DISEÑO DE PROTOCOLOS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS GENERADOS POR SISTEMAS DE EXPLORACIÓN MARÍTIMA Y OPERACIONES SUBACUÁTICAS EN LA ARMADA NACIONAL DE COLOMBIA

Mayor de I.M. YERSON ALEJANDRO TORRES BUENO

ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"
BOGOTÁ D.C., COLOMBIA
2025

DISEÑO DE PROTOCOLOS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS GENERADOS POR SISTEMAS DE EXPLORACIÓN MARÍTIMA Y OPERACIONES SUBACUÁTICAS EN LA ARMADA NACIONAL DE COLOMBIA

YERSON ALEJANDRO TORRES BUENO

Trabajo de Grado presentado como requisito para optar al título de profesional:
MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

Director
DO. SAMUEL IGNACIO RIVERA PAEZ

ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"
BOGOTÁ D.C., COLOMBIA
2025

TABLA DE CONTENIDO

Lista de Tablas

Tabla de ilustración

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del Director

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., Junio de 2025

Resumen

La creciente integración de tecnologías digitales en el ámbito marítimo ha transformado las operaciones de exploración y buceo de la Armada Nacional de Colombia. Sin embargo, esta evolución también ha incrementado significativamente la superficie de exposición a amenazas cibernéticas. El presente trabajo propone un protocolo de ciberseguridad diseñado específicamente para proteger los datos generados por sistemas de información y tecnologías subacuáticas, como los equipos de buceo CCR Liberty y los Vehículos Operados Remotamente (ROV) Seaeye Lynx 1160, empleados en misiones de inspección, salvamento y exploración del patrimonio cultural sumergido. La metodología empleada es de tipo descriptivo y cualitativo, basada en el análisis de riesgos bajo los criterios de confidencialidad, integridad y disponibilidad (CID), junto con la aplicación de normas internacionales ISO/IEC 27001 e IEC 62443. Se identificaron activos críticos, vulnerabilidades técnicas y riesgos asociados en los sistemas operativos de buceo, proponiendo medidas de mitigación estructuradas en capas. Como resultado, se construyó un protocolo técnico que articula buenas prácticas de ciberseguridad, controles operacionales, evaluación continua y trazabilidad, con el objetivo de fortalecer la defensa digital de los datos sensibles generados en entornos subacuáticos.

Palabras clave: ciberseguridad, buceo, ROV, CCR Liberty, Armada Nacional, ISO 27001, IEC 62443, protocolo, patrimonio sumergido.

Abstract

The increasing integration of digital technologies in the maritime domain has transformed the exploration and diving operations of the Colombian Navy. However, this evolution has also significantly expanded the surface vulnerable to cyber threats. This research proposes a cybersecurity protocol specifically designed to protect the data generated by information systems and underwater technologies, such as CCR Liberty diving equipment and Seaeye Lynx 1160 Remotely Operated Vehicles (ROVs), used in missions of inspection, salvage, and submerged cultural heritage exploration. The methodology employed is descriptive and qualitative, based on risk analysis under the criteria of confidentiality, integrity, and availability (CID), in conjunction with international standards ISO/IEC 27001 and IEC 62443. Critical assets, technical vulnerabilities, and associated risks in the Navy's diving operational systems were identified, and mitigation measures were proposed through a layered approach. As a result, a technical protocol was developed that incorporates best practices in cybersecurity, operational controls, continuous evaluation, and traceability, with the objective of strengthening the digital defense of sensitive data generated in underwater environments.

Keywords: cybersecurity, diving, ROV, CCR Liberty, Colombian Navy, ISO 27001, IEC 62443, protocol, submerged heritage.

Introducción

En el contexto de las operaciones de exploración subacuática y patrimonial realizadas por el Comando de Alistamiento de Buceo de la Armada Nacional, la protección de los datos generados por sistemas tecnológicos como los vehículos operados remotamente (ROV) y sistemas de respiración de circuito cerrado (CCR) se ha convertido en una necesidad crítica (Ammar & Khan, 2024). Estos sistemas recolectan información sensible que puede estar sujeta a riesgos derivados de amenazas cibernéticas, tales como el acceso no autorizado, la manipulación de datos y el sabotaje tecnológico (Li et al., 2024, como se citó en Ammar & Khan, 2024). A pesar del avance en los sistemas de navegación, sensores y comunicaciones navales, actualmente no existen protocolos específicos de ciberseguridad aplicados a la protección de dicha información (Akpan et al., 2022).

El desarrollo de esta investigación parte del reconocimiento de una vulnerabilidad operacional y estratégica que afecta directamente la seguridad de las operaciones navales, la integridad de los datos científicos y la conservación del patrimonio cultural sumergido, como es el caso del Galeón San José (Delgado, 2020). Así, este documento tiene como propósito proponer un protocolo técnico de ciberseguridad que permita mitigar los riesgos, asegurar la trazabilidad de los datos, garantizar su integridad y establecer un modelo operativo aplicable por el Comando de Alistamiento Buceo.

Esta investigación se fundamenta en un enfoque descriptivo y aplicado, mediante análisis documental y normativo con base en estándares internacionales como ISO/IEC 27001, NIST SP 800-82 e IEC 62443 (NQA, 2020), así como directrices de ciberdefensa institucional. La estructura de la monografía aborda inicialmente el problema de investigación, seguido de un marco referencial integral, una metodología científica clara, el diagnóstico del entorno tecnológico y operacional, el diseño del protocolo propuesto y una evaluación de viabilidad (Sampieri, Collado, & Lucio, 2014).

De esta manera, se contribuye al fortalecimiento de la ciberdefensa en el dominio marítimo, brindando herramientas prácticas y normativas que permitan proteger los datos estratégicos generados por la Armada Nacional en sus operaciones subacuáticas, incluyendo aquellas de alto valor como la inspección del Galeón San José.

1 Planteamiento del problema

1.1 Descripción del Problema

Las operaciones de exploración subacuática ejecutadas por el Comando de Alistamiento de Buceo de la Armada Nacional involucran la utilización de equipos y sistemas altamente especializados, tales como los ROV, CCR, ecosondas multihaz, sonares de barrido lateral, sensores inerciales y plataformas oceanográficas (Ferri et al., 2017, p. 4). La información recolectada por estos sistemas es almacenada en discos duros, bases de datos locales y sistemas distribuidos, muchos de los cuales carecen de mecanismos robustos de protección, encriptación, trazabilidad o respaldo (Ammar & Khan, 2024).

Esta situación genera una alta exposición frente a amenazas cibernéticas como el ransomware, la manipulación de información, la interceptación de señales, la alteración de coordenadas GNSS y la denegación de servicio (DoS) (Guananga Reyna & Rodríguez Espinosa, 2023). La inexistencia de un protocolo formal de ciberseguridad para estas plataformas representa una vulnerabilidad estructural para la defensa nacional, la seguridad marítima y la protección del patrimonio arqueológico sumergido de la Nación (Weerth, 2020, p. 5).

1.2 Formulación del problema

¿Qué protocolo de ciberseguridad puede diseñarse para proteger los datos generados por sistemas de exploración marítima y operaciones subacuáticas realizadas por el Comando de Buceo de la Armada Nacional de Colombia?

1.3 Objetivo general

Implementar un protocolo integral de ciberseguridad que garantice la protección de los datos y sistemas utilizados en las operaciones de exploración marítima y subacuáticas de la Armada Nacional, integrando los dominios de Tecnologías de la Información (TI), Tecnologías Operativas (TO) y Ciberseguridad (CS), conforme a estándares internacionales y al entorno operacional naval.

1.4 Objetivos específicos

- Analizar las vulnerabilidades existentes en la gestión de los datos generados por los sistemas de exploración marítima y operaciones subacuáticas del Comando de Alistamiento de Buceo, considerando amenazas cibernéticas y riesgos operacionales.

- Examinar las mejores prácticas internacionales y los marcos normativos aplicables a la protección de infraestructuras críticas, sistemas ciberfísicos y tecnologías subacuáticas en entornos militares y científicos.
- Diseñar un protocolo integral de ciberseguridad para la Armada Nacional de Colombia, que articule mecanismos técnicos, normativos y operativos para la protección y el acceso seguro a la información reservada generada durante misiones subacuáticas.

1.5 Justificación

La protección de los datos generados durante las operaciones subacuáticas no solo es un imperativo técnico, sino una necesidad estratégica para la Armada Nacional de Colombia. La creciente dependencia de sistemas ciberfísicos, como los equipos CCR Liberty y los ROV Seaeye Lynx, implica que cualquier vulnerabilidad en la infraestructura digital puede traducirse en pérdidas operacionales, compromisos de información clasificada o incluso en riesgos para la vida de los buzos desplegados en entornos extremos (Tamarkar & Patra, 2018).

La ausencia de protocolos específicos para salvaguardar los datos recolectados en este tipo de misiones deja expuestos activos críticos, como bases de datos operacionales, sensores conectados, firmware no autenticado y comunicaciones digitales sin cifrado. Según Verma, Singh, Kumar, & Sharma, (2025), "la falta de una política de ciberseguridad adaptada a los sistemas subacuáticos puede generar vectores de ataque persistentes que los protocolos tradicionales no detectan". Esto es especialmente relevante en escenarios como el del Galeón San José, donde las evidencias recolectadas tienen valor legal, científico, económico y geopolítico.

Adicionalmente, los estándares internacionales como ISO/IEC 2700, que de acuerdo con Joseph y Fred (2023). “marco de referencia para que las organizaciones puedan establecer, implementar, mantener y mejorar continuamente su seguridad de la información”, e IEC 62443 ofrecen lineamientos robustos para el diseño de controles de seguridad, pero su aplicación efectiva requiere ser adaptada al contexto operacional de la institución. En este sentido, el presente trabajo pretende cubrir un vacío metodológico y normativo, proponiendo un protocolo técnico y operacional que pueda ser adoptado por el Comando de Alistamiento de Buceo y sus Departamentos como herramienta de protección de la información generada durante sus misiones.

Desde el punto de vista académico y práctico, esta investigación también aporta una perspectiva interdisciplinaria entre ciberseguridad, defensa, tecnología marina y gobernanza digital, como afirma el siguiente autor:

> "En ciberseguridad, se entiende por riesgo la probabilidad de que una amenaza pueda explotar las vulnerabilidades de un activo que represente un cierto impacto para una organización. Estos riesgos deben afrontarse de manera integral (es decir, teniendo en cuenta todos y cada uno de los factores que pueden influir en la exposición de los activos a determinadas amenazas) a fin de identificar las salvaguardas (técnicas, organizacionales, procedimentales, contractuales o legales) que ayudarán a reducir ese riesgo a límites aceptables." (Organización Marítima Internacional [OMI], 2022)

1.6 Delimitación

La investigación se limita al estudio de los sistemas tecnológicos actualmente empleados por el Comando de Buceo de la Armada Nacional, con especial atención en los ROV, CCR, plataformas oceanográficas, sensores acústicos, GNSS y sistemas de almacenamiento de datos (Ferri et al., 2017, p. 6). La propuesta del protocolo se circunscribe al ámbito operativo nacional, en el marco doctrinal, técnico y legal vigente hasta el año 2025.

2 Capítulo 2 - Marco referencial

2.1 Antecedentes

El desarrollo de protocolos de ciberseguridad en entornos marítimos ha sido abordado de manera fragmentada en la literatura, con énfasis en infraestructuras críticas portuarias, redes navales y sistemas de navegación satelital. En el contexto colombiano, se identifican vacíos normativos y técnicos en cuanto a la protección de datos generados en operaciones subacuáticas, especialmente en misiones científicas, de rescate o de conservación patrimonial, como las ejecutadas por el Comando de Alisamiento de Buceo a través de los Departamentos de buceo de la Armada Nacional.

Estudios como los de Guananga Reyna y Rodríguez Espinosa (2023) plantean la necesidad de adaptar los marcos de ciberseguridad a los sistemas subacuáticos automatizados, considerando la particularidad de los sensores y protocolos de comunicación utilizados en operaciones a profundidad. Igualmente, Weerth (2020) documenta cómo los narcotraficantes

han aprovechado debilidades tecnológicas en subsistemas marítimos, lo cual evidencia el uso creciente del ciberespacio como dominio de conflicto en el entorno naval.

Por su parte, Ammar & Khan, (2024) advierten sobre la falta de segmentación de redes y la ausencia de cifrado extremo a extremo en sistemas como los ROV y CCR, lo que los convierte en blancos vulnerables para ataques persistentes avanzados (APT). En términos de aplicación doctrinal, Guananga Reyna, L. A., & Rodríguez Espinosa, M. (2023), sostiene que la Armada Nacional debe integrar las capacidades de su Centro de Operaciones de Seguridad (SOC) con las operaciones subacuáticas, bajo una arquitectura de protección activa basada en la doctrina de defensa en profundidad. La ilustración 1 presenta una síntesis cronológica de estos hitos clave en la evolución de las capacidades tecnológicas subacuáticas y los desarrollos normativos en ciberseguridad marítima, desde la primera exploración del Galeón San José hasta las iniciativas recientes lideradas por la Armada Nacional.

Ilustración 1. Evolución de la ciberseguridad marítima en Colombia (línea de tiempo).

Nota: Línea de tiempo que presenta los principales hitos tecnológicos, normativos y operativos relacionados con la evolución de los sistemas de exploración marítima y la ciberseguridad aplicada en el contexto naval colombiano, con énfasis en el caso del Galeón San José y la modernización de capacidades de la Armada Nacional. Fuente: Elaboración propia con base en datos de Weerth (2020), Guananga Reyna y Rodríguez Espinosa (2023), y documentos oficiales de la Armada Nacional de Colombia.

2.2 Marco teórico

El presente trabajo de investigación se basa en la intersección entre la ciberseguridad, la protección de infraestructuras críticas y el despliegue de sistemas ciberfísicos en ambientes

marítimos, particularmente en operaciones subacuáticas como las desarrolladas por la Armada Nacional de Colombia, a través de sus unidades de Buceo.

La ciberseguridad se define como el conjunto de herramientas, políticas, conceptos de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas y tecnologías que pueden usarse para proteger los activos de una organización frente a ataques del ciberespacio (Organización Internacional de Normalización [ISO], 2012). Esta disciplina abarca la protección de la información, sistemas, redes, servicios y dispositivos frente a accesos no autorizados, alteraciones, destrucción o interrupciones.

En entornos operacionales complejos, como los marítimos, se integran sistemas ciberfísicos (CPS): redes de dispositivos que combinan hardware, software embebido, sensores, actuadores y canales de comunicación para interactuar con el entorno físico (Guerrero-Bonilla, González-Vázquez, & Gómez-Aguilar, 2022). Estos sistemas pueden ser altamente vulnerables debido a la exposición a condiciones extremas, la dependencia de sensores y la conectividad constante.

En el ámbito de la infraestructura crítica, se considera crítica toda aquella infraestructura cuya alteración, interrupción o destrucción pueda tener un impacto significativo en la seguridad nacional, la economía o la salud pública. En el caso de la Armada Nacional, los datos generados por sistemas como los ROV (Remotely Operated Vehicles), CCR (Closed Circuit Rebreathers), sistemas de comando y control y estaciones de monitoreo se clasifican como activos críticos por su relevancia estratégica y operacional.

Desde el punto de vista doctrinal, los marcos de referencia como ISO/IEC 27001 (ISO, 2022) para sistemas de gestión de seguridad de la información, NIST SP 800-53 para controles de seguridad y privacidad (National Institute of Standards and Technology [NIST], 2020), e IEC 62443 para entornos industriales, ofrecen lineamientos técnicos y normativos ampliamente aceptados para reducir riesgos, gestionar vulnerabilidades y fortalecer la resiliencia digital (Instituto Nacional de Ciberseguridad [INCIBE], 2023).

Finalmente, la literatura especializada también enfatiza la necesidad de adoptar una estrategia de defensa en profundidad, que integre múltiples capas de protección, física, lógica, de red, de procesos y estratégica y promueva la capacidad institucional de detectar, responder y recuperarse ante incidentes cibernéticos (Verma et al., 2025).

2.2.1 Sistemas ciber físicos en operaciones subacuáticas

Los sistemas ciberfísicos (CPS) constituyen una arquitectura tecnológica que integra componentes físicos (hardware, sensores, actuadores) con módulos digitales (software embebido, algoritmos de control, redes de comunicación), permitiendo la interacción directa con el entorno físico en tiempo real (Guerrero-Bonilla, Parra-Velandia & Cruz, 2022). En el contexto marítimo, los CPS permiten ejecutar misiones de exploración, monitoreo ambiental, rescate o investigación arqueológica mediante una interacción sincronizada entre plataformas físicas sumergibles y centros de comando costeros o embarcados.

Dentro de las operaciones subacuáticas de la Armada Nacional, destacan como CPS los vehículos operados remotamente (ROV), como el Seaeye Lynx, capaces de transmitir imágenes, datos georreferenciados y lecturas de sensores desde profundidades superiores a los 600 metros. Igualmente, los equipos de respiración de circuito cerrado (CCR), como el CCR Liberty, incorporan sensores electrónicos que monitorean gases, profundidad y temperatura, enviando datos a microcontroladores que gestionan la mezcla respirable en tiempo real. Además, plataformas oceanográficas, ecosondas, sonares de barrido lateral y sistemas de navegación inercial forman parte de la arquitectura de CPS aplicada en el Comando de Buceo.

Estos sistemas, aunque altamente sofisticados, enfrentan riesgos crecientes en términos de ciberseguridad. Entre los más relevantes se encuentran: la manipulación remota del firmware, el secuestro de señales GNSS, la inyección de datos falsos (spoofing), la denegación de servicio (DoS) y el acceso no autorizado a las transmisiones de video y datos operacionales (Ahmad et al., 2024, p. 5). Este tipo de amenazas puede comprometer la integridad de las operaciones, alterar resultados científicos o permitir la filtración de información clasificada, lo que representa un riesgo estratégico para la soberanía marítima y la defensa nacional (Guananga Reyna & Rodríguez Espinosa, 2023, p. 7).

