Escuela Superior De Guerra “General Rafael Reyes Prieto”

"Sistema de Gestión de Vulnerabilidades ciberneticas en un Buque tipo OPV-93C: Aplicación de la metodología STRIDE y el Modelo DREAD"

CC. Ospina Arango Juan Sebastián

CC. Parra Montañez Diego Enrique

MY. Martínez Rueda Julián Aldeisy

MY. Suarez Rojas Jerson Enrique

Curso De Estado Mayor

Gestión de Riesgos

Jaider Ospina Navas

02 de Marzo de 2025

"Sistema de Gestión de Vulnerabilidades ciberneticas en un Buque tipo OPV-93C: Aplicación de la metodología STRIDE y el Modelo DREAD"

"La seguridad no es un producto, es un proceso" (Schneier, 2000, p. 317)

Introducción

El Buque tipo OPV-93C Patrullero de Zona Económica Exclusiva es el tercer buque construido por COTECMAR para la Armada Nacional (ARC, 2017, p. 1) y desempeña tareas de defensa de la soberanía nacional, protección de los intereses marítimos, interdicción marítima, seguridad y control del tráfico marítimo, búsqueda y rescate, control medio ambiental, operaciones de paz y apoyo humanitario.

Figura 1.

Buque tipo OPV-93C Patrullero de Zona Económica Exclusiva (Tascon, Quintero, & Sejnaul, 211, p. 1)

El buque cuenta con una eslora de 93 m, manga de 14,2 metros, puntal 6,5 metros, calado de 4,5 metros, con un desplazamiento de 2400 toneladas, autonomía de 45 días y una velocidad máxima de 22 nudos. Dispone de un hangar para un helicóptero Sea Hawk S-70B, cubierta de

vuelo, espacio para un bote interceptor de Guardacostas, dos botes de rescate, capacidad de suministro eléctrico para un contenedor de 20 pies y una grúa con capacidad de 5,5 toneladas.

Descripción del escenario

Para mantener la resiliencia operacional en escenarios de conflicto y operaciones navales, y con el objetivo de anticipar vulnerabilidades y diseñar estrategias de mitigación, se debe implementar el "sistema de gestión de la Información" (ISO/IEC 27001, 2022, p. 2) para la gestión de vulnerabilidades cibernéticas del buque OPV-93C. Este sistema cumple funciones clave como la identificación de amenazas, la evaluación de riesgos, la implementación de medidas de protección y la respuesta ante incidentes cibernéticos garantizando la protección de los sistemas críticos de la Unidad.

Su aplicación requiere la realización de análisis semanales, considerando escenarios dinámicos y cambiantes en las cuatro áreas de mayor riesgo a bordo: cuarto de máquinas, puente de gobierno, cuarto de radio y Centro de Información de Combate (CIC). A través de este enfoque, se fortalece la capacidad del buque para detectar amenazas, responder a incidentes y garantizar la integridad y disponibilidad de sus sistemas de mando y control en entornos operativos complejos.

La integración del Sistema de Gestión de Vulnerabilidades Cibernéticas garantiza un enfoque proactivo y adaptativo para la protección de los sistemas digitales y tecnológicos del OPV-93C, minimizando el impacto de ataques cibernéticos y asegurando la continuidad operativa en misiones estratégicas.

Tabla 1

Áreas de aplicación del sistema de Gestión de Vulnerabilidades ciberneticas en un Buque tipo OPV93C

Áreas de aplicación del sistema de Gestión de Vulnerabilidades ciberneticas en un Buque tipo OPV-93C	
Áreas de la Unidad	**Descripción**
Cuarto de Maquinas	Es el área donde se alojan los sistemas de propulsión y generación de energía. Aquí se encuentran los motores, generadores, bombas, sistemas de control y monitoreo, y equipos auxiliares que permiten el funcionamiento mecánico y eléctrico del buque.

