MARCIM-WG
Juego de guerra de ciberdefensa marítima para la apropiación estratégica de respuestas ante crisis cibernéticas

Capitán de Corbeta Diego Edison Cabuya Padilla

Monografía para optar al título profesional:
Magíster en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Capitán de Corbeta Diego Edison Cabuya Padilla
Identificación	**:**	80932698
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Daniel Diaz López, PhD
Tutor temático	**:**	Carlos Alfonso Castañeda Marroquín, PhD
Fecha de entrega	**:**	12 de Junio de 2025
Extensión	**:**	14598 palabras (introducción a conclusiones)

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que esta monografía fue escrita de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Esta monografía es enteramente mi propio trabajo y no ha sido presentada para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia *Creative Commons*: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que esta monografía sea publicada por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

MARCIM-WG Juego de guerra de ciberdefensa marítima para la apropiación estratégica de respuestas ante crisis cibernéticas

MARCIM-WG Maritime Cyberdefense Wargame for the Strategic Appropriation of Responses to Cyber Crisis Scenarios

Diego Edison Cabuya Padilla[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: la presente monografía presenta MARCIM-WG, un juego de guerra de ciberdefensa marítima diseñado para facilitar la apropiación estratégica de procedimientos y protocolos de respuesta ante crisis cibernéticas. Basado en el modelo computacional SERDUX-MARCIM y siguiendo la metodología del NATO *Wargaming Handbook*, el juego simula escenarios realistas en infraestructuras marítimas críticas, permitiendo a actores estratégicos experimentar, analizar y mejorar su capacidad de toma de decisiones. A través de un entorno híbrido que combina tablero físico y simulación computacional, los participantes gestionan recursos limitados, enfrentan dinámicas de fricción y evalúan el impacto de sus acciones en tiempo real. El diseño promueve el desarrollo de competencias en los tres niveles de la Conciencia Situacional Cibernética (CSA): percepción, comprensión y proyección. Los resultados son analizados mediante evaluaciones, observaciones y salidas del modelo, generando insumos útiles para la formación, la evaluación estratégica y la mejora de capacidades institucionales en ciberdefensa marítima.

Palabras clave: Ciberdefensa; Ciberseguridad; Defensa; Juego de Guerra; Marítimo; Naval.

Abstract: This document presents MARCIM-WG, a maritime cyberdefense wargame designed to facilitate the strategic appropriation of procedures and protocols for responding to cyber crises. Based on the computational model SERDUX-MARCIM and structured according to the methodology of the NATO Wargaming Handbook, the game simulates realistic scenarios involving critical maritime infrastructures, enabling strategic-level actors to experiment, analyze, and enhance their decision-making capabilities. Through a hybrid environment combining a physical board and computational simulation, participants manage limited resources, face friction dynamics, and assess the consequences of their actions in real time. The design fosters the development of competencies across the three levels of Cyber Situational Awareness (CSA): perception, comprehension, and projection. Outcomes are assessed through surveys, observations, and model outputs, generating valuable insights for training, strategic evaluation, and institutional capacity building in maritime cyberdefense.

Keywords: Cyberdefense; Cybersecurity; Defense; Wargame; Maritime; Naval.

---

[1] Capitán de Corbeta de la Armada Nacional. Candidato a magíster en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Doctor en Ciencias del Mar, Ciberseguridad y Ciberdefensa Marítima, Escuela Naval de Cadetes "Almirante Padilla", Colombia. https://orcid.org/0000-0001-5338-9943 - Contacto: diego.cabuya@esdeg.edu.co.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Anexos

Introducción

La ciberdefensa, definida como el empleo de capacidades militares para enfrentar amenazas, ataques o actos hostiles de índole cibernética que impacten aspectos críticos como la sociedad, la soberanía o la seguridad nacional (Departamento Nacional de Planeación, 2017, p. 88), representa un campo de estudio que está avanzando hacia su madurez, con una producción científica relativamente baja (Shukla & Gochhait, 2020; Valencia-Arias et al., 2020). A pesar de esta limitada producción, la ciberdefensa es una prioridad reconocida nacional e internacionalmente. Desde 2011, países miembros de la OTAN como Estados Unidos, Alemania, Francia, Estonia y España han integrado la ciberdefensa dentro de sus estrategias nacionales de ciberseguridad, destacándose por sus avanzadas capacidades, cooperación internacional, y un fuerte enfoque en investigación, educación y conciencia situacional cibernética (Baezner & Cordey, 2019, pp. 7–11; Sabillon et al., 2016, pp. 68–78), así como la adopción de enfoques de modelado y simulación para incrementar la eficiencia operacional (North Atlantic Council, 2012, pp. 6–10).

Mientras que las naciones de la OTAN han consolidado estrategias de ciberdefensa avanzadas, América Latina ha logrado progresos en la gestión de la ciberseguridad, aunque enfrenta desafíos significativos en la estructuración de políticas y cooperación regional (Cornaglia & Vercelli, 2017, pp. 49–62; Izaguirre Olmedo, 2018, p. 178), junto con la necesidad de capacitar al personal no solo en habilidades técnicas, sino también en capacidades operativas, particularmente en maniobras desde una perspectiva militar(Junta Interamericana de Defensa, 2020, p. 20), y el uso de herramientas de modelado y simulación de entornos, escenarios, redes, efectos y comportamientos que permitan optimizar la toma de decisiones (Ganuza, 2020).

En Colombia, a partir de 2011 (Departamento Nacional de Planeación, 2011), se han promovido políticas de desarrollo enfocadas en la seguridad y defensa del ciberespacio, las cuales,

sin embargo, aún revelan carencias en la preparación legal y organizacional, pese a sus avances en medidas técnicas (Departamento Nacional de Planeación, 2020, pp. 10–27; International Telecommunication Union, 2024). En el ámbito de la ciberdefensa, el Departamento Nacional de Planeación (2020) señala que Colombia posee capacidades moderadas que necesitan mejoras significativas en tres áreas críticas: insuficiencias en la seguridad digital de ciudadanos, entidades públicas y privadas; la falta de adopción de modelos, estándares y marcos de trabajo actualizados en seguridad digital; y un desarrollo inadecuado del marco de gobernanza para la seguridad digital.

Por otra parte, el poder marítimo se configura como la combinación de intereses marítimos y capacidades navales orientadas a su protección (Till, 2007). En el caso colombiano, estos intereses abarcan la seguridad marítima, el comercio, la industria naval y la conservación del medio marino (Ramírez-Cabrales et al., 2021). Así, el poder marítimo trasciende la concepción tradicional basada exclusivamente en la fuerza naval, al incorporar nuevas dimensiones como la capacidad para responder a amenazas emergentes en el ciberespacio.

En esta línea, la ciberdefensa marítima se orienta a la protección de infraestructuras críticas del poder marítimo, salvaguardando los sistemas digitales que sostienen las operaciones marítimas y garantizando la continuidad de las actividades estratégicas en el entorno marítimo. Su relevancia resulta evidente al considerar que más del 80 % del comercio mundial depende del transporte marítimo (United Nations Conference on Trade and Development - UNCTAD, 2024), lo cual convierte a este sector en un objetivo prioritario para actores maliciosos. La creciente sofisticación y frecuencia de los ciberataques en los últimos años ha puesto en evidencia su vulnerabilidad (Alcaide & Llave, 2020; Symes et al., 2024), afectando no solo la integridad de la información y la operatividad de los sistemas, sino también la seguridad de las tripulaciones, las embarcaciones y sus cargas (Mraković & Vojinović, 2019, pp. 132–136).

Una de las aproximaciones más recientes en el ámbito de la ciberdefensa marítima es el proyecto de investigación MARCIM - "Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima a nivel estratégico" (D. E. Cabuya-Padilla & Castaneda-Marroquin, 2024, p. 178). Este proyecto aporta significativamente al estudio de la ciberdefensa marítima mediante el modelamiento y simulación, estableciendo un marco que facilita un entorno de simulación para que los investigadores comprendan su complejidad y sus procesos clave. Esto incluye el desarrollo y prueba de hipótesis de trabajo, visualización de emergencias y dinámicas estratégicas, y anticipación del comportamiento en escenarios de ataques y defensas cibernéticas.

Adicionalmente, MARCIM incluye el modelo matemático y computacional SERDUX-MARCIM (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025), que permite analizar y prever la propagación de ciberataques en infraestructuras marítimas, considerando características específicas de los ataques y las redes, así como las capacidades de los objetivos y atacantes. También propone una metodología de evaluación de riesgos cibernéticos que determina la probabilidad de ataques y asiste en la toma de decisiones. En esta investigación se destacan dos aspectos importantes. Primero, la Conciencia Situacional Cibernética – CSA como elemento crucial tanto en la ciberseguridad como en la ciberdefensa, afectando procesos y actividades a niveles estratégico, táctico y operativo; SERDUX-MARCIM se enfoca en el nivel estratégico del CSA, permitiendo que a este nivel se tomen decisiones basadas en escenarios de ciberataques sobre infraestructuras marítimas. Segundo, como validaciones futuras, se planteó desarrollar un juego de guerra de ciberdefensa marítima que permita a los experimentadores de nivel estratégico probar hipótesis y evaluar cursos de acción en escenarios realistas, así como promover la apropiación de procedimientos y protocolos de respuesta ante crisis cibernéticas (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025).

En respuesta a estos desafíos y contexto planteado, los juegos de guerra son una herramienta clave para la validación de estrategias en defensa (Weiner, 1959). Estas simulaciones permiten evaluar escenarios de conflicto, anticipar respuestas y mejorar la toma de decisiones en entornos de alta incertidumbre (Mayer et al., 2016). En el ámbito de la ciberdefensa, los juegos de guerra cibernéticos han cobrado relevancia en la evaluación de capacidades, entrenamiento y planeamiento estratégico (Bodeau et al., 2018). Existen diversas modalidades, como los ejercicios de mesa, donde los participantes responden a eventos simulados; los juegos de captura la bandera, que enfrentan equipos defensivos contra ofensivos en entornos simulados; y los ejercicios de equipo rojo-azul, que recrean ataques reales para mejorar la preparación operativa (Bodeau et al., 2018; Curry & Drage, 2018). Estas simulaciones no solo fortalecen la resiliencia cibernética de las organizaciones, sino que también permiten integrar herramientas tecnológicas avanzadas para modelar escenarios complejos; la combinación de métodos de simulación con sistemas de análisis computarizado facilita la gestión de la alta complejidad de la guerra cibernética.