Por estas razones, la caracterización técnica y operativa de los CPS utilizados en ambientes subacuáticos se constituye en un pilar fundamental para el diseño del protocolo de ciberseguridad propuesto en esta investigación.

2.2.2 Principios de ciberseguridad

La ciberseguridad, en su dimensión más estructural, se fundamenta en tres principios esenciales: confidencialidad, integridad y disponibilidad, conocidos como la triada CIA (Confidentiality, Integrity, Availability). Estos pilares definen la base sobre la cual se diseñan los controles,

protocolos y políticas de protección digital en cualquier entorno operativo (Organización Internacional de Normalización [ISO], 2012, p. 2).

- **Confidencialidad** implica restringir el acceso a los datos únicamente a personas autorizadas, evitando filtraciones que puedan comprometer operaciones sensibles.
- **Integridad** busca garantizar que la información no sea modificada de manera indebida o accidental durante su almacenamiento o transmisión.
- **Disponibilidad** asegura que los sistemas, servicios y datos estén accesibles y operativos cuando se requieran, especialmente durante misiones críticas o en escenarios de emergencia.

Además de estos principios, cobra relevancia el concepto de defensa en profundidad, que propone la DISEÑO de múltiples capas de protección para evitar que una falla comprometa todo el sistema. Estas capas incluyen controles físicos, lógicos, de red, de aplicación, de usuarios y de procesos (Verma & Raza, 2025, p. 6).

Por otra parte, la ciberresiliencia se ha convertido en un componente clave de la seguridad moderna. Este concepto hace referencia a la capacidad institucional de anticiparse, resistir, recuperarse y adaptarse frente a incidentes cibernéticos sin comprometer sus funciones esenciales (NIST, 2020, p. 19). En entornos navales como el del Comando de Buceo, la ciberresiliencia es indispensable para garantizar continuidad operativa, trazabilidad de datos recolectados por los ROV o CCR, y protección de información crítica durante misiones estratégicas.

Integrar estos principios en el diseño de un protocolo robusto no solo mejora la postura de seguridad digital, sino que fortalece la capacidad operativa general de la Armada frente a amenazas emergentes del ciberespacio.

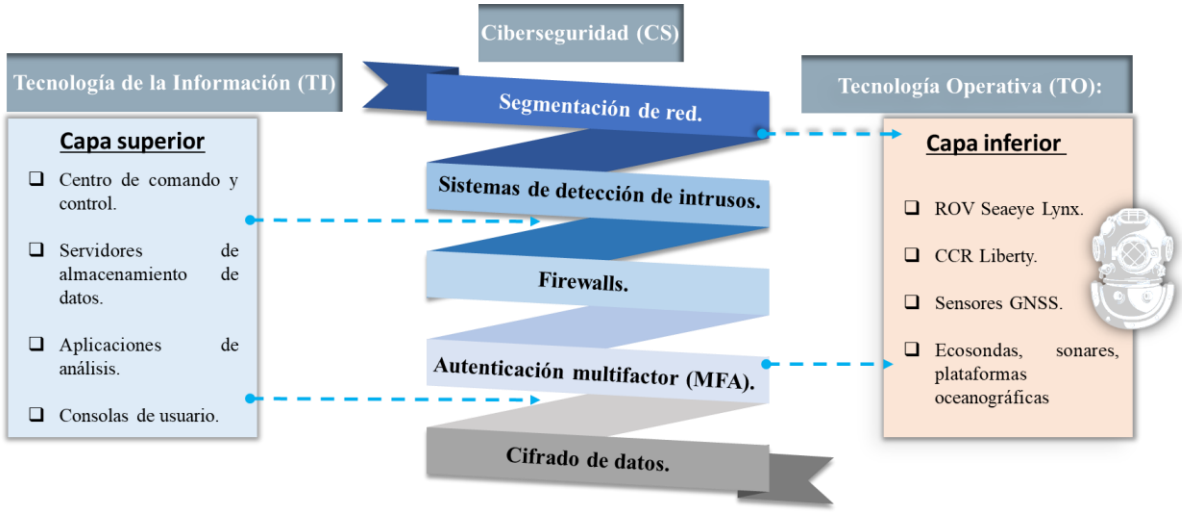
2.2.3 Convergencia TI–TO–CS

En la actualidad, los entornos operacionales complejos, como las plataformas navales, exigen una convergencia efectiva entre Tecnologías de la Información **(TI),** Tecnologías Operativas **(TO)** y Ciberseguridad **(CS)**. Esta integración implica armonizar los sistemas de procesamiento de datos, comunicación, análisis y supervisión (TI), con los sistemas físicos y de control que gestionan procesos operacionales en tiempo real (TO), bajo un enfoque de protección continua frente a amenazas del ciberespacio (CS) (Guananga Reyna & Rodríguez Espinosa, 2023).

Esta convergencia digital es clave para mantener la interoperabilidad entre los ROV, sensores, plataformas oceanográficas y centros de comando. Sin embargo, también introduce nuevos vectores de ataque en la frontera TI–TO, donde históricamente existían barreras físicas o desconexiones de red.

Las interacciones entre dominios deben ser cuidadosamente diseñadas y gestionadas. Por ejemplo, la transmisión de datos desde un ROV sumergido a un sistema de almacenamiento terrestre puede cruzar múltiples redes y dispositivos, cada uno con sus propias vulnerabilidades. Si no existen controles robustos, un atacante puede explotar esas brechas para acceder al sistema, manipular datos, interrumpir el servicio o comprometer la seguridad del personal operativo (Ahmad et al., 2024, p. 5).

Ilustración 2. Convergencia TI–TO–CS en operaciones subacuáticas del Comando de Buceo



Fuente: Elaboración propia con base en Guananga Reyna y Rodríguez Espinosa (2023) y datos operacionales del Comando de Alistamiento de Buceo de la Armada Nacional.

Entre los **fallos comunes en la integración TI–TO**, se destacan:

- Ausencia de segmentación de redes.
- Uso de firmware desactualizado en equipos de campo.
- Protocolos de comunicación inseguros (como Modbus sin cifrado).
- Pobre gestión de identidades y accesos en plataformas compartidas.

Frente a este panorama, el diseño de un protocolo de ciberseguridad debe considerar no solo los aspectos tecnológicos, sino también la estructura operativa de la Armada Nacional, sus

niveles de mando, jerarquías de decisión, tiempos de respuesta y condiciones ambientales del entorno marítimo.

Tabla 1. Comparación de normas de ciberseguridad aplicables al entorno subacuático naval

Norma	Fortalezas	Limitaciones	Aplicabilidad al entorno naval colombiano
ISO/IEC 27001	Enfoque integral para gestionar riesgos de seguridad de la información en cualquier tipo de organización.	Requiere adaptación específica al entorno TO y marino.	Proporciona base sólida para SGSI del Comando de Buceo; adaptable a unidades navales.
IEC 62443	Diseñada específicamente para sistemas de automatización industrial (IACS) y entornos TO.	Complejidad de DISEÑO; requiere conocimiento técnico profundo.	Útil para proteger ROV, CCR y sensores integrados en ambientes subacuáticos.
NIST SP 800-53 Rev. 5	Altamente detallada; utilizada por agencias gubernamentales; amplia cobertura de controles técnicos y organizativos.	Volumen elevado de controles; difícil de aplicar en operaciones tácticas sin simplificación.	Relevante para operaciones militares; permite integración con arquitectura de ciberdefensa nacional.

Fuente: Elaboración propia con base en ISO (2022), IEC (2018) y NIST (2020).

3 Metodología

3.1 Tipo y enfoque de investigación

Esta investigación se enmarca dentro del enfoque **cualitativo de tipo descriptivo-aplicado**, orientado a comprender e intervenir sobre una problemática específica del entorno militar: la ausencia de un protocolo de ciberseguridad para la protección de los datos generados por los sistemas de exploración subacuática empleados por el Comando de Alistamiento de Buceo de la Armada Nacional.

El enfoque **descriptivo** permite analizar detalladamente las características de los sistemas tecnológicos utilizados (como los ROV, CCR y sensores oceanográficos), identificar las vulnerabilidades existentes, y examinar el entorno normativo aplicable. Según Sampieri, Collado, & Lucio, (2014), la investigación descriptiva “busca especificar las propiedades, características y rasgos importantes de cualquier fenómeno que se analice” lo que resulta

especialmente adecuado para el estudio de activos tecnológicos estratégicos y sus riesgos asociados.

Por su parte, el carácter aplicado de esta investigación se refleja en su propósito final: diseñar un protocolo de ciberseguridad técnicamente viable, normativamente sustentado y operativamente adaptable a las condiciones del entorno marítimo colombiano. Este protocolo busca ser implementado como herramienta de gestión dentro de los procesos doctrinales y operacionales del Comando de Alistamiento de Buceo.

En cuanto a su alcance, se trata de una investigación documental, basada en fuentes bibliográficas especializadas, normas técnicas internacionales (como ISO/IEC 27001, IEC 62443, NIST SP 800-53), doctrina de ciberdefensa nacional e informes institucionales de la Armada Nacional.

3.2 Método de análisis

El presente estudio adopta un método de análisis cualitativo de tipo inductivo-deductivo, que permite construir conocimiento a partir del examen detallado de evidencias técnicas, normativas y contextuales, y posteriormente formular una propuesta aplicable al entorno militar colombiano (Sampieri et al., 2014).

Desde el enfoque inductivo, se realiza una revisión y análisis crítico de casos reales, documentos institucionales, doctrinas de ciberseguridad, normativa internacional y experiencias tecnológicas aplicadas en operaciones subacuáticas. Este análisis permite identificar patrones comunes, brechas de seguridad, y elementos operacionales clave en la gestión de datos recolectados por sistemas como los ROV o los CCR. Así mismo, se consideran incidentes documentados en literatura especializada que demuestran el uso del ciberespacio como dominio de conflicto en el ámbito marítimo (Weerth, 2020).

Luego, mediante un proceso deductivo, los hallazgos se organizan en una estructura lógica que permite diseñar un protocolo de ciberseguridad coherente con los principios doctrinales de la Armada Nacional, las capacidades técnicas del Comando de Alistamiento de Buceo y los estándares internacionales de protección de infraestructuras críticas. Este protocolo se formula a partir de matrices de análisis comparativo y principios de diseño orientado a la defensa en profundidad.

El método también incluye elementos del análisis de contenido, con base en la codificación conceptual de documentos normativos como la ISO/IEC 27001, la IEC 62443 y el NIST SP 800-53 Rev. 5, lo que facilita la extracción de requisitos técnicos y su aplicación al entorno naval colombiano (ISO, 2022).

3.3 Técnicas e instrumentos de recolección de información

La técnica principal empleada en esta investigación es la revisión documental sistemática, entendida como el proceso de selección, organización, análisis y extracción de información relevante a partir de fuentes bibliográficas, técnicas, normativas y doctrinales especializadas en ciberseguridad, tecnología subacuática y defensa nacional. Esta técnica permite comprender el estado del arte, identificar vacíos, y construir criterios de diseño para un protocolo operativo de ciberseguridad.

Según Sampieri et al., (2014), la recolección documental consiste en "la obtención de datos a través de materiales que contienen información registrada de forma escrita o audiovisual, relevante para los propósitos del estudio". Para ello, se utilizaron como instrumentos de apoyo:

- Una matriz de análisis normativo y técnico, en la cual se compararon normas internacionales como ISO/IEC 27001, IEC 62443, y NIST SP 800-53 Rev. 5, valorando sus principios, alcances, requisitos y aplicabilidad en entornos marítimos y militares.
- Una tabla de caracterización de sistemas ciberfísicos, aplicada a los equipos utilizados por el Comando de Alistamiento de Buceo, como los ROV Seaeye Lynx, los CCR Liberty, ecosondas multihaz, sensores GNSS y plataformas oceanográficas.
- Un cuadro de análisis de amenazas y vulnerabilidades, basado en fuentes como el *National Cyber Threat Assessment 2025–2026* (Canadian Centre for Cyber Security, 2023) y doctrinas como *NATO Cyber Defence 2000–2022*, que permitió categorizar riesgos por actor, vector de ataque, criticidad del activo y posibles impactos operacionales (Atkinson, 2023).

Las fuentes utilizadas fueron seleccionadas bajo criterios de actualidad, pertinencia temática, confiabilidad institucional y aplicabilidad al contexto colombiano. Asimismo, se incorporaron documentos internos como el Plan Estratégico del Comando de Buceo 2024–2027, que orientan las líneas de desarrollo de capacidades operativas y digitales de la unidad. (Comando de Alistamiento de Buceo, 2024).

3.4 Universo y muestra

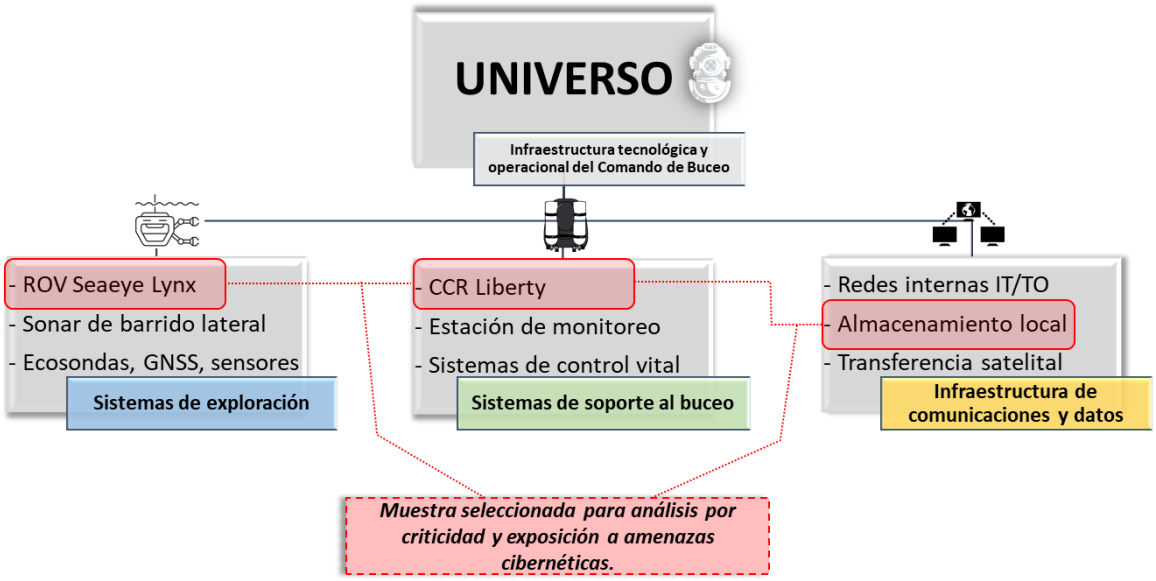
El universo de esta investigación está constituido por los sistemas tecnológicos, procesos operacionales y de infraestructuras de información empleados por el Comando de Alistamiento de Buceo de la Armada Nacional de Colombia en sus operaciones de exploración marítima y subacuática. Dicho universo incluye plataformas tecnológicas de las más importantes como los vehículos operados remotamente (ROV), sistemas de respiración de circuito cerrado (CCR), sensores acústicos, estaciones de comando y control, enlaces de comunicaciones satelitales, redes internas y dispositivos de almacenamiento de datos generados durante misiones científicas, patrimoniales o de seguridad (COBUC, 2024).

Para efectos del análisis y diseño del protocolo de ciberseguridad, se delimita una muestra intencionada de carácter no probabilístico, compuesta por los siguientes elementos críticos:

- **Sistemas de información** embarcados, que integran hardware, software, redes TO/TI y estaciones de monitoreo para la recopilación, procesamiento, almacenamiento y visualización de los datos obtenidos durante misiones subacuáticas.
- El sistema **ROV Seaeye Lynx**, utilizado en campañas subacuáticas de inspección profunda, con énfasis en los sistemas de navegación, comunicación y almacenamiento.
- El sistema **CCR Liberty**, como unidad autónoma de respiración empleada por buzos técnicos en condiciones de alta presión.
- Los dispositivos de almacenamiento externo y redes de transferencia de datos utilizados para la consolidación de información recolectada en misiones como las del **Galeón San José**.

La selección de esta muestra responde a su relevancia operativa, su exposición potencial a amenazas cibernéticas y su carácter representativo de la arquitectura tecnológica del Comando de Buceo. Así mismo, permite realizar un diagnóstico específico y aplicar los marcos normativos y de gestión de riesgos abordados en la presente investigación, con miras a proponer un protocolo robusto, adaptado al contexto institucional y operacional de la Armada Nacional.

Ilustración 3. Universo y muestra seleccionada para el análisis de ciberseguridad en operaciones subacuáticas.



Fuente: Elaboración propia con base en Ferri et al. (2017) y Ahmad et al. (2024).

3.5 Técnicas de análisis de la información

Para esta investigación, se aplicará un análisis documental cualitativo y comparativo, sustentado en la revisión sistemática de normas técnicas, políticas institucionales, artículos científicos y reportes especializados en ciberseguridad, ciberdefensa e infraestructura crítica en el ámbito marítimo.

Este análisis se desarrollará en tres niveles:

- **Nivel descriptivo:**

  Se identificarán y sistematizarán los elementos clave de las fuentes revisadas, tales como marcos normativos (ISO/IEC 27001, IEC 62443, NIST SP 800-53), buenas prácticas internacionales, vulnerabilidades técnicas y casos documentados en el entorno naval y subacuático (Guananga Reyna & Rodríguez Espinosa, 2023).

- **Nivel interpretativo:**

  Se contrastará la información recolectada con las condiciones actuales del Comando de Alistamiento de Buceo de la Armada Nacional, buscando establecer relaciones entre las brechas identificadas y los componentes del modelo de defensa en profundidad (Ammar & Khan, 2024).

- **Nivel propositivo:**

A partir del diagnóstico, se establecerán lineamientos estratégicos y se diseñará un protocolo técnico-normativo de ciberseguridad para los sistemas y datos críticos identificados, bajo criterios de aplicabilidad operativa, alineación institucional y cumplimiento normativo (OMI, 2022).