Puente de Gobierno	Es el centro de mando y control del buque. En el puente se gestionan la navegación, la maniobra y la toma de decisiones estratégicas. Se integran sistemas de radar, GPS, cartografía digital, control de la hélice y sistemas de comunicación con la tripulación
Cuarto de Radio	Esta área es responsable de todas las comunicaciones del buque con entidades externas (otras embarcaciones, autoridades portuarias, organismos de rescate, etc.). Se manejan radios, sistemas satelitales y equipos de cifrado para mantener comunicaciones seguras y fiables.
Centro de Información de combate (CIC)	El CIC es el núcleo de gestión de la información táctica en situaciones de combate o de alto riesgo. Se integran datos de múltiples sensores (radar, sonar, sistemas de guerra electrónica) para evaluar la situación y coordinar respuestas operativas

Análisis de riesgos

A bordo de la Unidad todos los departamentos se reúnen mensualmente bajo el liderazgo del departamento de ciberseguridad se utiliza la metodología STRIDE "para identificar y clasificar las amenazas ciberneticas" (Praerit & Kohnfelder , 2023, p. 1), esta metodología, desarrollada por Microsoft, permite analizar las amenazas que afectan las operaciones navales, clasificándolas en seis categorías principales (tabla 2).

De acuerdo con el mapa de procesos de la unidad, la metodología STRIDE se aplica en 4 áreas críticas de la Unidad: Área 1 (cuarto de máquinas), Área 2 (puente de gobierno), Área 3 (cuarto de radio) y Área 4 (centro de información de combate CIC). Su objetivo es identificar amenazas cibernéticas, evaluando la probabilidad de ocurrencia y el impacto de la materialización del riesgo de cada amenaza sobre las operaciones. Con este análisis, se determina un índice de criticidad, permitiendo enfocar los esfuerzos en la mitigación de las vulnerabilidades más significativas.

Tabla 2

Relación de amenazas con base en la metodología STRIDE

DESCRIPCION	AMENAZAS	
Suplantación de identidad Un atacante suplanta la señal del GPS del buque (GPS Spoofing), enviando coordenadas falsas y desviando la embarcación de su curso real.	**SPOOFING**	**A1**
Manipulación de datos Un atacante modifica los datos del sistema de navegación o radar del buque para alterar la información sobre obstáculos, rutas seguras o tráfico marítimo.	**TAMPERING**	**A2**
Repudio o negación de acciones Un oficial de a bordo manipula registros de acceso a los sistemas electrónicos del barco y luego niega haber realizado cambios no autorizados en el sistema de control del buque.	**REPUDIATION**	**A3**
Disclosure (Divulgación de información) Un ciberdelincuente accede sin autorización a planes de navegación, datos de carga o comunicaciones de la tripulación, exponiendo información sensible a piratas o actores maliciosos.	**IINFORMATIO DISCLOSURE**	**A4**
Denegación de servicio - DoS Un ataque DoS sobre el sistema de comunicaciones satelitales del buque impide la transmisión de datos con la base en tierra, dejando a la tripulación sin contacto.	**DENIAL OF SERVICE**	**A5**
Elevación de privilegios Un atacante con acceso limitado a los sistemas del barco logra escalar privilegios y obtiene control total sobre el Sistema de Gestión del Buque (Vessel Management System - VMS), comprometiendo su operación.	**ELEVATION PRIVILEGE**	**A6**

En la reunión semanal de ciberseguridad a bordo de la unidad, se presentan las amenazas que afectan la operación, permitiendo que cada jefe de departamento evalúe la probabilidad de ocurrencia (%) (Tabla 3). Esta calificación se basa en los factores de riesgo que determinan dicha probabilidad (Tabla 4) y en el impacto de la materialización del riesgo, el cual se valora en una escala de 1 a 5 (Tabla 5).

Tabla 3

Matriz de probabilidad de ocurrencia con base en la metodología STRIDE

		PROBABILIDAD DE OCURRENCIA				PROMEDIO
		AREAS DEL BUQUE TIPO OPV80 (PATRULLERA OCEANICA)				
AMENAZAS		CUARTO MAQUINAS	PUENTE DE GOBIERNO	CUARTO DE RADIO	CENTRO DE INFORMACION DE COMBATE	
SPOOFING	A1	75%	90%	65%	90%	80%
TAMPERING	A2	75%	90%	65%	90%	80%
REPUDIATION	A3	50%	90%	25%	90%	64%
IINFORMATIO DISCLOSURE	A4	25%	90%	90%	90%	74%
DENIAL OF SERVICE	A5	25%	90%	90%	90%	74%
ELEVATION PRIVILEGE	A6	25%	75%	65%	90%	64%

Tabla 4

Factores de riesgo que determinan cada probabilidad con base en la metodología STRIDE

