSAT con señales falsificadas, lo que puede ocurrir a escala mundial, nacional o regional, dependiendo de los objetivos, motivaciones, capacidades y recursos del atacante. Por ejemplo, esto puede lograrse de forma realista con un ejército de drones baratos que lleven un dispositivo de falsificación COSPAS-SARSAT en las ubicaciones GPS exactas donde se desea falsificar la señal. Se requiere precisión en la geolocalización, ya que los satélites utilizan multilateración (MLAT) en la señal de origen, y cualquier discrepancia con la ubicación GPS codificada en los paquetes podría utilizarse fácilmente para detectar y marcar estas señales como falsas.

  Aunque puede ser evidente para el Centro de Coordinación SAR que un ciberataque está en curso, puede ser difícil distinguir entre señales reales y falsas dado el

abrumador número de señales SAR entrantes, lo que plantea un riesgo de agotamiento de los recursos SAR o de priorizar erróneamente los objetivos.

5.12.4. Estrategias de mitigación en los sistemas EPIRB.

El mismo trabajo, (Costin, Khandker, Turtiainen, & Hämäläinen, 2023), propone 3 estrategias de mitigación para mejorar los sistemas EPIRB:

- *"Necesidad de autenticidad de los mensajes. Falta de firmas digitales seguras para la autenticidad de mensajes y protocolos a fin de evitar ataques de suplantación de identidad.*
- *Necesidad fortificar de los mensajes. Falta de secuencias/tokens aleatorios, únicos y no reutilizables en mensajes o protocolos que no se basen en "challenge-response" para evitar ataques de repetición.*
- *Necesidad de ID aleatorios y confidenciales. Generar los ID de cada dispositivo COSPAS-SARSAT (por ejemplo, EPIRB, PLB, ELT) de forma aleatoria (es decir, no secuencial, no predecible). Además, estos ID confidenciales (como parte de la protección de datos), para que los posibles atacantes potenciales no puedan encontrarlos fácilmente y tengan menos éxito."* (Costin, Khandker, Turtiainen, & Hämäläinen, 2023, pág. 6)

5.13. IT, ordenadores de gestión del buque.

En la industria marítima se emplean varios tipos de redes para la recopilación y procesamiento de los datos generados por las redes IT. De las más empleadas son: SHIPNET, SAFENET, System C3I, RICE 10, Ship2000 System, Smart Ship y TSCE.

Estas tecnologías tienen muchas vulnerabilidades de seguridad ya que el diseño y la configuración de los enlaces de comunicación entre las redes de "IT" prestan poca atención a los métodos de autenticación y encriptación, lo que hace que haya sistemas potencialmente vulnerables y obsoletos en Internet.

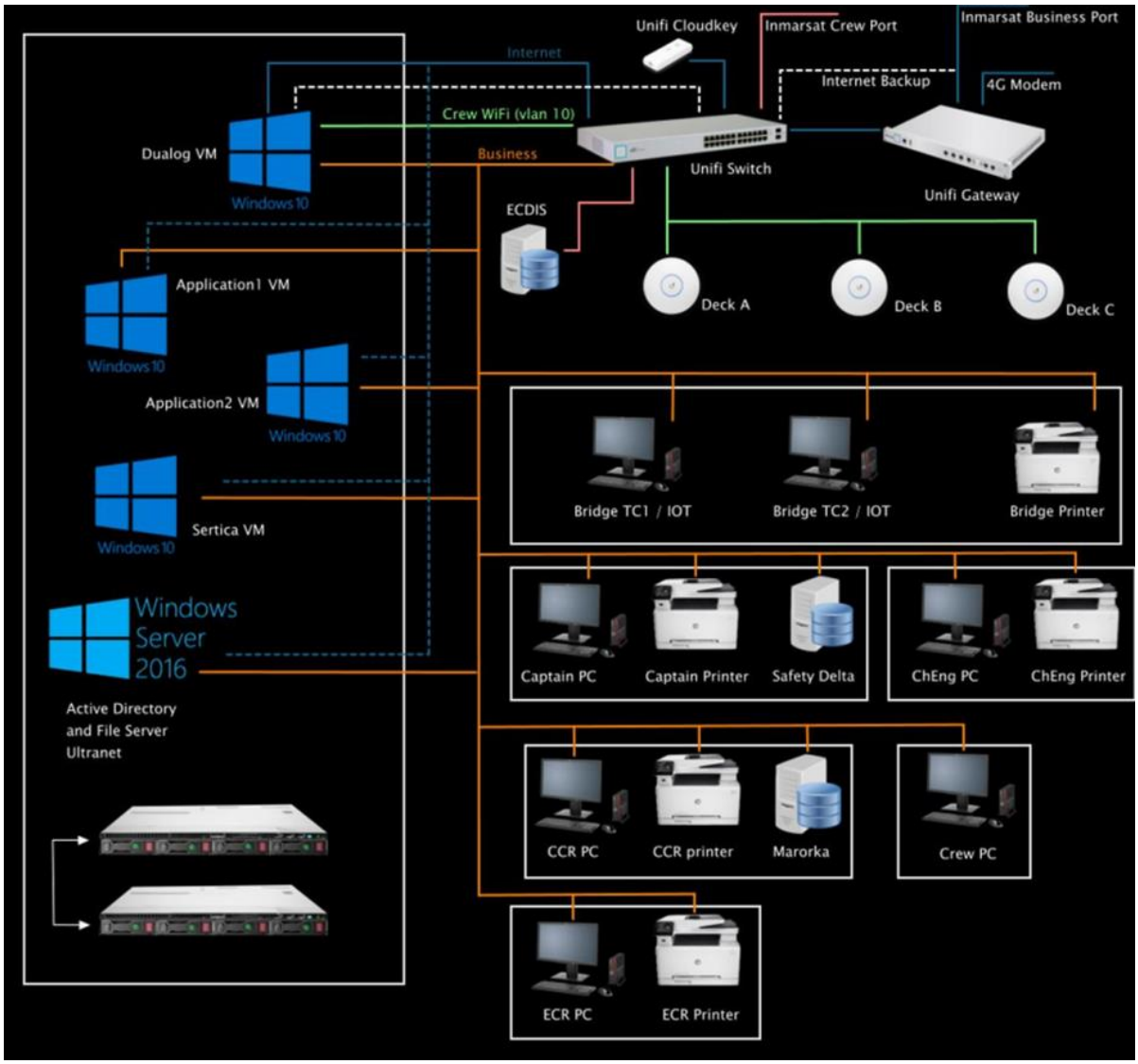
Actualmente muchos de los sistemas informáticos a bordo están conectados a instalaciones en tierra o tienen gestión y acceso remoto desde tierra, lo que aumenta el riesgo de amenazas sistemáticas y continuas. Las auditorías internas, la digitalización burocrática de los informes y partes, los requisitos legales y los requisitos de supervisión y gestión a distancia aumentan la necesidad de sistemas informáticos y de la interconectividad a la red en la industria naval moderna; sin embargo, estos sistemas aumentarán el tamaño de

exposición de ataque a los equipos de seguridad que se deben defender y crearán puntos de acceso adicionales que los atacantes podrían utilizar para entrar en el sistema del buque desde un fallo que tan siquiera está a bordo.

Por lo tanto, las vulnerabilidades de estos sistemas automatizados deben ser investigadas cuidadosamente. Además, las redes de control críticas internas deben estar aisladas de las redes informáticas y de Internet del buque en una zona segura.

Por otra parte, el factor humano se vuelve aún más difícil de prever con el complejo ecosistema interconectado en el sector marítimo. La falta de una cultura de ciberseguridad puede ser beneficiosa para cualquier atacante que quiera acceder a un buque y a sus sistemas a robar información real o interrumpir las operaciones del buque.

Ilustración 11 "Distribución típica de una red IT" (Hyra, 2019, pág. 59)



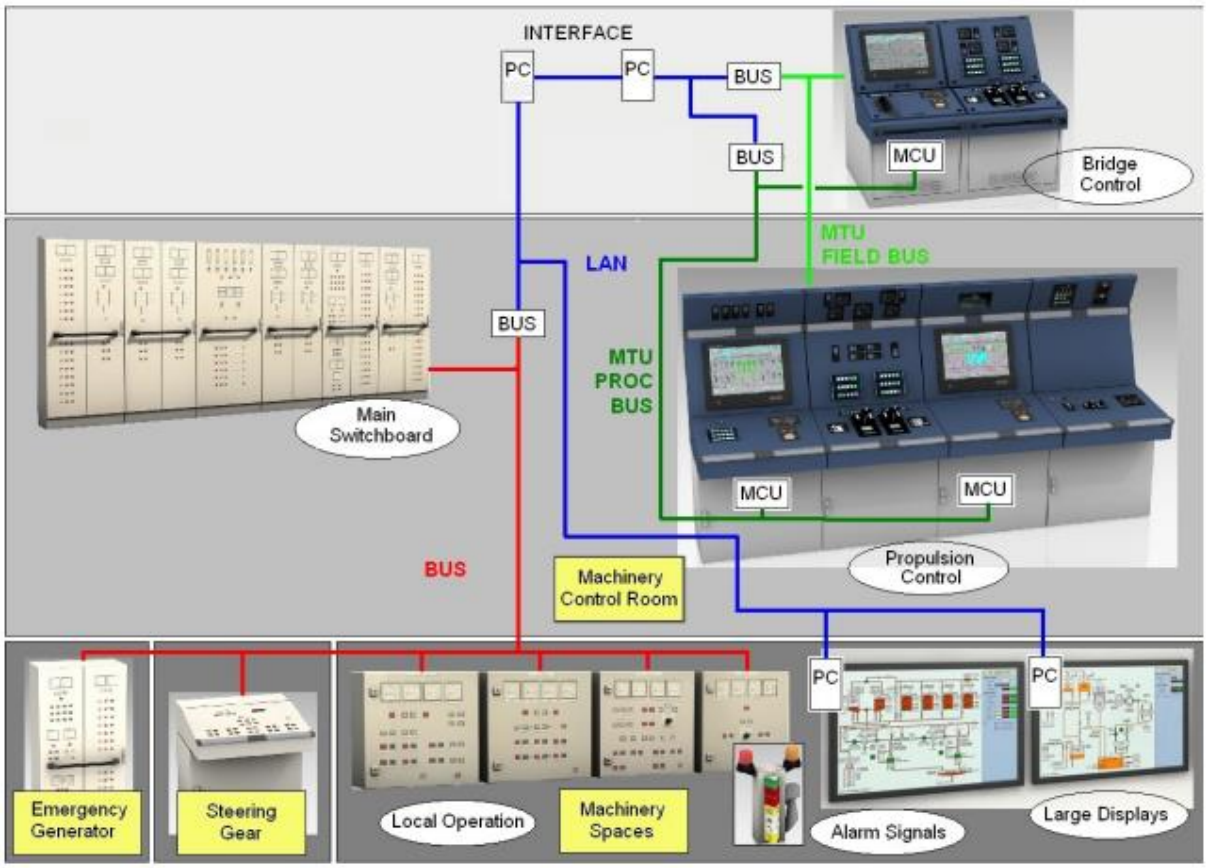
6. Ciberataques a los sistemas de control industrial, sistemas auxiliares, gobierno, propulsión del buque, protocolos de conexión entre sistemas y redes.

Los ciberataques a los sistemas de control industrial, sistemas auxiliares, gobierno y propulsión del buque representan una creciente preocupación en el entorno marítimo. Estos ataques tienen como objetivo comprometer la seguridad y el funcionamiento de los sistemas informáticos y de control utilizados en los buques. Desde el acceso no autorizado a sistemas críticos hasta el robo de información confidencial o la manipulación de datos, estos ataques pueden tener consecuencias graves, incluyendo la interrupción de las operaciones marítimas, la pérdida de control del buque e incluso poner en peligro la seguridad de la tripulación. Para contrarrestar esta amenaza, es crucial implementar medidas de seguridad sólidas, políticas claras de gestión de incidentes y estar al tanto de las normativas y estándares de seguridad cibernética en el sector marítimo. La protección de los sistemas marítimos es fundamental para garantizar un entorno seguro y confiable en los mares.

6.1. Red de sistemas de control de motor, planta eléctrica y gobierno del buque.

La red de sistemas de control de motor, planta eléctrica y gobierno del buque constituye una parte fundamental en la operación eficiente y segura de las embarcaciones. Estos sistemas están diseñados para supervisar y controlar el funcionamiento de los motores, la generación y distribución de energía eléctrica, así como la navegación y maniobras del buque. Esta red interconecta una variedad de dispositivos y sistemas críticos, permitiendo el monitoreo en tiempo real, la toma de decisiones y la respuesta adecuada ante situaciones operativas y de seguridad. La fiabilidad y la integridad de esta red son esenciales para garantizar un rendimiento óptimo, evitar averías catastróficas y garantizar la seguridad de la tripulación y la carga. Con el avance de la tecnología, también surge la necesidad de proteger esta red contra posibles ciberataques, lo que requiere implementar medidas de seguridad robustas y mantenerse actualizado sobre las mejores prácticas en el ámbito de la seguridad cibernética marítima. En resumen, la red de sistemas de control de motor, planta eléctrica y gobierno del buque desempeña un papel vital en el funcionamiento seguro y eficiente de las embarcaciones, y su protección y seguridad son aspectos fundamentales en la industria marítima.

Ilustración 12 "Interconexión de los sistemas de un buque" (Hyra, 2019, pág. 58)



En el caso de la imagen anterior podemos observar varias líneas que distribuyen la información y control entre los diversos paneles del buque. En este caso la línea azul, una red LAN, conecta todos los sistemas del buque gracias a convertidores de señal, marcados como BUS. Estos convertidores generalmente cambian la señal a los protocolos NMEA o CAN. La línea roja es la conexión entre los sistemas críticos del buque, gobierno, cuadros eléctricos principales y sistemas auxiliares como bombas, caldera y demás. La línea verde oscura es la conexión entre los paneles de control del puente y la sala de máquinas. De igual forma la línea verde claro es una conexión redundante.

La red de sistemas de control de motor, planta eléctrica y gobierno del buque está estrechamente relacionada con las redes de área local (LAN). En un buque, la LAN se utiliza para interconectar los diferentes sistemas y dispositivos de control, proporcionando una infraestructura de comunicación confiable y eficiente. La LAN permite la transmisión de datos críticos entre los sistemas de control de motor, planta eléctrica y gobierno, permitiendo el monitoreo en tiempo real, la coordinación de operaciones y la toma de decisiones informadas. Además, la LAN también puede conectar otros dispositivos a bordo, como sistemas de navegación, comunicaciones y entretenimiento. Es fundamental que la LAN esté diseñada y

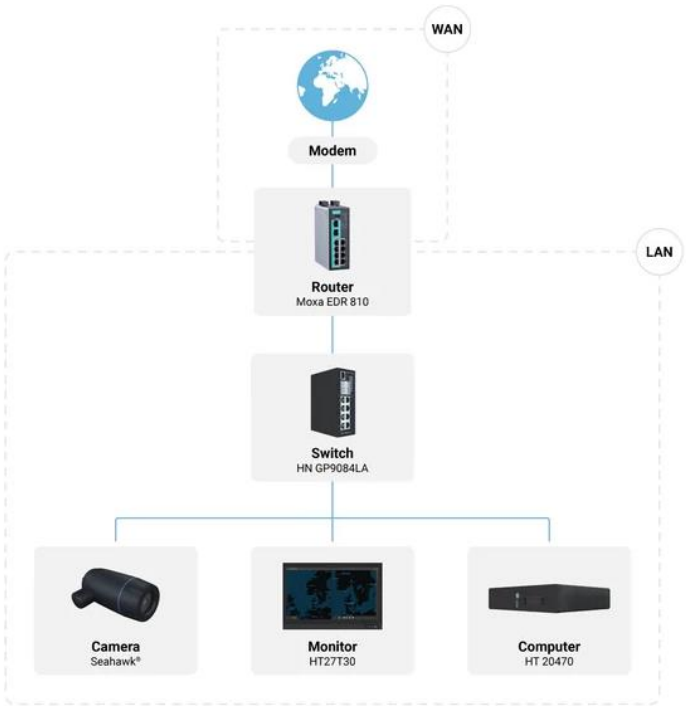
configurada adecuadamente para garantizar un rendimiento óptimo y una comunicación segura entre los sistemas del buque. Además, consideraciones como la redundancia, la seguridad de la red y la protección contra ciberataques también son relevantes tanto para la red de sistemas de control como para las redes LAN a bordo del buque.