Así las cosas, los juegos de guerra cibernéticos se consolidan como una herramienta clave para evaluar vulnerabilidades en infraestructuras críticas, mejorar la coordinación entre actores estratégicos y optimizar la toma de decisiones en situaciones de crisis. Su implementación permite simular ataques en entornos controlados, mejorar la respuesta ante incidentes y desarrollar estrategias adaptativas para proteger los sistemas críticos.

Formulación del problema

En este contexto, el problema identificado es la insuficiencia de herramientas especializadas para promover la apropiación a nivel estratégico de procedimientos y protocolos de respuesta ante crisis cibernéticas dentro del ámbito de la ciberdefensa marítima, y en resumen se sustenta por las siguientes razones:

- Se están implementando medidas de ciberdefensa a nivel internacional, enfocadas en mejorar la conciencia situacional cibernética como componentes cruciales de las estrategias de seguridad nacional.
- En América Latina, se evidencia una preparación insuficiente en la gestión de la ciberseguridad y ciberdefensa, lo que resalta la necesidad de su fortalecimiento.
- Los Estados deben adoptar un enfoque proactivo en la gestión de la ciberdefensa, utilizando herramientas y escenarios de simulación avanzados para optimizar la toma de decisiones.
- En Colombia, es fundamental fortalecer las capacidades de seguridad digital del sector público y mejorar las herramientas para la conciencia situacional cibernética.
- Se evidencia una escasez de iniciativas documentadas, a nivel académico u organizacional, sobre herramientas especializadas, como juegos de guerra, para fomentar la adopción estratégica de protocolos de respuesta a crisis cibernéticas en el ámbito de la ciberdefensa marítima.
- El proyecto MARCIM subraya la importancia de la Conciencia Situacional Cibernética (CSA). Adicionalmente, propone el desarrollo de un juego de guerra de ciberdefensa marítima que, utilizando el modelo matemático y computacional SERDUX-MARCIM, permite a los estrategas probar hipótesis y evaluar cursos de acción en entornos realistas.

Así las cosas, la pregunta de investigación planteada es la siguiente ¿Cuáles son las especificaciones de diseño de un juego de guerra de ciberdefensa marítima que facilite la apropiación a nivel estratégico de procedimientos y protocolos de respuesta ante crisis cibernéticas?

Objetivos

Para dar respuesta a la pregunta, se plantea como objetivo general diseñar un juego de guerra de ciberdefensa marítima que facilite la apropiación a nivel estratégico de procedimientos y protocolos de respuesta ante crisis cibernéticas. Complementariamente, se plantean los siguientes objetivos específicos:

- Formular las especificaciones de diseño de alto nivel (HLD) del juego de guerra de ciberdefensa marítima.
- Elaborar las especificaciones de diseño de bajo nivel (LLD) del juego de guerra de ciberdefensa marítima.
- Estructurar un escenario para el juego de guerra que represente una situación de crisis de ciberdefensa marítima.
- Validar conceptualmente el juego de guerra con el escenario diseñado de una situación de crisis de ciberdefensa marítima.

Como resultado de lo anterior, el presente documento se estructura en cuatro capítulos que responden a cada uno de los objetivos específicos planteados con el propósito de cumplir el objetivo general. Del desarrollo de este se concluye principalmente que el diseño e implementación del juego de guerra MARCIM-WG constituye una herramienta innovadora, robusta y replicable para fortalecer la Conciencia Situacional Cibernética (CSA) en el ámbito estratégico de la ciberdefensa marítima.

Estado del arte

El presente estado del arte se organiza en torno a cuatro ejes temáticos fundamentales: (i) ciberdefensa; (ii) ciberseguridad y ciberdefensa marítima; y (iii) juegos de guerra aplicados a la ciberseguridad y la ciberdefensa. Cada uno de estos ejes fue abordado mediante estudios bibliométricos actualizados y revisiones sistemáticas que permitieron identificar avances significativos, vacíos persistentes y contribuciones relevantes en relación con el objetivo general de esta investigación. La línea de ciberdefensa retoma y actualiza los hallazgos del estudio de Valencia-Arias et al. (2020); en el ámbito de la ciberseguridad y ciberdefensa marítima, se profundiza el análisis desarrollado por Cabuya et al. (2022), extendido hasta 2025; finalmente, la dimensión de juegos de guerra en ciberseguridad y ciberdefensa parte de la revisión realizada por García y Cabuya-Padilla (2022), también actualizada hasta el presente año. Los estudios bibliométricos y bibliográficos revelan la ausencia de investigaciones que aborden directamente la pregunta planteada, aunque identifican trabajos clave que contextualizan el problema y evidencian avances relevantes en las áreas analizadas.

Shiva et al. (2010), Damodaran y Wagner (2020) y Sarjakivi et al. (2024) coinciden en la utilidad de marcos como la teoría de juegos y la simulación estratégica para modelar decisiones en ciberdefensa, destacando la descentralización, inteligencia de amenazas y conciencia situacional como claves para enfrentar crisis en entornos complejos y dinámicos.

Jacq et al. (2019) destacan el reto creciente de proteger buques como sistemas complejos, proponiendo soluciones operativas como la fusión de datos, visualización y compartición de situaciones. Sin embargo, se señala que estos enfoques son más aplicables a niveles tácticos y operacionales, y presentan limitaciones al extrapolarlos a simulaciones estratégicas, especialmente cuando se requiere representar redes marítimas amplias. Desde una perspectiva estratégica, el

artículo resalta que el ciberespacio constituye una infraestructura crítica para el poder marítimo. La ciberdefensa marítima, por tanto, exige herramientas que combinen análisis estratégico, riesgo cibernético y dinámica de amenazas.

Bodeau et al. (2018) y Katsantonis (2019) proponen marcos para diseñar ejercicios adaptables a diversos entornos. El primero se enfoca en infraestructuras críticas, integrando aspectos técnicos y comerciales. El segundo enfatiza el aprendizaje continuo y la conciencia cibernética desde un enfoque educativo. Ambos destacan la utilidad de los juegos híbridos para representar contextos realistas y medir la eficacia de las respuestas cibernéticas.

Valente y Reith (2024) señalan que los juegos serios son una herramienta formativa eficaz, especialmente en entornos como el Departamento de Defensa de EE. UU. Para ello, se propone un enfoque que integre TI y TO, considerando las infraestructuras físicas como parte esencial de la formación en ciberseguridad.

Finalmente, Onduto (2021) concluye que la gamificación mejora el aprendizaje en ciberseguridad, aunque la mayoría de los juegos carecen de validación a largo plazo y contextualización del riesgo. Se observa una escasez de enfoques dirigidos al personal organizacional o al poder marítimo, evidenciando un vacío que MARCIM-WG busca cubrir.

Como hallazgos generales del estado del arte, se identifican lo siguientes:

- **Brecha temática:** a pesar del avance en simulaciones y juegos de guerra en ciberdefensa, no existen aplicaciones robustas enfocadas en el ámbito marítimo. El poder marítimo requiere adaptaciones específicas que consideren su complejidad.
- **Enfoque reactivo:** muchos modelos actuales privilegian la detección y mitigación, sin incorporar estrategias de anticipación, disuasión o recuperación, fundamentales para un enfoque integral de ciberdefensa en el poder marítimo.

- **Limitaciones de modelos existentes:** los modelos matemáticos tradicionales enfrentan restricciones al ser trasladados a entornos navales operacionales.
- **Deficiencia en CSA específica:** aunque se reconoce la importancia de la Conciencia Situacional Cibernética (CSA), hay pocos juegos o simulaciones que la desarrollen específicamente en el contexto del poder marítimo.
- **Necesidad de herramientas híbridas:** la combinación de modelado matemático, visualización interactiva, tableros físicos y simulación computacional representa una oportunidad innovadora para fortalecer la formación en ciberdefensa marítima.

En síntesis, MARCIM-WG responde a un vacío identificado en la literatura: la falta de herramientas estratégicas que integren ciberdefensa, poder marítimo y gamificación. La propuesta articula elementos pedagógicos, técnicos y estratégicos en un modelo híbrido que busca mejorar la preparación ante cibercrisis, fortalecer la CSA y optimizar la toma de decisiones en entornos complejos del dominio marítimo.

Complementariamente, frente al uso de dinámicas de juego y gamificación en contextos estratégicos, esta área ha demostrado ser una herramienta valiosa en distintos campos como la gestión del conocimiento, la formación de capital humano y la toma de decisiones públicas. Diversos estudios coinciden en que la gamificación potencia la motivación, promueve la apropiación del conocimiento y mejora la eficacia en entornos complejos.

Lira (2022) resalta que la implementación de estrategias gamificadas en organizaciones promueve la apropiación, transferencia y codificación del conocimiento, especialmente cuando se vinculan con emociones, recompensas y retos significativos. Estas estrategias no solo fortalecen las competencias blandas como la comunicación y la toma de decisiones, sino que facilitan la transferencia de conocimientos tácitos y explícitos dentro del entorno laboral.

En el ámbito de las políticas públicas, Harguindéguy et al. (2023) señalan que la gamificación ha sido subutilizada pese a su potencial. A través de experiencias como simulaciones tipo Diplomacy, metodologías Lego Serious Play o concursos gamificados, se evidencia que los juegos bien diseñados fortalecen la participación, la reflexión estratégica y el aprendizaje experiencial, esenciales para el análisis y diseño de políticas complejas. Complementariamente, Ovallos et al. (2016) destacan que la gamificación aplicada a la gestión de la innovación organizacional permite impulsar el compromiso y la participación de los miembros de una organización. Adicionalmente, evidencia cómo la gamificación puede convertirse en una estrategia facilitadora de cambio, adaptación y aprendizaje organizacional en entornos de alta complejidad.