FACTORES DE RIESGO QUE DETERMINAN LA PROBABILIDAD	
PC O SERVIDORES	25%
RED	25%
INFORMACIÓN CLASIFICADA O DE VALOR	15%
ENTRENAMIENTO DEL PERSONAL EN CIBER	10%
SISTEMAS SCADA	25%
	100%

Tabla 5

Impacto del riesgo de cada amenaza con base en la metodología STRIDE

		IMPACTO DEL RIESGO				PROMEDIO	IMPACTO DEL RIESGO
		AREAS					
AMENAZAS		CUARTO MAQUINAS	PUENTE DE GOBIERNO	CUARTO DE RADIO	CENTRO DE INFORMACION DE COMBATE		
SPOOFING	A1	4	5	3	5	4,25	ALTO
TAMPERING	A2	4	5	3	5	4,25	ALTO
REPUDIATION	A3	2	5	1	5	3,25	MEDIO
IINFORMATIO DISCLOSURE	A4	1	5	5	5	4	ALTO
DENIAL OF SERVICE	A5	1	5	5	5	4	ALTO
ELEVATION PRIVILEGE	A6	1	4	3	5	3,25	MEDIO

Una vez consolidada y analizada la información, se ponderan las calificaciones de las diferentes áreas, lo que permite generar una matriz de riesgos. Esta matriz identifica las amenazas cibernéticas, estableciendo la relación entre la probabilidad de ocurrencia, el impacto del riesgo y el índice de criticidad (Tabla 6).

Tabla 6

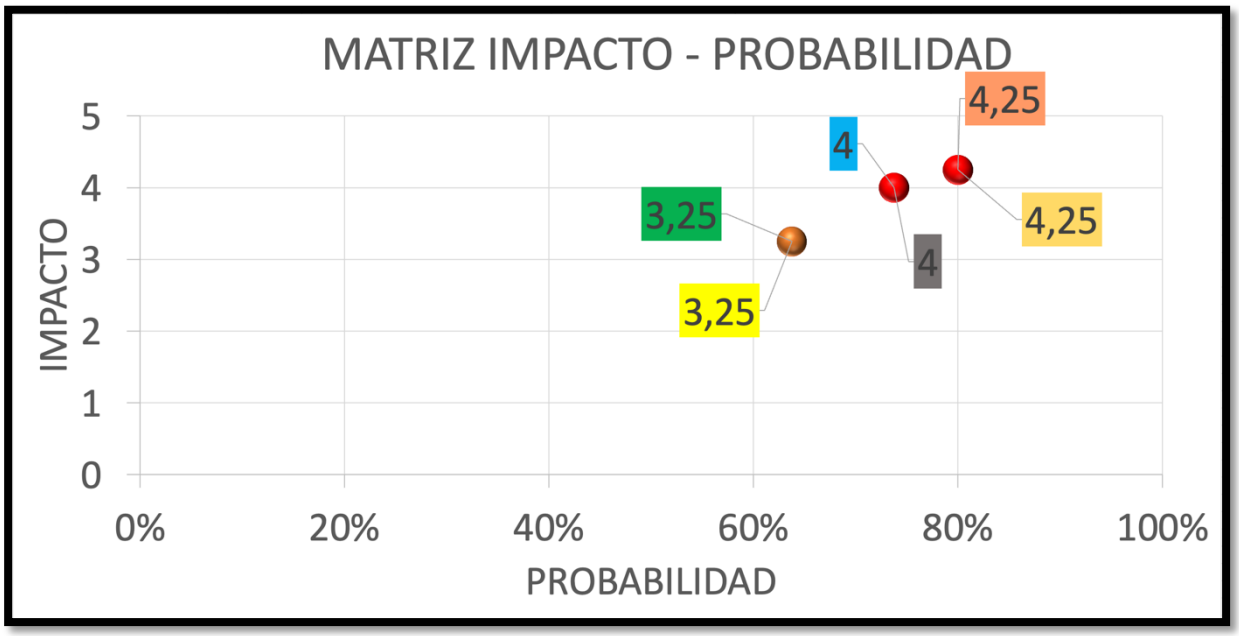
Matriz de riesgo con base en la metodología STRIDE

AMENAZAS		PROBABILIDAD DE OCURRENCIA	IMPACTO DEL RIESGO	INDICE DE CRITICIDAD(P X I)
SPOOFING	A1	80%	4,25	3,4
TAMPERING	A2	80%	4,25	3,4
REPUDIATION	A3	64%	3,25	2,071875
INFORMATIO DISCLOSURE	A4	74%	4	2,95
DENIAL OF SERVICE	A5	74%	4	2,95
ELEVATION PRIVILEGE	A6	64%	3,25	2,071875

Resultados del análisis de riesgo del sistema de gestión de vulnerabilidades cibernéticas del buque OPV-93C, representados a través de un gráfico de burbuja (Figura 2).