6.2. Redes de área local, LAN.

"Una red de área local (LAN) es un conjunto de dispositivos conectados entre sí en una ubicación física, como un edificio, una oficina o un hogar. Una LAN puede ser pequeña o grande, desde una red doméstica con un usuario hasta una red empresarial con miles de usuarios y dispositivos en una oficina o escuela. Independientemente de su tamaño, la única característica que define a una LAN es que conecta dispositivos que se encuentran en un área única y limitada", (CISCO, 2020). En un buque las redes LAN son la estructura principal de comunicación entre ordenadores.

En la imagen siguiente podemos ver la diferencia entre una red LAN (Local Area Network) y una red WAN (Wide Area Network). La red dentro del buque se considerará red LAN, la comunicación con otra red fuera del buque se considera una red WAN. Un ejemplo sería la conexión de la red LAN del buque a través de internet con la red LAN de un proveedor. Se han conectado dos redes LAN a través de una red WAN.

Ilustración 13 "Estructura redes LAN y WAN" (Hatteland Tecnology, 2020)



6.2.1. Factores de riesgo en redes LAN.

Aunque una red LAN cerrada donde no se tenga acceso a internet parece un sistema completamente seguro a las amenazas externas, existen varios factores que podrían poner en riesgo la integridad del sistema.

- El uso de memorias USB para mover los archivos de estas redes a otros ordenadores es un factor de riesgo, ya que bajo un ataque dirigido este pen drive podría convertirse en un “caballo de Troya” e infectar la red LAN.
- Todos los dispositivos con conexión a internet que se añadan a la red LAN podrían significar una puerta de acceso al sistema. Caso bastante común, ya que en ciertas redes se requiere de un ordenador externo para configurar un nuevo dispositivo, sensor o controlador. Un ejemplo sería el de actualizar una red de PLC puesto que se ha añadido un nuevo dispositivo o sistema en el buque.

6.2.2. Técnicas de mitigación para redes LAN.

En este caso hablamos de buenas prácticas a realizar por la tripulación o los técnicos encargados del sistema.

- Formatear cualquier memoria externa que se vaya a emplear en la red LAN, de esta manera se garantiza que esta no este infectada y no contenga código malicioso que pudiera poner en riesgo los dispositivos dentro de la red.
- Los equipos de la red deberían tener una protección antivirus y actualizarse de forma manual al menos una vez a la semana.
- Un sistema de control de dispositivos para cada máquina, que impida la conexión de memorias USB u otros dispositivos de almacenamiento, salvo las que estén en una lista de dispositivos de confianza.
- Prohibición del uso de smartphones y otros dispositivos con conexión a Internet en el lugar donde se encuentra nuestra red aislada.
- Todos los dispositivos, ordenadores o sistemas fuera de la red que se requieran por mantenimiento deberían ser de uso exclusivo de esas funciones. Estos también deben tener un antivirus y mantener las actualizaciones al día.

6.3. Estándar Ethernet.

Ethernet es un estándar de red de área local (LAN) que permite la comunicación de datos entre dispositivos conectados en una red local. Fue desarrollado en los años 1970 y se ha convertido en el método más común para conectar computadoras, dispositivos de red y otros equipos en una red de área local. El ethernet utiliza un cableado físico para transmitir los datos en forma de paquetes. Los cables Ethernet más comunes son los cables de par trenzado, que constan de varios pares de cables trenzados en una cubierta protectora. Estos cables se conectan a través de conectores RJ-45, que se insertan en los puertos Ethernet de los dispositivos. El estándar Ethernet define varios aspectos de la comunicación, como la velocidad de transmisión de datos, la codificación de los datos, el método de acceso al medio y el formato de los paquetes de datos. Las velocidades de transmisión más comunes son 10 Mbps, 100 Mbps, 1 Gbps (Gigabit Ethernet) y 10 Gbps (10 Gigabit Ethernet), aunque también existen velocidades más altas. Ethernet es un estándar de red que permite la conexión y comunicación de dispositivos en una red local, utilizando cables físicos y transmitiendo datos en forma de paquetes. Es uno de los pilares fundamentales de las redes de área local y ha evolucionado a lo largo de los años para ofrecer velocidades cada vez más altas y mayor capacidad de transmisión de datos.

6.3.1. Categorías cables Ethernet.

Dentro de ethernet se encuentran varias categorías, o generaciones para sus cables, donde se han ido mejorando progresivamente las capacidades de la red. En la siguiente tabla se presentan las más importantes con sus características.

Tabla 6 "Categorias principales de cables ethernet"

Categoría	Velocidad máxima	Frecuencia máxima
CAT 5	100 Mbps, (15,5 MB/s de descarga)	100 MHz
CAT 5E	1.000 Mbps (150,5 MB/s de descarga)	100 MHz
CAT 6	1.000 Mbps (150,5 MB/s de descarga)	250 MHz
CAT 6A	10.000 Mbps (1.250 MB/s ó 1,25 GB/s de descarga)	500 MHz

CAT 7	10.000 Mbps (1.250 MB/s de descarga)	600 MHz
CAT 7A	10.000 Mbps (1.250 MB/s ó 1,25 GB/s de descarga)	1.000 MHz (1 GHz)
CAT 8	40.000 Mbps (5.000 MB/s ó 5 GB/s de descarga)	2.000 MHz (2 GHz)

6.4. Protocolos CAN BUS.

"El estándar de bus CAN (Controller Area Network) se desarrolló en la década de 1980 y se utiliza ampliamente en redes de automóviles, vehículos y aviación, entre otras. El bus CAN se introdujo en el entorno marítimo con la adopción de la norma NMEA 2000 (National Marine Electronics Association) a finales de la década de 1990." (Kessler, 2021)

6.4.1. Estructura y comunicación en el protocolo CAN BUS.

El protocolo de bus CAN es un bus de difusión en el que cualquier dispositivo puede transmitir cuando está preparado y no tiene que esperar a ser sondeado por alguna estación o controlador maestro; la norma de bus CAN lo denomina protocolo "multimaster" porque todos los dispositivos se comunican en un mismo nivel.

El protocolo CAN BUS puede trasmitir a una velocidad máxima de 5 Mbps (megabits por segundo) con un alcance de hasta 40 metros a su velocidad máxima, por el contrario, a velocidades de transmisión inferiores de 50 kbps (kilobits por segundo), la red puede comunicarse hasta los 1000 metros.

6.4.2. Clasificación y normas ISO en el protocolo CAN BUS.

La especificación genérica global del bus CAN está contenida en cuatro normas de la Organización Internacional de Normalización (ISO):

- ISO 11519-1 describe una interfaz serie de baja velocidad (125 kbps).
- ISO 11898-1 describe el formato de trama de la capa de enlace de datos y la señalización de la capa física.
- ISO 11898-2 describe la interfaz de alta velocidad (1 Mbps o 5 Mbps).
- ISO 11898-3 describe una interfaz de baja velocidad y tolerante a fallos.

6.4.3. Relación entre CAN BUS y NMEA.

NMEA 2000 es la única de estas normas estándares que funcionan a través del bus CAN teniendo un uso tremendamente extendido.

6.4.4. Ciberseguridad del protocolo CAN BUS.

La confidencialidad de los protocolos CAN BUS y por ende del NMEA2000 es nula, ya que los mensajes dentro de la red carecen de cifrado, siendo susceptibles a ataques de MITM (Man-In-The-Middle) donde un atacante podría modificar la red añadiendo un dispositivo malicioso que monitoree el tráfico de esta red y pueda atacar en momentos críticos realizando un ataque de DoS (denegación de servicio) colapsando la red. Otra opción sería realizando ataques de inyección de código enviando mensajes erróneos a diferentes sistemas dentro de la red, como por ejemplo correcciones al piloto automático para desviar el rumbo unos cuantos grados, o hasta el punto de colisionar el buque. (Pen Test Partners, 2018)

La integridad de los bits se garantiza en el bus CAN mediante el uso de un cálculo CRC; el receptor calcula un valor de suma de comprobación diferente al contenido en el campo CRC del mensaje, esto indica que se ha producido un error de bits durante la transmisión. Un dispositivo malicioso puede enviar bits espurios en la línea, forzando tales errores de transmisión, haciendo que el aparato receptor ignore una transmisión que debería ser real. Un número suficiente de estos errores de bits podría hacer creer a otros dispositivos en la red que el bus de comunicación no es fiable y poner la red en fallo.

Los estándares NMEA 2000 y CAN bus no incluyen marcas de tiempo en el cuerpo del mensaje, por lo que no proporcionan integridad temporal. Esto abre la red a un ataque de repetición, en el que un mensaje legítimo es almacenado y retransmitido posteriormente por un dispositivo fraudulento.

6.4.5. Técnicas de mitigación en el protocolo CAN BUS.

En primer lugar, el uso de la criptografía podría emplearse para garantizar la confidencialidad de la comunicación entre dos nodos de la red y así proteger la red con un cifrado único a esa red, donde un dispositivo malicioso no tuviera la clave de cifrado no podría monitorizar los datos entre los componentes de la red.

Otra estrategia de mitigación sencilla es la segmentación de la red, en la que una red se subdivide en varias subredes, normalmente basadas en su función. NMEA 2000 limita el bus CAN a segmentos de cable a segmentos de cable de no más de 200 m de longitud al

emplear una velocidad de transmisión de 250 kbps. CAN pueden añadir seguridad al sistema separando las redes por secciones, pasajeros/tripulación, entretenimiento, sala de máquinas, equipos de navegación y otras en segmentos de red diferentes. Aunque este diseño encarece la implantación y el mantenimiento, limita el acceso a sistemas críticos por parte de los atacantes. Por contra segmenta la interconexión de redes y limita las funcionalidades de las mismas.

Un sistema de detección de intrusiones (IDS) se emplea habitualmente en una red para detectar ciberataques y responder a ellos. Un IDS basado en host es generalmente un software que reside en un nodo de la red y analiza el tráfico que entra y sale del nodo para detectar comportamientos anómalos. Un IDS basado en red es un dispositivo físico en la red que monitoriza el tráfico de red para detectar comportamientos anómalos. Por el tamaño de las redes NMEA un IDS basado en host no sería viable, ya que se requeriría de cambios en los propios dispositivos de la red, sin embargo, un IDS basado en red podría conectarse fácilmente a un bus CAN sin afectar a la red.

6.5. Protocolos NMEA.

La asociación NMEA (National Marine Electronics Association) fue fundada en 1957 por un grupo de fabricantes de electrónica marina con el objetivo de establecer un sistema común de comunicación entre diferentes marcas de equipos electrónicos navales. El primer protocolo estándar desarrollado por NMEA fue el NMEA 0183, que todavía es ampliamente utilizado por la mayoría de los equipos electrónicos a bordo de embarcaciones.

El protocolo NMEA 0183 define los requisitos de transmisión de datos y tiempos en formato serial a una velocidad de 4800 baudios. Establece la norma de que cada equipo sea emisor de datos NMEA y pueda ser recibido por múltiples receptores.

Con NMEA 0183, un instrumento emite datos hacia uno o varios instrumentos receptores. Por ejemplo, un GPS envía señales al plotter, al radar y al piloto automático. Sin embargo, el protocolo NMEA 0183 tiene limitaciones cuando se trata de recibir múltiples señales que se transmiten simultáneamente.

La versión, NMEA 2000, mejora significativamente la velocidad de transmisión empleando el CAN BUS.

Por último, el protocolo se ha modernizado en 2020 con la salida del OneNet

6.5.1. Tipos de NMEA.

Existen tres estándares NMEA dominantes para comunicación de instrumentación dentro de una embarcación:

- NMEA 0183, introducido en 1983, funciona con líneas serie 232/422 de la Electronic Industries Alliance (EIA) a 4.800 o 38.400 bits por segundo (bps). Esta norma es la base de la norma 61162-1 de la Comisión Electrotécnica Internacional (CEI) y se emplea en la Recomendación M.1371-5 del Sector de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-R) para transmisiones por aire a una velocidad de 9.600 bps. La versión V4.11 de NMEA 0183 se publicó en 2018.
- NMEA 2000 se publicó en 2001 e introdujo un formato de mensaje simplificado y un conjunto de mensajes PGN para admitir una gran variedad de dispositivos marítimos. Esta norma funciona a velocidades de hasta 250 kbps a través del bus CAN. NMEA 2000 se adoptó como IEC 61162-3; la edición 3.101 se publicó en 2016.
- OneNet es el miembro más reciente de la familia de normas NMEA. Lanzado en 2020, OneNet emplea un superconjunto del conjunto de mensajes NMEA 2000. Los dispositivos OneNet intercambian datos utilizando paquetes de Protocolo de Internet versión 6 (IPv6) que se ejecutan a través de una red de área local Ethernet a velocidades de hasta 10 Gbps y emplea IP Security (IPsec) para una comunicación segura entre dispositivos.

6.5.2. OneNet en NMEA.

El estándar NMEA OneNet es una evolución del estándar NMEA 2000 y se presenta como un estándar industrial abierto. Proporciona una infraestructura de red para dispositivos y servicios marinos basados en IPv6, lo que permite que los protocolos de aplicación OneNet coexistan con otros protocolos y servicios que operan en paralelo en la misma red.

Los dispositivos OneNet utilizan el Servidor de Nombres de Dominio Multicast (mDNS) para ser descubiertos en la red local. Este servidor se utiliza para resolver nombres de host en direcciones IP dentro de redes pequeñas que no cuentan con un servidor de nombres local. Cada aplicación OneNet tiene un ID de aplicación único asignado durante la producción o generado al ejecutarse la aplicación.

La información de la aplicación OneNet, como el nombre del producto, el código de producto NMEA, el modelo, etc., se almacena en formato JSON con codificación UTF-8 en un recurso denominado Application Information Resource (AIR). Un dispositivo OneNet puede solicitar el AIR de otros dispositivos OneNet a través de una solicitud HTTP GET, lo que permite identificar los servicios accesibles por otros dispositivos.

OneNet cuenta con un Modo Seguro que se respalda mediante el Servicio de Emparejamiento de OneNet. Este servicio permite que los dispositivos autorizados intercambien datos a través de un túnel encriptado. Para establecer este túnel seguro, una aplicación de Dispositivo de Interfaz Humana (HID) realiza una conexión HTTPS al Servicio de Emparejamiento para emparejar el dispositivo a la Red Segura. Se utiliza Diffie-Hellman Anónimo como conjunto de cifrado para la conexión. Una vez establecida la conexión HTTPS, se procede al emparejamiento.

Los dispositivos OneNet cuentan con un proceso de verificación único para identificar qué aplicaciones están certificadas por OneNet. Esto se logra utilizando el Servicio de Información de Aplicaciones (AIS), que también se utiliza para intercambiar AIR. El AIS proporciona el Recurso de Información de Certificación (CIR) que contiene mensajes de Sintaxis de Mensajes Criptográficos (CMS) para verificar la certificación.

6.5.3. Ciberseguridad en los protocolos NMEA.

Como ya se ha explicado en el apartado 6.4.4. las vulnerabilidades del protocolo NMEA2000 se comparten con el protocolo de CAN BUS, de esta manera solo se presentarán de los protocolos NMEA0183 y de OneNet.