Estas observaciones se alinean con lo propuesto por Rosen y Kerr (2024), quienes destacan que los juegos de aprendizaje aplicados a contextos estratégicos mejoran la comprensión y la toma de decisiones al proporcionar ambientes seguros donde el error genera aprendizaje. En el mismo sentido, Bodeau et al. (2018) y Katsantonis et al. (2019) enfatizan en que los juegos de guerra y los juegos serios fomentan la conciencia situacional y la preparación cibernética, al permitir una evaluación práctica de las capacidades institucionales ante amenazas reales.

Adicionalmente, el NATO Wargaming Handbook (2023) clasifica los juegos estratégicos en juegos analíticos y de aprendizaje. Los primeros generan datos para validar estrategias; los segundos desarrollan habilidades en escenarios simulados, contribuyendo así a mejorar la calidad de las decisiones y la coordinación interinstitucional en escenarios de crisis.

En síntesis, la literatura especializada respalda la gamificación como una estrategia efectiva a nivel estratégico para facilitar el aprendizaje activo, fortalecer el pensamiento sistémico, mejorar la gestión del conocimiento y preparar a los actores estratégicos para enfrentar desafíos complejos e inciertos, como los propios del ciberespacio y la defensa nacional.

Metodología

Esta investigación se fundamenta en el enfoque metodológico de Jaqueline Hurtado de Barrera (2010, p. 92), adoptando un nivel de complejidad comprensivo, que busca explicar las situaciones generadas por el evento estudiado. Para ello, se emplea el método de síntesis a través de revisión y análisis documental del tema de investigación, el cual permite analizar la interrelación de los elementos clave del objeto de estudio, relacionándolos con el conjunto y su función dentro del problema investigado (Méndez Álvarez, 2020, p. 128).

El estudio se enmarca en una investigación proyectiva, ya que busca proponer soluciones a una problemática específica mediante la indagación y el diseño de un modelo que oriente cómo deberían estructurarse ciertos procesos para lograr sus objetivos de manera efectiva (Hurtado de Barrera, 2010, pp. 114–116). En este caso, el resultado proyectado es un juego de guerra de ciberdefensa marítima, diseñado para fomentar la apropiación estratégica de procedimientos y protocolos de respuesta ante crisis cibernéticas, fortaleciendo así la capacidad de reacción en entornos marítimos digitalizados.

Procedimiento Metodológico

El procedimiento metodológico seguido en esta investigación se estructura en cuatro fases, alineadas con los objetivos específicos del estudio y fundamentadas en la guía metodológica para el diseño de juegos de guerra descrita en el "*Wargaming Handbook*" de la OTAN (Allied Command Transformation, 2023).

A continuación, se detalla cada una de las fases, resaltando sus componentes principales:

Fase 1 - Especificaciones de diseño de alto nivel (HLD) de MARCIM-WG

En esta fase se definen los requisitos estratégicos que delimitan el alcance y orientan conceptualmente el diseño del juego de guerra MARCIM-WG. Se establece el marco general del ejercicio, identificando los elementos clave que sustentan su configuración inicial y garantizan su alineación con los objetivos propuestos. Esta fase incluye los siguientes componentes:

- **Características generales:** presenta los elementos esenciales que configuran la naturaleza del juego MARCIM-WG, incluyendo temática, identificación del problema, tipo de juego de guerra, objetivos, elementos esenciales de diseño, restricciones, limitaciones, supuestos, método general de adjudicación, fuerzas y elementos involucrados en la ejecución y resultados esperados.
- **Equipo de juego de guerra:** definición de los roles clave y sus responsabilidades dentro de las fases de diseño, ejecución y análisis del ejercicio.

Fase 2 - Especificaciones de diseño de bajo nivel (LLD) del de MARCIM-WG

Esta fase se centra en la implementación operativa del juego de guerra, definiendo en detalle sus mecanismos, reglas, componentes físicos y lógica computacional. Su propósito es garantizar la viabilidad técnica y metodológica del juego, en concordancia con los lineamientos establecidos en la fase de diseño de alto nivel (HLD). Los aspectos principales incluyen:

- **Guía del Juego de Guerra:** descripción detallada de la dinámica del juego, que abarca los objetivos de los jugadores, reglas, estructura de ejecución, duración y organización de rondas, acciones permitidas, interacciones posibles y método de adjudicación.
- **Adaptación del modelo SERDUX-MARCIM:** ajuste del modelo computacional para su integración operativa con los elementos físicos y lógicos del juego, asegurando su funcionalidad en cada fase del evento.

Fase 3 - Estructuración de un escenario de crisis de ciberdefensa marítima

En esta fase se diseña el escenario central que da contexto y coherencia a la simulación estratégica del juego de guerra. Este escenario debe representar una situación crítica, plausible y operativamente relevante para el dominio de la ciberdefensa marítima, permitiendo evaluar decisiones bajo condiciones de incertidumbre, presión y escalamiento progresivo. Su propósito es facilitar la inmersión del participante en un entorno complejo, estimulando la toma de decisiones informadas y realistas frente a un incidente cibernético de alto impacto. Los elementos fundamentales que componen esta fase incluyen: contexto temporal, geografía, entorno, caracterización de elementos principales (objetivo, atacante y ciberataque), evento inicial (situación detonante), objetivo de los jugadores, elementos bajo control de los jugadores y configuración del modelo computacional MARCIM-WG.

Fase 4 - Validación conceptual de MARCIM-WG

La validación conceptual tiene como finalidad garantizar la coherencia metodológica, consistencia lógica y efectividad operativa del juego MARCIM-WG antes de su implementación formal. Para ello, se desarrollan pruebas y ajustes iterativos en un entorno controlado, permitiendo identificar mejoras en la dinámica del juego, la funcionalidad del modelo computacional y la claridad de la interfaz. Las actividades principales incluyen: definición de configuraciones del modelo computacional, ejecución y análisis de simulaciones, y pruebas de juego.

MARCIM-WG Juego de guerra de ciberdefensa marítima

1. Especificaciones de Diseño de Alto Nivel (HLD) de MARCIM-WG

Este capítulo establece los requisitos fundamentales, diseño inicial, que delimitan el alcance, la dirección y el éxito del juego de guerra.

1.1. Características generales

Esta sección describe los elementos clave del juego MARCIM-WG: su estructura conceptual, tipo, objetivos y fundamentos operativos. El diseño se alinea con el NATO *Wargaming Handbook* (2023) y las particularidades de la ciberdefensa marítima. El juego simula decisiones estratégicas ante crisis cibernéticas, fortaleciendo la conciencia situacional y permitiendo ensayar respuestas con capacidades institucionales, operativas y tecnológicas.

1.1.1. Temática

MARCIM-WG se desarrolla en el ámbito de la ciberdefensa marítima, entendida como la capacidad estratégica y operativa del Estado para proteger, prevenir y contrarrestar incidentes de naturaleza cibernética que afecten al poder marítimo nacional. Esta función es ejercida principalmente por la Armada de la República de Colombia (ARC), en el caso de Colombia, en articulación con otras instituciones del sector defensa, organismos estatales y actores del sector privado (D. Cabuya-Padilla & Castaneda-Marroquin, 2025).

1.1.2. Identificación del problema

En el contexto estratégico de la ciberdefensa marítima, se ha identificado una deficiencia crítica: la limitada apropiación, a nivel estratégico, de procedimientos y protocolos de respuesta ante crisis cibernéticas. Esta carencia se traduce en una baja capacidad institucional para anticipar, contener y gestionar incidentes cibernéticos que puedan afectar el poder marítimo nacional.

La complejidad de los entornos operacionales, la evolución constante de las amenazas cibernéticas, y la insuficiencia de herramientas especializadas para el entrenamiento estratégico en este dominio, refuerzan la necesidad de contar con soluciones metodológicas y tecnológicas que faciliten el aprendizaje, la toma de decisiones y la evaluación de respuestas en situaciones de crisis.

1.1.3. Tipo de juego de guerra

MARCIM-WG – Juego de Guerra de Ciberdefensa Marítima se enmarca en la categoría de **Juegos de Aprendizaje** (Rosen & Kerr, 2024) de acuerdo con la clasificación establecida por el NATO *Wargaming Handbook* (2023). Este tipo de juego está orientado a la formación y entrenamiento estratégico, brindando a los participantes la oportunidad de tomar decisiones en contextos desafiantes, evaluar sus implicaciones, y recibir retroalimentación.

En el caso de MARCIM-WG, el objetivo formativo se centra en el fortalecimiento de la Conciencia Situacional Cibernética (Endsley, 1995; Franke & Brynielsson, 2014), CSA por sus siglas en inglés, a nivel estratégico, en el contexto de crisis dentro del ámbito de la ciberdefensa marítima. El juego permite a los participantes aplicar conocimientos recientemente adquiridos, así como explorar conceptos y procedimientos que no dominan completamente.

1.1.4. Objetivos del juego de guerra

Objetivo general

Diseñar un entorno estructurado que facilite el análisis estratégico de la propagación de un ciberataque sobre una red crítica en el ámbito de la ciberdefensa marítima, permitiendo a los participantes evaluar procesos de toma de decisiones y estrategias de respuesta ante incidentes cibernéticos. Este entorno contribuye al desarrollo integral de los tres niveles de la Conciencia Situacional Cibernética (CSA), según lo propuesto por Endsley (1995) y extendido por Franke y Brynielsson (2014): percepción, comprensión y proyección.

Objetivos específicos

- **Percepción:** identificar elementos clave en el desarrollo de una crisis cibernética marítima, tales como hitos, anomalías y cambios significativos en el entorno.
- **Comprensión:** analizar e interpretar la información disponible durante la crisis para evaluar su relevancia, implicaciones y posibles amenazas o vulnerabilidades.
- **Proyección:** anticipar la evolución del incidente, valorar su impacto potencial y determinar estrategias proactivas de respuesta y mitigación.