Figura 2.

Analisis de riesgo del sistema de gestión de vulnerabilidades cibernéticas del buque OPV-93C



La metodología DREAD se utiliza para la "evaluación de riesgos en el contexto de la seguridad de la información" (Kirtley, 2023, p. 2), permitiendo clasificar el riesgo asociado a una vulnerabilidad específica a través de cinco factores claves (Tabla 7);

- Daño: Impacto que una amenaza puede causar.
- Reproducibilidad: Facilidad con la que un ataque puede repetirse.
- Explotabilidad: Probabilidad o facilidad para explotar la vulnerabilidad (Kurtz, 2025, p. 34).
- Usuarios afectados: Cantidad de usuarios finales impactados si la amenaza es explotada.
- Capacidad de descubrimiento: Probabilidad de que un atacante identifique la vulnerabilidad.

Para llevar a cabo el análisis de riesgo mediante la sinergia de las metodologías STRIDE y DREAD, se procede a validar los parámetros establecidos en la reunión de ciberseguridad a bordo de la unidad. Durante este proceso, se identificó que las amenazas A1 y A4 presentan una correlación entre su impacto y nivel de criticidad, mientras que la amenaza A5 redujo su nivel de criticidad de alto a medio. En contraste, la amenaza A6 aumentó su nivel de criticidad de medio a alto, lo que requiere su consideración dentro del diseño de controles de seguridad.

Tabla 7

Analisis de riesgo mediante la sinergia de las metodologías STRIDE y DREAD.

			D - Damage Potential (Potencial de Daño) ¿Cuánto daño puede causar el ataque? Si el ataque solo molesta un poco, la puntuación es baja. Si puede robar datos importantes o destruir sistemas, la puntuación es alta.	R - Reproducibility (Reproducibilidad) ¿Qué tan fácil es repetir el ataque? Si el ataque es difícil y solo funciona en casos raros, la puntuación es baja. Si cualquiera puede hacerlo fácilmente una y otra vez, la puntuación es alta.	E - Exploitability (Explotabilidad) ¿Qué tan fácil es explotar la vulnerabilidad? Si se necesitan herramientas avanzadas o conocimientos expertos, la puntuación es baja. Si un hacker novato puede hacerlo con un programa básico, la puntuación es alta.	A - Affected Users (Usuarios Afectados) ¿Cuántas personas se ven afectadas? Si solo afecta a un usuario o a pocos, la puntuación es baja. Si afecta a miles o millones de usuarios, la puntuación es alta.	D - Discoverability (Descubribilidad) ¿Qué tan fácil es encontrar la vulnerabilidad? Si solo un experto con acceso especial puede descubrirla, la puntuación es baja. Si es fácil de encontrar con herramientas comunes, la puntuación es alta.		
	AMENAZAS		DAÑO	REPRODUCIBILIDAD	EXPLOTABILIDAD	AFECTADOS (USUARIOS)	DESCUBRIMIENTO	CALIFICACIÓN FINAL	NIVEL
Suplantación de identidad Un atacante suplanta la señal del GPS del buque (GPS Spoofing), enviando coordenadas falsas y desviando la embarcación de su curso real.	SPOOFING	A1	8	5	8	8	5	7	ALTA
Manipulación de datos Ejemplo en un buque: Un atacante modifica los datos del sistema de navegación o radar del buque para alterar la información sobre obstáculos, rutas seguras o tráfico marítimo.	TAMPERING	A2	9	6	9	9	6	8	ALTA
Repudio o negación de acciones Un oficial de a bordo manipula registros de acceso a los sistemas electrónicos del barco y luego niega haber realizado cambios no autorizados en el sistema de control del buque.	REPUDIATION	A3	7	4	6	7	5	6	MEDIO
Disclosure (Divulgación de información) Un ciberdelincuente accede sin autorización a planes de navegación, datos de carga o comunicaciones de la tripulación, exponiendo información sensible a piratas o actores maliciosos.	INFORMATIO DISCLOSURE	A4	7	8	8	7	6	7	ALTA
(Denegación de servicio - DoS) Un ataque DoS sobre el sistema de comunicaciones satelitales del buque impide la transmisión de datos con la base en tierra, dejando a la tripulación sin contacto.	DENIAL OF SERVICE	A5	6	7	7	6	6	6	MEDIO
Elevación de privilegios Un atacante con acceso limitado a los sistemas del barco logra escalar privilegios y obtiene control total sobre el Sistema de Gestión del Buque (Vessel Management System - VMS), comprometiendo su operación.	ELEVATION PRIVILEGE	A6	7	6	7	7	6	7	ALTA