NMEA0183 no tiene autenticación, validación del mensaje o encriptado, todo se envía en texto plano. De esta forma el protocolo es débil a los ataques de MITM (man-in-the-middle) donde se puede monitorizar el tráfico de la red y, o bien, realizar un ataque de repetición simulando un mensaje, realizar un ataque de DoS saturando la red o modificar los mensajes de la red para modificar la dirección del buque a través del piloto automático. En el artículo (Pen Tester Partners, 2018), se explican las modificaciones que se deben realizar a las sentencias del GPS para modificar los grados que se quiera el rumbo del buque.

OneNet: Las redes IPv6 y las evoluciones de estas permiten cifrar el contenido de los mensajes con claves únicas ligadas a cada dispositivo, lo que mejora la resiliencia de la red a ataques de DoS y spoofing, aun así, siguen siendo vulnerables a este tipo de ataques realizados de forma más sofisticada.

En una red OneNet, el HID (Dispositivo de Interfaz Humana) desempeña un papel importante al proporcionar información de configuración de red a los dispositivos recién conectados. Es responsabilidad del HID comunicar a la aplicación OneNet, que se ejecuta en un dispositivo, si se debe activar el modo seguro para que el dispositivo sea operativo. Cabe

destacar que solo el HID puede iniciar y ejecutar la activación del modo seguro. Sin embargo, esta exclusividad de control que tiene el HID puede ser aprovechada por un atacante al falsificar un HID. Al hacerlo, el atacante puede engañar a un dispositivo OneNet para que se comunique con un dispositivo falso a través del Modo Seguro. Esto puede llevar a la extracción de información sensible o incluso al control total del dispositivo objetivo por parte del atacante. Además, al cambiar un dispositivo a un canal seguro separado, este dispositivo ya no podrá comunicarse con otros dispositivos en el canal seguro original. Esto puede crear una situación en la que la comunicación se vea limitada o interrumpida entre dispositivos legítimos que operan en diferentes canales seguros. De esta forma el sistema es vulnerable a los ataques de MITM si se ha vulnerado la seguridad con un spoofing de HID, el dispositivo podría funcionar correctamente y solo monitorear el tráfico para recopilar datos.

6.5.4. Técnicas de mitigación en los protocolos NMEA.

Actualizar las redes NMEA de los buques al protocolo OneNet mejora la seguridad en varios aspectos, empezando por el cifrado. También mejora la seguridad gracias a la capacidad de validar la trasmisión de datos gracias a los ID únicos de cada dispositivo, lo que permite comprobar la integridad y tamaño de la red.

“El protocolo OneNet dificulta los ataques de repetición de mensaje, un problema endémico de los protocolos NMEA anteriores ya que se usa un número entero de 32 bits sin signo denominado Número de Secuencia (SQN) para evitar ataques de repetición”. (Tran, Keene, Fretheim, & Tsikerdekis , 2021, pág. 247)

Es crucial tomar medidas de seguridad adecuadas para proteger la red OneNet, como garantizar la autenticidad y la integridad de los HID y evitar la falsificación de dispositivos. Además, es importante implementar mecanismos de seguridad sólidos para evitar intrusiones y garantizar una comunicación segura entre los dispositivos en la red OneNet.

6.6. Sistemas SCADA / RTU.

Un sistema SCADA (Supervisory Control and Data Acquisition) es un sistema de control y supervisión utilizado en entornos industriales para monitorear y controlar procesos y operaciones. Consiste en una combinación de hardware y software que recopila datos en tiempo real de sensores y dispositivos de campo, los muestra en una interfaz gráfica y permite a los operadores tomar decisiones y controlar los sistemas desde una ubicación centralizada.

Por otro lado, un sistema RTU (Remote Terminal Unit) es un dispositivo utilizado en sistemas de control y monitoreo remoto. Es una unidad de terminales remotas que recopila datos de sensores y dispositivos de campo, los procesa y los transmite a una ubicación central para su análisis y supervisión. Las RTU suelen estar ubicadas en sitios remotos y se comunican con el sistema SCADA a través de redes de comunicación.

6.6.1. Diferencias entre SCADA y RTU.

Las principales diferencias entre un sistema SCADA y un sistema RTU son:

- Funcionalidad: Un sistema SCADA es una solución de software y hardware integral que ofrece funciones de supervisión, control y adquisición de datos. Permite una visualización detallada y el control de procesos complejos desde una ubicación centralizada. Por otro lado, una RTU es un dispositivo autónomo que se encarga de recopilar datos en el campo y transmitirlos al sistema SCADA para su análisis.
- Ubicación y comunicación: Un sistema SCADA generalmente se encuentra en una ubicación central, como una sala de control, y se comunica con dispositivos de campo a través de redes de comunicación, como Ethernet o redes inalámbricas. Por el contrario, una RTU se instala cerca de los dispositivos y sensores de campo y se comunica con el sistema SCADA a través de enlaces de comunicación, como redes de área amplia (WAN), líneas telefónicas o redes celulares.
- Complejidad y capacidad de procesamiento: Los sistemas SCADA son más complejos y tienen una mayor capacidad de procesamiento y almacenamiento de datos. Pueden manejar múltiples dispositivos y sistemas, así como recopilar y mostrar datos en tiempo real. Las RTU, en cambio, están diseñadas para tareas específicas de recopilación y transmisión de datos en el campo, con capacidades de procesamiento más limitadas.

En resumen, un sistema SCADA es una solución integral de control y supervisión que permite monitorear y controlar procesos desde una ubicación centralizada, mientras que una RTU es un dispositivo utilizado para la recopilación y transmisión de datos en el campo hacia el sistema SCADA. Ambos desempeñan roles complementarios en la implementación de sistemas de control y monitoreo industrial.

6.6.1. SCADA y RTU en los buques.

En los barcos, los sistemas SCADA (Supervisory Control and Data Acquisition) y los RTU (Remote Terminal Unit) desempeñan un papel crucial en el control y la supervisión de diversas operaciones y sistemas críticos a bordo.

Los sistemas SCADA en los barcos se utilizan para supervisar y controlar una amplia gama de procesos y sistemas, como el control del motor, la gestión de la planta eléctrica, el gobierno y el sistema de propulsión, el sistema de gestión de carga, el sistema de detección de incendios, entre otros. Estos sistemas recopilan datos en tiempo real de sensores y dispositivos de campo, y los transmiten a una ubicación central donde se procesan, analizan y presentan a los operadores en una interfaz gráfica. Los operadores pueden monitorear el rendimiento, realizar ajustes y tomar decisiones informadas para garantizar un funcionamiento seguro y eficiente del buque.

Por otro lado, los RTU se utilizan en los barcos para la recopilación y transmisión de datos desde los dispositivos y sensores de campo hacia el sistema SCADA. Estos dispositivos autónomos están ubicados en diferentes áreas del buque y están conectados a los sensores y equipos locales. Recopilan datos, como la temperatura, la presión, la velocidad, el nivel de combustible, entre otros, y los transmiten a través de redes de comunicación al sistema SCADA para su análisis y monitoreo centralizado.

En cuanto a la estructura de la red, tanto los sistemas SCADA como los RTU se integran en una red de comunicación a bordo del buque. Esta red puede estar basada en tecnologías como Ethernet, redes inalámbricas, redes de área local (LAN) y redes de área amplia (WAN), conectada a internet. Los sistemas SCADA se conectan a los RTU y otros dispositivos a través de esta red, permitiendo la transmisión bidireccional de datos y comandos.

Ilustración 14"Sistema SCADA de una planta EDAR (Estación Depuradora de Aguas Residuales)" (WICO, s.f.)

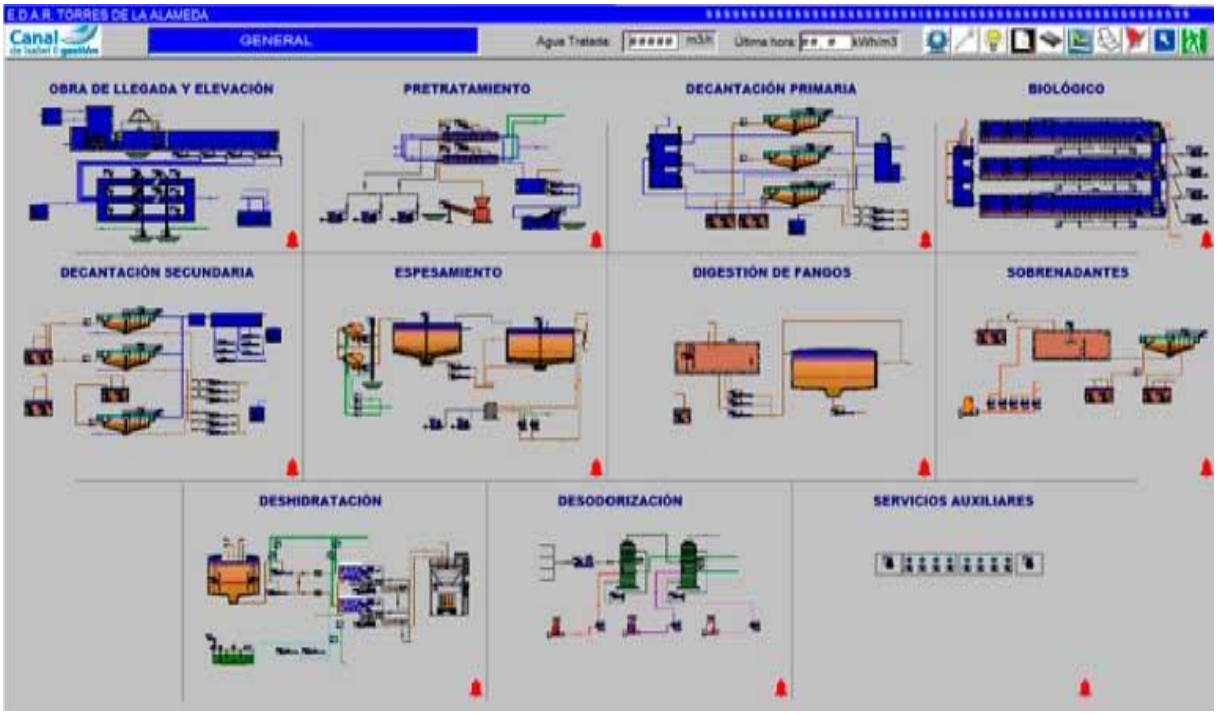
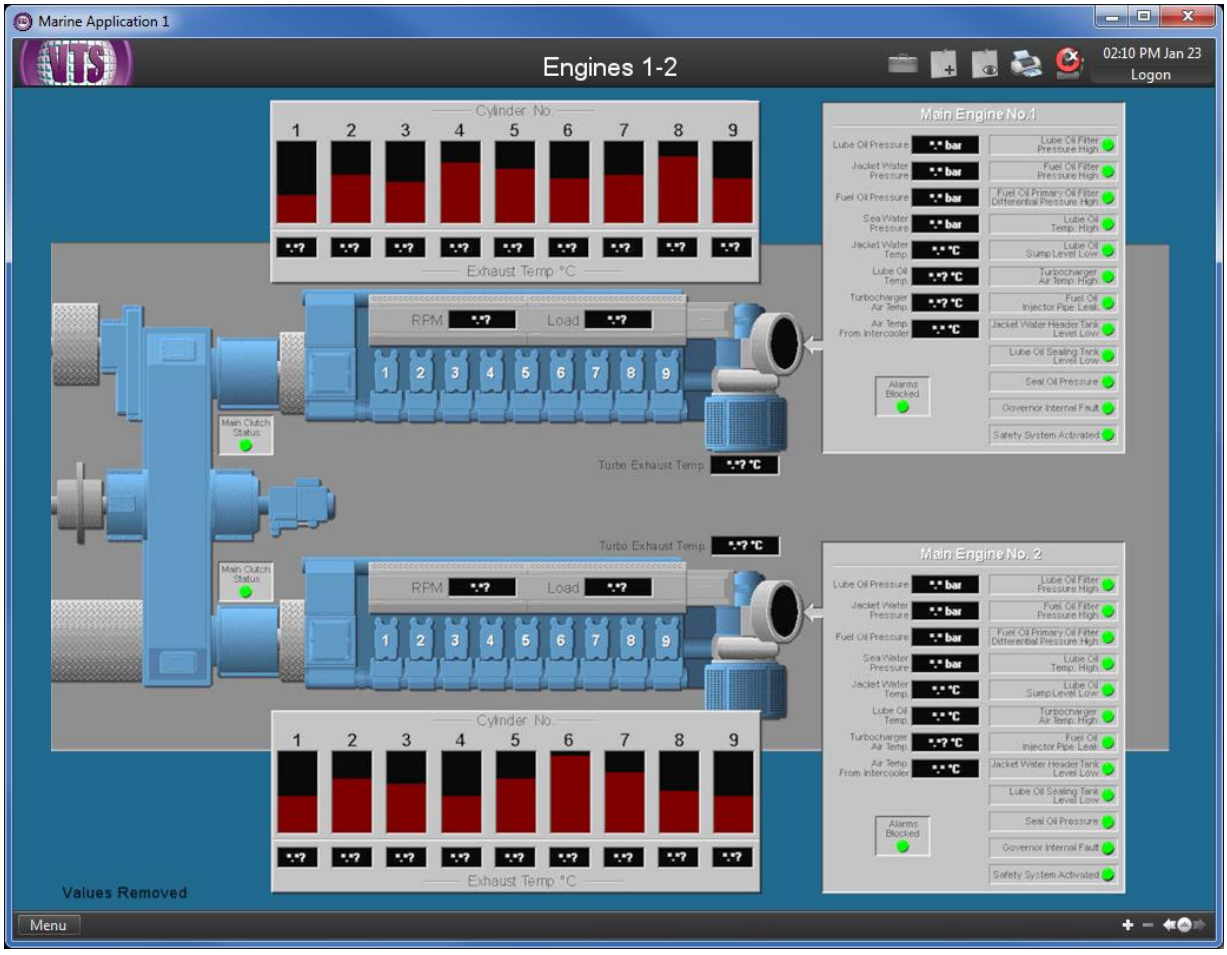


Ilustración 15 "Sistema SCADA, página de control de los MMPP del buque" (VTSCADA, s.f.)



6.6.1. Mitigación de ciberataques en sistemas SCADA y RTU.

En cuanto a la ciberseguridad, es crucial proteger tanto los sistemas SCADA como los RTU en los barcos. Algunas consideraciones sobre la ciberseguridad de estos sistemas incluyen:

- Segmentación de red: Se debe establecer una segmentación adecuada de la red para evitar el acceso no autorizado a los sistemas SCADA y los RTU. Esto ayuda a prevenir la propagación de ciberataques en caso de una violación de seguridad.
- Autenticación y acceso seguro: Se deben implementar medidas de autenticación sólidas para controlar el acceso a los sistemas SCADA y los RTU. Esto incluye el uso de contraseñas seguras, autenticación de dos factores y control de acceso basado en roles.
- Actualizaciones y parches de seguridad: Es importante mantener los sistemas SCADA y los RTU actualizados con los últimos parches de seguridad y actualizaciones del fabricante para corregir posibles vulnerabilidades conocidas.
- Monitoreo continuo: Se debe implementar un sistema de monitoreo continuo de la seguridad para detectar y responder rápidamente a posibles amenazas y anomalías en la red y los sistemas SCADA.

Se deben tener en cuenta las técnicas de mitigación mencionadas en los apartados de redes LAN, protocolo CAN BUS y los protocolos NMEA, ya que estas tecnologías son las que conforman las redes SCADA y los RTU.

6.7. Programmable Logic Controller, PLC.

PLC (Programmable Logic Controller) es un dispositivo electrónico utilizado en sistemas de automatización industrial para controlar y supervisar procesos y maquinaria. También se conoce como controlador lógico programable o autómata programable.

El PLC está diseñado para recibir señales de entrada de sensores y otros dispositivos, procesar la información según un programa específico y luego enviar señales de salida a actuadores y otros dispositivos para controlar el funcionamiento del sistema.