1.1.5. Elementos esenciales de diseño

MARCIM-WG se fundamenta y adapta los cuatro elementos esenciales de un juego de guerra definidos por el NATO *Wargaming Handbook* (2023): decisiones, fricción, consecuencias y narrativa. Cada uno de estos elementos se implementa de manera articulada para garantizar una experiencia significativa de aprendizaje estratégico en ciberdefensa marítima, así:

Decisiones

Los jugadores tienen la capacidad de elegir cómo responder ante los desafíos introducidos por el juego. Se fomenta la toma de decisiones independiente, permitiendo a los participantes explorar múltiples cursos de acción y adoptar enfoques innovadores ante una crisis cibernética (Allied Command Transformation, 2023).

Fricción

Se introducen elementos de fricción mediante las mecánicas del juego, para condicionar las decisiones de los jugadores, generar nuevas perspectivas y revelar brechas en las estrategias (Allied Command Transformation, 2023). En MARCIM-WG, la fricción se manifiesta a través de:

- **Fuerza Oponente:** representa al atacante y al ciberataque, ambos con características y capacidades definidas e implementadas en el modelo de simulación. Estos elementos actúan como adversarios activos durante el desarrollo del juego.
- **Inyecciones guiadas:** situaciones o eventos predefinidos introducidos por el equipo de control mediante cartas especiales o fichas de capacidad. Estas inyecciones modifican el estado del juego e impulsan decisiones reactivas de los jugadores.
- **Competencia por recursos escasos:** los jugadores deben priorizar la asignación de capacidades cibernéticas en contextos de recursos limitados. Esto simula la necesidad de tomar decisiones bajo presión, optimizando las inversiones.
- **Información incompleta o conflictiva:** el juego obliga a los jugadores a tomar decisiones con información parcial, en coherencia con el principio de la "niebla de la guerra" (Von Clausewitz & Naville, 1977), lo que añade realismo e incertidumbre a la toma de decisiones estratégicas.
- **Introducción de nuevos conceptos o capacidades:** se incorporan elementos novedosos en el juego, mediante cartas especiales, que presentan procedimientos, capacidades o amenazas no conocidas previamente por los jugadores. Esto permite evaluar su respuesta ante la aparición de nuevas variables estratégicas.
- **Consecuencias:** cada decisión tomada por los jugadores tiene un efecto observable en el desarrollo del juego. Este principio se implementa a través del proceso de adjudicación, el cual traduce las decisiones en resultados cuantitativos mediante la simulación computacional. Este mecanismo asegura la retroalimentación inmediata, clara y lógica, fortaleciendo la comprensión sobre los impactos de sus acciones.

Narrativa

MARCIM-WG, a través del diseño del escenario, se estructura en torno a una narrativa creíble y contextualizada en el ámbito de la ciberdefensa marítima. Esta narrativa guía la secuencia de eventos y dota de coherencia al desarrollo del juego. Busca involucrar a los participantes a través de una representación realista de una crisis cibernética, proporcionando un entorno inmersivo y funcional para la toma de decisiones estratégicas (Allied Command Transformation, 2023).

1.1.6. Restricciones, limitaciones y supuestos

Restricciones

- **Capacidad computacional mínima:** el modelo emplea tasas dinámicas y enfoques múltiples, exigiendo un entorno de simulación con recursos técnicos adecuados.
- **Escalabilidad limitada:** al representar redes marítimas extensas o complejas, pueden surgir restricciones en la cantidad de nodos y conexiones modelables.
- **Estructura de red fija:** la red objetivo se define al inicio y no admite modificaciones estructurales durante la simulación.
- **Simplificación del entorno:** para garantizar viabilidad computacional, se abstraen ciertos elementos del ecosistema marítimo, reduciendo su fidelidad representacional.

Limitaciones

- **Disponibilidad de datos:** la parametrización del modelo puede verse afectada por la falta de información precisa sobre el objetivo, el atacante y el ciberataque.
- **Brecha de experticia:** los participantes estratégicos podrían no contar con conocimientos técnicos suficientes para comprender a fondo ciertas dinámicas del modelo.

- **Restricción temporal:** el tiempo limitado del ejercicio reduce la exploración de escenarios y decisiones alternativas.
- **Falta de detalle táctico-operacional**: al centrarse en el nivel estratégico, el juego no incluye información detallada de niveles tácticos u operacionales, limitando un análisis multinivel.

Supuestos (asunciones)

- Se asume que los participantes cuentan con conocimientos básicos sobre ciberseguridad, gestión de crisis y propios del entorno marítimo, suficientes para desempeñar su rol estratégico dentro del juego.
- Se considera que las decisiones tomadas por los jugadores reflejan su razonamiento estratégico dentro del marco del escenario presentado, y no necesariamente sus conocimientos técnicos detallados.
- Se presume que el entorno simulado y la narrativa del juego son comprendidos y aceptados como plausibles por los participantes.
- Se espera que los resultados de la simulación reflejen razonablemente los efectos esperados de las decisiones, conforme a los parámetros del modelo.

1.1.7. Método general de adjudicación

El sistema de adjudicación de MARCIM-WG está basado en un enfoque analíticamente asistido, conforme a la clasificación del NATO *Wargaming Handbook* (2023). En este enfoque, las decisiones de los jugadores no se resuelven únicamente por juicio experto o consenso, sino que son ingresadas en un modelo computacional que simula sus efectos y genera salidas cuantitativas para ser interpretadas en el contexto del juego. Entre las características se destacan:

- La representación estructurada de decisiones tomadas por los jugadores, traducidas en valores configurables dentro del modelo.
- La simulación automática de resultados a partir de dichas configuraciones, en niveles de red y de nodo.
- La retroalimentación inmediata y visual mediante tableros físicos y gráficos generados por el simulador.
- La interpretación guiada de los resultados por parte del adjudicador, facilitando la comprensión del impacto de las decisiones y del comportamiento emergente.

Para MARCIM-WG las decisiones estratégicas de los jugadores se introducen en el modelo SERDUX-MARCIM (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025), el cual ha sido desarrollado para analizar, pronosticar y representar la evolución de un ciberataque sobre una infraestructura marítima. Caracterizado por (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025):

- **Adaptación de modelos epidemiológicos compartimentales:** modelos como SIR (Bjørnstad et al., 2020a), SEIR (Bjørnstad et al., 2020b) y sus variantes son empleados para representar la transición de los nodos a través de diferentes estados de compromiso frente al ciberataque.
- **Alineación con metodologías y estándares reconocidos:** el modelo está estructurado conforme a principios aceptados internacionalmente en evaluación de riesgos cibernéticos, como OWASP (OWASP Foundation, 2017), MITRE (Strom et al., 2018), ISACA (ISACA, 2016), NIST (National Institute of Standards and Technology - NIST, 2024), y los lineamientos de la OMI (Karim, 2022), lo que facilita su compatibilidad con marcos existentes y refuerza la validez de sus resultados.

- **Incorporación de tasas dinámicas dependientes del tiempo:** los parámetros de transición están modulados por factores como el tipo de ataque, la estructura de la red y las capacidades defensivas del objetivo y del atacante, lo cual permite capturar la evolución temporal realista del incidente.
- **Heterogeneidad estructural de la red simulada:** se contempla la variabilidad de los activos cibernéticos que componen las redes marítimas, permitiendo simular escenarios a nivel tanto micro (nodo) como macro (red completa).
- **Representación explícita de interacciones entre entidades:** al integrar los componentes objetivo–atacante–ciberataque, el modelo permite simular no solo la propagación del ataque, sino también las consecuencias de las decisiones estratégicas de defensa.
- **El modelo incorpora las características del ataque, de la red objetivo y de las capacidades defensivas del jugador:** permitiendo observar la evolución dinámica del sistema bajo condiciones realistas.
- **Incorpora una metodología de evaluación de riesgos cibernéticos:** que permite estimar la probabilidad de impacto y sustentar la toma de decisiones.

El modelo de adjudicación está implementado en un entorno híbrido de simulación que combina Matlab (MathWorks, 1994), Python(Python Software Foundation, 2023) y NetLogo (Wilensky, 2016), lo que facilita la ejecución computacional y la visualización de resultados, igualmente, garantiza que las consecuencias de cada acción tomada por los jugadores estén fundamentadas en un sistema lógico, consistente y basado en datos. Asimismo, permite observar los efectos de decisiones complejas en entornos de incertidumbre controlada.

1.1.8. Fuerzas y elementos involucrados en la ejecución

MARCIM-WG se apoya en la lógica del modelo SERDUX-MARCIM para definir los actores y elementos clave que intervienen en la simulación. Estos actores representan entidades funcionales dentro de un escenario de ciberdefensa marítima, clasificadas en tres categorías: actores marítimos, actores de defensa y seguridad, y actores de amenaza cibernética. A continuación, se explican las tres categorías adaptadas de SERDUX-MARCIM (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025).

Actor marítimo (Objetivo)

Representa una organización marítima vulnerable, considerada como el objetivo del ciberataque. Este actor posee una configuración de red propia, compuesta por activos interconectados que permiten su operación. La red, está compuesta por un conjunto de nodos, donde cada nodo corresponde a un activo cibernético individual (por ejemplo, servidores, sensores, sistemas de navegación, embarcaciones o estaciones de control).

Cada nodo puede encontrarse en uno de los seis estados definidos en el modelo SERDUX-MARCIM: *Susceptible* - Susceptible (S), Expuesto (E), Resistente (R), Degradado (D), No disponible (U) y Destruido (X). La definición de estos seis estados se presenta en la Tabla 1.

Tabla 1. Estados del modelo.