Diseño de controles de seguridad

El diseño de los controles de seguridad se basa en la metodología MITRE ATT&CK, a través del enfoque MITRE Cyber Resiliency Framework (CREF). Este marco establece objetivos y metas, y mapea las técnicas de ataque a los controles NIST SP 800-53 R4, proporcionando una estructura para fortalecer la resiliencia cibernética en los sistemas de información (MITRE, 2013, p. 2). Además, se aplica para anticiparse, prepararse, resistir, recuperarse y evolucionar frente a las amenazas cibernéticas presentadas, incluyendo los ataques persistentes avanzados (APT).

A continuación, se presentan las medidas y políticas de seguridad de la información aplicadas dentro de los controles de seguridad para cada amenaza, impacto y estrategia de mitigación, de acuerdo con la metodología STRIDE

Controles contra la amenaza de SPOOFING A1.

Tabla 8

Relacion y controles de la amenaza de SPOOFING, impacto y medidas de mitigacion mediante el sistema de gestión de vulnerabilidades cibernéticas en el buque OPV-93C

Relacion y controles de la amenaza de SPOOFING, impacto y medidas de mitigacion			
Cuarto de maquinas	**Puente de gobierno**	**Cuarto de radio**	**Centro de información de combate**
Autenticación multifactor (MFA) en sistemas SCADA: Evitar accesos no autorizados al sistema de control del buque.	Uso de GPS con autenticación y verificación GNSS (Multi-constelación): Comparar señales de distintos sistemas (GPS, GLONASS, Galileo).	Cifrado de comunicaciones: Implementar estándares como AES-256 en radios militares o en comunicaciones satelitales.	Fusión de datos de múltiples sensores: Comparar información de radar, sonar, LIDAR y cámaras ópticas.
Redundancia de sensores y validación cruzada: Comparar lecturas de múltiples	Integración de navegación inercial (INS): Mantener la	Canales de respaldo y redundancia: Implementar	Redundancia operativa: Mantener sistemas manuales y protocolos de

sensores para detectar datos falsificados.	trayectoria en caso de interferencia GPS.	comunicación secundaria segura en caso de interferencia.	verificación visual en caso de interferencia digital.
Monitoreo en tiempo real: Implementar IDS (Intrusion Detection Systems) específicos para sistemas SCADA.	Protección contra interferencias electromagnéticas: Blindaje y filtros de señal para evitar spoofing de radiofrecuencia.	Frecuencia saltable (Frequency Hopping Spread Spectrum - FHSS): Cambio continuo de frecuencias para evitar intercepciones.	Análisis de patrones y detección de anomalías en el tráfico de red: Identificar manipulación de datos.
Segregación de redes OT/IT: Aislar redes industriales de redes administrativas para evitar ataques remotos.	Monitoreo de señales AIS con análisis de anomalías: Detectar cambios inusuales en la ubicación del buque.	Autenticación de transmisiones: Usar firmas digitales para validar mensajes críticos.	Autenticación de sistemas de detección: Firmas digitales en transmisiones de datos críticos.

Controles contra la amenaza de TAMPERING A2.

Tabla 9.

Relacion y controles de la amenaza de TAMPERING, impacto y medidas de mitigacion mediante el sistema de gestión de vulnerabilidades cibernéticas en el buque OPV-93C

Relacion y controles de la amenaza de TAMPERING, impacto y medidas de mitigacion			
Cuarto de maquinas	**Puente de gobierno**	**Cuarto de radio**	**Centro de información de combate**
Firmas digitales en firmware.	Validación cruzada (GPS+INS).	Autenticación criptográfica en AIS/GMDSS.	Control de integridad de datos tácticos.
Firewalls OT y segmentación de red.	Whitelisting en software de navegación.	Análisis de tráfico RF para detectar anomalías.	Sistemas de detección de intrusos en C2.
Control de integridad en dispositivos SCADA.	Monitoreo continuo de datos del radar/ECDIS.	Firewalls en redes de comunicación marítima.	Redundancia de sensores de combate.