El programa del PLC se crea utilizando un lenguaje de programación especializado, como lenguaje ladder, lenguaje de bloques funcionales (FBD), lenguaje de instrucciones (IL) o lenguaje de texto estructurado (ST). Estos lenguajes permiten a los programadores definir la lógica de control y las secuencias de operación requeridas para el sistema automatizado.

Los PLC son ampliamente utilizados en la industria debido a su capacidad para controlar de manera eficiente y confiable una amplia gama de procesos, como control de temperatura, control de velocidad, control de movimiento, control de nivel, control de presión, entre otros. También son flexibles y se pueden reprogramar fácilmente para adaptarse a diferentes requisitos de control.

Además, los PLC ofrecen ventajas como la modularidad, lo que permite una fácil expansión o reemplazo de módulos, y la capacidad de comunicarse con otros dispositivos y sistemas, como interfaces de operador humano-máquina (HMI), computadoras y redes industriales, lo que facilita la supervisión y el control centralizado de los procesos industriales.

6.7.1. Componentes principales de un PLC.

- Fuente de alimentación, según el modelo el sistema trabajará con 120V AC o 24V DC.
- CPU o unidad central de procesamiento: el “cerebro del PLC”, incluso los PLC pequeños y no modulares contienen una CPU. Las señales de entrada proceden de las tarjetas de E/S, y los programas lógicos toman decisiones basadas en las señales. Si es necesario, la CPU ordena que las salidas se activen y desactiven a medida que cambian las señales y las condiciones. Los programas pueden incluir funciones avanzadas como operaciones matemáticas, cronometraje, recuento e intercambio de información a través de protocolos de red.
- Unidad de memoria que almacena los datos de las entradas y el programa que debe ejecutar el procesador.
- Interfaz de entrada y salida, donde el controlador recibe y envía datos desde/hacia dispositivos externos.

- Interfaz de comunicaciones para recibir y transmitir datos en redes de comunicación desde/hacia PLC remotos.
- Módulos I/O (Input / output): Módulos analógicos o digitales de entradas o salidas. Sensores, botones, interruptores, relés, solenoides e incluso dispositivos conectados en red comparten información con las señales de I/O conectadas a los terminales de las tarjetas. Estas tarjetas pueden elegirse en función de las necesidades de cada máquina e instalación.

Fuera del conjunto del PLC podemos encontrar 2 elementos importantes, el dispositivo de programación y la interfaz hombre-máquina (HMI). El dispositivo de programación puede ser un ordenador de sobremesa, un portátil o un instrumento portátil del mismo fabricante. La HMI proporciona un método para mostrar información y obtener entradas, modelando el sistema de control en su conjunto. Las HMI no suelen proporcionar ninguna forma de modificar el programa lógico. (Control Automation, 2022)

6.7.2. Firmware de un PLC.

El firmware es la infraestructura del sistema y cumple las funciones fundamentales, como controlar el hardware y otros equipos de comunicación. El sistema operativo y el software se basan en firmware para implementar funciones específicas. Por ejemplo, el sistema básico de I/O (BIOS) de un ordenador es un firmware. El firmware del PLC generalmente admite la actualización en línea, mientras que su comprobación de integridad no suele ser estricta, lo que hace que el firmware no se actualice correctamente, algo que podría desembocar en ser fácilmente manipulado por piratas informáticos.

El sistema PLC se compone generalmente de hardware, firmware y software. El firmware simultáneamente proporciona interfaces para hardware y software

6.7.3. Aplicaciones de los PLC en los buques.

Control de motores y propulsión: Los PLC se utilizan para controlar los motores principales y auxiliares del barco, así como los sistemas de propulsión.

Control de sistemas de generación de energía: Los PLC se utilizan para controlar los sistemas de generación de energía a bordo, como los generadores diésel. El PLC supervisa la carga eléctrica, el equilibrio de potencia y las secuencias de arranque y parada de los generadores, asegurando un suministro eléctrico estable y confiable.

Control de sistemas de navegación, estabilidad y lastre: Los PLC se emplean en los sistemas de navegación, estabilidad y control del barco, como el control del piloto automático,

el control de la posición del timón o el control de las bombas de lastre. Estos sistemas ayudan a mantener el rumbo, controlar la dirección y garantizar una navegación precisa y segura.

Control de sistemas de seguridad y alarma: Los PLC se utilizan para supervisar y controlar los sistemas de seguridad y alarma a bordo. Esto incluye la detección de incendios, el control de puertas y accesos, los sistemas de alarma de inundación, los sistemas de seguridad contra colisiones, entre otros. El PLC activa las alarmas correspondientes y toma medidas de seguridad adecuadas en caso de emergencia.

Control de sistemas de carga y descarga: En barcos de carga y buques de transporte, los PLC se utilizan para controlar los sistemas de carga y descarga, como las grúas y los sistemas de manejo de carga. El PLC coordina y supervisa las operaciones de carga y descarga, asegurando una manipulación de carga eficiente y segura.

Actualmente los PLC son el elemento vertebrador en los sistemas de control de un buque, en todos los departamentos del barco.

6.7.4. Seguridad en los PLC.

Antes del descubrimiento del gusano informático Stuxnet en junio de 2010, se prestaba escasa atención a la seguridad de los autómatas programables. Los autómatas programables modernos suelen incorporar sistemas operativos en tiempo real, los cuales pueden ser vulnerables a ataques similares a los dirigidos a los sistemas operativos de escritorio, como Microsoft Windows. Los PLC también pueden ser blanco de ataques si se logra controlar la computadora con la que se comunican, las redes en las que se encuentran, los protocolos de comunicación que utilizan o incluso la estructura misma del firmware.

Desde 2011, estas preocupaciones han ido en aumento a medida que se ha vuelto más común la interconexión de los PLC en entornos de red, conectando las redes de la planta con otros sistemas externos, como redes de monitoreo o puertos de mantenimiento de los fabricantes. Esta creación de redes expone a los PLC a mayores riesgos de seguridad, ya que pueden convertirse en puntos de entrada para posibles ataques o intrusiones.

Es importante destacar que la seguridad de los autómatas programables es un aspecto crítico a considerar en la actualidad, dado el aumento de la conectividad y la interdependencia de los sistemas industriales. La protección de estos sistemas es esencial para salvaguardar la integridad, confidencialidad y disponibilidad de los procesos industriales y evitar posibles impactos negativos en la seguridad y la productividad.

6.7.5. Seguridad del firmware en los PLC.

Muchos PLC permiten a los usuarios descargar actualizaciones de firmware de forma remota, y la verificación del firmware puede detectar si el firmware ha sido modificado intencionadamente.

Una vulnerabilidad clave asociada a los PLC es la confianza inherente del proceso de verificación del firmware, que se basa en un CRC y una suma de comprobación como mecanismo de validez. El CRC y el checksum se comprueban para verificar que el firmware no ha sido corrompido, pero este mecanismo no puede detectar manipulación intencionada.

Para realizar un ataque al firmware, primero se estudia por ingeniería inversa el PLC para que el código que se va a inyectar tenga las características y cumpla las necesidades de control del sistema y así pueda pasar desapercibido. A continuación, se insertan instrucciones en el firmware sin afectar negativamente a la estabilidad del software. Por último, el firmware es reempaquetado para ejecutar ataques de denegación de servicio (DoS) en las siguientes condiciones:

- Forzar al PLC a terminar operaciones después de una cantidad predeterminada de tiempo.
- Forzar al PLC a terminar las operaciones al recibir una señal de control.
- Forzar al PLC a terminar operaciones al recibir una señal de control y realizar una modificación permanente en el código que impida a su propietario recuperar el control del dispositivo.

Ataque de denegación de servicio, DoS. El ataque más sencillo es un fallo forzado basado en un temporizador. Este ataque consiste en instalar el código en el PLC, después de que el temporizador expira, el ataque hace que el PLC falle y deje de funcionar hasta que se reinicie. De la misma forma se puede colocar un contador que después de un número especifico de ciclos de trabajo haga fallar al sistema, o bien saltándose pasos o ignorando setpoint o seguridades.

La implementación de este ataque requiere una zona de memoria para insertar las líneas del contador y la colocación del código en un lugar correcto dentro del programa para que se ejecute la línea de código y se realice el ataque.

En la publicación (Schuett, Butts, & Dunlap, 2014) se explica el proceso de obtención de datos, modificación del código y los filtros que deben realizarse al código malicioso antes de inyectarlo al PLC objetivo. En resumen, por ingeniería inversa se catalogan los diferentes componentes y procesos del PLC, tras esto se modifica el código de actualización de firmware

del propio fabricante y con un lector de código se inyectan las nuevas líneas que desencadenarán el ataque. Este código se comprueba en una máquina virtual para comprobar el funcionamiento correcto de las modificaciones realizadas al código. Tras esto se "lanza" o bien como un ataque dirigido a una organización o sistema suplantando al fabricante, o se publica en la red para intentar afectar a la mayor cantidad de dispositivos posibles. Ambos acercamientos requieren de técnicas de phishing, o bien para engañar a los técnicos o suplantando al fabricante.

6.7.6. Técnicas de mitigación en firmware de los PLC.

En el artículo, (Xiaojun , Zhuoran , & Yanbin , 2020) se proponen dos técnicas para garantizar que los PLC mantengan su firmware intacto e inalterable.

"El primer método es el mecanismo de autenticación. El archivo de inicio del sistema PLC incluye BOOT.BIN, devicetree. Dtb, uImage y uramdisk.image. La cadena de confianza se basa en el código de firmware BL0 como base de confianza. El enlace de arranque mide la seguridad del siguiente arranque y extiende el valor métrico al PCR. Sólo si el siguiente enlace de arranque es seguro, se le transferirá el control.

El segundo método es la comprobación de integridad. Cuando el dispositivo se enciende, el segmento de código hash en cada archivo es llamado por la orden de arranque del sistema para realizar la comprobación de integridad. Si el valor hash no coincide con el valor estándar almacenado previamente, el archivo se borrará directamente. Todos los archivos de inicio se verificarán sucesivamente para asegurarse de que, una vez modificado un archivo de inicio, el dispositivo no pueda iniciarse, garantizando la seguridad del firmware del PLC." (Xiaojun , Zhuoran , & Yanbin , 2020, pág. 75)

6.7.7. Seguridad de red en los PLC.

Dado que el equipo PLC es el controlador central de SCADA, las interferencias en el funcionamiento del PLC pueden causar pérdidas irreversibles. Existen numerosos problemas de seguridad en la comunicación entre el SCADA y los PLC en la red. Una vez que el sistema SCADA se conecta a Internet, es más probable que esta amenaza potencial para el sistema SCADA sea explotada por los atacantes.

Replay Attack: El ataque de repetición o "replay attack" puede ser lanzado por la misma dirección de host para la captura o por otro host en la misma red. Ambos ataques de repetición son eficaces y capaces de iniciar y detener el PLC. "*Ataque consistente en capturar una transmisión de datos correcta y reproducirla posteriormente. Es un ataque típico para capturar secuencias de autenticación correctas y reproducirlas luego para que el atacante logre los*

mismos derechos de acceso" (CNI, s.f.). Con este ataque se puede suplantar la identidad del usuario o robar las credenciales. En otros casos, si estos mensajes se repitieran de forma masiva, podrían llegar a saturar la red y convertirse en un ataque de denegación de servicio al verse la red colapsada.

Ataques de Hombre en el medio (Man-in-the-middle, MITM): Entre el ordenador principal, o master, y el PLC se utilizan los protocolos TCP/IP y COTP, mientras que Ethernet adopta el protocolo de resolución de direcciones ARP. Esta comunicación es susceptible de sufrir un ataque MITM (Man-in-the-middle attack). El ataque Man-in-the-middle puede ser activo o pasivo. El modo pasivo consiste en supervisar el tráfico de comunicaciones del PLC y obtener datos; el modo activo consiste en manipular datos y comandos para controlar el PLC e interferir en el funcionamiento normal del sistema.

Ataque sigiloso de modificación de comandos (Stealth command modification attack): es una combinación de ataque de repetición y ataque man-in-the-middle. Se utiliza para obtener la comunicación entre PCS7 (nombre que recibe el master en los sistemas Siemens) y PLC y reproducir otros comandos en modo oculto para interferir en el funcionamiento del PLC.

Gusano informático para PLC: El malware del gusano se aprovecha de la funcionalidad del PLC por la cual se realiza un escaneo cíclico al terminal el programa cada 100ms. Esta funcionalidad permite al atacante modificar el contenido del programa cada ciclo. El virus PLC llama a funciones del sistema, luego aprovecha el protocolo propietario para conectarse con otros PLCs, y luego falsifica la comunicación, inyectándose finalmente en el PLC a través del datagrama. El virus se oculta guardándose en la memoria de ejecución y este se replica cada vez que se ejecuta el escaneo. Este gusano así puede propagarse por la red al resto de PLC vía proxy. Así con solo un PLC infectado se pueden modificar valores en toda la red alterando el funcionamiento de la misma con la intención de comprometer el sistema, modificar valores clave o simplemente corromper el sistema y la red.

6.7.8. Técnicas de mitigación en la seguridad de red en los PLC.

Una propuesta de mitigación de ataques propuesta en el trabajo (Xiaojun , Zhuoran , & Yanbin , 2020) expone que añadir un sniffer de red podría controlar la identidad, dirección y metadatos de los comandos que están en la red. Así se podría comprobar si los datos pertenecen a los sistemas dentro de la red y estando estos componentes de la red identificados con un número único evitar ataques externos, ya que, además, se tendría monitoreo de los puertos externos y su algún mensaje entrara por esos puertos sin tener los

privilegios necesarios se invalidarían automáticamente y el dispositivo externo quedaría vetado de la red. Las consideraciones serían:

- Detección de intrusiones externas: El sistema de supervisión controla si se activa el servicio de conexión remota en el host de red o si se añaden procesos o puertos no autorizados. Esto ayuda a determinar si el sistema ha sido objeto de una intrusión desde una red externa. Si se detectan modificaciones en la estructura de la red, el sistema de supervisión notifica sobre ellas.
- Detección de comandos desconocidos: El sistema de supervisión puede capturar el tráfico de datos en el sistema industrial. Si se identifica un comando de lectura OPC proveniente de una fuente desconocida, esto puede indicar una posible intrusión en la capa de red de supervisión.
- Detección de manipulación en comandos de escritura: Debido a la sensibilidad de los comandos de escritura, se puede utilizar un método de detección de consistencia. El sistema de supervisión obtiene los datos del comando de escritura desde el dispositivo en la capa subyacente y los compara con los valores detectados por el software de supervisión para determinar si ha habido alguna manipulación.
- Detección de procesos y puertos no autorizados: El sistema puede identificar incrementos en procesos y puertos en el host de la red industrial del sistema de control. También puede detectar comandos de lectura y escritura provenientes de fuentes desconocidas y compararlos con los valores de parámetros del software de supervisión para verificar e interceptar dichos comandos. Sin embargo, esta verificación comparativa se basa en la confiabilidad del software de supervisión.

Es importante tener en cuenta que, si el sistema de supervisión, el sniffer, es atacado y controlado, el programa malicioso puede ocultarse, invalidando la verificación de instrucciones de lectura y escritura. Esto puede afectar los requisitos de tiempo real de los sistemas de control industrial.

6.8. Human Machine Interface, HMI.

Un HMI (Human Machine Interface), también conocido como interfaz hombre-máquina, es un sistema o dispositivo que permite la interacción entre humanos y máquinas. Proporciona una interfaz gráfica intuitiva y fácil de usar para que los operadores supervisen y controlen los sistemas y procesos en tiempo real. Un HMI puede consistir en pantallas táctiles, paneles de control, botones, luces indicadoras y otros elementos que permiten a los usuarios interactuar con los sistemas automatizados.

En el contexto marítimo, los HMI juegan un papel esencial en los barcos. Permiten a los operadores monitorear y controlar los sistemas críticos, como el motor, la planta eléctrica, la navegación, el sistema de propulsión y otros sistemas auxiliares. Los HMI proporcionan una representación visual clara de los datos recopilados de los sensores y dispositivos de campo, lo que facilita la toma de decisiones rápidas y precisas.