Estado	Nombre	Descripción
S	Susceptible	Nodo vulnerable ante una amenaza específica por carecer de las contramedidas necesarias.
E	Expuesto	Nodo que ha tenido contacto con nodos comprometidos y puede estar en riesgo de ser atacado.
R	Resistente	Nodo protegido mediante controles de seguridad que impiden la acción de la amenaza.
D	Degradado	Nodo parcialmente afectado por un ciberataque con reducción funcional.
U	No Disponible	Nodo completamente inoperativo, ya sea por el ataque o por decisión estratégica del administrador.
X	Destruido	Nodo irrecuperable, dañado por un ciberataque severo.

Fuente: elaboración propia basado en Cabuya-Padilla et. al (2025).

Actor de defensa y seguridad

Corresponde a la segunda línea de defensa ante el ciberataque. Este actor puede reforzar las capacidades operacionales del objetivo mediante acciones como análisis del entorno, identificación de amenazas, aplicación de inteligencia cibernética o implementación de medidas defensivas. Su rol es transversal, ya que contribuye al fortalecimiento de las decisiones del actor marítimo y a la recuperación del sistema afectado.

Actor de amenaza cibernética (Atacante)

El actor de amenaza cibernética representa a la entidad que lanza el ciberataque dentro del marco del modelo. Esta entidad puede corresponder a un individuo, grupo organizado o actor estatal que actúa con intencionalidad ofensiva para afectar la disponibilidad, integridad o confiabilidad de los activos pertenecientes al objetivo.

En el modelo, el atacante se configura a partir de dos parámetros esenciales:

- **Factor del atacante (FA):** representa el nivel de agresividad, sofisticación técnica y capacidad ofensiva del atacante. Este factor influye directamente en la eficiencia del ciberataque y su capacidad para evadir los mecanismos de defensa del objetivo.
- **Factor de vulnerabilidad (FV):** expresa el grado de exposición del objetivo ante el atacante. Este valor considera aspectos como la antigüedad de los sistemas, la presencia de brechas de seguridad, y el estado general de preparación.

Desde la lógica del juego MARCIM-WG, este actor se comporta como un generador de fricción dentro del sistema, ya que sus acciones obligan al jugador a tomar decisiones estratégicas para mitigar o contrarrestar los efectos adversos. Sus capacidades ofensivas se modelan dentro del simulador, sin intervención directa del jugador, lo que permite establecer condiciones de amenaza persistente y estructurada con base en configuraciones predefinidas.

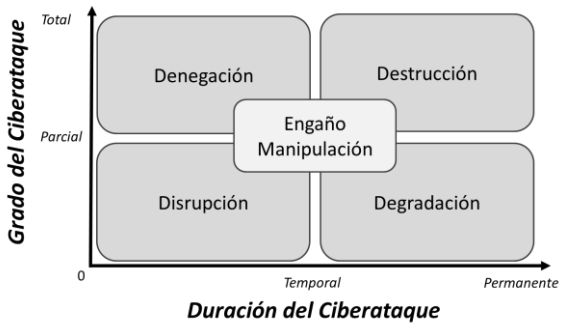
Ciberataque

Esta es la herramienta o ciberarma que puede utilizar el actor de amenaza cibernética (Atacante) para generar efectos sobre el actor marítimo (Objetivo) y tiene los siguientes dos parámetros:

- **Grado de ciberataque (Ψ)**: representa la severidad o profundidad técnica del ataque.
- **Duración del ciberataque (δ)**: indica el tiempo en el que el ataque permanece activo o tiene efecto sobre la red objetivo.

Los efectos del ciberataque se categorizan de la siguiente manera (Figura 1) (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025):

Figura 1. Efectos de un ciberataque



Fuente: (Cabuya Padilla, 2024; D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025)

- **Interrumpir (Demorar):** se genera una pérdida temporal de funcionalidad, retrasando el cumplimiento de los objetivos del sistema.
- **Degradar:** el activo continúa operando, pero con eficiencia reducida o bajo condiciones limitadas.
- **Denegar:** impide completamente el acceso o el uso de un activo durante un tiempo.
- **Destruir:** el activo queda completamente inservible y no puede ser restaurado sin una reconstrucción total.
- **Engañar:** se manipula la percepción del objetivo, distorsionando la información para inducir decisiones erróneas.

1.1.9. Resultados esperados

El desarrollo del juego de guerra MARCIM-WG está orientado a generar en los participantes una mejora sustancial en la apropiación estratégica de procedimientos y protocolos de respuesta ante crisis cibernéticas en el entorno marítimo. Esta apropiación se manifiesta a través del desarrollo de los tres objetivos específicos planteados, que buscan fortalecer las competencias en los tres niveles de la Conciencia Situacional Cibernética (CSA): percepción, comprensión y proyección.

Como parte del proceso de evaluación, se aplicarán dos instrumentos de evaluación, Previa y Posterior. Estos instrumentos cumplirán dos propósitos principales:

- Evaluar el desarrollo de competencias en los tres niveles de CSA (percepción, comprensión y proyección), en correspondencia con los objetivos del juego.
- Caracterizar a los participantes y recoger retroalimentación cualitativa sobre el diseño, la dinámica del juego, el escenario propuesto y la utilidad percibida del ejercicio.

Los resultados de del instrumento de evaluación, junto con las salidas del modelo de simulación y las observaciones del director del juego, conformarán el **Informe del Juego de Guerra**. Este informe contendrá los hallazgos clave del ejercicio y será entregado al patrocinador y demás partes interesadas. La elaboración de este reporte forma parte integral del ciclo de aprendizaje propuesto, y podrá alimentar futuros eventos o iniciativas que se apoyen en los conocimientos adquiridos durante el desarrollo del juego.

Para finalizar la Tabla 2 resume las características generales de MARCIM-WG.

Tabla 2. Características generales de MARCIM-WG.

Característica		Descripción
Temática	Ciberdefensa Marítima	Entendida como la capacidad estratégica y operativa del Estado para proteger, prevenir y contrarrestar incidentes de naturaleza cibernética que afecten al poder marítimo nacional.
	Planteamiento	Entorno simulado de toma de decisiones estratégicas en escenarios de crisis cibernética marítima,
Problema	Limitada apropiación estratégica de procedimientos y protocolos de respuesta ante crisis cibernéticas, lo que reduce la capacidad institucional para anticipar, contener y gestionar incidentes que comprometan el poder marítimo nacional.	
Tipo de Juego de Guerra	Juego de Aprendizaje	Diseñado para la formación y el entrenamiento estratégico, permite a los participantes tomar decisiones en contextos desafiantes, evaluar sus efectos y recibir retroalimentación significativa sobre sus acciones.
Objetivos del Juego de Guerra	General	Establecer un entorno estructurado que permita analizar la toma de decisiones y las estrategias de respuesta ante incidentes cibernéticos en el contexto de la ciberdefensa marítima.
	Específicos	Percepción: identificar hitos, anomalías y cambios clave en el desarrollo de la crisis. Comprensión: analizar e interpretar la información disponible para evaluar amenazas, implicaciones y vulnerabilidades. Proyección: anticipar la evolución del incidente, su impacto y formular estrategias proactivas de respuesta y mitigación.
Elementos Esenciales de Diseño	Decisiones	Los jugadores tienen la capacidad de elegir cómo responder ante los desafíos introducidos por el juego.
	Fricción	Se introducen elementos con el objetivo de condicionar las decisiones de los jugadores y generar nuevas perspectivas.
	Consecuencias	Cada decisión de los jugadores impacta directamente el desarrollo del juego. Este efecto se operacionaliza mediante el proceso de adjudicación, que traduce las decisiones en resultados cuantitativos a través del modelo SERDUX-MARCIM.
	Narrativa	El diseño del escenario incorpora una narrativa creíble y contextualizada en ciberdefensa marítima, en el marc o de una crisis cibernética.
Restricciones, Limitaciones y Supuestos	Restricciones	Capacidad computacional mínima
		Escalabilidad limitada
		Estructura de red fija
		Simplificación del entorno
	Limitaciones	Disponibilidad de datos
		Brecha de experticia
		Restricción temporal
		Falta de detalle táctico-operacional
	Supuestos	Se asume que los participantes cuentan con conocimientos básicos
		Se considera que las decisiones tomadas por los jugadores reflejan su razonamiento estratégico.
		Se presume que el entorno simulado y la narrativa del juego son comprendidos y aceptados como plausibles.
		Se espera que los resultados de la simulación reflejen razonablemente los efectos esperados de las decisiones.
Método de Adjudicación	Analíticamente asistido	Las decisiones de los jugadores no se resuelven únicamente por juicio experto o consenso, sino que son ingresadas en un modelo computacional, SERDUX-MARCIM, que simula sus efectos y genera salidas cuantitativas para ser interpretadas en el contexto del juego.
Fuerzas y elementos de ejecución	Objetivo	Representa una organización marítima vulnerable, considerada como el objetivo del ciberataque.
	Atacante	Individuo, grupo organizado o actor estatal que busca afectar la disponibilidad, integridad o confiabilidad de los activos del objetivo.
	Ciberataque	Es la herramienta o ciberarma que puede utilizar el Atacante para generar efectos sobre el Objetivo.
Resultados	Informe del Juego de Guerra	Contiene los hallazgos clave del ejercicio y será entregado al patrocinador y demás partes interesadas. La elaboración de este reporte forma parte integral del ciclo de aprendizaje propuesto.

Fuente: elaboración propia.

1.2. Equipo de juego de guerra

La ejecución del juego de guerra MARCIM-WG requiere la participación de un equipo multidisciplinar conformado por diversos roles, organizados en función de las cuatro fases del proceso metodológico: diseño, desarrollo, ejecución, y análisis y reporte. Estos roles, adaptados a la escala y objetivos del ejercicio, aseguran la planificación coherente, la implementación rigurosa y la evaluación efectiva del juego.

En el caso de MARCIM-WG, se han definido tres equipos principales siguiendo la metodología del NATO *Wargaming Handbook* (2023): el equipo de diseño y desarrollo, el equipo de ejecución, y el equipo de análisis y reporte.