Controles contra la amenaza de REPUDIATION A3.

Tabla 10

Relacion y controles de la amenaza de REPUDIATION, impacto y medidas de mitigacion mediante el sistema de gestión de vulnerabilidades cibernéticas en el buque OPV-93C

Relacion y controles de la amenaza de REPUDIATION, impacto y medidas de mitigacion			
Cuarto de maquinas	**Puente de gobierno**	**Cuarto de radio**	**Centro de información de combate**
Logs inmutables en sistemas SCADA.	Registro de cambios en ECDIS con firmas digitales.	Registro digital de transmisiones.	Logs firmados digitalmente en C2.
Autenticación multifactorial (MFA).	Monitoreo en tiempo real de alteraciones de rutas.	Autenticación reforzada en sistemas de radio.	Uso de almacenamiento forense inmutable.
Uso de blockchain para trazabilidad.	Auditoría automática de accesos a sistemas de navegación.	Monitoreo de tráfico de comunicación para detectar anomalías.	Implementación de inteligencia artificial para detección de alteraciones.

Controles contra la amenaza de INFORMATION DISCLOSURE A4.

Tabla 11

Relacion y controles de la amenaza de INFORMATION DISCLOSURE, impacto y medidas de mitigacion mediante el sistema de gestión de vulnerabilidades cibernéticas en el buque OPV-93C

Relacion y controles de la amenaza de INFORMATION DISCLOSURE, impacto y medidas de mitigacion			
Cuarto de maquinas	**Puente de gobierno**	**Cuarto de radio**	**Centro de información de combate**
Cifrado de datos en SCADA.	Uso de VPN y cifrado en ECDIS.	Protección con cifrado en comunicaciones marítimas.	Implementación de redes seguras y segmentadas.

Control de acceso basado en roles (RBAC).	Autenticación multifactor en sistemas de navegación.	Monitoreo de tráfico de comunicaciones.	Uso de hardware seguro para el almacenamiento de datos.
Implementación de DLP (Data Loss Prevention).	Restricción de acceso a registros de navegación.	Uso de protocolos seguros en radio (TLS, AES).	Clasificación y control de acceso a información táctica.

Controles contra la amenaza de DENIAL OF SERVICE A5.

Tabla 12

Relacion y controles de la amenaza de DENIAL OF SERVICE, impacto y medidas de mitigacion mediante el sistema de gestión de vulnerabilidades cibernéticas en el buque OPV-93C

Relacion y controles de la amenaza de DENIAL OF SERVICE, impacto y medidas de mitigacion			
Cuarto de maquinas	**Puente de gobierno**	**Cuarto de radio**	**Centro de información de combate**
Firewalls y filtrado de tráfico en SCADA.	Balanceo de carga y redundancia en sistemas de navegación.	Uso de técnicas de salto de frecuencia en radio.	Implementación de sistemas anti-DDoS en redes C2.
Segmentación de redes operacionales.	Monitoreo y análisis de tráfico en sistemas de navegación.	Redundancia en sistemas de comunicación.	Pruebas de resiliencia y capacidad ante ataques DoS.
Uso de inteligencia artificial para detección temprana.	Respaldo de datos críticos en almacenamiento seguro.	Implementación de listas blancas en comunicaciones.	Aislamiento de sistemas críticos para evitar interrupciones.

Controles contra la amenaza de ELEVATION OF PRIVILEGE A6.

Tabla 13

Relacion y controles de la amenaza de ELEVATION OF PRIVILEGE, impacto y medidas de mitigacion mediante el sistema de gestión de vulnerabilidades cibernéticas en el buque OPV-93C

Relacion y controles de la amenaza de ELEVATION OF PRIVILEGE, impacto y medidas de mitigacion			
Cuarto de maquinas	**Puente de gobierno**	**Cuarto de radio**	**Centro de información de combate**
Principio de privilegio mínimo en SCADA.	Autenticación multifactorial en sistemas de gobierno.	Control estricto de usuarios en comunicaciones.	Segmentación de privilegios en sistemas de combate.
Monitoreo continuo de accesos y actividades.	Implementación de Zero Trust en navegación.	Uso de certificados digitales en radio.	Supervisión y auditoría de accesos en tiempo real.
Rotación de credenciales de alta seguridad.	Registro y análisis de eventos de seguridad.	Control de acceso basado en comportamiento.	Implementación de técnicas de detección de anomalías.