La técnica de análisis también se apoyará en herramientas de matriz comparativa, esquemas de clasificación de riesgos (como STRIDE y CIA), y taxonomías propias del entorno naval para visualizar las relaciones entre amenazas, activos, impactos y salvaguardas.

3.6 Técnicas de validación

Para garantizar la validez interna y externa del diseño del protocolo de ciberseguridad propuesto, esta investigación adoptará un proceso de validación por juicio de expertos. Esta técnica permite contrastar la coherencia, aplicabilidad y suficiencia del instrumento teórico propuesto frente a los criterios técnicos y operativos establecidos en el ámbito de la Armada Nacional y la ciberseguridad naval y el procedimiento contempla:

- **Selección de expertos**: Se acudirá a un panel conformado por profesionales con experiencia comprobada en ciberseguridad militar, operaciones subacuáticas, gestión de sistemas críticos e DISEÑO de normas internacionales como ISO/IEC 27001 y NIST SP 800-82.

  Esta selección incluirá al menos un representante del Comando de Alistamiento de Buceo, un oficial del SOC (Centro de Operaciones de Seguridad) de la Armada, y un académico del área de ciberdefensa (NATO, 2022).
- **Instrumento de validación**: Se elaborará una ficha de validación estructurada, basada en criterios como pertinencia, claridad conceptual, relevancia técnica, factibilidad operativa y alineación doctrinal. Cada experto evaluará el protocolo con base en estos criterios utilizando una escala tipo Likert.
- **Análisis de resultados**: Las observaciones serán procesadas mediante análisis cualitativo y ajustes al protocolo según patrones de consenso. El nivel de acuerdo entre los jueces se considerará válido si supera el 80% de conformidad.

Esta técnica permite fortalecer la robustez del modelo propuesto, incorporando retroalimentación especializada para garantizar su viabilidad institucional y operativa. El principal aporte de esta investigación es aplicar marcos normativos internacionales (ISO/IEC

27001, IEC 62443, NIST) en un entorno operacional subacuático colombiano, un vacío doctrinal y técnico no cubierto previamente.

3.7 Consideraciones Éticas

Esta investigación respeta los principios fundamentales de la ética en la investigación científica, especialmente en lo concerniente al manejo de información institucional, la integridad académica y la responsabilidad profesional, en ese sentido:

- **Confidencialidad y reserva de la información**: Toda la información institucional analizada, especialmente aquella relacionada con las capacidades tecnológicas, operaciones subacuáticas, equipos empleados o prácticas internas del Comando de Alistamiento de Buceo, será tratada con carácter reservado, evitando su divulgación pública o indebida. La propuesta del protocolo no comprometerá detalles operacionales sensibles ni clasificará información confidencial (OMI, 2022).
- **Respeto a la institución**: Se mantendrá un enfoque propositivo, basado en la mejora de los procesos internos de seguridad digital, evitando juicios de valor que afecten la imagen institucional. El lenguaje del trabajo es técnico, respetuoso y orientado a fortalecer la protección de los intereses estratégicos nacionales.
- **Integridad académica**: Todas las fuentes utilizadas, ya sean documentos técnicos, normas, artículos o informes, serán debidamente citadas conforme a las normas APA 7, y se garantizará la originalidad del texto mediante control de plagio y supervisión metodológica permanente (Sampieri et al., 2014).

Este enfoque garantiza que la propuesta sea ética, rigurosa y útil tanto para la Armada Nacional como para el desarrollo académico de la Maestría en Ciberseguridad y Ciberdefensa.

4 Análisis y resultados

4.1 Caracterización de sistemas de información y tecnologías subacuáticas

Los Sistemas de Información (SI) y las Bases de Datos (BD) son actualmente una necesidad fundamental para las grandes organizaciones, empresas y Fuerzas Militares, en el caso del Comando de Buceo de la Armada Nacional, resultan esenciales en el proceso para la modernización, digitalización y fortalecimiento institucional. Estos sistemas permiten almacenar, procesar, recuperar y proteger información relevante e histórica para las actividades de buceo, facilitando la toma de decisiones estratégicas y operacionales. Según el Plan de

Desarrollo Naval, la Armada Nacional ha venido robusteciendo sus capacidades institucionales mediante la incorporación progresiva de tecnologías de vigilancia, análisis y protección digital, incluyendo herramientas especializadas de monitoreo y sistemas avanzados de gestión de eventos de seguridad, como parte de su fortalecimiento en ciberseguridad, por tal motivo se requiere de una correcta caracterización de estos sistemas es esencial para identificar los activos críticos que requieren medidas de protección cibernética diferenciadas, a continuación, se presentan los principales componentes tecnológicos sujetos a análisis de riesgo:

Tabla 2. Clasificación y vulnerabilidades de los sistemas críticos en operaciones marítimas y subacuáticas

Tipo de sistema	Ejemplo en buceo/operación marítima	Función principal	Vulnerabilidades comunes
TI **(Tecnologías de la Información)**	Computadora de buceo avanzada, portátiles de los ROV, portátiles robótica DEBUS	Procesamiento, almacenamiento y visualización de datos; soporte a la toma de decisiones	Malware, acceso no autorizado, pérdida de datos, ataques de ransomware
OT **(Tecnologías de Operación)**	Sistema de control de propulsión ROV, sensores CCR (Control Room)	Control y automatización de procesos físicos (motores, válvulas, sensores)	Manipulación de señales, sabotaje, acceso remoto no autorizado, fallos de integridad
CPS **(Sistemas Ciberfísicos)**	ROV (vehículo operado remotamente)- CCR (Equipo Rebreathers)	Integración de sensores, actuadores y software para interactuar con el entorno físico en tiempo real	Intercepción de comunicaciones, manipulación remota, ataques a la integridad de datos y comandos

Fuente: Elaboración propia

4.1.1 Sistemas de información embarcados (TI):

Corresponden a los sistemas computacionales y de comunicación que permiten la operación, almacenamiento, visualización y gestión de datos a bordo de las unidades navales. Incluyen estaciones de monitoreo, servidores locales, redes LAN embarcadas, sistemas de comando y control (C2), y equipos con software especializado para la interpretación de imágenes y señales acústicas. Suelen operar con conexiones intermitentes a la red institucional o dispositivos externos, lo cual incrementa la superficie de exposición (Ahmad et al., 2024).

En el contexto marítimo, la convergencia de tecnologías de la información (TI), tecnologías de operación (OT) y sistemas ciberfísicos (CPS) ha incrementado la complejidad y los riesgos de ciberseguridad. La integración de estos sistemas permite una mayor eficiencia operativa, pero también amplía la superficie de ataque y las posibles vulnerabilidades, especialmente en entornos críticos como las operaciones subacuáticas y portuarias (Drougkas, Papanikolaou, & Belmonte, 2019).

A continuación, se presenta una tabla de los principales TI en el buceo sus vulnerabilidades en el contexto marítimo y subacuático:

Tabla 3. Sistemas TI en operaciones de buceo y subacuáticas: funciones y vulnerabilidades

Sistema TI	Ejemplo en buceo/operación subacuática	Función principal	Vulnerabilidades comunes
Estaciones de monitoreo	Consola de monitoreo en sala de control (control room)	Visualización y gestión de datos de buceo, seguimiento en tiempo real, condiciones ambientales y estado de equipos	Acceso no autorizado, manipulación de datos, malware
Servidores locales	Servidor de registro de inmersiones	Almacenamiento y procesamiento de datos de inmersiones, perfiles de buceo y video	Ransomware, pérdida de datos, ataques de denegación de servicio
Redes LAN embarcadas	Red interna de soporte a ROV y CCR	Comunicación entre consolas, sensores, actuadores y sistemas de soporte vital	Intercepción de tráfico, ataques internos, brechas de seguridad
Sistemas de comando y control (C2)	Software de gestión de operaciones subacuáticas	Coordinación y control de ROV, buzos y equipos de superficie	Suplantación de identidad, acceso remoto no autorizado
Equipos de interpretación de señales	Computadora de análisis de video y sonar	Procesamiento de imágenes, señales acústicas y video de ROV	Manipulación de resultados, explotación de vulnerabilidades
Sistemas de soporte vital digital	CCR (rebreather electrónico)	Monitoreo y ajuste automático de gases respirados por el buzo	Fallos de software, manipulación remota, errores de calibración
Dispositivos móviles de buceo	Tabletas o relojes inteligentes subacuáticos	Visualización de datos en tiempo real, comunicación y registro de parámetros	Pérdida de datos, acceso no autorizado, malware

Fuente: Elaboración propia con información de Ahmad et al. (2024)

4.1.2 Concepto general de OT en el entorno subacuático militar

Los dispositivos ciberfísicos operacionales (OT, por sus siglas en inglés) en el contexto del Comando de Alistamiento de Buceo de la Armada Nacional hacen referencia a los sistemas que interactúan directamente con el entorno físico subacuático, y que combinan hardware, sensores, actuadores, software embebido y canales de comunicación. Estos dispositivos permiten la ejecución de operaciones de inspección, monitoreo y documentación en ambientes extremos, integrando tecnologías como los ROV y CCR sistemas de navegación inercial y equipos de buceo de alta profundidad. Según Guerrero-Bonilla, Parra-Velandia & Cruz (2022), este tipo de sistemas ciberfísicos están diseñados para operar bajo condiciones ambientales hostiles, con alta precisión, autonomía y capacidad de retroalimentación.

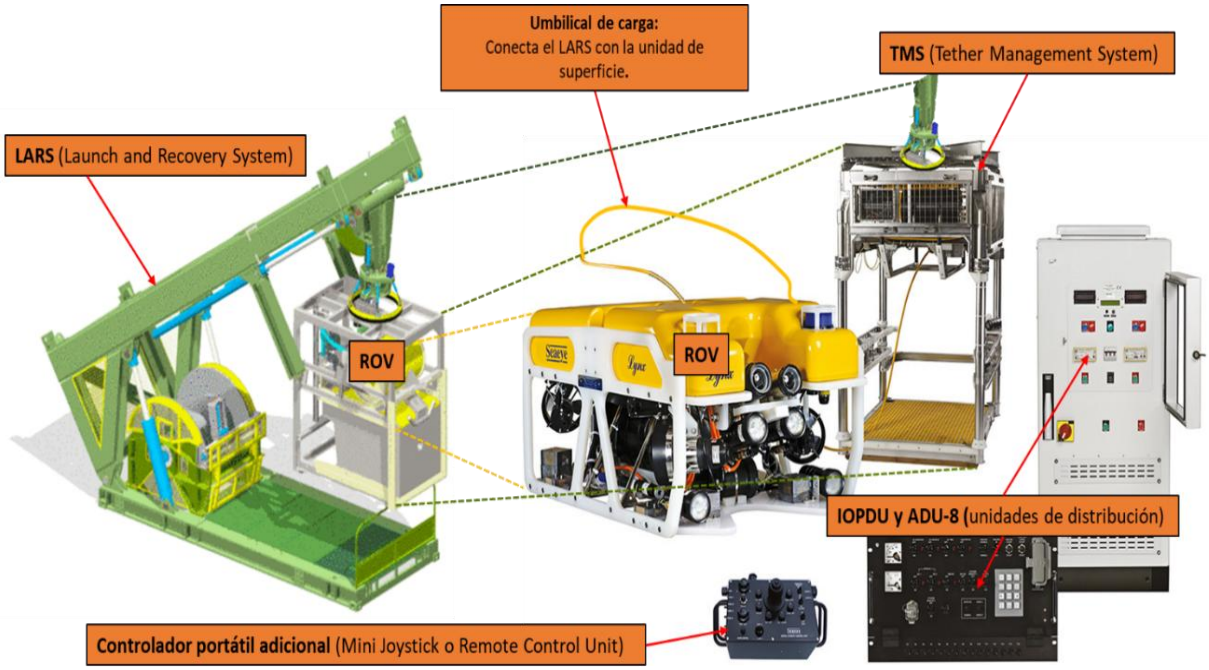
4.1.3 Sistemas ROV (Vehículos Operados Remotamente)

Los ROV son plataformas robóticas sumergibles no tripuladas, controladas desde superficie mediante cables umbilicales, y equipadas con sensores acústicos, cámaras, brazos manipuladores y módulos de navegación inercial. Estos sistemas permiten realizar inspecciones a gran profundidad, recolección de imágenes y operaciones de rescate subacuático con una elevada precisión operacional (Ferri et al., 2017). Sin embargo, la presencia de interfaces expuestas, software embebido no actualizado, módulos de telemetría, y conexiones remotas sin cifrado robusto los convierte en objetivos altamente vulnerables frente a amenazas cibernéticas como ataques de denegación de servicio (DoS), suplantación de señales GNSS, o toma de control del vehículo mediante exploits en el firmware (Guananga Reyna & Rodríguez Espinosa, 2023).

Según el análisis de Verma et al. (2025), los ROV utilizados en ambientes marítimos requieren mecanismos de defensa en profundidad que incluyan segmentación de red, autenticación multifactor y monitoreo de anomalías en tiempo real. En la Armada Nacional, el empleo del ROV Seaeye Lynx, operado desde plataformas oceanográficas, implica la integración de sistemas críticos a profundidades superiores a 500 metros, donde la indisponibilidad o manipulación de datos puede comprometer tanto la seguridad de la misión

como la evidencia recolectada en contextos arqueológicos sensibles, como el Galeón San José (Weerth, 2020).

Ilustración 4. Sistemas de Despliegue Operacional del ROV Lynx 1160



Fuente: Elaboración propia, con imágenes tomadas de (Seaeye Ltd., 2020).

En el contexto de las operaciones subacuáticas, los Vehículos Operados Remotamente (ROV) como el Seaeye Lynx desempeñan un papel fundamental en la exploración, inspección y documentación del patrimonio cultural sumergido. Estos equipos incorporan múltiples componentes tecnológicos que interactúan entre sí a través de redes internas y enlaces de comunicación con estaciones de monitoreo en superficie. Sin embargo, cada uno de estos subsistemas representa una posible superficie de ataque cibernético que debe ser evaluada y protegida adecuadamente. La Tabla 4 presenta una caracterización técnica de los principales módulos del ROV, los riesgos de ciberseguridad asociados a cada uno y las medidas de mitigación recomendadas, tomando como referencia la documentación técnica del fabricante y fuentes especializadas en ciberseguridad marítima (Seaeye Ltd., 2020).

Tabla 4. Riesgos y Mitigaciones en Componentes Del ROV

Componente	Función	Riesgo asociado	Posibles vulnerabilidades	Fuente
Unidad de Control de Superficie (SCU)	Proporciona interfaz entre el operador y el ROV	Acceso no autorizado	Interceptación de comandos, manipulación remota	Seaeye Ltd., 2020
Tether Management System (TMS)	Maneja el cable umbilical y minimiza tensiones	Interrupción del enlace de comunicación	Daños físicos o sabotaje del tether	Seaeye Ltd., 2020
Cámaras y sensores ópticos/acústicos	Captura de video e imágenes, navegación	Manipulación de datos recolectados	Falsificación o pérdida de datos visuales	Seaeye Ltd., 2020
Propulsores (thrusters)	Movimiento y maniobra del ROV	Descontrol de navegación	Comandos maliciosos o interferencia electromagnética	Seaeye Ltd., 2020
Sensores de navegación (gyro, depth, compás)	Estabilización y localización	Alteración de posición	Suplantación de señales GNSS o spoofing	Seaeye Ltd., 2020
Módulo de telemetría	Transmisión de datos en tiempo real	Intercepción o denegación de señal	Falta de cifrado o autenticación de datos	Seaeye Ltd., 2020
Software de operación y diagnóstico	Control de misión, monitoreo y registros	Inyección de malware, manipulación de parámetros	Software sin actualizaciones ni autenticación	Seaeye Ltd., 2020

Fuente: Elaboración propia con información de Ahmad et al. (2024)

4.1.4 Sistema de Respiración de Circuito Cerrado (CCR Liberty)

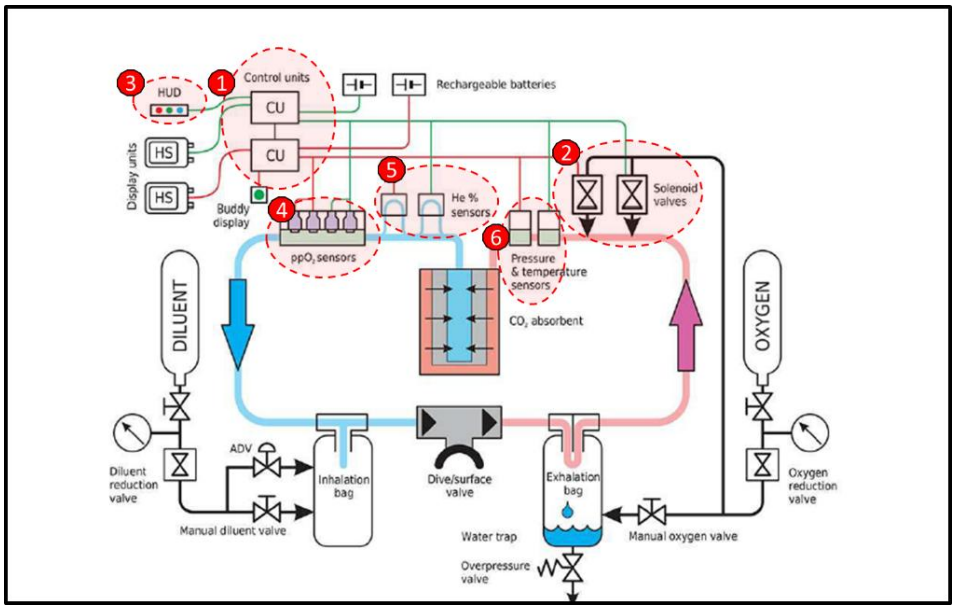
El CCR Liberty es un sistema de respiración de circuito cerrado utilizado por buzos técnicos y operativos del Departamento de Buceo y Salvamento de la Armada Nacional, para inmersiones prolongadas y profundas. Su arquitectura electrónica incluye una unidad de control central (CU), sensores de presión parcial de oxígeno (PPO_2), solenoides automáticos, una pantalla de visualización tipo HUD, y puertos de comunicación para transferencia de datos (Divesoft, 2025).