1.2.1. Equipo de diseño y desarrollo

Este equipo diseña, estructura y prepara todos los componentes necesarios para implementar MARCIM-WG, integrando narrativa estratégica con elementos técnicos y operativos. Está conformado por los siguientes roles:

- **Patrocinador:** institución impulsora del ejercicio (e.g., Comando Cibernético Naval, Escuela Superior de Guerra), define los objetivos de aprendizaje, valida el diseño y asigna recursos.
- **Director del juego:** supervisa el proyecto, lidera la planificación e integra metodologías. Articula la visión del patrocinador con el escenario y la lógica del modelo computacional.
- **Diseñador del juego:** define reglas, dinámicas, capacidades y elementos lúdicos. Integra los componentes cibernéticos, fichas, fricciones y cartas especiales, en coordinación con el director, el analista y el desarrollador.

- **Desarrollador del juego:** operativiza el diseño, produciendo materiales físicos (tablero, fichas, cartas) y preparando la infraestructura para el modelo computacional.
- **Diseñador del escenario:** elabora el contexto narrativo y técnico (actores, geografía, amenazas, cronología). Asegura coherencia y realismo en situaciones simuladas de crisis cibernética marítima.
- **Gestor del evento:** coordina logística y soporte operativo: espacios, conectividad, seguridad de la información y respaldo técnico. Su rol es clave antes y durante el ejercicio.

1.2.2. Equipo de ejecución

Este equipo opera el juego durante su desarrollo práctico, asegurando el cumplimiento de las fases, la integración adecuada de decisiones en el sistema y el logro de los objetivos formativos. Está conformado por los siguientes roles:

- **Director del juego:** mantiene su función de supervisión durante la ejecución del juego, asegurando que la ejecución, garantiza la coherencia metodológica y actúa como enlace entre equipo técnico y participantes.
- **Gestor del evento:** continúa su labor durante la ejecución, asegurando condiciones logísticas, conectividad, soporte técnico y protección de la información durante toda la jornada.
- **Jugadores:** representan al "Objetivo" y toman decisiones estratégicas ante la crisis simulada. Se espera que sean actores de nivel estratégico del entorno marítimo (e.g., oficiales navales, funcionarios gubernamentales, directivos de infraestructura crítica), con conocimientos básicos en ciberseguridad y habilidades analítica.

- **Adjudicador:** traduce las decisiones de los jugadores en parámetros para el sistema de adjudicación, interpreta los resultados de la simulación y actualiza el tablero físico con base en los efectos observados.
- **Facilitador:** modera la dinámica del juego, vela por el cumplimiento de reglas y tiempos, estimula la discusión estratégica y resuelve dudas operativas.
- **Equipos no jugadores:** representados funcionalmente por el adjudicador, comprenden el atacante y el ciberataque. Aunque no son controlados directamente, su configuración inicial y evolución son gestionadas por el equipo de control y afectan el desarrollo del juego.

1.2.3. Equipo de análisis y reporte

En la fase final del juego, este equipo se encarga de sistematizar los resultados del juego, generar conclusiones estratégicas y retroalimentar al patrocinador mediante un informe técnico claro, objetivo y alineado con los objetivos del ejercicio. Sus roles clave son:

- **Patrocinador:** revisa el informe final, participa en la sesión de retroalimentación y valida los hallazgos frente a sus expectativas. Puede solicitar información adicional y orientar acciones futuras.
- **Director del juego:** supervisa la elaboración del reporte, asegura la coherencia entre resultados, decisiones y observaciones, y actúa como puente entre el analista y el patrocinador.
- **Analista:** recoge, procesa e interpreta la información del ejercicio. Evalúa el desarrollo de la Conciencia Situacional Cibernética (CSA), analiza el comportamiento de los jugadores y los efectos del modelo computacional, y gestiona evaluaciones y datos para consolidar el informe técnico.

Para finalizar la Tabla 3 resume las características generales de MARCIM-WG.

Tabla 3. Equipo de juego de guerra

Equipo		Descripción
Diseño y Desarrollo	Patrocinador	Representa la entidad impulsora del ejercicio, quien define el propósito del juego y los objetivos de aprendizaje esperados.
	Director del juego	Responsable de la supervisión integral del proyecto.
	Diseñador del juego	Define reglas, dinámicas, capacidades y elementos lúdicos. Integra los componentes cibernéticos, fichas, fricciones y cartas especiales, en coordinación con el director, el analista y el desarrollador.
	Desarrollador del juego	Operativiza el diseño, produciendo materiales físicos (tablero, fichas, cartas) y preparando la infraestructura para el modelo computacional.
	Diseñador del escenario	Construye el contexto narrativo y técnico del juego, definiendo actores, geografía, cronología, amenazas y condiciones iniciales.
	Gestor del evento	Coordina logística y soporte operativo: espacios, conectividad, seguridad de la información y respaldo técnico. Su rol es clave antes y durante el ejercicio.
Ejecución	Director del juego	Supervisa la ejecución, garantiza la coherencia metodológica y actúa como enlace entre equipo técnico y participantes.
	Gestor del evento	Asegura condiciones logísticas, conectividad, soporte técnico y protección de la información durante toda la jornada.
	Jugadores	Son los actores principales del juego, responsables de tomar decisiones estratégicas ante el escenario propuesto, asumiendo el rol del Objetivo.
	Adjudicador	Traduce las decisiones de los jugadores en parámetros para el sistema de adjudicación, interpreta los resultados de la simulación y actualiza el tablero físico con base en los efectos observados.
	Facilitador	Modera la dinámica del juego, vela por el cumplimiento de reglas y tiempos, estimula la discusión estratégica y resuelve dudas operativas.
	Equipos no jugadores	Este rol es asumido funcionalmente por el adjudicador y está representado por el atacante y el ciberataque.
Análisis y Reporte	Patrocinador	Revisa el informe final, participa en la sesión de retroalimentación y valida los hallazgos frente a sus expectativas. Puede solicitar información adicional y orientar acciones futuras.
	Director del juego	Supervisa la elaboración del reporte, asegura la coherencia entre resultados, decisiones y observaciones, y actúa como puente entre el analista y el patrocinador.
	Analista	Responsable de la recolección, procesamiento e interpretación de la información generada durante el juego.

Fuente: elaboración propia.

2. Especificaciones de Diseño de Bajo Nivel (LLD) de MARCIM-WG

Este capítulo tiene como finalidad operacionalizar los lineamientos conceptuales y estratégicos definidos en el Capítulo 1, traduciéndolos en elementos tácticos y funcionales que garanticen la viabilidad técnica y la jugabilidad efectiva del sistema. Se abordan aquí la formulación detallada de reglas, dinámicas, componentes físicos y la integración operativa del modelo computacional SERDUX-MARCIM, junto con la adaptación de una metodología híbrida tipo TTX propuesta por Cabuya-Padilla et al. (2025), en concordancia con los requerimientos metodológicos del juego de guerra MARCIM-WG.

2.1. Guía del Juego de Guerra

La Guía del Juego de Guerra MARCIM-WG, incluida en el Anexo 1, constituye el producto central de esta fase. En este anexo se consolidan los resultados del prototipado de componentes y se especifican las reglas, mecánicas y condiciones de ejecución del juego. La Tabla 4 presenta un resumen de los principales elementos incluidos en dicha guía, cuya descripción detallada puede consultarse en el anexo correspondiente.

Figura 2. Logo símbolo MARCIM-WG

Fuente: elaboración propia asistida por IA.

Tabla 4. Elemento de la Guía del Juego de Guerra MARCIM-WG

Sección	Contenido Resumido	Subtemas Asociados
I. Reglas	Reglas éticas y operativas.	Chatham House Rule Reglas generales del juego
II. Características Generales	Definición de los elementos esenciales que enmarcan el juego de guerra.	Temática Planteamiento Tipo de juego Elementos esenciales Método de adjudicación Fuerzas y elementos de ejecución
III. Objetivos del Juego	Objetivo general del ejercicio y metas específicas del participante basadas en CSA.	Objetivo general Objetivos específicos Objetivo del jugador
IV. Roles del Juego	Descripción de los roles clave.	Patrocinador Director del juego Gestor del evento Jugadores Jugador líder Adjudicador Facilitador Equipos no jugadores Analista
V. Tipos de Actores en la narrativa	Identificación de la tipología de actores enmarcada en el juego de guerra.	Objetivo: o Marítimo o Defensa y seguridad o Coordinación y cooperación Atacante: o Amenazas cibernéticas
VI. Elementos del Juego	Descripción y función de los componentes con los que interactúan los jugadores, facilitador y adjudicador.	Tablero de juego Fichas de capacidad Fichas indicadoras de nivel BitMarCoins (BMC) Cartas especiales Dados Sistema de adjudicación
VII. Escenario	Intensión del escenario y fases.	
VIII. Desarrollo y Ejecución	Descripción y caracterización de las tres fases que componen el juego de guerra.	Fase A: preparación Fase B: ejecución (rondas 0 a 5) Fase C: cierre y evaluación
IX. Información exclusiva del Facilitador/Adjudicador	Información detallada de los elementos de uso exclusivo del facilitador y adjudicador, que incorporan principalmente los elementos de fricción.	Procedimientos e información de las cartas especiales Información del ciberataque y pago *ransomware* Planilla de registro
X. Glosario	Definiciones clave sobre ciberseguridad, amenazas, armas, eventos e incidentes.	

Fuente: elaboración propia.

2.2. Adaptación del modelo SERDUX-MARCIM para MARCIM-WG

2.2.1. Cambios y adaptaciones al modelo SERDUX-MARCIM

El sistema de adjudicación del juego de guerra se implementa mediante el software MARCIM-WG, un programa computacional desarrollado en el entorno de simulación NetLogo (Wilensky, 2016; Wilensky & Rand, 2015) con módulos integrados en Python (Python Software Foundation, 2023). Este software constituye una adaptación operativa y funcional del modelo matemático-computacional SERDUX-MARCIM (D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025)

El modelo SERDUX-MARCIM fue desarrollado en el marco del proyecto de investigación "MARCIM: Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima a nivel estratégico" (D. E. Cabuya-Padilla & Castaneda-Marroquin, 2024) y se encuentra registrado ante la Dirección Nacional de Derechos de Autor del Ministerio del Interior de Colombia bajo el número 13-103-139, con fecha 15 de abril de 2025.