El uso de HMI en los barcos mejora la eficiencia operativa al brindar a los operadores una visión general del estado de los sistemas y las condiciones del buque. Los datos en tiempo real se presentan de manera comprensible y visualmente atractiva, lo que permite una supervisión más efectiva y una respuesta rápida a cualquier anomalía o emergencia.

Además, los HMI también mejoran la seguridad a bordo al proporcionar alarmas y notificaciones visuales y audibles en caso de situaciones críticas. Los operadores pueden recibir alertas tempranas sobre posibles fallas o condiciones anormales, lo que les permite tomar medidas correctivas de inmediato y minimizar los riesgos potenciales.

Los HMI son componentes clave en los barcos, ya que permiten a los operadores interactuar con los sistemas críticos a bordo de manera eficiente y segura. Proporcionan una interfaz intuitiva y visualmente atractiva para monitorear, controlar y tomar decisiones informadas en tiempo real, lo que mejora tanto la eficiencia operativa como la seguridad en el entorno marítimo.

6.8.1. Vulnerabilidades principales de los HMI.

El uso creciente de PC industriales (IPC) y otras interfaces hombre-máquina (HMI) conlleva una mayor vulnerabilidad. Aunque el IPC está fabricado para soportar condiciones industriales, es posible que siga ejecutando una versión comercial de Windows, por lo que es susceptible a todas las vulnerabilidades que conlleva ese sistema operativo. Al menos uno de cada tres dispositivos sigue ejecutando Windows XP, que Microsoft ya no admite. En un entorno industrial es difícil y caro mantener un software antivirus, por lo que, si un virus infecta un IPC, podría afectar a todo el sistema. Emplear sistemas que no se actualizan facilita los ataques, parchear un ordenador no solo actualiza herramientas y software, también corrige los fallos de los desarrolladores. Fallos que se pueden emplear para vulnerar la seguridad.

Aunque los HMI se encuentran en zonas críticas del buque, como la sala de máquinas o el puente, es común emplear dispositivos de memoria externa como USB para realizar un volcado de datos para su posterior análisis. Proteger los ordenadores donde se gestionan esos datos es clave, ya que el trasvase continuo de información entre un ordenador y otro

podría llevar a infectar el HMI, y por tanto la red SCADA, aunque la red sea cerrada, puesto que no se ha securizado el ordenador que gestiona la información y que suele estar conectado a internet.

De la misma forma la comunicación de los HMI con el resto de componentes de la red es importante. Como se ha mencionado en la seguridad de las redes LAN, si la red no tiene un cifrado y los firmwares de los equipos no están actualizados, un dispositivo malicioso que se añada a la red de forma clandestina podría realizar ataques de MITM o DoS. Así, los HMI tienen vulnerabilidades similares a las expuestas en los PLC, tanto para su firmware como para la red.

6.8.2. Técnicas de mitigación en los HMI.

Las técnicas de mitigación mencionadas en los apartados 6.7.6. “Técnicas de mitigación en firmware en los PLC” y 6.7.8. “Técnicas de mitigación en la seguridad de red en los PLC” son aplicables para los HMI.

Como añadido al tratarse de la interfaz entre la máquina y el usuario, se consideran varios aspectos sobre la ciberseguridad física del dispositivo y su acceso:

- Implementar medidas de autenticación seguras: utilizar contraseñas sólidas y únicas para el acceso al HMI. Implementar la autenticación de dos factores para agregar una capa adicional de seguridad. Además, es recomendable establecer políticas de cambio de contraseñas periódicas y evitar el uso de credenciales predeterminadas.
- Políticas de acceso y privilegios: Limitar el acceso al HMI solo a usuarios autorizados y asignar niveles de privilegios adecuados. Esto ayuda a prevenir accesos no autorizados y minimiza el riesgo de manipulación malintencionada de la configuración del sistema.
- Monitorizar y registrar las actividades: Implementar herramientas y sistemas de monitoreo para supervisar y registrar las actividades en el HMI. Esto permite detectar comportamientos anómalos y proporciona una traza de auditoría en caso de incidentes de seguridad.
- Capacitar a los usuarios: Brindar capacitación y concienciación sobre ciberseguridad a los usuarios del HMI. Esto incluye la educación sobre prácticas seguras de contraseña, la identificación de posibles ataques de ingeniería social y la importancia de informar cualquier actividad sospechosa.

7. Demostración: “Jamming con GNURadio y Hack RF”.

7.1. Introducción a la demostración de GNURadio y HackRF como herramientas de hacking.

Este apartado proporciona detalles técnicos sobre la demostración de ciberseguridad en la marina mercante que se llevará a cabo como parte del trabajo universitario. Se enfocará en el análisis del espectro radioeléctrico y la simulación de un ataque de jamming utilizando el dispositivo HackRF y el programa GNURadio. Presentaremos información sobre GNURadio, HackRF, los dispositivos objetivo y el procedimiento utilizado en la demostración. El anexo busca destacar la importancia de proteger las comunicaciones y ofrecer recomendaciones de seguridad para prevenir ataques similares

7.1.1. Objetivo de la demostración.

El objetivo de esta demostración es resaltar la importancia de la ciberseguridad en la marina mercante y mostrar cómo se pueden analizar las comunicaciones en las frecuencias de las emisoras de VHF portátiles utilizadas en los buques convencionales. Además, se simulará un ataque de jamming para demostrar la vulnerabilidad de estas comunicaciones y enfatizar la necesidad de implementar medidas de protección adecuadas.

7.1.2. Importancia de la ciberseguridad en la marina mercante.

La ciberseguridad desempeña un papel fundamental en la marina mercante, donde la comunicación efectiva y segura es esencial para la seguridad de los buques y las tripulaciones. La protección de las comunicaciones críticas a bordo, la prevención de posibles ataques y la salvaguardia de la integridad y confidencialidad de los datos son aspectos vitales en este entorno. La exposición de las vulnerabilidades en las emisoras de VHF portátiles y los ataques de jamming resaltarán los riesgos y la necesidad de implementar medidas de seguridad adecuadas.

7.1.3. Descripción general de los conceptos clave abordados en la demostración.

En esta demostración, se abordarán conceptos clave como el análisis del espectro radioeléctrico, que permitirá identificar las frecuencias de transmisión empleadas en las emisoras de VHF portátiles utilizadas en los buques. Además, se mostrará cómo se puede simular un ataque de jamming para resaltar la vulnerabilidad de las comunicaciones no seguras y cómo esto puede afectar la operación y seguridad de los buques. Estos conceptos

enfatizarán la necesidad de adoptar medidas proactivas y estrategias de ciberseguridad sólidas en la marina mercante.

7.2. Programa utilizado: GNURadio.

7.2.1. Descripción de GNURadio y su función en la demostración.

GNU Radio es un software de código abierto y una caja de herramientas de procesamiento de señales que proporciona un entorno flexible para el desarrollo de sistemas de radio definidos por software. En esta demostración, GNU Radio desempeña un papel fundamental al permitirnos analizar el espectro radioeléctrico, identificar las frecuencias de las emisoras de VHF portátiles y simular un ataque de jamming. Proporciona una interfaz gráfica intuitiva y una amplia variedad de bloques de procesamiento de señales para realizar estas tareas.

7.2.2. Principales características y capacidades relevantes para la demostración.

GNU Radio ofrece una amplia gama de capacidades para el procesamiento de señales, incluyendo filtros, moduladores, demoduladores, decodificadores y muchos otros bloques funcionales que son esenciales para el análisis del espectro y la simulación de ataques de jamming. Además, cuenta con una comunidad activa que contribuye con módulos adicionales y mejoras constantes, lo que lo convierte en una herramienta versátil y en constante evolución.

7.2.3. Justificación de la elección de GNURadio para este escenario específico.

La elección de GNU Radio para esta demostración se basa en su amplia aceptación en la comunidad de radio definida por software y su capacidad para adaptarse a diversas aplicaciones. Su flexibilidad, capacidad de personalización y facilidad de uso hacen que sea una opción ideal para analizar el espectro radioeléctrico y simular ataques de jamming. Además, al ser un software de código abierto, GNU Radio permite el acceso a su código fuente, lo que facilita la comprensión y personalización de los algoritmos utilizados.

7.3. Dispositivo utilizado: HackRF.

7.3.1. Descripción del dispositivo HackRF.

El HackRF es un transceptor de radio de bajo costo y de código abierto que permite la recepción y transmisión de señales en un amplio rango de frecuencias. Es un dispositivo versátil que se utiliza en aplicaciones de radio definida por software y puede ser programado para realizar diversas funciones, como el análisis del espectro, la decodificación de señales y la generación de señales de jamming.

7.3.2. Funciones y capacidades clave del HackRF para la demostración.

El HackRF ofrece una amplia gama de frecuencias de operación, lo que lo hace adecuado para analizar el espectro radioeléctrico en las frecuencias de las emisoras de VHF portátiles utilizadas en la marina mercante. También permite la transmisión de señales, lo que nos permite simular un ataque de jamming en la demostración. Además, su capacidad de muestreo y su flexibilidad programable hacen del HackRF una herramienta poderosa para el procesamiento de señales.

7.3.3. Ventajas y razones para elegir el HackRF en este contexto.

La elección del HackRF se basa en su asequibilidad, su naturaleza de código abierto y su amplia aceptación en la comunidad de radio definida por software. Sus capacidades de recepción y transmisión, combinadas con su flexibilidad programable, lo convierten en una opción ideal para llevar a cabo la demostración de ciberseguridad en la marina mercante. Además, su amplio soporte y documentación disponible facilitan su integración y uso en este escenario.

7.4. Tipos de dispositivos atacados.

7.4.1. VHF portátiles en banda marina (GMDSS).

En esta demostración, nos enfocaremos en los dispositivos VHF portátiles utilizados en la banda marina del Sistema Mundial de Socorro y Seguridad Marítimo (GMDSS, por sus siglas en inglés). Estas emisoras operan en un rango de frecuencias VHF entre 156 y 162 MHz y son vulnerables a posibles ataques de jamming. Estas emisoras de VHF son cruciales para las comunicaciones de emergencia y seguridad en la marina mercante, ya que permiten la comunicación entre los buques y las estaciones terrestres en situaciones críticas. Es vital

garantizar la integridad y confidencialidad de estas comunicaciones para proteger la vida de las personas en el mar.

7.4.2. Justificación de la selección de este tipo de dispositivo como objetivo de la demostración.

Al centrarnos en las emisoras de VHF en banda marina del GMDSS, buscamos resaltar la importancia de proteger las comunicaciones críticas en la marina mercante. Estos dispositivos son fundamentales para la seguridad y el rescate en situaciones de emergencia en el mar. Al simular un ataque de jamming en estas emisoras, destacaremos los riesgos asociados con la falta de seguridad en las comunicaciones marítimas y la necesidad de implementar medidas de protección adecuadas.

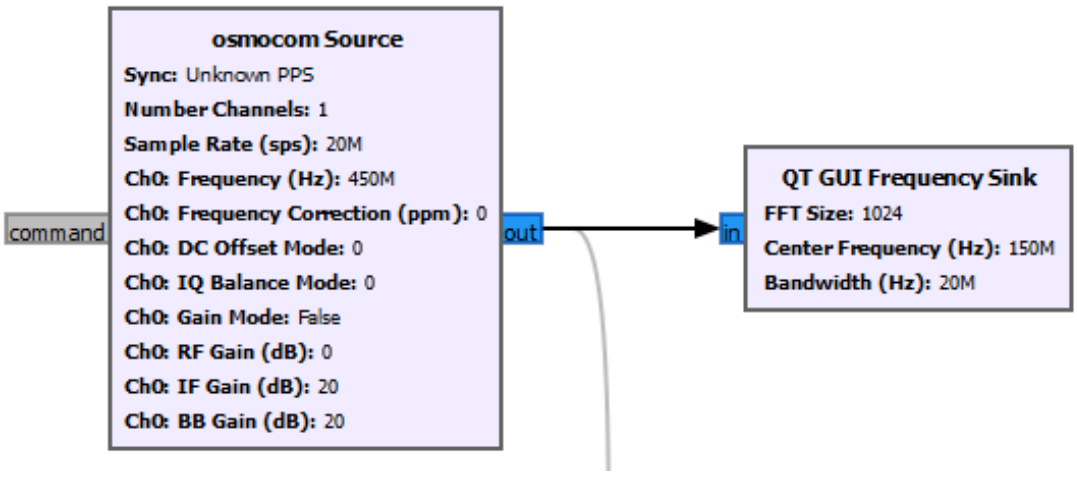
7.5. Procedimiento de la demostración.

7.5.1. Análisis del espectro radioeléctrico en las frecuencias de las emisoras de VHF portátiles.

Utilizando el HackRF y el programa GNURadio, se llevará a cabo un análisis del espectro para identificar las frecuencias de transmisión empleadas por las emisoras de VHF, aunque esto no sería necesario en caso de las transmisiones en los canales definidos en el GMDSS. Esto permitirá visualizar el espectro radioeléctrico y detectar posibles interferencias o señales no autorizadas.

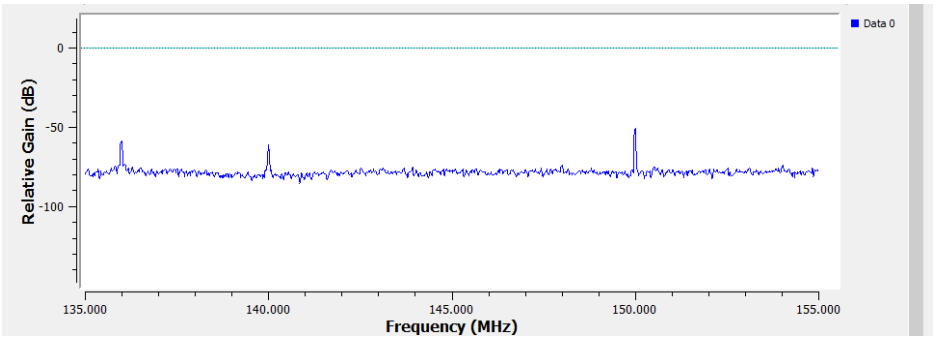
Para el análisis preliminar se empleará el siguiente conjunto de bloques.

Ilustración 16 "Conjunto de bloques en GNURadio para un analizador de espectro simple en banda VHF"



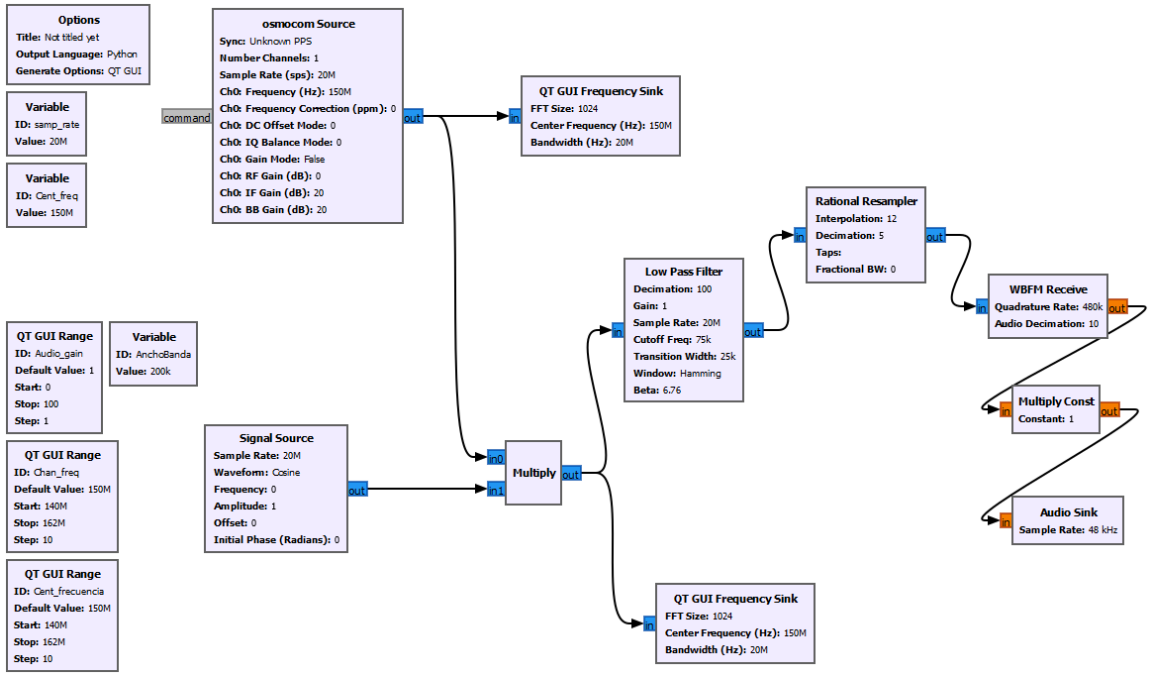
Los bloques “osmocom Source” y “QT GUI Frecuency Sink”, generan un analizador de espectro muy simple, el cual nos permite visualizar el rango de frecuencias que se necesite. “Osmocom Source” es el bloque que activa el Hack RF y le indica que debe hacer y cómo. En este caso, recepción de señal entre los 140Mhz y los 160Mhz. El bloque “QT GUI Frecuency Sink” permite visualizar que está recibiendo el dispositivo HackRF, ya que genera una gráfica ganancia/ frecuencia que presenta las señales en el ancho de banda deseado.