Este equipo, al operar en entornos extremos y mantener en tiempo real la mezcla respiratoria óptima, depende en gran medida de la integridad de sus componentes electrónicos

y su software embebido. Como señala Tamarkar y Patra (2018), cualquier alteración en sensores o algoritmos puede desencadenar errores críticos, como hipoxia o hiperventilación, que ponen en riesgo la vida del buzo. Además, al contar con puertos de entrada y salida para análisis posterior de datos, existe una superficie de ataque potencial para la manipulación o extracción de información operativa sensible.

Los riesgos asociados incluyen manipulación de firmware, spoofing de sensores, interceptación de comandos de control, fallos de autenticación en el HUD, y explotación de puertos de datos para inyección de malware o fuga de información (Ammar, M et al., 2024). A pesar de estar diseñado como un sistema autónomo, su integración con software externo para análisis y mantenimiento técnico representa un vector de amenaza que, si no se gestiona adecuadamente, puede ser explotado por actores maliciosos.

Ilustración 5. Componentes vulnerables a ciberataques en el CCR Liberty



Fuente: Diagrama funcional del CCR Liberty, que muestra el flujo de gases, la arquitectura de sensores y válvulas, y las conexiones entre módulos electrónicos y unidades de control (Divesoft, 2025).

Por ello, el CCR debe ser tratado como un activo ciberfísico crítico, con la correspondiente segmentación de sus interfaces, protocolos seguros para la transferencia de información, autenticación multifactor en sus accesos físicos y digitales, y auditorías periódicas del firmware que lo controla (Guananga Reyna & Rodríguez Espinosa, 2023).

Tabla 5. Caracterización técnica del CCR Liberty y sus riesgos asociados

Componente	Función	Riesgo asociado	Posibles vulnerabilidades	Fuente
Unidad de control (CU)	Administra sensores, control de gases y alarmas.	Fallo en la lógica de control; manipulación del firmware.	Firmware no actualizado, sin firma digital, susceptible a acceso físico o remoto no autorizado.	Divesoft, 2025
Sensores de oxígeno y presión	Miden parámetros vitales para la mezcla de gases respirables.	Lecturas falsas o manipuladas.	Sensores descalibrados, mal mantenidos o susceptibles a inyección de datos por interferencia electromagnética.	Divesoft, 2025
Pantalla y sistema de interfaz	Proporciona información en tiempo real al buzo.	Alteración de datos mostrados; errores de interpretación.	Pantalla sin cifrado en el canal de comunicación, posible manipulación si se conecta a sistemas externos no seguros.	Divesoft, 2025
Baterías y fuente de energía	Proveen energía continua a los componentes electrónicos.	Interrupción súbita del sistema.	Sobrecarga, interferencia o sabotaje físico que provoque apagado del sistema.	Divesoft, 2025
Firmware del sistema	Controla los ciclos automáticos de gas y alarmas.	Modificación o corrupción de firmware.	Ausencia de validación de integridad, acceso sin autenticación a puertos de carga o actualización.	Divesoft, 2025
Conectividad externa (puertos USB)	Permite descargar datos de inmersión o actualizar el sistema.	Fuga de información o infección por malware.	Uso de memorias USB sin validación, ausencia de medidas de control de dispositivos externos.	Divesoft, 2025

Fuente: Elaboración propia con información de Divesoft (2025)

Finalmente las plataformas oceanográficas y sensores acústicos forman parte del ecosistema tecnológico del Comando de Alistamiento de Buceo, sin embargo este trabajo se enfoca únicamente en los sistemas con mayor protagonismo en la recolección directa y análisis de datos críticos: ROV, CCR, sistemas TI y estaciones de monitoreo. Se excluyen los sensores acústicos por su carácter complementario en las misiones analizadas.

4.1.5 Estaciones de monitoreo y sistemas de almacenamiento de datos

Las estaciones de monitoreo ya sea desde tierra o embarcadas constituyen nodos críticos en la arquitectura operativa de los sistemas subacuáticos, ya que permiten la **recolección,**

visualización y análisis en tiempo real de los datos generados por plataformas como el ROV, el CCR y sensores asociados. Estas estaciones integran hardware especializado (consolas, pantallas, unidades de procesamiento) y software de visualización y registro, que permiten interpretar imágenes, señales acústicas, trayectorias, condiciones ambientales y otros parámetros vitales durante las misiones subacuáticas (Seaeye Ltd., 2020).

Asimismo, los sistemas de almacenamiento de datos, tanto temporales como permanentes, desempeñan un rol fundamental en la trazabilidad, seguridad y disponibilidad de la información recolectada. En la práctica, esto implica el uso de discos duros externos, servidores locales, NAS (Network Attached Storage) y, ocasionalmente, enlaces hacia nubes institucionales o respaldos desconectados. Sin embargo, en múltiples ocasiones estas soluciones no cuentan con mecanismos de cifrado, redundancia o monitoreo de integridad, lo cual incrementa el riesgo de pérdidas de información, manipulación de evidencias o accesos no autorizados (NIST, 2020).

Desde la perspectiva de la ciberseguridad, estos sistemas de monitoreo y almacenamiento representan **superficies de ataque críticas** si no están aislados o reforzados adecuadamente. Fallos en la autenticación de usuarios, conexiones USB abiertas, falta de registros de auditoría o software desactualizado son vectores comunes de vulnerabilidad que podrían ser aprovechados por actores maliciosos para comprometer la cadena de custodia digital de los datos sensibles recolectados durante las operaciones de buceo militar o arqueología subacuática (Ammar & Khan, 2024).

Tabla 5. Componentes de las estaciones de monitoreo y sistemas de almacenamiento de datos

Componente	Función	Riesgo asociado	Posibles vulnerabilidades	Fuente
Consola de monitoreo	Visualización en tiempo real de datos del ROV, CCR y sensores.	Acceso no autorizado a datos en tiempo real.	Falta de autenticación, interfaz web sin cifrado, puertos abiertos.	Seaeye Ltd., 2020
Unidad de procesamiento (CPU)	Procesamiento de imágenes, señales acústicas y datos de misión.	Inyección de código malicioso o corrupción de datos.	Software desactualizado, falta de antivirus, conexión USB abierta.	González et al., 2024

Almacenamiento local (disco duro)	Resguardo temporal o permanente de datos recolectados.	Pérdida o manipulación de evidencias digitales.	Ausencia de cifrado, mala gestión de respaldos, falta de redundancia.	Ammar & Khan, 2024
NAS o servidor embarcado	Acceso compartido y almacenamiento estructurado de información.	Fuga de información o interrupción del servicio.	Credenciales débiles, configuración por defecto, falta de segmentación de red.	González et al., 2024
Software de visualización	Interpretación gráfica de imágenes, trayectorias y señales acústicas.	Manipulación o alteración de parámetros visuales.	Vulnerabilidades en el código, falta de actualizaciones, plugins sin control de seguridad.	Seaeye Ltd., 2020
Interfaces externas (USB/Ethernet)	Transferencia de datos a medios físicos o redes institucionales.	Inserción de malware o robo de información.	Uso no controlado de dispositivos, ausencia de protocolos de control de acceso físico.	Ammar & Khan, 2024

Fuente: Elaboración propia con base en Seaeye Ltd. (2020), y Ammar y Khan (2024).

4.1.6 Identificación de riesgos asociados a los sistemas TI, TO y CS en el entorno subacuático

La operación de sistemas ciberfísicos en misiones subacuáticas de la Armada Nacional involucra una compleja interacción entre Tecnologías de la Información (TI), Tecnologías Operativas (TO) y mecanismos de Ciberseguridad (CS). Esta convergencia tecnológica, aunque esencial para la eficacia y seguridad de las operaciones, también amplía la superficie de exposición a amenazas, incrementando el riesgo de incidentes que pueden afectar la integridad de la misión, la seguridad del personal y la protección de información crítica. De acuerdo con Ahmad y Khan (2024), los entornos marítimos presentan desafíos específicos como la conectividad limitada, la hostilidad del ambiente físico y las restricciones logísticas para actualizaciones o mantenimiento, lo cual incrementa los riesgos operacionales.

Entre los principales riesgos identificados en este entorno se encuentran:

- Accesos no autorizados a redes TI embarcadas.
- Suplantación de identidades o alteración de señales en sistemas de navegación y sensores.

- Infección de malware a través de medios extraíbles.
- Fallos de firmware en componentes del CCR o del ROV.
- Interferencia en las comunicaciones entre plataformas y estaciones remotas.
- Filtración de información reservada.

Estos riesgos afectan directamente a los dispositivos ciberfísicos OT. A continuación, en la Tabla 6, se presentan los riesgos agrupados por dominio para su análisis detallado.

Tabla 6. Riesgos principales asociados a los dominios TI, TO y CS en operaciones subacuáticas

Dominio	Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación	Referencia
TI	Acceso no autorizado	Ingreso indebido a estaciones de monitoreo o servidores sin credenciales válidas. Puede permitir manipulación de datos críticos o sabotaje de operaciones.	Alto	Media	Autenticación multifactor, monitoreo de accesos, segmentación de red	ISO/IEC 27001, IEC 62443
TI	Pérdida de integridad de datos	Modificación no detectada de archivos de misión o bitácoras, afectando la toma de decisiones y la trazabilidad.	Alto	Baja	Hashing, control de versiones, auditoría de cambios	ISO/IEC 27001
TO	Fallo de sensores o actuadores	Interrupción de lectura de variables o errores en ejecución de comandos, lo que puede poner en riesgo la vida de los buzos o la misión.	Crítico	Media	Redundancia, pruebas periódicas, monitoreo en tiempo real	IEC 62443
TO	Fallo de energía o desconexión	Desactivación inesperada de ROV o CCR por corte eléctrico o desconexión, comprometiendo la	Crítico	Baja	UPS, sistemas de respaldo, alarmas de desconexión	IEC 62443

		seguridad de la operación.				
CPS	Inyección de malware por USB	Introducción de código malicioso por medios removibles, que puede comprometer sistemas críticos.	Alto	Media	Políticas de uso de USB, escaneo automático, control físico	NIST SP 800-53
CPS	Fuga de datos clasificados	Exposición de datos sensibles por falta de cifrado o políticas de control, con riesgo de espionaje o sabotaje.	Crítico	Baja	Cifrado, DLP, control de accesos, capacitación	ISO/IEC 27001

Fuente: Elaboración propia con base en Verma et al. (2025), Ammar y Khan (2024), y Seaeye Ltd. (2020)

4.2 Tecnologías subacuáticas automatizadas (análisis por tipología y riesgos).

Las operaciones subacuáticas modernas han evolucionado desde prácticas puramente manuales hacia entornos altamente automatizados, donde convergen tecnologías robóticas, sistemas ciberfísicos y redes digitales. En el contexto militar colombiano, las tecnologías subacuáticas automatizadas permiten realizar inspecciones, exploraciones, rescates, mantenimiento y vigilancia del patrimonio cultural sumergido, integrando dispositivos como los ROV (Remotely Operated Vehicles), sistemas CCR (Closed Circuit Rebreather), sensores acústicos y plataformas de monitoreo con capacidades de procesamiento embarcado.

Estas tecnologías, si bien aumentan la capacidad operacional, también amplían la superficie de ataque digital al depender de hardware sensible, firmware configurable, conexiones seriales y redes de datos en condiciones extremas (Ammar et al., 2024). Por lo tanto, su análisis no debe limitarse a lo funcional u operativo, sino que debe considerar su arquitectura, vulnerabilidades cibernéticas y medidas de mitigación.

Con base en los manuales técnicos analizados y la doctrina internacional de acuerdo Seaeye Ltd., (2020) y Divesoft, (2025), se han clasificado los sistemas en tres categorías principales: tecnologías de intervención (ROV), tecnologías de soporte vital (CCR) y tecnologías de información (TI), tal como se resume en la siguiente tabla.

Tabla 7. Dispositivos ciberfísicos OT en operaciones subacuáticas y marítimas

Tipología tecnológica	Dispositivo representativo	Función principal	Riesgos técnicos	Riesgos cibernéticos	Fuente
Tecnología de intervención	ROV Seaeye Lynx	Exploración e inspección subacuática	Falla en propulsores, cámaras	Intervención remota, manipulación de datos	Seaeye Ltd., 2020
Tecnología de soporte vital	CCR Liberty	Reciclado de gases y autonomía de buceo	Fallos en sensores de PPO2	Modificación del firmware, lectura remota	Divesoft, 2025
Tecnología de información	Estaciones de monitoreo	Gestión y visualización de datos embarcados	Fallos de red, sobrecalentamiento	Sniffing de datos, acceso no autorizado	Ahmad et al., 2024
Tecnología de comunicaciones	Red táctica, red satelital	Transmisión de datos y control remoto	Pérdida de señal, interferencias	Intercepción, denegación de servicio	Perales Garat, 2021
Tecnología de gestión	Servidores, PDM-Tierra	Procesamiento y almacenamiento de datos	Fallos de hardware, corrupción de datos	Ransomware, acceso no autorizado	Rodriguez, 2024
Tecnología móvil	Dispositivo móvil, GPS	Monitoreo y control en campo	Daño físico, pérdida de dispositivo	Robo de credenciales, spoofing de GPS	Bimco, 2021

Fuente: Elaboración propia basada en Perales Garat (2021), y BIMCO (2021).

4.3 Clasificación de riesgos cibernéticos en operaciones subacuáticas

Las operaciones subacuáticas de la Armada Nacional de Colombia se desarrollan en entornos híbridos donde convergen infraestructuras físicas, sistemas operativos y componentes digitales. Esta sinergia entre plataformas embarcadas, vehículos operados remotamente (ROV) y sistemas de soporte vital como los CCR, requiere una evaluación rigurosa de los riesgos cibernéticos asociados.

Desde la perspectiva doctrinal, se adopta el modelo **CIA** (Confidencialidad, Integridad y Disponibilidad) como base para la clasificación y evaluación de riesgos, lo cual permite identificar las amenazas que pueden comprometer los datos, interrumpir la operación o alterar los sistemas críticos (Guananga Reyna & Rodríguez Espinosa, 2023). A esto se suman

elementos del enfoque Defense in Depth, que recomienda múltiples capas de protección para enfrentar ataques en distintas fases (Ammar & Khan, 2024).

Principales categorías de riesgos cibernéticos:

- **Malware y ransomware:**

  Los sistemas críticos pueden ser infectados por software malicioso, comprometiendo la disponibilidad y confidencialidad de datos y controles. Un ataque de ransomware puede paralizar la operación de servidores, ROVs o sistemas de monitoreo, como se evidenció en el caso del puerto de Barcelona (Rodriguez, 2024).

- **Phishing y robo de credenciales:**

  El acceso no autorizado a plataformas de control o monitoreo puede lograrse mediante técnicas de ingeniería social, permitiendo a los atacantes manipular remotamente dispositivos como ROVs o servidores (Rodriguez, 2024).

- **Ataques de denegación de servicio (DDoS):**

  La saturación de redes tácticas o satelitales puede interrumpir la comunicación entre superficie y dispositivos subacuáticos, afectando la coordinación y la seguridad de las operaciones (BIMCO, 2021).

- **Intervención y manipulación de señales:**

  Los sistemas de posicionamiento (GPS) y comunicación pueden ser objeto de spoofing o jamming, alterando la navegación de ROVs o la transmisión de datos críticos (Perales Garat, 2021).

- **Acceso no autorizado y explotación de vulnerabilidades:**

  La explotación de fallos en el software o hardware de servidores, CCR o dispositivos móviles puede permitir el control remoto o la extracción de información sensible (Rodriguez, 2024).

- **Riesgos asociados a la convergencia IT/OT:**

  La integración de sistemas de información (TI) y operativos (OT) incrementa la complejidad y la posibilidad de que una brecha en un sistema administrativo afecte directamente a los dispositivos de campo (BIMCO, 2021).

- **Ataques en entornos aislados (air-gapped):**

- Incluso en sistemas sin conexión a internet, como los control rooms de ROVs donde la información se transfiere solo mediante discos duros custodiados, existen riesgos. El caso de Stuxnet demostró que el malware puede introducirse a través de dispositivos extraíbles (USB, discos duros externos) y permanecer inactivo hasta encontrar el objetivo, comprometiendo la integridad y el funcionamiento de los sistemas críticos. Un disco duro infectado podría alterar los datos del ROV, sabotear operaciones o propagarse a otros sistemas sensibles, evidenciando que el aislamiento físico no garantiza la inmunidad frente a ataques avanzados (BIMCO, 2021).

A continuación, se presenta una tabla que clasifica los principales riesgos cibernéticos identificados en los sistemas embarcados, los ROV Seaeye Lynx y los CCR Liberty, basándose en evidencia documental y experiencias operacionales de unidades de buceo.