Roles y responsabilidades basado en el diseño e implementacion de controles de seguridad

A través de la matriz RACI, se identifican los roles y responsabilidades del personal de la unidad para la implementación de controles y mitigación de riesgos cibernéticos. Seguir esta metodología permite clarificar “la distribución de responsabilidades, reduciendo la ambigüedad y optimizando la eficiencia en la ejecución de tareas” (Martins, 2025, p. 2). En este contexto, se han definido e identificado los siguientes roles clave (tabla 14):

- CISO (Chief Information Security Officer): Jefe del Departamento de Ciberseguridad, encargado de aprobar estrategias y asumir la responsabilidad a nivel estratégico.
- Oficial de Ciberseguridad: Responsable directo de la implementación técnica y ejecución de las tareas de seguridad.
- Equipo de Ciberseguridad: Grupo de especialistas encargados del soporte técnico, análisis y mantenimiento de la infraestructura de seguridad.
- Suboficial auditor de Seguridad: Responsable de verificar el cumplimiento de normativas y mejores prácticas de ciberseguridad (consultado para validaciones).
- Comandante de la Unidad: Director de Tecnología de la unidad, informado sobre avances, resultados y estado de la seguridad cibernética.

Tabla 14

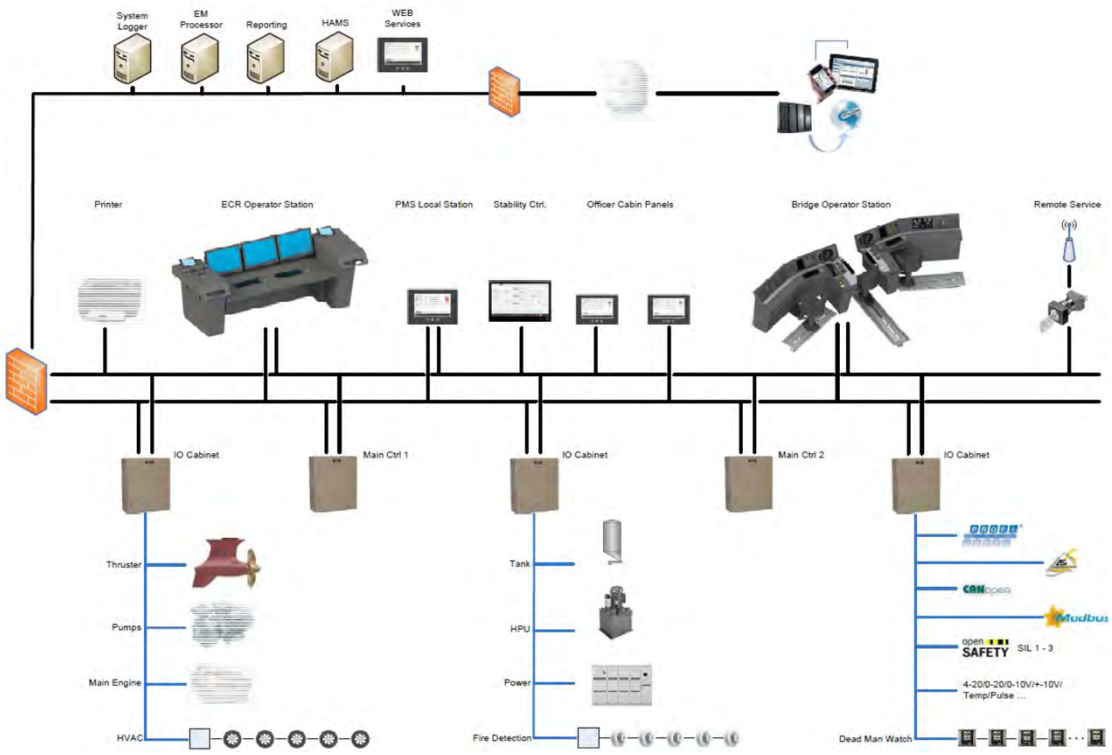
Matriz RACI Roles y responsabilidades basado en el diseño e implementacion de controles de ciberseguridad en el buque OPV-93C.