Ilustración 17 "Analizador de espectro en GNURadio en banda VHF"



En este caso, solo podemos ver las señales en la gráfica, sin interactuar con ellas. Algo que tiene poco interés. Añadiendo unos bloques al programa podemos seleccionar la frecuencia que queremos escuchar, procesar la señal y amplificarla.

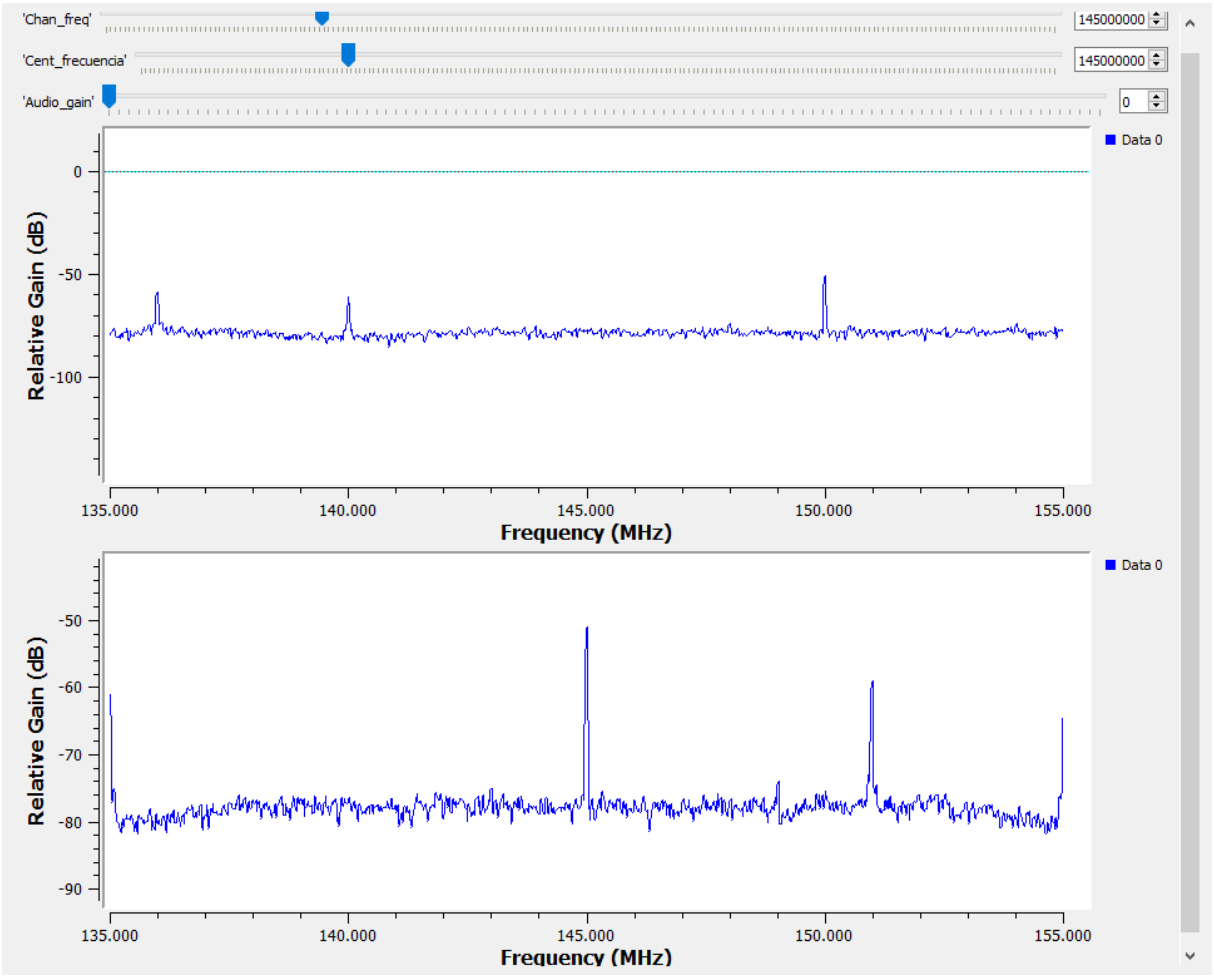
Ilustración 18 "Conjunto de bloques en GNURadio para un analizador de espectros en VHF con posibilidad de escucha de la frecuencia"



Añadimos una fuente de señal para heterodinar la señal recibida, procesarla y demodularla para enviarla en la tarjeta de sonido del PC y reproducirla. De esta forma trabajando con 20MHz de muestras estas se deben reducir a los 48KHz para ser procesadas. Esto se consigue ya que. 20MHz dividido entre 100 son 200kHz, multiplicado por 12 y dividido por 5, 480KHz y dividido por 10, 48KHz. Estas operaciones se realizan con los bloques “Low Pass Filter”, “Rational Resampler” y “WBFM Recive”. Después la señal se amplifica en ganancia, “Multiply Const” y se envía a la tarjeta de sonido a la frecuencia necesaria en “Audio Sink”.

Ahora al ejecutar el programa contamos con otra gráfica más y 3 barras con las que podemos interactuar. Una de ellas nos permite elegir la frecuencia de escucha, otra desplazar el centro de la nueva gráfica para visualizar la frecuencia y una última que nos permite controlar la ganancia de la señal y en definitiva, su volumen.

Ilustración 19 "Gráfica de analizador de espectros con selector de frecuencia."

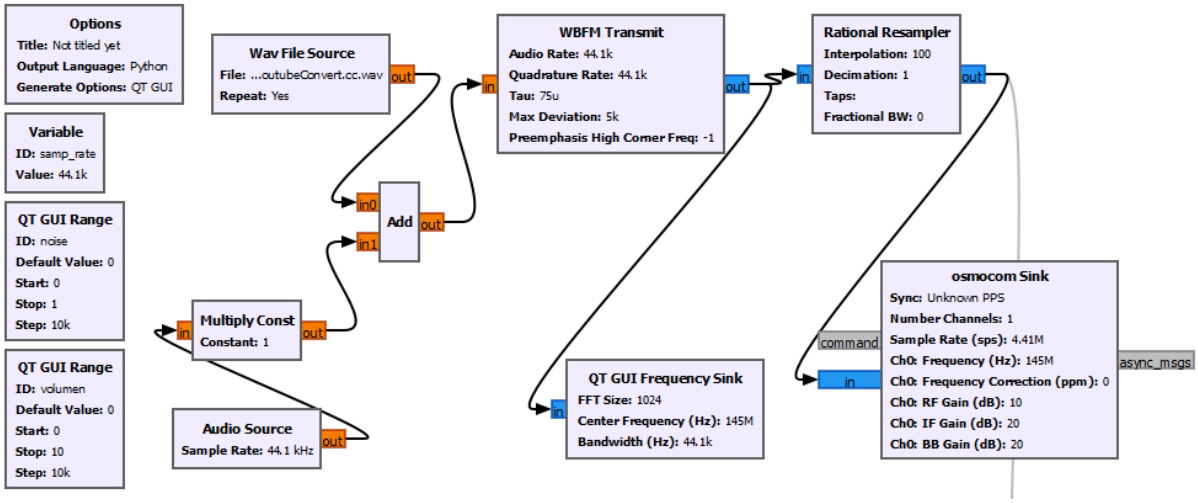


De esta manera podemos identificar las frecuencias en uso y ponernos a la “escucha” en cualquier frecuencia.

7.5.2. Simulación de un ataque de jamming.

Mediante la programación del HackRF y la configuración adecuada en GNURadio, se simulará un ataque de jamming dirigido a las emisoras de VHF. Esto implicará la generación de señales de interferencia en las frecuencias de transmisión, lo que demostrará la vulnerabilidad de las comunicaciones y la importancia de implementar medidas de protección.

Ilustración 20 "Conjunto de bloques para transmisor de radiofrecuencia en la banda de VHF en GNURadio"



Para este caso se ha construido un transmisor de señal en el rango de VHF. En primer lugar, se selecciona una fuente de audio o ruido para mezclarla con la señal proveniente de la tarjeta de sonido. Tras todo este proceso esta señal de audio de muestrea a la frecuencia deseada en el bloque “WBFM Transmit” se multiplica por 100 en el siguiente bloque, “Rational Resampler” modificando la ratio de sampleo en el transmisor “osmocom Sink”. El resultado es que en las radios vecinas empleando esa frecuencia de recepción recibirán de forma ininterrumpida la señal que el HackRF transmite por encima de las comunicaciones convencionales en ese canal.

En este caso la potencia de transmisión del HackRF es bastante baja, del orden menor de 1w. De esta forma no tenemos un alcance muy destacado ni una potencia de transmisión capaz de eclipsar a transmisores convencionales. Esto se puede suplir fácilmente añadiendo amplificadores en la salida de antena del HackRF para amplificar la potencia de transmisión.

8. Conclusiones.

8.1. Conclusiones sobre los sistemas GMDSS, gestión y de ayuda a la navegación del buque.

La seguridad cibernética de los equipos críticos de comunicaciones y ayudas a la navegación en buques es de vital importancia para garantizar la integridad de las operaciones marítimas. En un mundo cada vez más conectado, es fundamental implementar medidas sólidas para mitigar los riesgos y fortalecer la resiliencia de estos sistemas.

Una estrategia efectiva para mejorar la seguridad cibernética de estos equipos incluye puntos comunes y técnicas recomendadas. En primer lugar, es esencial contar con una sólida política de seguridad cibernética que abarque todos los aspectos relevantes de los sistemas marítimos. Además, es fundamental concienciar y capacitar al personal en seguridad cibernética para que comprendan los riesgos y las mejores prácticas.

La segmentación de red es una técnica clave para mejorar la seguridad. Separar los sistemas críticos en segmentos de red aislados y protegidos ayuda a limitar la propagación de posibles ataques cibernéticos. También se debe proteger la señal de navegación mediante técnicas de autenticación y monitoreo de la integridad de las señales.

El control de acceso estricto es otro aspecto crucial. Establecer políticas rigurosas de acceso y autenticación para los equipos críticos ayuda a prevenir accesos no autorizados. Además, se recomienda implementar sistemas de detección de intrusiones y supervisión en tiempo real para identificar y mitigar ataques cibernéticos de manera oportuna.

Realizar copias de seguridad periódicas de los datos críticos y desarrollar un plan de recuperación ante desastres son medidas indispensables. Esto permitirá restaurar los sistemas y datos rápidamente en caso de una brecha de seguridad.

Por último, es importante realizar evaluaciones de seguridad independientes para identificar posibles vulnerabilidades y tomar medidas correctivas antes de que se produzcan incidentes reales.

En conclusión, mejorar la seguridad cibernética de los equipos críticos de comunicaciones y ayudas a la navegación en buques requiere la implementación de medidas sólidas, como contar con una política de seguridad, capacitar al personal, segmentar las redes, proteger las señales de navegación, establecer controles de acceso, realizar copias de seguridad y evaluaciones de seguridad independientes. Al seguir estas recomendaciones, se podrá mitigar el riesgo de ciberataques y garantizar una navegación segura y confiable.

8.2. Conclusiones sobre los sistemas de control industrial, sistemas auxiliares, gobierno, propulsión del buque, protocolos de conexión entre sistemas y redes.

Los avances tecnológicos han traído consigo numerosos beneficios en términos de eficiencia y automatización, pero también han aumentado los riesgos de ciberataques y amenazas a la integridad de las redes y sistemas a bordo. A lo largo de este trabajo hemos explorado diversas áreas de preocupación en la ciberseguridad marítima, desde las redes LAN hasta los protocolos de comunicación como CAN BUS y NMEA. También hemos examinado la importancia de la seguridad en los sistemas SCADA, los RTU, los HMI y los PLC, que desempeñan roles críticos en el control y la supervisión de las operaciones en los buques.

Para mitigar los riesgos y fortalecer la ciberseguridad en los buques, es fundamental implementar una serie de medidas y buenas prácticas. La segmentación de red, mediante la creación de subredes y la restricción del acceso, ayuda a limitar la propagación de ciberataques y proteger los sistemas críticos. La protección antivirus y las actualizaciones regulares de software son esenciales para detectar y prevenir amenazas de malware y vulnerabilidades conocidas. Además, la autenticación sólida y el control de acceso adecuado garantizan que solo personal autorizado pueda interactuar con los sistemas y dispositivos. La implementación de sistemas de detección de intrusiones, ya sea basados en host o en red, permite una vigilancia constante del tráfico y la detección temprana de comportamientos anómalos.

La adopción de protocolos de comunicación más seguros, como OneNet, proporciona mejoras en la confidencialidad, autenticidad e integridad de los datos transmitidos. La utilización de técnicas de criptografía y claves únicas para cada dispositivo fortalece la protección contra ataques de interceptación y manipulación de datos.

En resumen, la ciberseguridad en los buques requiere una combinación de medidas técnicas, prácticas operativas y concienciación del personal. La colaboración entre los fabricantes de equipos marítimos, los operadores de buques y los organismos reguladores es fundamental para establecer estándares y mejores prácticas que garanticen un entorno marítimo seguro y protegido contra las amenazas cibernéticas. La ciberseguridad debe ser una prioridad en el diseño, la implementación y el mantenimiento de los sistemas marítimos, y la formación continua del personal en materia de seguridad cibernética es esencial. Solo a través de un enfoque integral y proactivo hacia la ciberseguridad podremos enfrentar los desafíos y riesgos emergentes en el mundo digitalizado de los buques y proteger de manera efectiva las operaciones y la vida en el mar.

8.3. Conclusiones sobre GNU Radio y HackRF como herramientas de hacking

En esta demostración de ciberseguridad en la marina mercante, se ha logrado realizar un ataque de jamming exitoso a una VHF portátil, partiendo desde cero en radios definidas por software. Esta experiencia personal destaca la importancia crítica de abordar y fortalecer la seguridad de las comunicaciones en la marina mercante.

La demostración ha revelado la vulnerabilidad de las frecuencias abiertas y regladas, como el canal 16 utilizado ampliamente en la marina mercante. Esta frecuencia precisa empleada por todos los buques resulta ser un objetivo vulnerable para ataques de jamming.

La capacidad de analizar el espectro radioeléctrico y detectar las frecuencias exactas utilizadas en las emisoras de VHF portátiles destaca la importancia de contar con herramientas como el HackRF y el programa GNURadio. Estas herramientas han demostrado ser valiosas para comprender las vulnerabilidades y los riesgos asociados con las comunicaciones marítimas

Con base en esta experiencia personal, se recomienda que los profesionales y el personal marítimo adquieran un mayor conocimiento y comprensión de los riesgos cibernéticos en el entorno marítimo. Esto incluye el desarrollo de habilidades y capacidades para detectar y mitigar posibles ataques de ciberseguridad.