Tabla 8. Riesgos cibernéticos por sistema crítico subacuático y portuario

Sistema o componente	Riesgo sobre la Confidencialidad	Riesgo sobre la Integridad	Riesgo sobre la Disponibilidad	Riesgos adicionales relevantes	Fuente
ROV	Intercepción de video/telemetría, robo de datos de misión	Manipulación de comandos, alteración de registros de operación	Denegación de servicio, sabotaje remoto	Secuestro del ROV, manipulación física, propagación de malware vía USB	Perales Garat (2021); Rodriguez (2024)
CCR	Acceso a datos biométricos y parámetros vitales	Modificación de firmware, alteración de mezclas de gases	Inutilización del sistema, bloqueo de sensores	Riesgo vital para el buzo, manipulación de alarmas	Perales Garat (2021)
Servidor remoto	Robo de información sensible, fuga de datos	Alteración de bases de datos, manipulación de logs	Ransomware, caída del sistema	Ataques persistentes avanzados (APT), propagación de malware	Rodriguez (2024); BIMCO (2021)
Dispositivo móvil	Robo de credenciales, acceso a datos de control	Manipulación de apps, alteración de configuraciones	Bloqueo del dispositivo, malware	Phishing, acceso no autorizado a sistemas OT	Perales Garat (2021)

Red táctica	Intercepción de comunicaciones, espionaje	Manipulación de mensajes, inyección de comandos falsos	Saturación de red (DDoS), pérdida de conectividad	Spoofing, ataques de intermediario (MITM)	BIMCO (2021)
Red satelital	Intercepción de datos transmitidos	Alteración de señales, spoofing GPS	Jamming, pérdida de enlace	Manipulación de navegación, pérdida de sincronización	Perales Garat (2021)
Servidores	Acceso a información crítica, fuga de datos	Manipulación de software, alteración de registros	Ransomware, denegación de servicio	Ataques de cadena de suministro, insiders	Rodriguez (2024); BIMCO (2021)
PDM-Tierra	Robo de datos de misión y control	Manipulación de parámetros de misión	Inaccesibilidad al sistema, sabotaje	Acceso remoto no autorizado, manipulación de órdenes	BIMCO (2021)
Buques	Intercepción de datos AIS/GPS, fuga de información de carga	Manipulación de rutas, alteración de sistemas de navegación	Bloqueo de sistemas críticos, sabotaje	Spoofing AIS/GPS, ataques a sistemas de control	Perales Garat (2021)

Fuente: Elaboración propia basada en Perales Garat (2021), Rodriguez (2024), , BIMCO (2021).

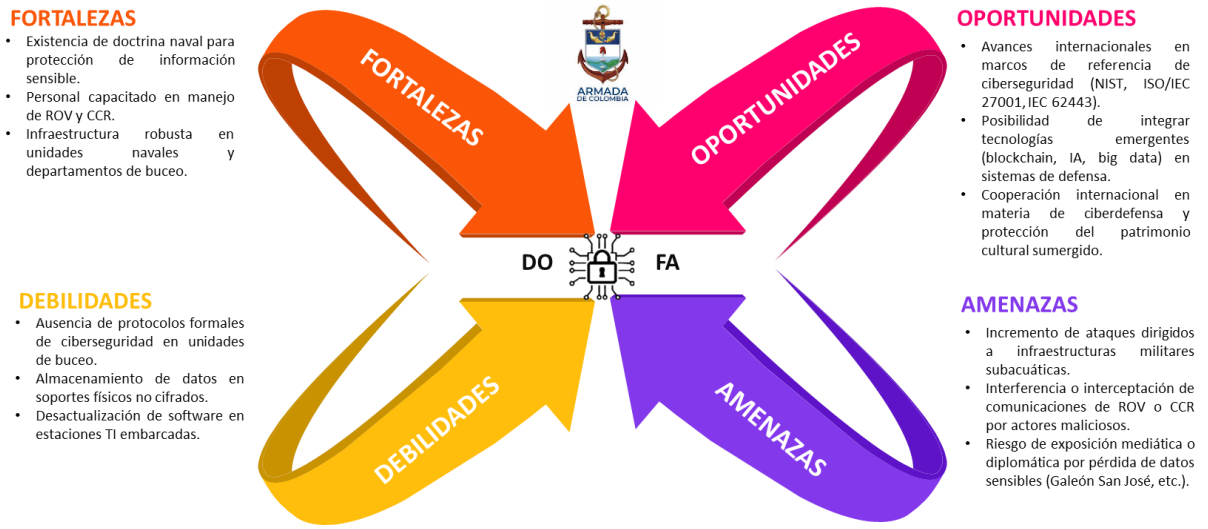
4.4 Diagnóstico de vulnerabilidades técnicas y procedimentales (Matriz DOFA)

El diagnóstico DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas) constituye una herramienta estratégica fundamental para evaluar el estado actual de la ciberseguridad en las operaciones subacuáticas. En este contexto, permite integrar tanto los aspectos técnicos (infraestructura, sistemas, software, hardware) como los procedimentales (protocolos, formación del talento humano, coordinación interinstitucional) a fin de orientar la toma de decisiones sobre mitigación de riesgos.

Este tipo de análisis es especialmente útil en organizaciones militares, donde la DISEÑO de medidas de ciberdefensa debe considerar los entornos híbridos y las condiciones de operación en tiempo real. Además, el uso de esta herramienta ha sido recomendado en evaluaciones comparativas de ciberseguridad organizacional por parte de organismos internacionales como la OTAN y el NIST (NIST, 2023).

A continuación, se presenta una **matriz DOFA adaptada a los sistemas críticos empleados por la Armada Nacional de Colombia en misiones subacuáticas**.

Ilustración 5. Matriz DOFA para diagnóstico de ciberseguridad en operaciones subacuáticas



Fuente: Elaboración propia con base en Ammad & Khan (2024), NIST (2023), Guananga Reyna & Rodríguez Espinosa (2023).

4.5 Evaluación de impactos potenciales sobre las operaciones y el patrimonio cultural sumergido

En el contexto de las operaciones subacuáticas lideradas por la Armada Nacional de Colombia, la exposición a riesgos cibernéticos no solo compromete la continuidad operativa, sino que puede generar afectaciones críticas al patrimonio cultural sumergido, como en el caso del Galeón San José. Estos impactos potenciales pueden clasificarse en tres dimensiones principales:

4.5.1 Impactos sobre las operaciones militares subacuáticas

La interrupción de misiones es uno de los riesgos más inmediatos: un ciberataque dirigido a los sistemas de información embarcados, enlaces de comunicaciones o sistemas de navegación (GNSS, sonar, etc.) puede obligar a abortar misiones de exploración o rescate en tiempo real, afectando la seguridad y la eficacia de las operaciones (Ammad & Khan, 2024). Además, la desinformación táctica, producto de la alteración de datos recogidos por sensores o ROVs, puede inducir errores en la toma de decisiones operacionales, poniendo en riesgo tanto al personal de buceo como la localización de objetivos subacuáticos (Verma et al., 2025). Finalmente, la infiltración en sistemas críticos puede escalar a compromisos de red más amplios,

incluyendo centros de comando o sistemas logísticos navales, lo que incrementa la superficie de ataque y la gravedad de las consecuencias (Guananga Reyna & Rodríguez Espinosa, 2023).

4.5.2 Impactos sobre el patrimonio cultural sumergido

La manipulación o destrucción de registros digitales obtenidos por el ROVs puede hacer irrepetible la documentación de sitios arqueológicos, como el Galeón San José, afectando la integridad de la memoria histórica y científica (BIMCO, 2021). Asimismo, la filtración de datos sobre localización o hallazgos arqueológicos puede favorecer saqueos, disputas jurídicas o conflictos diplomáticos, poniendo en riesgo la soberanía y la reputación internacional de Colombia (Ferri et al., 2017). Por otro lado, la alteración de instrucciones enviadas a ROVs o plataformas de intervención puede conllevar daños accidentales sobre estructuras sumergidas de alto valor histórico (Seaeye Ltd., 2020).

Las brechas de seguridad pueden debilitar la confianza interinstitucional, afectando la cooperación entre la Armada, el Ministerio de Cultura y entidades científicas, especialmente en proyectos sensibles (Rojas Niño, 2014). Además, incidentes asociados a la pérdida de información clasificada pueden derivar en investigaciones jurídicas, sanciones o modificaciones a los acuerdos de cooperación nacional e internacional, lo que podría limitar futuras investigaciones y campañas de la protección del patrimonio cultural y sumergido. (Drougkas et al., 2020).

4.6 Casos de referencia internacional

El análisis de experiencias internacionales en ciberseguridad aplicada a entornos subacuáticos y marítimos permite identificar prácticas efectivas, errores comunes y lecciones aprendidas que pueden ser adaptadas al contexto colombiano. A continuación, se presentan tres casos relevantes:

4.6.1 Caso 1: Protección de infraestructuras críticas marítimas – Estados Unidos

En el marco de las políticas del Department of Homeland Security (DHS), Estados Unidos ha desarrollado estrategias avanzadas de ciberseguridad para la protección de infraestructuras críticas marítimas, incluyendo puertos, sistemas de navegación y vehículos operados remotamente. Estas estrategias priorizan la integración entre tecnologías de la información (TI) y tecnologías operacionales (OT), siguiendo marcos normativos como el NIST SP 800-82, que

establece directrices para la gestión segura de sistemas industriales y de control en entornos marítimos (NIST, 2015).

La arquitectura de dispositivos ciberfísicos OT, evidencian la complejidad y la superficie de ataque de los sistemas marítimos modernos, donde convergen redes tácticas, servidores, plataformas de datos en tierra, ROVs, redes satelitales, buques, sistemas de buceo y dispositivos móviles (Drougkas et al., 2019). Esta interconexión exige la DISEÑO de Centros de Operaciones de Seguridad Marítima (Maritime SOC), que permiten el monitoreo continuo de amenazas, la detección temprana de incidentes y la respuesta coordinada ante ataques cibernéticos, reduciendo así el riesgo de interrupciones operacionales y daños a la infraestructura crítica (US Coast Guard, 2020).

- **Lección aplicable**: La experiencia estadounidense demuestra que la integración de TI y OT bajo marcos normativos robustos, junto con la operación de Maritime SOC, es fundamental para reducir el tiempo de detección y respuesta ante ciberataques, especialmente en escenarios de alta criticidad operativa y logística (NIST, 2015).

4.6.2 Caso 2: Incidente en red de sensores oceanográficos – Noruega

Según informes de la European Union Agency for Cybersecurity (ENISA), las redes de sensores y sistemas distribuidos en el entorno marítimo europeo han sido identificados como objetivos potenciales de ataques de denegación de servicio (DDoS) y otras amenazas cibernéticas, afectando la continuidad operativa y la resiliencia de infraestructuras críticas (ENISA, 2023).

- **Lección aplicable**: Lección aplicable: La resiliencia cibernética de los nodos distribuidos en zonas marítimas debe incluir capacidades de operación autónoma y protocolos de redundancia en la cadena de comunicación.

4.6.3 Caso 3: Riesgos de interferencia cibernética en vehículos ROV militares

Diversos informes de la OTAN y de agencias de ciberseguridad han advertido sobre la creciente vulnerabilidad de los vehículos operados remotamente (ROV) utilizados en operaciones militares y de inspección subacuática. Entre los riesgos identificados se encuentran la manipulación de señales de navegación, la interferencia en los sistemas de control y la explotación de accesos no autorizados, incluyendo conexiones inalámbricas inseguras (NATO, 2022).

- **Lección aplicable:** La protección de los sistemas ROV debe contemplar la segmentación de redes, el control riguroso de accesos físicos y digitales, y el uso de cifrado en tiempo real en los enlaces de control y video.

4.7 Controles técnicos actuales y medidas de resiliencia en los sistemas TI, TO y CS del Comando de Buceo

Tras el análisis de la arquitectura de dispositivos ciberfísicos OT, es fundamental detallar los controles técnicos y las medidas de resiliencia implementadas en los sistemas de Tecnologías de la Información (TI), Tecnologías Operacionales (TO) y Ciberseguridad (CS) del Comando de Alistamiento de Buceo. La protección de estos sistemas es esencial para garantizar la continuidad operativa y la seguridad de las misiones subacuáticas y marítimas, considerando la creciente sofisticación de las amenazas cibernéticas (BIMCO, 2021).

En el dominio TI, se han adoptado controles como la segmentación de redes, la autenticación multifactor, el uso de firewalls y sistemas de detección de intrusos (IDS/IPS), así como la actualización periódica de software y la realización de copias de seguridad bajo la regla 3-2-1 (Perales Garat, 2021). Estos controles buscan proteger la confidencialidad, integridad y disponibilidad de la información crítica, minimizando el riesgo de ataques como ransomware, phishing y acceso no autorizado.

En el ámbito TO, los controles se centran en la protección de sistemas industriales y de control, como los servidores de operación, los ROV, los sistemas de propulsión y los sensores ambientales. Se deben implementar medidas como la segmentación de redes OT, la restricción de accesos físicos y lógicos, la monitorización continua de eventos y la aplicación de parches de seguridad específicos para dispositivos industriales (BIMCO, 2021).

En cuanto a la ciberseguridad (CS), el Comando de Alistamiento de Buceo debe fortalecer la resiliencia mediante la creación de equipos de respuesta a incidentes, la capacitación continua del personal, la realización de pruebas de penetración (PENTEST) y la colaboración con organismos nacionales e internacionales para el intercambio de inteligencia sobre amenazas (Rojas Niño J. E., 2014). Además, se promueve la cultura de ciberseguridad y la concienciación del personal como barrera fundamental frente a ataques de ingeniería social y errores humanos.

La integración de estos controles técnicos, junto con la adopción de planes de contingencia y recuperación ante desastres, permite al Comando de Buceo anticipar, resistir y recuperarse de incidentes cibernéticos, fortaleciendo así su capacidad de respuesta y adaptabilidad en un entorno operativo cada vez más digitalizado y expuesto a riesgos emergentes (BIMCO, 2021).

Tabla 9. Controles técnicos actuales, alcance y brechas en los sistemas TI, TO y CS del Comando de Buceo

Dominio / Sistema	Controles técnicos actuales	Alcance operativo	Brechas detectadas	Fuente
TI (Sistemas de información embarcados, servidores, dispositivos móviles, servidor remoto)	Autenticación por usuario y contraseña, segmentación de redes LAN internas, firewalls de perímetro, backups periódicos, políticas de acceso, antivirus.	Protección básica frente a accesos no autorizados, aislamiento de segmentos críticos, respaldo de datos.	No existe cifrado de datos en tránsito, ausencia de integración con SOC, falta de monitoreo en tiempo real, políticas de contraseñas débiles.	NIST (2020); Ahmad & Khan (2024); Perales Garat (2021)
TO (ROV, CCR, PDM-Tierra, red táctica, buques, GPS)	Firmware propietario con acceso restringido, protocolos de comunicación cerrados, redundancia de sensores críticos, control de acceso físico, monitoreo de señales.	Garantiza integridad operativa, continuidad de misión, protección ante fallos de sensores y manipulación física.	Falta de cifrado en la telemetría, limitadas medidas contra manipulación remota, actualizaciones de seguridad poco frecuentes, escaso monitoreo de anomalías.	Seaeye Ltd. (2020); Divesoft (2025); Drougkas et al. (2020)
CS (Plataformas de control y monitoreo, estaciones de monitoreo, almacenamiento local)	Estaciones de monitoreo con software especializado, almacenamiento local en servidores sin conexión directa a Internet, segmentación de red, control de acceso lógico.	Minimiza exposición directa a Internet, reduce vector de ataque externo, protege la integridad de los datos operativos.	Dificultad para aplicar parches de seguridad oportunos, falta de monitoreo continuo basado en SIEM, escasa automatización de alertas y respuesta.	BIMCO (2021); INFRAESTRUCTURA PORTUARIA.pdf; RodriguezCarlos2024.pdf

Fuente: Elaboración propia basada en NIST (2020) y COBUC (2024).

En la tabla anterior se resume los controles técnicos actuales, su alcance y las principales brechas identificadas en los sistemas TI, TO y CS del Comando de Buceo, en correspondencia con los dispositivos ciberfísicos OT representados en la figura anterior. Este análisis permite identificar áreas prioritarias para fortalecer la resiliencia y la ciberseguridad en las operaciones subacuáticas y marítimas.

4.8 Análisis de brechas (Gap Analysis final)

El análisis de vulnerabilidades realizado en los apartados anteriores, junto con la caracterización de dispositivos ciberfísicos OT (Ilustración 4) y la identificación de riesgos técnicos en TI, TO y CS, permite establecer un mapa de brechas estructurales en la arquitectura de ciberseguridad del Comando de Alistamiento de Buceo. Este *gap analysis* constituye el puente entre el diagnóstico (Cap. 4) y la propuesta del protocolo (Cap. 5), mostrando qué elementos existen actualmente, cuáles son insuficientes y qué áreas demandan medidas inmediatas.

4.8.1 Principales brechas identificadas por dominio tecnológico

4.8.1.1 Domino TI (Información embarcada: servidores, redes internas, dispositivos móviles, nube remota).

- Los sistemas aplican controles básicos (firewalls de perímetro, antivirus y respaldos), pero presentan ausencia de cifrado de datos en tránsito, credenciales débiles y falta de integración con **el** SOC de la Armada.
- No existe un sistema de monitoreo en tiempo real (SIEM) que permita detectar incidentes en fase temprana, lo que amplía la exposición a ransomware o accesos no autorizados.
- La política de copias 3-2-1 no está aplicada de manera homogénea en los distintos niveles de almacenamiento (embarcado – remoto – nube).

4.8.1.2 Dominio TO (ROV, CCR, PDM-Tierra, red táctica, buques, GPS/GNSS, sensores)

- Los ROV Seaeye Lynx y los CCR Liberty utilizan firmware propietario y protocolos cerrados que limitan la auditoría y gestión de vulnerabilidades.
- La telemetría no está cifrada ni firmada digitalmente, exponiéndose a riesgos de spoofing y manipulación de sensores.

- Las redes tácticas y satelitales carecen de segmentación avanzada por zonas/conductos (IEC 62443), lo que amplía la superficie de ataque si un nodo es comprometido.
- Existe baja frecuencia en la aplicación de parches de seguridad y carencia de procedimientos de "*stop seguro*" o failover probado en caso de sabotaje digital.

4.8.1.3 Dominio CS (Plataformas de ciberseguridad y monitoreo, estaciones locales, políticas navales)

- Aunque los sistemas de monitoreo local han reducido la exposición directa a Internet, no cuentan con automatización de alertas ni capacidades de respuesta adaptativa frente a incidentes.
- Las estaciones de control funcionan aisladas, sin integración plena con el **CSIRT Naval** ni con el SOC, limitando la trazabilidad y coordinación.
- La gestión de roles y responsabilidades en ciberseguridad todavía es difusa, con vacíos en la definición de responsables por activo y suplentes, lo que debilita la trazabilidad operacional.