Actividad	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Diseño de controles de seguridad	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Navegación, Ingeniería y Comunicaciones	Toda la tripulación
Implementación de controles contra SPOOFING (aplicar tabla 8)	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Ingeniería	Toda la tripulación
Implementación de controles contra TAMPERING (aplicar tabla 9)	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Navegación	Toda la tripulación
Implementación de controles contra REPUDIATION (aplicar tabla 10)	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Comunicaciones	Toda la tripulación
Implementación de controles contra INFORMATION DISCLOSURE (aplicar tabla 11)	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Seguridad de la Información	Toda la tripulación
Implementación de controles contra DENIAL OF SERVICE (aplicar tabla 12)	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Comunicaciones y Seguridad	Toda la tripulación
Implementación de controles contra ELEVATION OF PRIVILEGE (aplicar tabla 13)	Equipo y Oficial de Ciberseguridad	Comando del Buque y validado por CISO	Oficiales de Seguridad y Comando del Buque	Toda la tripulación

En la figura 3 se presenta la arquitectura de red del sistema de gestión de vulnerabilidades cibernéticas del buque OPV-93C, incluyendo la segmentación de redes, monitoreo, redundancia y medidas de proteccion contra amenazas ciberneticas.

Figura 3.

Arquitectura y tipologia de red (tecnologia OT sistema SCADA) para el sistema de gestión de vulnerabilidades cibernéticas del buque OPV-93C



Conclusiones

La implementación de un Sistema de Gestión de Vulnerabilidades cibernéticas es esencial para salvaguardar la integridad operativa del buque OPV-93C. Este sistema no solo identifica y mitiga amenazas, sino que también establece un marco claro y cohesivo para la gestión de riesgos cibernéticos, mejorando la seguridad marítima y la eficacia en las misiones de defensa y ayuda humanitaria.

El uso del marco MITRE Cyber Resiliency Framework (CREF) en el diseño del sistema de gestión de vulnerabilidades permite anticiparse y prepararse para las amenazas cibernéticas, garantizando que el buque no solo responda a incidentes, sino que también se recupere y evolucione frente a ellos. Este enfoque proactivo fortalece la resiliencia cibernética del OPV-93C y minimiza el impacto de cualquier ataque potencial.

El Sistema de Gestión de Vulnerabilidades cibernéticas implantado en el buque OPV-93C fomenta una cultura de seguridad que se refleja en la capacitación continua del personal y en la actualización constante de protocolos de seguridad. Esta mentalidad proactiva no solo protege al buque de amenazas, sino que también asegura que el equipo esté preparado y bien informado, lo que resulta tener Operaciones Navales más seguras y eficientes.

La aplicación de la matriz RACI es crucial para definir y asignar roles y responsabilidades en el equipo de ciberseguridad a bordo del OPV-93C. Esto promueve una mejor colaboración, evita confusiones y asegura que cada aspecto de la gestión de vulnerabilidades se maneje de manera eficiente y responsable, maximizando la efectividad de las medidas de seguridad implementadas.

Bibliografía

ARC. (2017). *Armada Nacional.* Obtenido de https://www.armada.mil.co/es/content/entra-en-funcionamiento-tercera-opv-hecha-en-colombia.

ISO/IEC 27001. (2022). *Seguridad de la información, ciberseguridad y protección de la privacida Sistemas de gestión de la seguridad de la información Requisitos. Organización Internacional de Normalización.*

Kirtley, N. (2023). *DREAD Modelado de amenazas.* Obtenido de https://threat-modeling.com/dread-threat-modeling/

Kurtz, G. (2025). *Crowdstrike Global Threat Report.*

Martins, J. (2025). *Matriz Raci: qué es, cómo crearla con ejemplos y alternativas online.* osana.

MITRE. (2013). *Cyber Resiliency and NIST Special Publication 800-53. Rev 4 Controls.*

Praerit , G., & Kohnfelder , L. (2023). *Amenazas de Microsoft Threat Modeling Tool STRIDE.*

Schneier, B. (2000). *Secrets & Lies. Digital Security in a Networked world.* Madrid.

Tascon, O., Quintero, J., & Sejnaul, A. (211). Fuerzas Armadas. *La experiencia de Cotecmar en la implementation de mecanismos de transferencia tecnológica para el Proyecto Offshore Patrol Vessel - OPV*, 1.