El modelo computacional MARCIM-WG, como adaptación del SERDUX-MARCIM, incorpora las siguientes modificaciones generales:

- **Reducción dimensional del modelo:** Se simplificaron las variables del modelo matemático SERDUX-MARCIM, seleccionando los niveles superiores (0 a 3) e integrando el nivel 4 dentro del nivel 3, con el fin de optimizar la jugabilidad del sistema.
- **Rediseño de la interfaz gráfica:** se ajustó la visualización del entorno para adecuarlo al contexto de MARCIM-WG, eliminando funciones específicas del análisis de ecuaciones diferenciales y mejorando la experiencia visual del usuario.
- **Localización lingüística:** toda la interfaz gráfica fue traducida al idioma español.

- **Integración del escenario narrativo:** se incorporaron directamente en el simulador las variables y condiciones propias del escenario diseñado, permitiendo su carga mediante controles interactivos.
- **Acciones especiales:** se añadieron controles para activar las cartas especiales del juego, asegurando su integración coherente dentro de la simulación.

Con estas adaptaciones, el software MARCIM-WG fue presentado y registrado como obra inédita derivada ante la Dirección Nacional de Derechos de Autor del Ministerio del Interior de Colombia, bajo el número 13-103-397, con fecha 12 de mayo de 2025 (ver Anexo 3).

La guía de uso del software MARCIM-WG junto con el código fuente se encuentra disponible para consulta abierta en el repositorio del proyecto en https://github.com/diegocabuya/SERDUX-MARCIM/tree/main/MARCIM-WG.

Complementariamente, el Anexo 4 contiene una explicación resumida del entorno visual y del código fuente adaptado.

Figura 3. Vista general diseño visual del modelo computacional MARCIM-WG

Fuente: elaboración propia.

2.3. Competencias y resultados de aprendizaje

En el marco del juego de guerra MARCIM-WG, se han formulado tres competencias específicas orientadas al fortalecimiento de la Conciencia Situacional Cibernética (CSA) en el nivel estratégico. Estas competencias permiten evaluar el desempeño de los participantes en escenarios de crisis cibernética, simulando entornos complejos de decisión en el ámbito marítimo. Cada competencia está alineada con las tres fases del modelo de CSA: percepción, comprensión y proyección (Endsley, 1995; Paul & Whitley, 2013), y responde a las exigencias estratégicas de la ciberdefensa marítima.

Además, estas competencias han sido diseñadas no solo como ejes formativos del juego, sino también como criterios de evaluación a ser validados mediante instrumentos específicos de medición antes y después de la experiencia lúdico-estratégica, con el fin de verificar el aprendizaje logrado por los participantes.

2.3.1. Competencia 1 - Percepción estratégica del entorno cibernético del poder marítimo

Capacidad para identificar, jerarquizar y comprender los elementos críticos del entorno digital del poder marítimo, incluyendo activos, amenazas, capacidades defensivas y condiciones sistémicas en tiempo real.

a) Dimensiones o variables observables

- Análisis situacional de activos críticos y vulnerabilidades del sistema.
- Reconocimiento de indicadores de amenaza y elementos disruptivos del entorno digital.
- Comprensión de los factores que determinan el nivel de riesgo cibernético.

Esta competencia se activa mediante la interpretación de información representada en el tablero y el modelo computacional, tales como nodos degradados, capacidades activas, tipo de ataque, nivel de riesgo cibernético y estado de servicios esenciales.

b) Resultados de aprendizaje

General:

Reconoce e interpreta los elementos críticos del entorno cibernético del poder marítimo, comprendiendo la estructura de activos, las amenazas relevantes y el nivel de riesgo asociado en un escenario simulado de crisis.

Específicos:

- **RA1.1** Identifica correctamente activos, nodos y capacidades críticas vulnerables del sistema marítimo simulado.
- **RA1.2** Reconoce con precisión las amenazas activas y sus implicaciones tácticas y estratégicas.
- **RA1.3** Identifica y valora el nivel de los riesgos cibernéticos en función de su impacto operacional, probabilidad y urgencia de atención.

2.3.2. Competencia 2 - Comprensión integrada de escenarios de cibercrisis en el poder marítimo

Capacidad para analizar la evolución de un ciberataque complejo en la red de un actor del poder marítimo, comprendiendo la lógica del atacante, las capacidades defensivas, las fases de una crisis cibernética y su relación con los principios de la gestión de incidentes.

a) Dimensiones o variables observables

- Secuencia lógica y dinámica evolutiva de un ciberataque en redes de actores marítimos.

- Gestión estratégica de capacidades defensivas, de seguridad y sostenimiento en contextos de crisis.
- Comprensión estructurada de las fases de una crisis cibernética y su vínculo con la toma de decisiones.
- Aplicación de marcos normativos de gestión de incidentes, especialmente la norma ISO/IEC 27035.
- Análisis integral de implicaciones operacionales, políticas y doctrinales de las decisiones tomadas.

Esta competencia se activa en contextos de toma de decisiones bajo presión, gestión de recursos limitados, enfrentamiento de fricción operativa y uso estratégico de cartas especiales en el juego.

b) Resultados de aprendizaje

General:

Analiza integralmente la dinámica de una cibercrisis en redes marítimas, evaluando eventos, capacidades defensivas y normativas aplicables, para sustentar decisiones estratégicas en entornos complejos.

Específicos:

- **RA2.1** Analiza la evolución del ciberataque, identificando relaciones causales y patrones tácticos.
- **RA2.2** Evalúa las capacidades cibernéticas de un actor del poder marítimo, diferenciando entre ciberseguridad, ciberdefensa y funciones de soporte.
- **RA2.3** Reconoce las fases de la crisis cibernética y propone acciones acordes a cada etapa.

- **RA2.4** Aplica los principios de la norma ISO/IEC 27035, vinculando las decisiones del juego con acciones concretas de gestión de incidentes.
- **RA2.5** Analiza las consecuencias estratégicas de sus decisiones durante el juego, considerando impactos técnicos, operacionales, políticos y doctrinales.

2.3.3. Competencia 3 - Proyección estratégica de escenarios futuros en entornos cibernéticos complejos

Capacidad para anticipar escenarios futuros del ciberataque, formular respuestas estratégicas adaptativas y evaluar las consecuencias de decisiones propias o adversarias, incluyendo consideraciones éticas, legales y estratégicas.

a) Dimensiones o variables observables

- Anticipación del comportamiento del atacante y posibles escenarios ofensivos.
- Evaluación del impacto de decisiones propias sobre la red, servicios y continuidad operativa.
- Análisis estratégico de decisiones críticas en contextos de alta complejidad cibernética.

Esta competencia se desarrolla en los momentos finales de cada ronda del juego, donde los participantes deben anticipar consecuencias, justificar decisiones y evaluar su impacto.

b) Resultados de aprendizaje

General:

Anticipa escenarios futuros de evolución del ciberataque, formulando respuestas estratégicas coherentes con principios éticos, legales y doctrinales, y evaluando sus efectos en la red y en la continuidad operativa.

Específicos:

- **RA3.1** Formula hipótesis estratégicas plausibles sobre la evolución del ciberataque y el comportamiento del adversario.
- **RA3.2** Evalúa el efecto de sus decisiones sobre la red marítima y plantea medidas preventivas o correctivas.
- **RA3.3** Reflexiona sobre las implicaciones operativas, éticas y doctrinales de estrategias como el pago de rescates, retaliaciones cibernéticas (ofensiva) o fallas estructurales del sistema.

2.3.4. Evaluación de competencias y resultados de aprendizaje

Con el propósito de evaluar los resultados de aprendizaje derivados de la participación en el juego de guerra MARCIM-WG, se diseñó un instrumento de evaluación formativa con función comparativa orientado a medir el desarrollo o mejora de las competencias formuladas. Esta herramienta se encuentra alineada con los objetivos del juego y permite establecer una comparación entre el nivel de entrada y el nivel alcanzado por los participantes, con base en los resultados de aprendizaje definidos. El contenido detallado del instrumento se presenta en el Anexo 5.

El objetivo del instrumento es evaluar el nivel de conocimientos estratégicos antes y después de la experiencia en el juego de guerra MARCIM-WG, en relación con los resultados de aprendizaje asociados al desarrollo de la Conciencia Situacional Cibernética (CSA). Esta evaluación permite identificar el grado de apropiación de conceptos clave mediante una medición comparativa pre y posjuego.

El instrumento consta de 25 preguntas distribuidas en torno a las tres competencias y a los resultados de aprendizaje definidos para el juego, tal como se presenta en la Tabla 5.

Tabla 5. Distribución del instrumento por competencias y resultados de aprendizaje

Competencia 1 - Percepción estratégica del entorno cibernético del poder marítimo	
RA 1.1	Preguntas: 1 - 2 - 3
RA 1.2	Preguntas: 4 - 5 - 6
RA 1.3	Preguntas: 7 - 8 - 9
Competencia 2 - Comprensión integrada de escenarios de cibercrisis en el poder marítimo	
RA 2.1	Preguntas: 10 -11
RA 2.2	Preguntas: 12 - 13
RA 2.3	Preguntas: 14 - 15
RA 2.4	Preguntas: 16 - 17
RA 2.5	Preguntas: 18 - 19
Competencia 3 - Proyección estratégica de escenarios futuros en entornos complejos	
RA 3.1	Preguntas: 20 – 21
RA 3.2	Preguntas: 22 -23
RA 3.3	Preguntas: 24 - 25

Fuente: elaboración propia.