En conclusión, esta demostración ha proporcionado una valiosa experiencia personal al realizar un ataque de jamming a una VHF portátil en la marina mercante. Destaca la importancia de tomar medidas proactivas para garantizar la seguridad y la integridad de las comunicaciones a bordo de los buques. Esta experiencia personal resalta la necesidad de mejorar la conciencia y la capacitación en ciberseguridad para proteger eficazmente las comunicaciones en el ámbito marítimo.

9. Bibliografía

1. (INCIBE), V. R. (9 de julio de 2020). *Spoofing y jamming sobre los GNSS*. Obtenido de https://www.incibe-cert.es/blog/spoofing-y-jamming-los-gnss
2. *10 Types of Social Engineering Attacks*. (28 de diciembre de 2021). Obtenido de https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/
3. Airport Technology. (8 de julio de 2022). *Protecting emergency communication systems with HF and VHF radio solutions*. Obtenido de https://www.airport-technology.com/sponsored/protecting-emergency-communications-infrastructure-with-hf-and-vhf-radio-solutions/
4. Akpan, F., Bendiab, G., Shiaeles , S., Karamperidis, S., & Michaloliakos , M. (22 de febrero de 2022). *Cybersecurity Challenges in the Maritime Sector.*
5. Alonso'', J. M. (17 de Noviembre de 2013). Salvados - Entrevista a Chema Alonso por Jordi Évole en Salvados. (J. É. Requena, Entrevistador)
6. Balduzzi, M., Pasta, A., & Wilhoit, K. (8 de diciembre de 2014). *A Security Evaluation of AIS.* Obtenido de https://www.madlab.it/papers/ais_acsac14.pdf
7. Baltic and International Maritime Council, BIMCO. (2020). *The Guidelines on Cyber Security Onboard Ships V4.* Obtenido de https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
8. BBC news. (6 de mayo de 2017). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. Obtenido de https://www.bbc.com/mundo/noticias-39800133
9. Bolentín Oficial del Estado, BOE. (28 de septiembre de 2015). *Ley 36/2015, de Seguridad Nacional.* Obtenido de https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf
10. Boletín Oficial del Estado, BOE. (1 de julio de 1993). *Código internacional de gestión de la seguridad operacional del buque y la prevención de la contaminación (Código Internacional de Gestión de la Seguridad CGS). Resolución A. 741(18), adoptada el 4 de noviembre de 1993, por la Conferencia de los Gobiernos.* Obtenido de https://boe.es/buscar/doc.php?id=BOE-A-1998-11898
11. Boletín Oficial del Estado, BOE. (8 de septiembre de 2018). *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. .* Obtenido de https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

12. Boletín Oficial del Estado, BOE. (26 de enero de 2021). *Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. .* Obtenido de https://www.boe.es/eli/es/rd/2021/01/26/43/dof/spa/pdf
13. Bugeja, J., Jönsson, D., & Jacobsson, A. (23 de marzo de 2018). *An Investigation of Vulnerabilities in Smart Connected Cameras.* Obtenido de https://www.diva-portal.org/smash/get/diva2:1409755/FULLTEXT01.pdf
14. Bureau Veritas. (s.f.). *Cybersecurity & Data Protection*. Obtenido de https://certification.bureauveritas.com/certification/cybersecurity-data-protection
15. Centro Criptológico Nacional, CCN. (2023). *Declaración de Aplicabilidad en el ENS.* Obtenido de https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3830-ccn-cert-bp-14-declaracion-de-aplicacibilidad-ens/file.html
16. CISCO. (2020). *What Is a LAN?* Obtenido de https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html#~what-it-is
17. CNI. (s.f.). *Glosario de terminos y abreviaturas*. Obtenido de https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=97.html
18. Control Automation. (10 de marzo de 2022). *What Is a PLC? An Introduction to Programmable Logic Controllers*. Obtenido de https://control.com/technical-articles/what-is-a-plc-an-introduction-to-programmable-logic-controllers/
19. Costin, A., Khandker, S., Turtiainen, H., & Hämäläinen, T. (16 de febrero de 2023). *Cybersecurity of COSPAS-SARSAT and EPIRB: threat and attacker models, exploits, future research.* Obtenido de https://arxiv.org/pdf/2302.08361.pdf
20. Crowdstrike. (28 de diciembre de 2021). *Cybersecurity 101 › Types of Social Engineering Attacks*. Obtenido de https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/
21. Crowdstrike, Kurt Baker. (13 de febrero de 2023). *10 Most common types of cyber attacks*. Obtenido de https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
22. Departamento de Seguridad Nacional Española. (s.f.). *Ley de Seguridad Nacional*. Obtenido de https://www.dsn.gob.es/es/sistema-seguridad-nacional/ley-seguridad-nacional

23. El Parlamento Europeo y El Consejo de La Unión Europea. (6 de julio de 2016). *DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y.* Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=es

24. Escuela PdR. (s.f.). *Centros de Comunicaciones Radiomarítimas* . Obtenido de http://www.practicasderadiocomunicaciones.com/Modules/Apuntes/tema23.aspx

25. Forsberg, J. (2022). *Cybersecurity of Maritime Communication Systems*. Obtenido de Spoofing attacks against AIS and DSC: https://www.diva-portal.org/smash/get/diva2:1705102/FULLTEXT01.pdf

26. Frisnit Navtex Decoder. (s.f.). *Navtex Data Format*. Obtenido de http://www.frisnit.com/navtex/?id=navtex_data_format

27. Harish, A., Tam, K., & Jones, K. (noviembre de 2022). *Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack.* Obtenido de https://www.researchgate.net/publication/365365607_Investigating_the_Security_and_Accessibility_of_Voyage_Data_Recorder_Data_using_a_USB_attack#:~:text=The%20results%20show%20that%20real-world%20VDR%20data%20might,a%20cyber-attack%20could%20therefore%20le

28. Hatteland Tecnology. (2020). *An introduction to computer networks on board ships*. Obtenido de Smart Ships: https://www.hattelandtechnology.com/blog/introduction-to-computer-networks-on-ships

29. Hipertextual. (30 de diciembre de 2011). *Nevil Maskelyne, el mago que se convirtió en el primer hacker de la historia*. Obtenido de https://hipertextual.com/2011/12/nevil-maskelyne-el-mago-que-se-convirtio-en-el-primer-hacker-de-la-historia

30. Hyra, B. (2019). *Analyzing the Attack Surface of Ships- Brace yourself cyber pirates are coming.* Obtenido de https://backend.orbit.dtu.dk/ws/portalfiles/portal/174011206/190401_Analyzing_the_Attack_Surface_of_Ships.pdf

31. IBM. (17 de noviembre de 2016). *What is the Internet of Things (IoT)?* Obtenido de https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

32. IBM. (2022). *What is cybersecurity?* Obtenido de https://www.ibm.com/topics/cybersecurity

33. IMO. (1 de Junio de 2016). *MSC.1-Circ.1526, INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.* Obtenido de https://www.gard.no/Content/21323229/MSC.1-Circ.1526.pdf

34. IMO. (5 de Junio de 2017). *MSC-FAL.1-Circ.3, GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.* Obtenido de https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

35. IMO. (s.f.). *Introduction To IMO*. Obtenido de https://www.imo.org/en/About/Pages/Default.aspx

36. IMO Maritime Safety Committee. (16 de Julio de 2017). *RESOLUTION MSC.428(98), MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS.* Obtenido de https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

37. IMO, International Maritime Organization. (1976). *SOLAS, Safety OfLife At Sea.* IMO, International Maritime Organization.

38. INCIBE, Instituto Nacional de Ciberseguridad. (9 de julio de 2020). *Spoofing y jamming sobre los GNSS*. Obtenido de https://www.incibe.es/incibe-cert/blog/spoofing-y-jamming-los-gnss

39. Instituto Español de Estudios Estratégicos, IEEE. (9 de diciembre de 2013). *Documento análisis de La Estrategia De Ciberseguridad Nacional .* Obtenido de https://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf

40. Instituto Hidrográfico de la Marina. (s.f.). *Aplicaciones, Avisos A navegantes*. Obtenido de https://armada.defensa.gob.es/ihm/Aplicaciones/Avisos/Index_GAN_xml.html

41. Instituto Nacional de Ciberseguridad de España, INCIBE. (2014). *Qué es INCIBE*. Obtenido de https://www.incibe.es/que-es-incibe

42. International Organization for Standardization, ISO. (Octubre de 2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Obtenido de https://www.iso.org/standard/82875.html

43. James MacKay, MetaCompliance. (2022). *5 Ejemplos De Ataques De Ingeniería Social*. Obtenido de https://www.metacompliance.com/es/blog/phishing-and-ransomware/5-examples-of-social-engineering-attacks

44. Jonggu , K., Bokjin, Y., Deokhwan , C., & Hangsoeb , C. (2009). *Development of Remote Alarm Module with Playback functions in Voyage Data Recorder.* Obtenido de https://www.researchgate.net/publication/238007201_Development_of_Remote_Alarm_Module_with_playback_functions_in_Voyage_Data_Recorder

45. Karpersky daily. (7 de mayo de 2015). *Seguridad de la información durante la Segunda Guerra Mundial: el hackeo de Enigma*. Obtenido de https://www.kaspersky.es/blog/ww2-enigma-hack/6028/

46. Kaspersky Daily . (18 de noviembre de 2014). *El origen de Stuxnet*. Obtenido de https://www.kaspersky.es/blog/el-origen-de-stuxnet/4887/

47. Kessler, G. C. (septiembre de 2021). *The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities.* Obtenido de https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-9cdfc8ae-7d9a-4b0e-9c51-b6355a9a0ceb

48. Marine In Sight. (20 de junio de 2022). *What is An Emergency Position Indicating Radio Beacon (EPIRB)?* Obtenido de https://www.marineinsight.com/marine-safety/what-is-epirb-emergency-position-indicating-radio-beacon/

49. MARLINK. (5 de junio de 2019). *What is Maritime VSAT?* Obtenido de https://marlink.com/what-is-maritime-vsat/

50. Ministerio de la presidencia, relaciones con las cortes y memoria democrática. (29 de marzo de 2022). *El Gobierno aprueba el Plan Nacional de Ciberseguridad.* Obtenido de https://www.mpr.gob.es/prencom/notas/Paginas/2022/290322-ciberseguridad.aspx

51. Ministerio de Transportes, Movilidad y Agenda Urbana. . (s.f.). *Red nacional de estaciones costeras para la seguridad de la vida humana en el mar*. Obtenido de https://www.mitma.gob.es/marina-mercante/nautica-de-recreo/normas-de-seguridad-y-recomendaciones/informacion-meteorologica/red-nacional-de-estaciones-costeras-servicio-movil-maritimo-seguridad-humana

52. Mohamed , A., Elochukwu , U., Hanan , H., David , B., Miroslav , B., Ivan , A., & Xavier , B. (22 de diciembre de 2021). *Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends.* Obtenido de https://www.mdpi.com/2078-2489/13/1/22

53. NATO (OTAN). (2021). *AIS (Automatic Identification System) Overview*. Obtenido de https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview#:~:text=Combined%20with%20a%20shore%20station,the%20hazards%20of%20marine%20navigation.&text=How%20AIS%20Works%3A,built%20into%20an%20AIS%20unit.

54. NATO Shipping Centre. (2021). *AIS (Automatic Identification System) overview*. Obtenido de https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview#:~:text=AIS%20works%20by%20taking%20your,built%20into%20an%20AIS%20unit.

55. NCC GROUP. (2014). *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security.* Obtenido de https://research.nccgroup.com/wp-content/uploads/2020/07/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

56. O'REILLY. (2022). *HTML5 Geolocation by Anthony T. Holdener*. Obtenido de https://www.oreilly.com/library/view/html5-geolocation/9781449308049/ch01.html

57. P.H. Meland, K. Bernsmed, E. Wille, Ø.J. Rødseth, & D.A. Nesheim. (septiembre de 2021). *TransNav; A Retrospective Analysis of Maritime Cyber Security Incidents.* Obtenido de https://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html

58. Parlamento Europeo y El Consejo de La Unión Europea. (14 de diciembre de 2022). *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la .* Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555&from=es

59. Pen Test Partners. (26 de marzo de 2018). *Crashing ships by hacking NMEA sentences*. Obtenido de https://www.pentestpartners.com/security-blog/crashing-ships-by-hacking-nmea-sentences/

60. Pen Tester Partners. (4 de junio de 2018). *Hacking, tracking, stealing and sinking ships*. Obtenido de https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/

61. Pereira, A. C. (2022). *La gestión de los riesgos ciberneticos en los sistemas de seguridad en buques y empreseas navieras.* Obtenido de https://armada.defensa.gob.es/archivo/rgm/2022/03/rgmmar2022cap03.pdf

62. Piccinelli , M., & Gubian, P. (2013). *Modern Ships Voyage Data Recorders: a Forensics Perspective on the Costa Concordia Shipwreck.* Obtenido de https://dfrws.org/sites/default/files/session-files/2013_USA_paper-modern_ships_voyage_data_recorders_-_a_forensics_perspective_on_the_costa_concordia_shipwreck.pdf

63. Presidencia del Gobierno, Gobierno de España. (2013). *Estrategia de Ciberseguridad Nacional .* Obtenido de https://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf

64. Presidencia del Gobierno, Gobierno de España. (5 de diciembre de 2013). *Estrategia de Seguridad Marítima Nacional.* Obtenido de file:///C:/Users/Usuario/Downloads/estrategia%20de%20seguridad%20maritima%20nacional.pdf

65. PrivacyPC, Craig Heffner. (s.f.). *Exploiting network surveillance cameras like a Hollywood hacker*. Obtenido de https://privacy-pc.com/articles/exploiting-network-surveillance-cameras-like-a-hollywood-hacker.html

66. REDES ZONE, Lorena Fernández. (11 de julio de 2020). *Buffer overflow: así funciona esta gran fuente de vulnerabilidades*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/fallo-buffer-overflow-desbordamiento-bufer-que-es/

67. RFC Series (ISSN 2070-1721). (agosto de 1996). *Internet Users' Glossary.* Obtenido de https://www.rfc-editor.org/rfc/rfc1983

68. ROHDE & SCHWARZ. (s.f.). *Receiving BEIDOU, GALILEO and GPS signals with MATLAB and R&S®IQR, R&T TSMW.* Obtenido de https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma203/1MA203_0e_BeiDouSWReceiver.pdf

69. Safety4Sea. (27 de abril de 2021). *What really happened at the Suez Canal?* Obtenido de https://safety4sea.com/cm-what-really-happened-at-the-suez-canal/

70. Salvamento Maritimo . (31 de 8 de 2017). *¿Qué es una RADIOBALIZA/EPIRB?* Obtenido de http://www.salvamentomaritimo.es/sala-de-comunicacion/blog/que-es-una-radiobalizaepirb

71. Salvamento Maritimo . (2021). *NAVTEX y avisos a navegantes*. Obtenido de http://www.salvamentomaritimo.es/mejora-tu-seguridad/control-y-servicios-en-la-mar/navtex-y-avisos-a-navegantes

72. Schuett, C., Butts, J., & Dunlap, S. (5 de febrero de 2014). *An evaluation of modification attacks on programmable logic controllers.* Obtenido de https://pdf.sciencedirectassets.com/277415/1-s2.0-S1874548214X00028/1-s2.0-S1874548214000055/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEJH%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIF%2B66xMFNq7DXnKwO2wpPSw7KZLq8DaYovhQDLTCKKKlAiEA6DkJ6c8YCm

73. Seong, K.-T., & Gwan-Hyung , K. (6 de diciembre de 2019). *Implementation of voyage data recording device using a digital forensics-based hash algorithm.* Obtenido de https://ijece.iaescore.com/index.php/IJECE/article/view/20666/13287

74. SOLAS Cap. 4º. (s.f.). *CAPÍTULO IV - Radiocomunicaciones* . Obtenido de https://personales.gestion.unican.es/martinji/Archivos/SolasCap4.pdf

75. Svilicic, B., Brčić, D., Žuškin, S., & Kalebić, D. (marzo de 2019). *Raising Awareness on Cyber Security of ECDIS.* Obtenido de https://pdfs.semanticscholar.org/d9b6/b2a588c00d802f2da0b2d0623a702d37e7f3.pdf?_gl=1*1rzq0br*_ga*ODMyMzgwOTY1LjE2ODU3MzkxODE.*_ga_H7P4ZT52H5*MTY4NTgwOTIxMy4yLjEuMTY4NTgxMDIwMy42MC4wLjA.