4.8.1.4 Síntesis de brechas críticas

De manera integrada, el *gap analysis* evidencia tres categorías de brechas:

- Brechas tecnológicas: ausencia de cifrado extremo a extremo, telemetría insegura en ROV/CCR, firmware no auditado y parches poco frecuentes.
- Brechas de monitoreo y respuesta: carencia de SIEM en TI y OT, baja automatización de alertas y falta de procedimientos claros de failover/stop seguro.
- Brechas de gobernanza y coordinación: indefinición de roles, escasa integración SOC–CSIRT–Comando de Buceo y ausencia de ejercicios de validación (red team/blue team) en el entorno subacuático.

4.8.2 Conexión hacia el protocolo

Estas brechas demuestran que la seguridad actual del Comando de Buceo se encuentra fragmentada, reactiva y orientada más a medidas aisladas que a una estrategia integral. Por tanto, resulta imprescindible articular un protocolo de ciberseguridad por capas (Defense in Depth) que cubra simultáneamente las dimensiones preventivas, detectivas y reactivas, bajo marcos internacionales (ISO/IEC 27001, IEC 62443, NIST 800-82), doctrina institucional y políticas nacionales.

En el siguiente capítulo se desarrolla este protocolo, con módulos de riesgos, controles, monitoreo, respuesta y capacitación, que buscan cerrar las brechas aquí identificadas y consolidar la protección de los sistemas TI, TO y CS del Comando de Buceo.

5 Capítulo 5 – Diseño del protocolo de ciberseguridad

5.1 Fundamento normativo

El diseño del protocolo de ciberseguridad para las operaciones subacuáticas de la Armada Nacional se sustenta en un marco normativo que combina estándares internacionales, doctrina institucional y políticas nacionales, asegurando la interoperabilidad y cumplimiento con los lineamientos de ciberdefensa y protección del patrimonio cultural sumergido.

5.1.1 Normas internacionales aplicables

- **ISO/IEC 27001:2022**: Estándar internacional para la gestión de la seguridad de la información, que proporciona el marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) aplicable a entornos navales y subacuáticos (servidores, redes, dispositivos móviles, etc.). (NQA, 2022).
- **IEC 62443**: Conjunto de normas específicas para la ciberseguridad en sistemas de control industrial (ICS) y tecnología operacional (TO), aplicables a ROV, CCR y plataformas oceanográficas (IEC, 2021).
- **NIST SP 800-82 Rev. 3**: Guía de seguridad para sistemas de control industrial, con énfasis en defensa en profundidad, monitoreo continuo y segmentación de redes (Stouffer, Tang, & Newhouse, 2022).

5.1.2 Doctrina institucional y marcos militares

- **Manual de Ciberdefensa de la OTAN (2000–2022)**: Establece principios de defensa activa, resiliencia y respuesta coordinada frente a amenazas cibernéticas en entornos militares multinacionales (NATO, 2022).
- **Política de Ciberseguridad y Ciberdefensa de las Fuerzas Militares de Colombia**: Define las responsabilidades de los comandos operacionales para la protección de infraestructuras críticas y sistemas de información militares, (Armada Nacional de Colombia, 2021).

- **El *Colombian Cyber Emergency Response Team* (ColCERT)** es el Equipo Nacional de Respuesta a Emergencias Cibernéticas de Colombia, adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (ColCERT, 2025).

5.1.3 Políticas Nacionales

- **Documento CONPES 3995 de 2020**, Política Nacional de Confianza y Seguridad Digital, que promueve capacidades de gestión de riesgos y protección de infraestructuras críticas (DNP, 2020).
- **MinTIC – Guía de Ciberseguridad para Infraestructuras Críticas**, Lineamientos técnicos para implementar controles de seguridad en redes y sistemas de misión crítica (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2020).
- **Ministerio de Defensa Nacional – Estrategia de Ciberdefensa**, plan de acción orientado a integrar de manera efectiva las capacidades de ciberseguridad militar en el desarrollo de operaciones navales y fluviales. Este enfoque busca fortalecer la protección de la información, los sistemas de mando y control, y las infraestructuras críticas asociadas, garantizando la resiliencia frente a amenazas del ciberespacio mediante políticas, procedimientos y controles de seguridad de la información (Ministerio de Defensa Nacional, 2023).

Tabla 10. Comparación de marcos normativos aplicables a la ciberseguridad en operaciones subacuáticas

Norma / Marco	Enfoque principal	Aplicabilidad a TI / TO	Fortalezas	Limitaciones	Uso en el protocolo (5.2–5.3)	Evidencia en documentos
ISO/IEC 27001:2022	Gestión de la seguridad de la información (SGSI)	TI y redes institucionales; soporte transversal a CS	Marco integral de gestión de riesgos y mejora continua; controles del Anexo A	No aborda especificidades de OT/entornos marítimos	Base del SGSI: políticas, roles, evaluación de riesgos, continuidad (RTO/RPO), copias 3-2-1, gestión de incidentes y SIEM	Lecciones de ransomware y necesidad de SIEM, backups y respuesta coordinada
IEC 62443 (serie)	Ciberseguridad en sistemas de automatización y control	TO: ROV, CCR, PDM-Tierra, redes tácticas; interfaz IT/OT	Segmentación por zonas y conductos; niveles de seguridad; hardening y gestión de parches/firmware	Requiere adaptación a plataformas navales/subacuáticas y equipos propietarios	Arquitectura OT por zonas/conductos; control/whitelisting de comandos en ROV/CCR; cifrado/firmado de telemetría; pruebas de "stop seguro" y failover	ENISA/Drougkas: segmentación portuaria; riesgos OT en puertos
NIST SP 800-82 Rev. 3	Seguridad en ICS con defensa en profundidad	TI/TO integrados	Inventario, monitoreo de anomalías, gestión de parches, telemetría segura	Orientado a ICS genéricos, no específico marítimo	Defensa en profundidad para CCR/ROV; listas blancas, ventanas de mantenimiento, detección de anomalías	Recomendaciones de monitoreo, parches y respuesta ante incidentes
NIST CSF	Marco de funciones Identify–Protect–Detect–Respond–Recover	Transversal TI/TO/CS	Flexible, permite roadmap, perfiles y métricas	No prescribe controles; requiere mapeo a 27001/62443/800-82	Estructurar fases del protocolo y KPIs; priorización y cronograma de adopción	Uso de indicadores y madurez en planes sectoriales
OMI MSC.428(98) y Directrices OMI 2017	Integrar riesgos ciber al ISM/seguridad marítima	Buques, instalaciones portuarias, Capacidades de Buceo	Obligatoriedad de gestionar riesgo ciber en el dominio marítimo	Guía de alto nivel; requiere aterrizaje técnico	Exigir evaluación ciber en planes de buque/instalación; auditorías y coordinación con autoridad marítima	Citas directas y rol de DIMAR en inspección y PBIP

Norma / Marco	Enfoque principal	Aplicabilidad a TI / TO	Fortalezas	Limitaciones	Uso en el protocolo (5.2–5.3)	Evidencia en documentos
Manual de Ciberdefensa de la OTAN (2000–2022)	Doctrina de ciberdefensa militar	TI/TO militares (CS)	Mando y control, coordinación multinacional, respuesta activa	General; no específico subacuático	Reglas de coordinaciónescalamiento con ColCERT/DIMAR; ejercicios conjuntos/tabletop	Necesidad de cooperación y respuesta coordinada
CONPES 3995 (2020) y Decreto 338/2022	Política nacional de seguridad/confianza digital y gobernanza	TI, infraestructuras críticas; coordinación nacional	Define roles, niveles de gobernanza, respuesta a incidentes	No provee guías técnicas OT detalladas	Gobernanza, roles y responsabilidades (5.2); flujo de reporte y coordinación (5.3)	Desarrollo de estrategia y rol de MinTIC/ColCERT/DIMAR
Guías MinTIC para Infraestructuras Críticas (2021)	Lineamientos técnicos y buenas prácticas	TI/TO en servicios esenciales	Checklists operativos, gestión de cambios y vulnerabilidades	No especializada en entorno naval	Baseline técnico para redes embarcadas/portuarias; puente entre 27001 y 62443	Recomendaciones de gobernanza y controles
BIMCO Guidelines 2021	Gestión de riesgo ciber a bordo	Buques, puente, CCR	Controles prácticos, roles y procedimientos	Menos detalle para ICS complejos/ROV	Procedimientos a bordo; hardening ECDIS/GNSS; gestión de proveedores	Riesgos en interfaz buque–puerto
USCG 2020; ENISA puertos 2019–2020	Buenas prácticas para buques/terminales y ciberseguridad portuaria	Operaciones marítimas; TO/CS	Casos prácticos, segmentación, inspecciones, resiliencia	Requiere adaptación local	Controles en interfaz buque–puerto; segmentación; contingencias	Modelos de riesgo, compartir info, ciberresiliencia
Perales Garat, MARSEC-20	Escenario y lecciones prácticas de ciberseguridad marítima	TO/CS; GNSS, AIS, VHF, radar	Evidencia empírica de jamming/spoofing y necesidad de resiliencia	Caso español; extrapolación requiere cautela	Medidas específicas: detección de spoofing GNSS/AIS, multiconstelación, procedimientos alternativos	Detalle de PENTEST, jamming GNSS/VHF/AIS y spoofing AIS

Fuente: Elaboración propia basada en las normas de ciberseguridad

5.2 Estructura del protocolo técnico

El protocolo técnico propuesto para la protección de los sistemas de información y tecnologías subacuáticas de la Armada Nacional de Colombia se estructura en módulos secuenciales que permiten una DISEÑO progresiva y sostenible. Estos módulos están diseñados para abordar de manera integral las dimensiones preventivas, detectivas y reactivas de la ciberseguridad, aplicadas de forma específica a los sistemas de información en toda la organización de buceo especialmente en los **ROV**, **CCR** y **plataformas de información embarcadas** empleadas en operaciones subacuáticas y de exploración del patrimonio cultural sumergido.

5.2.1 Módulos o fases del protocolo

- **El primer módulo** corresponde a la evaluación y gestión de riesgos cibernéticos, fundamentado en metodologías reconocidas como ISO/IEC 27005 y el modelo STRIDE, para identificar, clasificar y priorizar amenazas sobre sistemas críticos (ISO, 2022).
- **El segundo módulo** se centra en la DISEÑO de controles técnicos y procedimentales, alineados con las directrices internacionales de la IEC 62443 y las recomendaciones establecidas en el NIST Handbook 150 para la protección de sistemas de automatización industrial y de control. Este enfoque combinado garantiza la aplicación de medidas como segmentación de redes, autenticación multifactor, cifrado de datos en tránsito y en reposo, así como procedimientos estrictos de control de acceso físico y lógico. Asimismo, se incorpora una estrategia de ciberresiliencia operacional sustentada en ejercicios Red Team / Blue Team con enfoque Purple Team, orientados a verificar la eficacia de los controles implementados y evaluar la capacidad de respuesta ante incidentes en los sistemas de misión y redes de automatización naval. (Khalil, 2025)

  Estos ejercicios simulan escenarios de ataque y defensa basados en marcos como MITRE ATT&CK y D3FEND, permitiendo identificar vulnerabilidades en entornos operacionales (OT) y tecnológicos (IT), optimizar las detecciones y ajustar las medidas preventivas y correctivas en tiempo real (Kim et al., 2024). La integración de estos marcos técnicos y de entrenamiento continuo fortalece la cultura organizacional de ciberdefensa, asegurando la continuidad operación al, la protección de infraestructuras críticas y la mejora constante del protocolo de seguridad institucional (NIST, 2020).

- **El tercer módulo** aborda la monitorización y detección temprana de incidentes, integrando las capacidades de los Centros de Operaciones de Seguridad (SOC) de la Armada y el uso de sistemas SIEM (Security Information and Event Management) para el análisis en tiempo real de logs y alertas (NIST, 2020). En concordancia con los resultados de los ejercicios Red Team / Blue Team, este módulo permite ajustar las reglas de correlación, indicadores de compromiso (IoC) y umbrales de alerta derivados de las simulaciones ofensivas y defensivas, consolidando un ciclo continuo de mejora y aprendizaje operacional (Khalil, 2025).

  De esta manera, los hallazgos de los ejercicios del segundo módulo se integran al SOC como insumos de inteligencia técnica y táctica, fortaleciendo la detección proactiva y la respuesta temprana en entornos OT y TI de la Armada (Kim et al., 2024).
- **El cuarto módulo** se orienta a la **respuesta y recuperación ante incidentes**, incorporando procedimientos estandarizados basados en el NIST SP 800-61r2 y planes de continuidad de negocio y recuperación ante desastres (Business Continuity and Disaster Recovery – BCDR) adaptados al contexto naval y subacuático (NIST, 2012).

  En esta fase, se evalúa la eficacia de las estrategias defensivas ejecutadas por el Blue Team durante los ejercicios de ciberentrenamiento, y se consolidan los planes de respuesta ante incidentes reales a partir de las lecciones aprendidas y los indicadores de desempeño (MTTD, MTTR).

  Así, el ciclo completo Red/Blue/Purple fortalece la resiliencia cibernética organizacional, garantizando la continuidad de las operaciones críticas bajo estándares internacionales de gestión de incidentes y recuperación operacional (Khalil, 2025).

5.2.2 Definición de roles y responsabilidades

La asignación clara de roles y responsabilidades es crítica para la eficacia del protocolo: establece autoridad, líneas de comunicación y ámbitos de competencia. Debe alinearse con la doctrina de mando y control (C2) de la Armada Nacional y con buenas prácticas vigentes de gestión de seguridad de la información y de entornos OT/ICS (ISO/IEC 2700, 2022).

5.2.2.1 Estructura de roles

- Comandante del Comando de Alistamiento de Buceo (COBUC). Conduce la supervisión estratégica del protocolo, aprueba políticas y recursos, y coordina con el Comando de la

Armada, con DIMAR y con agencias nacionales e internacionales. Dirige la toma de decisiones en incidentes mayores que afecten la misión. (MinDefensa, 2023)

- Oficial de Seguridad de la Información (CISO). Diseña, implementa y actualiza el marco de control (ISO 27001/IEC 62443/NIST). Mantiene la matriz RACI, el mapa de riesgos y los indicadores de desempeño. Lidera la coordinación con autoridades competentes y el aseguramiento de cumplimiento (NIST SP 800-82, 2022).
- Jefe de Operaciones Subacuáticas. Traduce el protocolo a procedimientos de misión. Autoriza ventanas de mantenimiento y pruebas en ROV, CCR y sistemas embarcados. Verifica que el personal operativo cumpla las medidas de ciberseguridad antes, durante y después de cada inmersión. (IEC 62443-3-3, 2018).
- Administrador de Sistemas Embarcados. Configura, mantiene y actualiza hardware y software a bordo; gestiona identidades y accesos; ejecuta copias 3-2-1 y pruebas de restauración; integra registros al SIEM (NIST SP 800-82, 2022).
- Arquitecto/Administrador OT. Define zonas y conductos (IEC 62443), segmenta la red táctica, gestiona parches/firmware y control de cambios en equipos OT. Asegura telemetría autenticada y cifrada en enlaces radio/satélite (NIST SP 800-82, 2022).
- Operadores de ROV y de CCR. Ejecutan operaciones conforme a listas blancas de comandos, checklists de seguridad y bitácoras técnicas. Reportan anomalías, aplican procedimientos de “stop seguro” y protegen la integridad de datos recolectados (Liberty Systems, 2025).
- Responsable de Comunicaciones y Enlace Satelital. Opera y asegura la red satelital y vínculos de respaldo, aplica cifrado extremo a extremo y planes de conmutación (NIST SP 800-82, 2022).
- Equipo de Respuesta a Incidentes (CSIRT Naval). Detección, análisis, contención, erradicación y recuperación conforme a NIST SP 800-61 Rev. 3. Coordina comunicaciones internas/externas y las lecciones aprendidas. (NIST SP 800-61, 2022)
- Personal de Apoyo Logístico y Técnico. Garantiza repuestos, herramientas y recursos para continuidad operativa; controla calibraciones y sellos de seguridad en equipos críticos. (Armada Nacional, 2024).

Para ilustrar cómo deben integrarse los roles y responsabilidades establecidos en el protocolo, se presenta un escenario operativo realista asociado al **spoofing de señales GNSS** durante una misión con ROV.

Durante la operación subacuática, el Centro de Operaciones de Seguridad (SOC) Naval, mediante correlación de eventos en el SIEM, detecta un anómalo desvío en las coordenadas recibidas vía GPS que indica un posible ataque de spoofing GNSS. De inmediato, notifica al CSIRT Naval, que activa el protocolo de respuesta a incidentes (véase Cap. 5.2.4), enviando la alerta prioritaria al personal en la unidad marítima y estableciendo los canales de comunicación de contingencia.

En paralelo, el operador del ROV Seaeye Lynx, siguiendo los lineamientos del protocolo técnico OT, ejecuta el plan de failover hacia el sistema de navegación inercial (INS), aislando la señal GNSS comprometida y verificando la estabilidad de la misión mediante los sensores internos del vehículo.

Por su parte, el Comandante del Comando de Buceo activa el procedimiento de contingencia operacional definido en la doctrina, garantizando la seguridad de los buzos en CCR Liberty y ordenando la priorización de la misión de rescate de activos frente a objetivos secundarios, hasta que la confiabilidad de la señal y de la red táctica sea reestablecida.

Simultáneamente, el personal técnico de servidores embarcados y estaciones en tierra (PDM-Tierra) realiza un análisis forense preliminar para confirmar el origen del ataque, mientras la red táctica mantiene la comunicación redundante mediante enlace satelital seguro. El caso queda documentado en el sistema SIEM del SOC y se integran las lecciones aprendidas en la próxima auditoría anual de ciberseguridad (Cap. 6).

Este escenario evidencia cómo la asignación clara de responsabilidades y la coordinación en capas –SOC/CSIRT (detección y respuesta), operadores técnicos (mitigación táctica en OT), y nivel de mando (decisión operacional)– permiten contener un ataque cibernético en tiempo real y evitar una afectación decisiva sobre la misión subacuática.

5.2.2.2 Asignación por activo del esquema

Para cada activo del entorno (red táctica, red satelital, PDM-Tierra, servidores embarcados y remotos/nube, ROV, CCR, dispositivos móviles, buques, GPS/GNSS/AIS) se designa un dueño primario y un suplente. El dueño es responsable de: inventario y configuración segura, cumplimiento de parches, registro y monitoreo, planes de respaldo/recuperación y

validación periódica de controles. El suplente asegura continuidad y cobertura en turnos y operaciones (ISO/IEC 27001, 2018).

5.2.2.3 Coordinación por fases

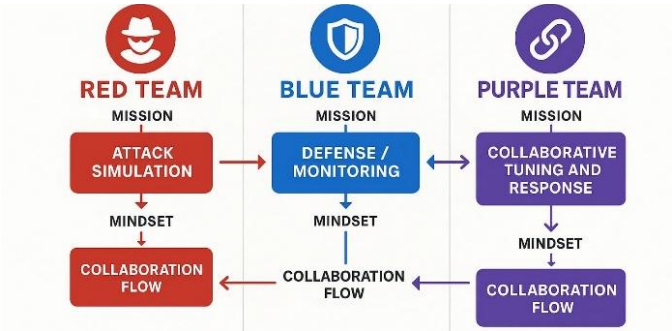
- **Antes del incidente**: el CISO asegura políticas y RACI; Operaciones y OT implementan segmentación, hardening y copias; el SOC/CSIRT valida reglas y ejercicios.
- **Durante el incidente**: el SOC alerta, el CSIRT lidera la respuesta y el COBUC decide sobre impacto en la misión.
- **Después del incidente**: se ejecuta recuperación con RTO/RPO definidos y se actualizan controles y procedimientos (NIST SP 800-61, 2022).

Este esquema promueve responsabilidad compartida, elimina vacíos de gestión explotables y fortalece la trazabilidad para auditoría y mejora continua (ISO/IEC 27001, 2018; IEC 62443-3-3, 2018; NIST SP 800-82, 2022; MinDefensa, 2023).

5.3 Estrategia de ciberresiliencia y ejercicios Red Team / Blue Team aplicados al entorno naval – subacuatico

La presente estrategia se fundamenta en el fortalecimiento de la ciberresiliencia institucional mediante la incorporación de ejercicios estructurados de ciberentrenamiento Red Team / Blue Team, adaptados al contexto operacional y tecnológico de la Armada Nacional de Colombia. Esta práctica permite validar de forma continua la eficacia de los controles técnicos y procedimentales definidos en el protocolo, garantizando que los sistemas de misión, las redes de automatización (OT) y los entornos tecnológicos (IT) mantengan una capacidad real de detección, respuesta y recuperación frente a incidentes cibernéticos.

Ilustración 6. Representación de la interacción entre equipos Red, Blue y Purple en ciberseguridad.



Fuente: Equipo rojo vs. equipo azul: Ataque, defensa y futuro de la ciberseguridad, con base en Khalil, M. (2025).

De acuerdo con Kim et al. (2024), los ejercicios Red/Blue Team constituyen un mecanismo sistemático para evaluar la seguridad de los sistemas de control industrial (ICS) a través de la simulación de escenarios reales de ataque y defensa, basados en marcos de referencia como MITRE ATT&CK para la ofensiva y D3FEND para la defensa. Estos ejercicios fomentan un proceso iterativo de mejora continua, donde las tácticas y técnicas ofensivas del Red Team se enfrentan a las defensas implementadas por el Blue Team, generando métricas de desempeño tales como el Mean Time to Detect (MTTD) y el Mean Time to Respond (MTTR), esenciales para medir la madurez de la respuesta cibernética (Kim et al., 2024).

Para el caso de esta investigación, en el ámbito subacuatico, la aplicación de esta estrategia se orienta a probar la integridad, disponibilidad y confidencialidad de los sistemas críticos involucrados en operaciones marítimas y subacuáticas, incluyendo los **sistemas ROV, sonar, GPS y comunicaciones tácticas**. La **IEC 62443** y el **NIST SP 800-61r2** establecen que las pruebas controladas de intrusión y respuesta constituyen elementos esenciales de una gestión de incidentes efectiva, al permitir identificar vulnerabilidades antes de que sean explotadas y fortalecer las capacidades humanas y tecnológicas (NIST, 2012).

Por su parte, Khalil (2025) destaca que los ejercicios deben evolucionar hacia un modelo **Purple Team**, donde la colaboración entre ofensiva y defensa promueva el intercambio inmediato de hallazgos y el ajuste de las reglas de detección, mejorando así la coordinación táctica entre el personal técnico, los operadores de misión y el Centro de Operaciones de Seguridad (SOC) naval. De esta forma, la estrategia Red/Blue Team no solo refuerza la ciberdefensa técnica, sino que también impulsa una **cultura organizacional de resiliencia**, donde la ciberseguridad se consolida como una capacidad operacional crítica dentro de la doctrina de defensa marítima nacional. (Khalil, 2025).

En síntesis, la integración de esta estrategia dentro del protocolo técnico garantiza una validación dinámica y continua de la seguridad, alineada con los estándares internacionales y con la doctrina de operaciones seguras de la Armada Nacional, fortaleciendo la protección del dominio cibernético naval y subacuátic**o** como parte esencial de la soberanía digital del Estado.

5.4 Plan de DISEÑO operacional

El plan de DISEÑO operacional del protocolo de ciberseguridad se concibe como un proceso **gradual, escalonado y medible**, orientado tanto a la mitigación de riesgos como a garantizar la continuidad operacional de los dispositivos ciberfísicos OT del Comando de Alistamiento de Buceo. Su diseño integra requisitos técnicos, humanos y organizacionales en sincronía con la doctrina C2 de la Armada Nacional y con las políticas nacionales de seguridad digital (DNP, 2020), al tiempo que se alinea con marcos internacionales de referencia como ISO/IEC 27001:2022, IEC 62443 y NIST SP 800-82 Rev. 3 (NIST, 2023).

5.4.1 Cronograma de adopción

El despliegue propuesto se articula en **cuatro fases secuenciales**, con hitos de validación y mecanismos de retroalimentación:

- **Fase de diagnóstico inicial (0–3 meses):** elaboración de inventario de activos críticos (red táctica, red satelital, ROV, CCR, servidores y móviles), aplicación de matrices de riesgo (ISO/IEC 27005) y definición de niveles de seguridad (SL) por zonas y conductos según IEC 62443.
- **Fase de DISEÑO técnica (4–9 meses):** segmentación de redes TI/OT, instalación de firewalls de nueva generación, despliegue de SIEM integrado al SOC naval, cifrado de enlaces satelitales y autenticación multifactor (MFA).
- **Fase de capacitación y prueba piloto (10–12 meses):** adiestramiento de operadores de ROV/CCR y administradores OT/TI en gestión de parches, hardening y respuesta a incidentes (NIST SP 800-61 Rev. 3), simulacro de ciberincidente en una unidad naval como laboratorio controlado.
- **Fase de consolidación y mejora continua (12–18 meses):** despliegue completo en todas las plataformas, validación de RTO/RPO, auditorías internas (ISO 27001) y externas (IEC 62443), ejercicios de mesa coordinados con CSIRT nacional e integración de lecciones aprendidas en un ciclo PDCA.

5.4.2 Requisitos técnicos y humanos

- **Técnicos:** arquitectura zonificada (IEC 62443), segmentación de tráfico crítico, cifrado extremo a extremo en telemetría ROV-PDM y en enlaces satelitales, copias de seguridad **3-2-1** con validación trimestral, redundancia de hardware en servidores embarcados/remotos, y detección de spoofing GNSS/AIS (Perales Garat, 2021).

- **Humanos:** designación de un **CISO naval** que lidere el SGSI, un administrador OT responsable del ciclo de vida de firmware/telemetría, operadores de ROV/CCR con competencias en ciberseguridad operacional, y un **CSIRT 24/7** especializado en entornos OT y marítimos.

5.4.3 Capacitación y sensibilización

La capacitación se plantea en **dos niveles complementarios**:

- **Nivel técnico:** personal TI/OT formado en segmentación, hardening, gestión de parches, monitoreo con SIEM y respuesta conforme a NIST (detección–contención–erradicación–recuperación). (NIST SP 800-61, 2022).
- **Nivel operativo:** buzos y técnicos capacitados en **ciberhigiene operacional**, listas de chequeo digitales, identificación temprana de anomalías en CCR/ROV y aplicación de protocolos de contingencia en misión. (NATO CCDCOE, 2022).

La sensibilización se refuerza con campañas periódicas, simulacros de intrusión coordinados por el SOC/CSIRT naval y ejercicios de cooperación interinstitucional (NATO CCDCOE, 2022).

5.4.4 Costos estimados y gestión del cambio

La DISEÑO considera tres líneas presupuestarias principales:

- **Tecnología:** adquisición de SIEM, licencias de cifrado, firewalls, autenticadores multifactor y dispositivos redundantes.
- **Capacitación:** formación técnica certificada (ISO 27001, IEC 62443) y entrenamientos con simuladores de incidentes marítimos/subacuáticos.
- **Gestión del cambio:** talleres de liderazgo y resiliencia organizacional, manuales de procedimientos, auditorías externas y certificaciones de cumplimiento.

La gestión del cambio debe garantizar que el protocolo se integre a la cultura naval, comunicando beneficios, estableciendo incentivos al cumplimiento y validando periódicamente el nivel de madurez cibernética mediante revisiones del Comando de Alistamiento de Buceo (MinDefensa, 2023).

5.5 Alcance, aplicabilidad y aspectos a reforzar

La propuesta de protocolo de ciberseguridad diseñada se constituye en una **solución viable y aplicable al Comando de Alistamiento de Buceo de la Armada Nacional**, al integrar de

manera coherente la protección de sistemas de información (TI), tecnologías operativas (OT) y sistemas ciberfísicos (CPS), articulando tanto la doctrina institucional colombiana como los marcos normativos internacionales de mayor relevancia (NIST SP 800-82 Rev. 3).

La experiencia documentada en el **ejercicio MARSEC-20**, donde se demostró la facilidad con la que atacantes pudieron comprometer sistemas portuarios, buques y entidades de defensa mediante PENTEST y spoofing de señales AIS/GNSS (Perales Garat, 2021), confirma la pertinencia de fortalecer la ciberdefensa naval bajo un enfoque de defensa en capas. Igualmente, las lecciones obtenidas del ataque de *ransomware* al Puerto de Barcelona en 2018, que paralizó la red corporativa y obligó a mantener operaciones manuales durante varios días, demuestran la necesidad de sistemas de respaldo resilientes (Rodríguez, 2024).

La aplicabilidad en el contexto colombiano se justifica además en la evidencia presentada en el estudio sobre **infraestructura portuaria nacional**, en el que se señala que la gobernanza fragmentada y la dependencia tecnológica incrementan la vulnerabilidad de los sistemas portuarios y navales, subrayando la necesidad de planes unificados de ciberseguridad y cooperación interinstitucional (Drougkas et al., 2020).

No obstante, para que la propuesta alcance un nivel integral de madurez estratégica dentro de la Armada Nacional, se recomienda incorporar tres refuerzos:

- **Simulación y ejercicios adversariales permanentes (Red Teaming):** tanto MARSEC-20 como los lineamientos de la OTAN han demostrado que los ejercicios de penetración y perturbación real son la vía más efectiva para descubrir brechas ocultas (Perales Garat, 2021).
- **Seguridad de la cadena de suministro y dependencia tecnológica:** el Comando de Alistamiento de Buceo, atreves de sus departamentos de buceo, utiliza equipos críticos importados (CCR, ROV, sistemas satelitales) que requieren protocolos estrictos de validación de firmware, control de parches y auditoría de proveedores externos (Drougkas et al., 2020).
- **Integración estratégica multinivel:** es clave que el protocolo se articule no solo al nivel táctico-operativo, sino también con el nivel estratégico, incluyendo a **DIMAR, ColCERT, el Comando Conjunto del Ciberespacio y redes de cooperación OTAN-OEA**, en línea con lo establecido en el Decreto 338 de 2022 sobre gobernanza de la seguridad digital en Colombia.

En conclusión, el protocolo propuesto no se limita a controles técnicos, sino que **fortalece la cultura organizacional de seguridad digital**, integra el factor humano y se posiciona como un **marco viable de ciberdefensa naval** para operaciones subacuáticas. Adicionalmente, responde a la urgencia de proteger infraestructuras críticas nacionales vinculadas con el comercio marítimo, la defensa y la soberanía nacional (MinDefensa, 2023).

6 Evaluación y mejora

6.1 Indicadores de desempeño del protocolo

La efectividad de un protocolo de ciberseguridad no se limita a su diseño e DISEÑO, sino que depende de su capacidad para demostrar resultados medibles en la protección de los activos críticos. En el caso de las operaciones subacuáticas de la Armada Nacional de Colombia, los **indicadores de desempeño (KPIs)** permiten evaluar la eficacia de los controles aplicados en sistemas TI, TO y CS, incluyendo estaciones de monitoreo, ROV, CCR y enlaces de comunicaciones.

De acuerdo con la norma ISO/IEC 27004, la medición del desempeño debe estar alineada con los objetivos de seguridad de la información y los riesgos previamente identificados (ISO, 2022). Del mismo modo, el marco NIST SP 800-55 Rev. 1 propone que los indicadores deben ser específicos, medibles, alcanzables, relevantes y trazables en el tiempo (NIST, 2021).

En coherencia con la estrategia de ciberresiliencia Red Team / Blue Team descrita en el Capítulo 5, se incorporan indicadores adicionales derivados de los ejercicios de ciberentrenamiento, que permiten evaluar la capacidad de detección, respuesta y mejora continua frente a escenarios simulados de ataque y defensa. Según Kim et al. (2024), la inclusión de métricas operacionales basadas en estos ejercicios posibilita medir la madurez de la respuesta cibernética y la eficacia real de los controles técnicos implementados en entornos OT y TI. Entre los indicadores derivados se destacan:

- **Cobertura de tácticas ATT&CK detectadas:** porcentaje de técnicas ofensivas del Red Team correctamente identificadas por el Blue Team.
- **Eficacia de contención:** proporción de ataques simulados mitigados dentro de los parámetros de seguridad establecidos.
- **Reducción de MTTD y MTTR:** disminución porcentual del tiempo medio de detección y respuesta entre ejercicios consecutivos.

- **Ajuste de reglas de detección:** cantidad de firmas, alertas o políticas del SIEM actualizadas tras los ejercicios.
- **Índice de corrección de vulnerabilidades:** número de fallas técnicas corregidas como resultado directo de las simulaciones.

De manera complementaria, se mantienen los KPIs clave definidos en el protocolo, en línea con las directrices del NIST (2023) y la ISO/IEC 27004, los cuales permiten evaluar la operación continua y el cumplimiento normativo:

- **MTTD (Mean Time to Detect):** tiempo medio para identificar incidentes, aplicable en servidores, SIEM y enlaces satelitales.
- **MTTR (Mean Time to Respond):** tiempo promedio de respuesta frente a ciberataques en ROV y CCR (comandos de emergencia, failover seguro).
- **Disponibilidad de sistemas críticos:** porcentaje de operación continua de ROV, CCR y servidores tácticos.
- **Cumplimiento normativo:** grado de alineación con ISO/IEC 27001 e IEC 62443 en dispositivos y redes OT.
- **Tasa de incidentes mitigados:** relación entre ataques detectados y ataques contenidos por el CSIRT naval.

Finalmente, los resultados obtenidos de estos indicadores deberán consolidarse mediante reportes del Centro de Operaciones de Seguridad (SOC) y del CSIRT naval, permitiendo generar análisis comparativos, tendencias e informes de madurez cibernética.

Estos datos no solo alimentan el proceso de mejora continua, sino que también fortalecen la cultura de evaluación basada en evidencia, como recomiendan Rodríguez (2024), la OEA (2021) y los marcos internacionales de gestión de ciberseguridad para infraestructuras críticas..

6.2 Estrategias de mejora continua

La mejora del protocolo está orientada a incorporar las lecciones aprendidas de incidentes reales y simulados, así como las tendencias internacionales en materia de ciberdefensa marítima. Este proceso se sustenta en la actualización periódica de los controles técnicos y procedimentales, la modernización de las infraestructuras y la cooperación interinstitucional.

- **Lecciones de incidentes internacionales:** los casos de ransomware en Barcelona y Maersk evidencian la necesidad de mantener políticas de respaldo tipo 3–2–1 y un SIEM activo capaz de detectar anomalías tempranas (Rodríguez, 2024).
- **Perturbaciones en sistemas AIS/GNSS (Marsec 20, 2021):** refuerzan la importancia de implementar equipos multiconstelación, redundancia de sensores y validación cruzada de señales mediante procedimientos de ciberentrenamiento y monitoreo continuo.
- **Tendencias internacionales:** el protocolo debe actualizarse periódicamente conforme a la Resolución MSC.428(98) de la Organización Marítima Internacional (OMI), las recomendaciones de BIMCO (2021) y los lineamientos de la Unión Europea en resiliencia portuaria (Drougkas et al., 2020).
- **Integración estratégica:** se propone que el Comando de Alistamiento de Buceo que mantenga una articulación directa con DIMAR, ColCERT, CSIRT gubernamental, y aliados internacionales (OTAN–OEA), a fin de garantizar cooperación, intercambio de inteligencia y actualización constante de buenas prácticas en ciberresiliencia naval.
- **Ciclo de mejora Red/Blue Team:** los resultados de los ejercicios se integrarán a los programas de entrenamiento y auditoría, generando un proceso dinámico de aprendizaje y actualización de las defensas.

De esta manera, cada ciclo de simulación se convierte en una fuente de optimización del protocolo, fortaleciendo la madurez cibernética del Comando de Alistamiento de Buceo y asegurando la continuidad operacional bajo los principios del PDCA (NATO CCDCOE, 2022).