76. TechTarget Security. (noviembre de 2021). *Nimda*. Obtenido de https://www.techtarget.com/searchsecurity/definition/Nimda

77. Tran, K., Keene, S., Fretheim, E., & Tsikerdekis , M. (14 de abril de 2021). *Marine Network Protocols and Security Risks.* Obtenido de https://www.mdpi.com/2624-800X/1/2/13

78. Verizon. (2022). *2022 Data Breach Investigations Report*. Obtenido de https://www.verizon.com/business/resources/reports/dbir/

79. VTSCADA. (s.f.). *Marine SCADA Systems*. Obtenido de https://www.vtscada.com/marine-systems-overview/

80. WICO. (s.f.). *SCADA de una EDAR (Estación depuradora de aguas residuales)*. Obtenido de https://wico.com.es/scada-de-una-edar/

81. Xiaojun , P., Zhuoran , W., & Yanbin , S. (28 de junio de 2020). *Review of PLC Security Issues in Industrial Control System.* Obtenido de https://www.proquest.com/openview/325a52cdb9e28bf03bfe2143d1dbd133/1?pq-origsite=gscholar&cbl=4585457

10. Anexos

01.- Anexo I. Glosario de acrónimos.

AIS: Automatic Identification System, en español, sistema de identificación automática, transmite la ubicación, identidad, rumbo y velocidad de las embarcaciones

ARP, protocolo: Address Resolution Protocol, en español, protocolo de resolución de direcciones. Es un protocolo de comunicaciones, vincula una dirección MAC o dirección física, con una dirección IP o dirección lógica.

BIMCO: “Baltic and International Maritime Council”. En español, “Consejo Marítimo Internacional y del Báltico”. Asociación internacional de transporte marítimo que representa a los armadores.

BIOS: “Basic Input/Output System” En español, sistema básico de entrada/salida. Es el firmware que se carga antes que el sistema operativo.

BOE: Boletín Oficial del Estado. Es el diario oficial nacional español dedicado a la publicación de leyes, disposiciones y actos de inserción obligatoria.

BUS, topología: Una red en bus es aquella topología que se caracteriza por tener un único bus de comunicaciones al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal.

CAN BUS: Controller Area Network. Protocolo orientado a mensajes desarrollado por la firma alemana Robert Bosch GmbH.

CCTV: Closed Circuit Television. En español, Circuito Cerrado de Televisión. Tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades

CERT: Computer Emergency Response Team. Centro de respuesta para incidentes de seguridad en tecnologías de la información.

CSIRT: Computer Security Incident Response Team. Equipo de Respuesta ante Incidencias de Seguridad Informáticas

CIA, triada: Confidencialidad, Integridad y Disponibilidad.

CNI: Centro Nacional de Inteligencia. Es el servicio de inteligencia de España, creado en 2002 como sucesor del antiguo Centro Superior de Información de la Defensa

COG: Course Over Ground. Es la dirección real de avance de un buque, entre dos puntos, sobre la superficie terrestre.

COLREG: Convention on the International Regulations for Preventing Collisions at Sea. Convenio sobre el Reglamento internacional para prevenir los abordajes adoptado por la Organización Marítima Internacional en 1972.

COSPAS-SARSAT: COSPAS es un acrónimo de las palabras rusas "Cosmicheskaya Sistema Poiska Avariynyh Sudov", que se traduce como "Sistema Espacial para la Búsqueda de buques en peligro". SARSAT es un acrónimo de Search And Rescue Satellite-Aided Tracking. Es un elemento de Sistema mundial de socorro y seguridad marítimos

CRC, cálculo: Cyclic Redundancy Check. En español verificación por redundancia cíclica. Es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.

DDoS: “Distributed Denial-of-Service”. En español, “ataque distribuido de denegación de servicio”. Es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado, proveniente de diversas fuentes, para que no pueda funcionar correctamente.

DNS: “Domain Name System”. En español “sistema de nombres de dominio”. Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada

DoS: “Denial-of-service attack”. En español, “Ataque de denegación de servicio”. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimo.

ECDIS: “Electronic Chart Display and Information System”. Español, “Sistema de información y visualización de cartas electrónicas”.

EMSA: “European Maritime Safety Agency”. La agencia comunitaria encargada de facilitar el asesoramiento técnico y asistencia en el ámbito de la seguridad y protección marítimas.

EPIRB: “Emergency Position Indicating Radio Beacon”. Aparato transmisor de radio utilizado en situaciones de emergencia para facilitar la localización de un barco, un avión o una persona que se encuentre en peligro.

GMSK: “Gaussian minimum shift keying”. En español “modulación por desplazamiento mínimo gaussiano”. Es un esquema de modulación digital por desplazamiento de frecuencia de fase continua.

GNSS: “Global Navigation Satellite System”. En español “sistema global de navegación por satélite”. Constelación de satélites que transmite rangos de señales utilizados para el posicionamiento y localización en cualquier parte del globo terrestre, ya sea en tierra, mar o aire.

GPS: “Global Positioning System”. En español, “Sistema de Posicionamiento Global”. Sistema estadounidense que permite a un dispositivo receptor localizar su propia posición en el globo.

HF: “High Frequency”. En español, “Alta frecuencia” u Onda corta. Banda del espectro electromagnético englobada entre los 3 y los 30 megahercios.

HID: “Human Interface Device”. En español, “dispositivo de interfaz humana”. Interfaces de usuario para computadores que interactúan directamente, tomando entradas provenientes de humanos, y pueden entregar una salida a los humanos.

HMI: “Human-Machine Interface”. En español, “Interfaz Humano-Maquina”. Panel que permite a un usuario comunicarse con una máquina, software o sistema.

HTTP: “Hypertext Transfer Protocol”. En español, “Protocolo de Transferencia de Hipertexto en español”. Protocolo de comunicación que permite las transferencias de información a través de archivos en la World Wide Web.

ICS: “Industrial Control Systems”. En español, “Sistemas de Control Industrial”. Término general que abarca varios tipos de sistemas de control e instrumentos asociados utilizados para el control de procesos industriales.

IGS, código: Código internacional de gestión de la seguridad operacional del buque y la prevención de la contaminación. Normativa internacional para la gestión y operación de los buques en condiciones de seguridad y la prevención de la contaminación.

IMO: “International Maritime Organization”. En español, OMI, “Organización Marítima Internacional”. Organismo especializado de las Naciones Unidas que promueve la cooperación entre Estados y la industria de transporte para mejorar la seguridad marítima y para prevenir la contaminación marina.

IoT: “Internet Of Things”. En español, “Internet de las Cosas”. Describe la red de objetos físicos ("cosas") que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet.

IPv4: “Internet Protocol version 4”. Formato de dirección estándar que permite que todas las máquinas en Internet se comuniquen entre sí

IPv6: “Internet Protocol version 6”. Actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.

IT: “Information Technology”. En español, TI, “Tecnología de la Información”. Lsa aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas

JSON, formato: “JavaScript Object Notation”. En español, “notación de objeto de JavaScript”. Es un formato de texto sencillo para el intercambio de datos.

LADDER, lenguaje: Lenguaje de programación gráfico muy popular dentro de los autómatas programables debido a que está basado en los esquemas eléctricos de control clásicos.

LAN: “Local Area Network”. En español, “Red de Área Local”. Red de computadoras que permite la comunicación y el intercambio de datos entre diferentes dispositivos a nivel local.

LSD: “Llamada Selectiva Digital”. En inglés, DSC, “Digital Selective Calling”. Técnica de transmisión automática de llamadas por radio de frecuencias medias (MF), altas (HF) o muy altas (VHF) que utiliza mensajes codificados en formato digital.

MAC, dirección: “Media Access Control”. La dirección MAC es dirección física de la tarjeta de red. Se trata de un identificador único que es asignado por el fabricante a cada equipo de hardware de red. MAC, se refiere al conjunto de protocolos comunicacionales por medio del cual, varios equipos o dispositivos conectados a la red acuerdan usar conjuntamente un determinado medio de transmisión.

MF: “Medium Frequency”. En español, OM, “Onda Media”. Banda del espectro electromagnético que ocupa el rango de frecuencias de 300 kilohercios a 3 megahercios.

MITM: “Man-In-The-Middle”. En español, “Ataque de Hombre en el Medio”. Ataque de intermediario, en el que el atacante adquiere la capacidad de leer, insertar y modificar a voluntad datos en la red o dispositivo atacado.

MLAT: “Multilateración”. Técnica de navegación basada en la medición de la diferencia de distancia a dos estaciones en posiciones conocidas por señales de emisión (emitidas) en tiempos conocidos. La multilateración es una técnica común en los sistemas de radionavegación, donde se conoce como navegación hiperbólica.

MMSI, número: “Maritime Mobile Service Identity ” Serie de nueve dígitos que identifica inequívocamente a cada estación del servicio móvil digital (estaciones costeras y estaciones de barco).

MRCC: “Maritime Rescue Co-ordination Centres”. Las alertas, llamadas y mensajes prioritarios de socorro transmitidos por la red Inmarsat se gestionan a través de sus Estaciones Terrestres (LES) o Estaciones de Acceso a Tierra (SAS) a los Centros de Coordinación de Salvamento Marítimo (MRCC) en tierra de todo el mundo.

NAVTEX: “NAVigational TEXt Messages”. sistema para transmitir y recibir automáticamente información sobre seguridad marítima utilizando la telegrafía de impresión directa de banda estrecha. Es uno de los equipos que se encuadran en el Sistema Mundial de Socorro y Seguridad Marítima.

NMEA, estándar: “National Marine Electronics Association”. Asociación fundada en 1957 por un grupo de fabricantes de electrónica para obtener un sistema común de comunicación entre las diferentes marcas de electrónica naval, generando los estándar NMEA.

OT: “Operation Tecnology”. En español, “Tecnología de las Operaciones”. Hardware y software para monitorear y controlar los procesos físicos, los dispositivos y la infraestructura

OTAN: “Organización del Tratado del Atlántico Norte”, En inglés, NATO, “North Atlantic Treaty Organization”. Alianza militar intergubernamental que se rige por el Tratado del Atlántico Norte o Tratado de Washington, firmado el 4 de abril de 1949.

PKI: “Public Key Infrastructure”. En español,” infraestructura de clave pública”. Conjunto de roles, políticas, hardware, software y procedimientos necesarios para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública.

PLC: “Programmable Logic Controller”. En español “Controlador Lógico Programable” Computadora utilizada en la ingeniería automática o automatización industrial, para automatizar procesos electromecánicos, electroneumáticos, electrohidráulicos, tales como el control de la maquinaria de un buque u otros procesos de producción.

RADAR: “RAdio Detecting And Ranging”. En español, “detección y localización por radio”. Sistema que usa ondas electromagnéticas para medir distancias, altitudes, direcciones y velocidades de objetos.

RJ-45: “Registered Jack - 45”. Interfaz física comúnmente utilizada para conectar redes de computadoras con cableado estructurado.

SART: “Search and Rescue Transponder”. Transpondedor autónomo y estanco destinado a un uso de emergencia en el mar. Estos dispositivos pueden ser un radar-SART o un AIS-SART basado en GPS.

SCADA: “Supervisory Control And Data Acquisition”. En español, “Control Supervisor y Adquisición de Datos”. Concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales

SMS: “Short Message Service”. Servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos entre teléfonos móviles.

SMSSM: “Sistema Mundial de Socorro y Seguridad Marítimos”. En inglés, GMDSS, “Global Maritime Distress Safety System”. Conjunto de procedimientos de seguridad, equipos y protocolos de comunicación diseñados para aumentar la seguridad, facilitar la navegación y el rescate de embarcaciones en peligro.

SoA: “Statement of Applicability”. En español “Declaración de Aplicabilidad”. Documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001.

SOLAS: “International Convention for the Safety of Life at Sea”. En español, “Convenio Internacional para la Seguridad de la Vida en el Mar”. El más importante de todos los tratados internacionales sobre la seguridad de los buques

SQL: “Structured Query Language”. Lenguaje específico de dominio, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos relacionales.

TIC: “Tecnologías de la Información y las Comunicaciones”. Término extensivo para la tecnología de la información (TI) que enfatiza el papel de las comunicaciones unificadas,1 la integración de las telecomunicaciones (líneas telefónicas y señales inalámbricas) y las computadoras, así como el software necesario, el middleware, almacenamiento, sistemas audiovisuales y producción audiovisual, que permiten a los usuarios acceder, almacenar, transmitir y manipular información.

TRB: “Toneladas de Registro Bruto”. En inglés, GRT, “gross register tonnage”. unidades GT

UE: “Unión Europea”. Comunidad política de derecho constituida en régimen sui géneris de organización internacional fundada para propiciar y acoger la integración y gobernanza en común de los Estados y las naciones de Europa.

UIN: “Unique Identifier Number”. Cadena numérica o alfanumérica asociada a una única entidad dentro de un sistema determinado

USB: “Universal Serial Bus”. En español “Bus Universal en Serie”. Bus de comunicaciones que sigue un estándar que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.

UTC: “Coordinated Universal Time”. Principal estándar de tiempo por el cual el mundo regula los relojes y el tiempo

UTF-8, codificación: “8-bit Unicode Transformation Format”. Formato de codificación de caracteres Unicode e ISO 10646 que utiliza símbolos de longitud variable.

VHF: “Very High Frequency”. En español, “muy alta frecuencia”. Se corresponde con la banda del espectro electromagnético que ocupa el rango de frecuencias de entre 30 y 300 megahercios.

VSAT: “Very Small Aperture Terminals”. En español, “terminal de apertura muy pequeña”. Redes privadas de comunicación de datos vía satélite para intercambio de información punto -punto o, punto-multipunto (broadcasting) o interactiva.

VSS: “video surveillance systems”. Sinónimo del CCTV

WAN: “Wide Area Network”. En español, “Red de Área Amplia”. Red de computadoras que une e interconecta varias redes de ámbito geográfico mayor, por ejemplo, redes de área local, aunque sus miembros no estén todos en una misma ubicación física.

XSS: “Cross-site scripting”. tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar.

Permiso de divulgación del Trabajo Final de Grado

El alumno **Adrián Rodríguez Machado**, autor del trabajo final de Grado titulado **"Ciberseguridad en la Marina Mercante"** y tutorizado por el/los profesor/es **José Agustín González Almeida,** a través del acto de presentación de este documento de forma oficial para su evaluación (registro en la plataforma de TFG), manifiesta que **PERMITE** la divulgación de este trabajo, una vez sea evaluado, y siempre con el consentimiento de su/s tutor/es, por parte de la Escuela Politécnica Superior de Ingeniería, del Departamento de Ingeniería Civil, Náutica y Marítima y de la Universidad de La Laguna, para que pueda ser consultado y referenciado por cualquier persona que así lo estime oportuno en un futuro.

Esta divulgación será realizada siempre que ambos, alumno y tutor/es del Trabajo Final de Grado, den su aprobación. Esta hoja supone el consentimiento por parte del alumno, mientras que el profesor, si así lo desea, lo hará constar en futuras reuniones, una vez finalizado el proceso de evaluación del mismo.