Tabla 11. Riesgos y medidas de mitigación en dispositivos ciberfísicos OT del Comando de Buceo

Sistema / Dispositivo	Riesgo sobre Confidencialidad	Riesgo sobre Integridad	Riesgo sobre Disponibilidad	Ejemplos de ataque (documentados)	Medidas de mitigación (normas / lecciones)
Red táctica naval	Interceptación de comunicaciones sensibles	Manipulación de órdenes de misión	DoS por interferencia electromagnética	Perturbación de VHF y spoofing AIS en MARSEC-20	Segmentación por Zonas/Conductos (IEC 62443), cifrado extremo a extremo, MFA
Red satelital	Espionaje de datos de enlace	Alteración de señal GNSS	Negación de posicionamiento (jamming)	Perturbación GPS y spoofing GNSS en Cartagena (MARSEC-20)	Receptores GNSS multiconstelación, cifrado de telemetría, redundancia con INS

Servidores (SOC/CSIRT)	Robo de credenciales	Alteración de logs o telemetría	Ransomware que paraliza operaciones	Puerto de Barcelona 2018: ransomware que obligó a operar manualmente	Backups 3-2-1 offline, SIEM monitorizando anomalías, gestión de parches (ISO 27001, NIST 800-82)
Servidor remoto	Acceso a datos clasificados (comunicaciones tierra-mar)	Inyección de malware	Caída del enlace CSIRT–operaciones	Compromiso de servidores portuarios en MARSEC-20	Arquitectura híbrida con firewalls dedicados, SOC naval redundante
ROV (vehículo submarino)	Robo de telemetría de misión	Inyección o spoofing de comandos	Bloqueo de control remoto en operación crítica	Interferencia OT en MARSEC-20; DoS contra sistemas OT	Whitelisting de comandos críticos, cifrado de enlace PDM–ROV, pruebas de failover seguro
CCR (rebreathers)	Exposición de datos biométricos del buzo	Manipulación de software / firmware de sensores	Malfuncionamiento en misión de buceo	Vector plausible de ataque por firmware malicioso (riesgo supply chain)	Validación de firmware propietario, auditoría de proveedores, redundancia de sensores O2
PDM – Tierra	Exposición de información de control	Alteración en telemetría del ROV	Pérdida total de enlace operativo	Spoofing de datos AIS/GNSS y telemetría manipulada	Firewalls de aplicación, segmentación IT/OT, SIEM de correlación en tiempo real
Dispositivo móvil	Acceso no autorizado a apps OT/TI	Instalación de malware (apps falsas)	Bloqueo de acceso al SOC o red táctica	Phishing y malware documentados en sector marítimo	MDM (Mobile Device Management), autenticación MFA, prohibición de USB no validados
Buques	Robo de datos logísticos/comerciales	Spoofing AIS y GPS	Denegación de servicios de navegación y propulsión	DoS, spoofing AIS y perturbación radar en MARSEC-20	Redundancia INS, hardening ECDIS, auditoría Código PBIP con riesgos cibernéticos

Fuente: Elaboración propia con base en Perales Garat (2021), y Rodríguez (2024), ISO/IEC 27001 (2022)

Los riesgos y medidas presentadas en la tabla también constituyen la base de los escenarios de ciberentrenamiento Red Team / Blue Team desarrollados en el marco del protocolo. A partir de esta matriz, se pueden **simular ataques dirigidos** (phishing, spoofing, DoS, manipulación de telemetría o ransomware) sobre los activos críticos identificados, por ejemplo, ROV, CCR, redes tácticas o servidores SOC, a fin de **evaluar la efectividad de los controles** y la capacidad de respuesta del personal naval. (Kim et al., 2024)

Esta aplicación práctica, sustentada en los marcos MITRE ATT&CK, D3FEND, IEC 62443 y NIST SP 800-61r2, permite traducir los riesgos teóricos en ejercicios operacionales de validación, fortaleciendo la ciberresiliencia institucional (Khalil, 2025). De este modo, la matriz no solo cumple una función diagnóstica, sino que se convierte en una herramienta activa de planificación, evaluación y mejora continua dentro del ciclo PDCA del protocolo de ciberseguridad.

7 Conclusiones

1) La investigación demostró que los sistemas de información embarcados, junto con los ROV Seaeye Lynx y los CCR Liberty, constituyen activos digitales críticos para la Armada Nacional. Su vulnerabilidad frente a ciberataques implica no solo un riesgo directo en la seguridad operacional subacuática, sino también en la protección del patrimonio cultural sumergido, incluyendo bienes estratégicos como el Galeón San José.
2) El análisis evidenció que no existen protocolos específicos de ciberseguridad adaptados al entorno subacuático colombiano, lo que incrementa el riesgo de pérdida de datos, sabotaje digital e interferencia en misiones estratégicas. Esta brecha coincide con advertencias internacionales sobre la urgencia de proteger las infraestructuras críticas marítimas y portuarias frente a vulnerabilidades globales (NATO CCDCOE, 2022).
3) La clasificación de riesgos bajo los modelos CIA (Confidencialidad, Integridad, Disponibilidad) **y** STRIDE permitió identificar amenazas críticas como el acceso no autorizado, manipulación de sensores, denegación de servicio y alteración de firmware**.** Estas condiciones reproducen hallazgos de ejercicios internacionales como MARSEC-20, donde se demostró la facilidad de manipular sistemas portuarios, radares y enlaces satelitales con escasas barreras defensivas (Perales Garat, 2021).
4) La aplicación de la matriz DOFA reveló fortalezas del Comando de Alistamiento de Buceo, tales como la existencia de capital humano especializado y una sólida doctrina naval; pero también debilidades como el almacenamiento de datos sin cifrar, falta de parches de seguridad actualizados y ausencia de monitoreo en tiempo real. Asimismo, se identificaron amenazas vinculadas a la dependencia tecnológica y la obsolescencia en sistemas OT, en concordancia con lo establecido por el NIST (2022) y la ISO/IEC 27001 (2022).

5) El protocolo de ciberseguridad diseñado —basado en los marcos ISO/IEC 27001, IEC 62443 y NIST SP 800-82— y contextualizado al entorno militar colombiano, constituye una respuesta integral y aplicable. El modelo propuesto articula cinco módulos: gestión de riesgos, controles técnicos y procedimentales, monitoreo continuo, respuesta ante incidentes y capacitación especializada, apoyados por una matriz RACI que garantiza trazabilidad y responsabilidades claras en cada fase.
6) La investigación propone la DISEÑO de ejercicios de ciberentrenamiento Red Team / Blue Team como parte del protocolo de ciberresiliencia del Comando de Alistamiento Buceo. Estos ejercicios permitirían validar la eficacia de los controles técnicos y fortalecer la capacidad institucional de respuesta ante incidentes, generando métricas como el MTTD y el MTTR para medir la madurez del sistema. En este sentido, la estrategia de resiliencia propuesta es viable, medible y replicable en otras unidades navales, contribuyendo al desarrollo de una cultura organizacional en ciberdefensa (Khalil, 2025).
7) Se comprobó que los sistemas de información, automatización y control (TI, TO y CS) empleados en operaciones subacuáticas son inherentemente complejos, y al incorporar medidas de ciberseguridad se incrementa su complejidad arquitectónica debido a la interdependencia entre componentes físicos, lógicos y de comunicación. Sin embargo, esta integración resulta esencial para garantizar la seguridad operacional, la disponibilidad de datos de misión y la protección del personal de buceo, consolidando así la defensa del dominio cibernético naval.
8) Finalmente, la investigación cumplió con los objetivos propuestos y respondió la pregunta central, al desarrollar e implementar un protocolo de ciberseguridad aplicable al entorno subacuático colombiano, que aborda la protección de la información generada durante operaciones de buceo y exploración marítima. El estudio consolidó un modelo técnico y doctrinal que integra cultura organizacional, entrenamiento cibernético y marcos normativos internacionales, proporcionando una base sólida para futuras políticas de ciberdefensa naval.
9) En síntesis, los resultados de esta investigación ofrecen un modelo replicable y escalable para el fortalecimiento de la ciberdefensa en operaciones marítimas y subacuáticas, combinando gobernanza, doctrina, controles técnicos y cooperación internacional. Este trabajo representa la primera propuesta doctrinal en Colombia enfocada en ciberseguridad

aplicada al dominio subacuático, integrando TI–OT–CS con la protección del patrimonio cultural sumergido y contribuyendo al ejercicio soberano del Estado en el dominio marítimo y ciberespacial.

8 Recomendaciones

1) Implementar un protocolo de ciberseguridad por capas (defense in depth) que articule medidas preventivas, detectivas y reactivas en los sistemas TI, TO y CS empleados en operaciones subacuáticas. Este enfoque permitirá contener amenazas desde sus etapas iniciales hasta su potencial explotación, alineándose con los lineamientos de la ISO/IEC 27001 para entornos TI y la familia IEC 62443 para infraestructuras OT, fortaleciendo la resiliencia y continuidad operacional del Comando de Buceo.
2) Integrar los sistemas de monitoreo de ROV, CCR y estaciones embarcadas al SOC naval, asegurando la vigilancia continua mediante plataformas SIEM (Security Information and Event Management) y la correlación de eventos en tiempo real. Esta integración permitirá la detección temprana de anomalías y ataques, garantizando una respuesta coordinada entre el CSIRT, las unidades tácticas y el personal embarcado, en consonancia con las mejores prácticas del NIST SP 800-137.
3) Establecer un programa de capacitación y concienciación permanente en ciberseguridad, dirigido a buzos tácticos, operadores de ROV/CCR y personal técnico del Comando de Buceo. El programa deberá incluir ejercicios de ciberentrenamiento Red Team / Blue Team, simulaciones de incidentes tipo ransomware y spoofing AIS/GNSS, así como prácticas de resiliencia operacional. Esto permitirá desarrollar una cultura organizacional de defensa cibernética, considerando el factor humano como la primera línea de protección (Kim et al., 2024).
4) Realizar auditorías técnicas periódicas (mínimo anuales) sobre los sistemas críticos TI, TO y CS, aplicando pruebas de penetración (pentesting), auditorías de firmware en CCR y ROV, y análisis de vulnerabilidades en enlaces satelitales y tácticos. Estas auditorías deben regirse por las normas ISO/IEC 27001, NIST SP 800-82 e IEC 62443, integrándose en un ciclo de mejora continua (PDCA) dentro del Sistema de Gestión de Seguridad de la Información (SGSI) institucional.

5) Fortalecer la cooperación interinstitucional e internacional, generando protocolos de coordinación entre la Armada Nacional, el Ministerio de Cultura, el MinTIC y organismos como la OMI, OEA y EMSA, a fin de garantizar la protección del patrimonio cultural sumergido frente a ciberamenazas. Esta articulación también permitirá la homologación de estándares de seguridad marítima, fomentando el intercambio de inteligencia y la interoperabilidad digital.
6) Priorizar la asignación de recursos financieros, tecnológicos y humanos para la adquisición de herramientas avanzadas de ciberseguridad (firewalls de última generación, cifrado extremo a extremo, honeypots OT, SIEM de nivel militar) y la consolidación de un CSIRT naval especializado en ciberdefensa subacuática. Este equipo deberá asumir funciones de monitoreo 24/7, respuesta a incidentes, gestión de vulnerabilidades y coordinación con los CERT nacionales (ColCERT, MCCE), asegurando la sostenibilidad del protocolo propuesto.

9 Bibliografía

Aubard, M., et al. (2024). Sonar-based Deep Learning in Underwater Robotics. arXiv:2402.03268v1.

Armada Nacional de Colombia. (2021). Manual para la elaboración del plan estratégico específico y los planes navales de la Armada Nacional (1.ª ed., versión final preliminar). Armada Nacional de Colombia.

Ammar, M., & Khan, I. A. (2024). Cyber attacks on maritime assets and their impacts on health and safety aboard: A holistic view [Preprint]. arXiv. https://arxiv.org/abs/2407.08406

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123–138. https://doi.org/10.3390/network2010009

Atkinson, Ryan J., "NATO Cyber Defence, 2000-2022" (2023). Electronic Thesis and Dissertation

Repository. 9700. https://ir.lib.uwo.ca/etd/9700

BIMCO. (2021). Guidelines on cyber security onboard ships (Version 4.0). Baltic and International Maritime Council, International Chamber of Shipping, INTERCARGO, INTERTANKO, CLIA, OCIMF, IUMI, International Group of P&I Clubs, ITF, & World Shipping Council. https://www.bimco.org/about-us-and-our-members/publications/guidelines-on-cyber-security-onboard-ships

Canadian Centre for Cyber Security. (2023). National cyber threat assessment 2025–2026. Government of Canada. https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Chatterjee, P., Gupta, P., & Sharma, R. (2024). *A cybersecurity framework using machine learning for red team/blue team exercises*. *Journal of Information Security and Applications*, 80, 103789. https://doi.org/10.1016/j.jisa.2024.103789

ColCERT. (2025). RFC 2350 – Colombian Cyber Emergency Response Team (ColCERT) (versión 2.0, 15 de mayo de 2025). Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.colcert.gov.co/800/w3-channel.html

Comando de Alistamiento de Buceo. (2024). Plan Estratégico Comando de Alistamiento de Buceo 2024–2027 [Documento institucional de uso interno]. Armada Nacional de Colombia.

Delgado, J. P. (2020). The Galleon San José: Almost four decades of legal struggles. International Journal of Nautical Archaeology, 49(2), 307–319. https://doi.org/10.1111/1095-9270.12420

Departamento Nacional de Planeación. (2020). Política nacional de seguridad digital 2020–2025 (Documento CONPES 3995). Consejo Nacional de Política Económica y Social. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Divesoft. (2025). CCR Liberty: Operation and user manual (Versión 2.17.3/100). Divesoft s.r.o.

Drougkas, A., Sarri, A., & Shapiro, S. (2019). Cybersecurity and resilience of smart hospitals. European Union Agency for Cybersecurity (ENISA).

ENISA. (2023). Threat Landscape for the Maritime Sector. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0

Ferri, G., Allotta, B., Costanzi, R., Ridolfi, A., Salaris, P., & Fanucci, L. (2017). Cooperative robotic networks for underwater surveillance: An overview. IET Radar, Sonar & Navigation, 11(12), 1740–1750. https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/iet-rsn.2017.0204

Guananga Reyna, L. A., & Rodríguez Espinosa, M. (2023). Cybersecurity in focus: A comparative analysis of threats and strategies in Latin American and Caribbean States. Latin American Institute of Cybersecurity.

Guerrero-Bonilla, M., Parra-Velandia, F. J., & Cruz, N. A. (2022). Sonar-Based Deep Learning in Underwater Robotics: An Overview. Universidad de los Andes, Facultad de Ingeniería, Departamento de Ingeniería Eléctrica y Electrónica.

Guerrero-Bonilla, C., González-Vázquez, J., & Gómez-Aguilar, M. (2022). Ciberseguridad en vehículos robóticos autónomos. Universidad de Salamanca.

Instituto Nacional de Ciberseguridad. (2023) El proceso de certificación en IEC62443-3-3. INCIBE. https://www.incibe.es/incibe-cert/blog/el-proceso-de-certificacion-en-iec62443-3-3

International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO.

Joseph, R., & Fred, A. (2023). Semi and self-supervised learning for multi-label classification: A review. arXiv. https://arxiv.org/abs/2301.05678

Kim, D., Jeon, S., Kim, K., Kang, J., Lee, S., & Seo, J. T. (2024). Guide to developing case-based attack scenarios and establishing defense strategies for cybersecurity exercise in ICS environment. The Journal of Supercomputing. https://doi.org/10.1007/s11227-024-06273-9

Khalil, M. (2025, mayo 2). Equipo rojo vs. equipo azul: Ataque, defensa y futuro de la ciberseguridad. DeepStrike. https://deepstrike.io/blog/red-team-vs-blue-team-cybersecurit

Ministerio de Defensa Nacional. (2023). Plan de seguridad y privacidad de la información. Ministerio de Defensa Nacional.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). Seguridad digital de Colombia. Gobierno de Colombia. https://www.mintic.gov.co/

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2020). NIST handbook 150:2020. U.S. Department of Commerce. https://doi.org/10.6028/NIST.HB.150-2020

NATO (2022). New Concept for NATO Cyber Defence. Brussels: NATO Communications and Information Agency.

NQA. (2020). ISO/IEC 27001: Guía de implantación del Sistema de Gestión de Seguridad de la Información (SGSI). NQA Global Assurance. https://www.nqa.com

Organización Internacional de Normalización. (2012). ISO 21500:2012 – Directrices para la dirección y gestión de proyectos (traducción oficial). ISO.

Organización Marítima Internacional. (2022). Directrices sobre la gestión de los riesgos cibernéticos marítimos (MSC-FAL.1/Circ.3/Rev.2). Londres: OMI.

Perales Garat, L. (2021). MARSEC-20. Un escenario de ciberseguridad marítima. En Intereses Marítimos de Colombia (pp. 733-742). Revista General de Marina.

Rodriguez, C. (2024). Tendencias y desafíos de la economía digital para los intereses marítimos de Colombia.

Rojas Niño, J. E. (2014). Infraestructura portuaria: Una aproximación desde la ciencia política (1.ª ed.). Universidad Militar Nueva Granada.

Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill Education.

Seaeye Ltd. (2020). Lynx 1160 ROV system: Operation and maintenance manual (Rev. 4). Saab Seaeye Ltd.

Stouffer, K., Tang, C., & Newhouse, W. (2022). Guide to operational technology (OT) security (NIST Special Publication 800-82 Revision 3, Initial Public Draft). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3.ipd

Tamarkar, A., & Patra, B. (2018). Cybersecurity threats and countermeasures: A review. Turkish Journal of Computer and Mathematics Education, 9(3), 1400–1404.

US Coast Guard. (2020). Vessel Cyber Risk Management Work Instruction. https://www.uscg.mil//

Verma, A., Singh, P., Kumar, R., & Sharma, M. (2025). Aprendizaje automático para la ciberseguridad de sistemas ciberfísicos robóticos: Una revisión. Revista de Investigación en Ciberseguridad y Robótica, 11(1), 22–38.

Weerth, S. (2020). Cocaine smuggling by narco-submarines from Latin America to Europe and Africa: Crime, law, and criminal justice. Colloquium on Transnational Criminal Justice, 1(1), 1–20. https://doi.org/10.2139/ssrn.3680740