Esta estrategia metodológica de evaluación permite no solo evidenciar el aprendizaje logrado por los participantes, sino también identificar patrones de mejora individual y colectiva en relación con las competencias estratégicas trabajadas. De esta manera, el instrumento contribuye a validar la eficacia del juego MARCIM-WG como herramienta pedagógica para el fortalecimiento de la Conciencia Situacional Cibernética en contextos de ciberdefensa marítima.

3. Escenario de crisis de ciberdefensa marítima

Este capítulo presenta la formulación del escenario estratégico del juego MARCIM-WG. Este escenario, completamente ficticio y diseñado con fines académicos, establece el contexto narrativo y técnico donde se desarrollará la simulación, permitiendo al jugador enfrentar una crisis cibernética en el entorno marítimo bajo condiciones de incertidumbre estratégica.

3.1. Estructura general

El escenario completo del juego de guerra MARCIM-WG se presenta en el Anexo 2 y constituye la base estructural para simular una crisis cibernética de alta complejidad en el marco del poder marítimo. De manera general, el escenario plantea una situación ficticia en la que la Marina de Guerra de **AMERIX** —país insular del Caribe con alta proyección regional— enfrenta una amenaza inminente sobre su red táctica de enlace (**LINKAMERIX**), como resultado de un ciberataque avanzado presuntamente planeado por el grupo **APT390 (PIGCYB)**, con apoyo del Estado-nación **ADVERSARIX**.

El escenario se desarrolla en seis apartados: (1) el **contexto temporal, geografía y entorno**, que describe la situación geoestratégica de AMERIX; (2) la **narrativa inicial**, que establece la escalada diplomática y las señales de alerta temprana; (3) la caracterización del **objetivo**, es decir, la red militar LINKAMERIX y su vulnerabilidad estructural; (4) el **perfil del atacante** (PIGCYB), su relación con ADVERSARIX y su historial ofensivo; (5) la descripción técnica del **ciberataque en preparación**, incluyendo vectores y herramientas como MALPIG; y (6) el **evento detonante y el objetivo de los participantes**, que sitúa a los jugadores como asesores estratégicos encargados de evitar la degradación crítica del sistema, manteniendo su nivel de servicio por encima del 70 %.

La evolución del escenario es dinámica y dependerá directamente de las decisiones que los jugadores adopten bajo condiciones de incertidumbre y presión estratégica. Cada acción tendrá consecuencias modeladas computacionalmente a través del sistema de adjudicación SERDUX-MARCIM, lo que permitirá observar, en tiempo real, la progresión del ciberataque, el impacto sobre la red LINKAMERIX y la capacidad de respuesta institucional.

3.2. Elementos bajo control de los participantes

Durante el desarrollo del juego, el facilitador entregará por rondas los elementos necesarios (Tabla 6) para que el jugador se integre de forma activa a la dinámica del juego de guerra explicada en el Capítulo 2.

Tabla 6. Elementos bajo control de los participantes.

Ronda	Fichas de Capacidad	BitMarCoins (criptodivisa)	Cartas Especiales
1	8*	2	8
2	8	0	0
3	8	0	0
4	8	0	0
5	8	0	0
TOTAL	**40**	**1**	**8**

Fuente: elaboración propia.

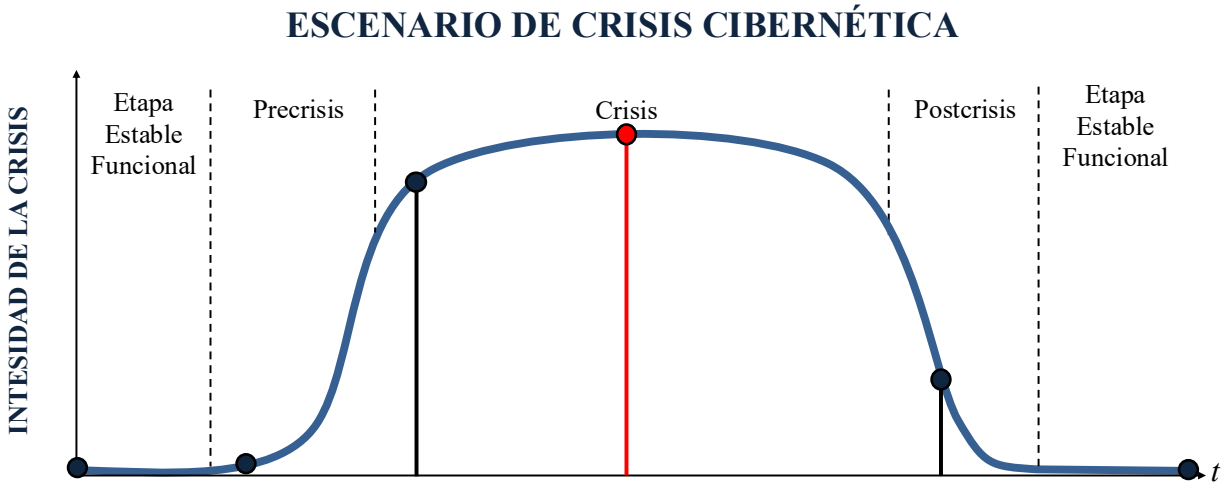
En la Ronda 1, el facilitador distribuirá las 8 fichas de capacidad de manera uniforme entre las 4 capacidades del objetivo, con el fin de familiarizar al jugador con la dinámica de toma de decisiones en la inversión de capacidades. Entre las Rondas 2 y 5, la distribución de fichas de capacidad, el uso de BitMarCoins y la activación de cartas especiales dependerán directamente de las decisiones estratégicas que adopten los jugadores durante el desarrollo del juego.

3.3. Configuración del modelo computacional MARCIM-WG

El escenario desarrollado es completamente ficticio y ha sido diseñado con fines académicos en el contexto de la ciberdefensa marítima. Su estructura permite al jugador alcanzar los objetivos del

juego a través de decisiones estratégicas, simulando la evolución de una crisis cibernética que afecta a un actor marítimo. Esta evolución recorre las fases de estabilidad funcional, precrisis, crisis, postcrisis y retorno a la estabilidad, como se ilustra en la Figura 4. Sin embargo, la trayectoria del escenario dependerá directamente de las decisiones adoptadas por el jugador, quien podría mantener al sistema en estado de crisis si sus acciones son ineficaces.

Figura 4. Dinámica del escenario de crisis.



Fuente: elaboración propia

Para reflejar esta dinámica, los valores asociados a las capacidades del atacante y del ciberataque se incrementan progresivamente en cada ronda, convirtiendo la amenaza inicial en un ciberataque con efectos destructivos, ejecutado por un actor sofisticado con capacidades superiores. La Tabla 7 presenta las características incorporadas en el modelo computacional que permiten representar esta escalada. Además, se incluyen parámetros clave del sistema de ecuaciones diferenciales que gobierna la evolución de los estados de los nodos, así como las condiciones iniciales de la red.

Este conjunto de parámetros —que abarca tasas de propagación, pérdida de resistencia, tiempo de ciberataque, entre otros— permite modelar con precisión la progresión del ciberataque,

el comportamiento de la red y la efectividad de las decisiones de los jugadores. También se define la duración en días simulados por ronda y el número de pasos que controlan la resolución temporal del modelo. En conjunto, estos valores configuran un entorno de simulación dinámico, adaptado al objetivo estratégico del juego y a la lógica de adjudicación computacional.

Tabla 7. Valores del escenario den el modelo computacional.

PARÁMETRO O VARIABLE DE SIMULACIÓN	**RONDA**				
	1	**2**	**3**	**4**	**5**
CONFIGURACIÓN INICIAL DE LA RED					
Número de conexiones por nodo	2				
Cantidad total de nodos	350				
susceptibles-inicial	300				
expuestos-inicial	40				
degradados-inicial	10				
no-disponibles-inicial	0				
SISTEMA DE ECUACIONES DIFERENCIALES					
tasa-propagacion-inicial-PRO0	0.25	0.5	0.75	1	1
tasa-no-disponibilidad-otras-causas-UOC	0.0025	0.0025	0.0025	0.0025	0.0025
parametro-tiempo-ciberataque-D-tf	240	240	240	240	240
stregth-damping-loss-resistance-LOR-a	0.01	0.01	0.01	0.01	0.01
time-damping-loss-resistance-LOR-m	120	48	12	120	120
pasos-sim	48	48	48	48	48
Días	2	2	2	2	2
ATACANTE					
factores-atacante-ATF	0.4	0.4	0.5	0.5	0.5
vulnerability-factors-VUF	0.4	0.4	0.5	0.5	0.5
CIBERATAQUE					
grado-ciberataque-ADE	0.1	0.4	0.5	0.7	0.7
duracion-ciberataque-ADU	0.1	0.4	0.5	0.7	0.7

Fuente: elaboración propia.

4. Validación conceptual del juego de guerra MARCIM-WG

Las pruebas de validación conceptual del juego MARCIM-WG se realizaron con base en el escenario estratégico de crisis presentado en el Capítulo 3. Se definieron tres configuraciones que representan trayectorias simuladas de respuesta del jugador: **pesimista, neutral y optimista**, diferenciadas por el uso de capacidades, cartas especiales y toma de decisiones ante el ciberataque.

En cada sesión participaron tres expertos que simularon un entorno estratégico de toma de decisiones bajo condiciones de incertidumbre (Figura 5), aplicando las reglas, componentes físicos y el sistema de adjudicación previamente definidos (Capítulo 1 y 2).

Figura 5. Sesión de validaciones del juego de guerra MARCIM-WG

Fuente: elaboración propia

Durante estas pruebas se evaluaron los siguientes aspectos clave:

- La fluidez y comprensión de la dinámica de juego en cada una de las fases (preparación, ejecución y cierre).
- La interacción adecuada entre los elementos físicos del juego (tablero, fichas, cartas especiales) y el modelo computacional.
- La coherencia entre las decisiones tomadas por los jugadores y los resultados generados por el sistema de adjudicación.
- La efectividad del flujo de adjudicación analíticamente asistida, basada en la lógica de simulación por estados de SERDUX-MARCIM.
- La respuesta del sistema ante configuraciones y decisiones distintas en cada ronda.

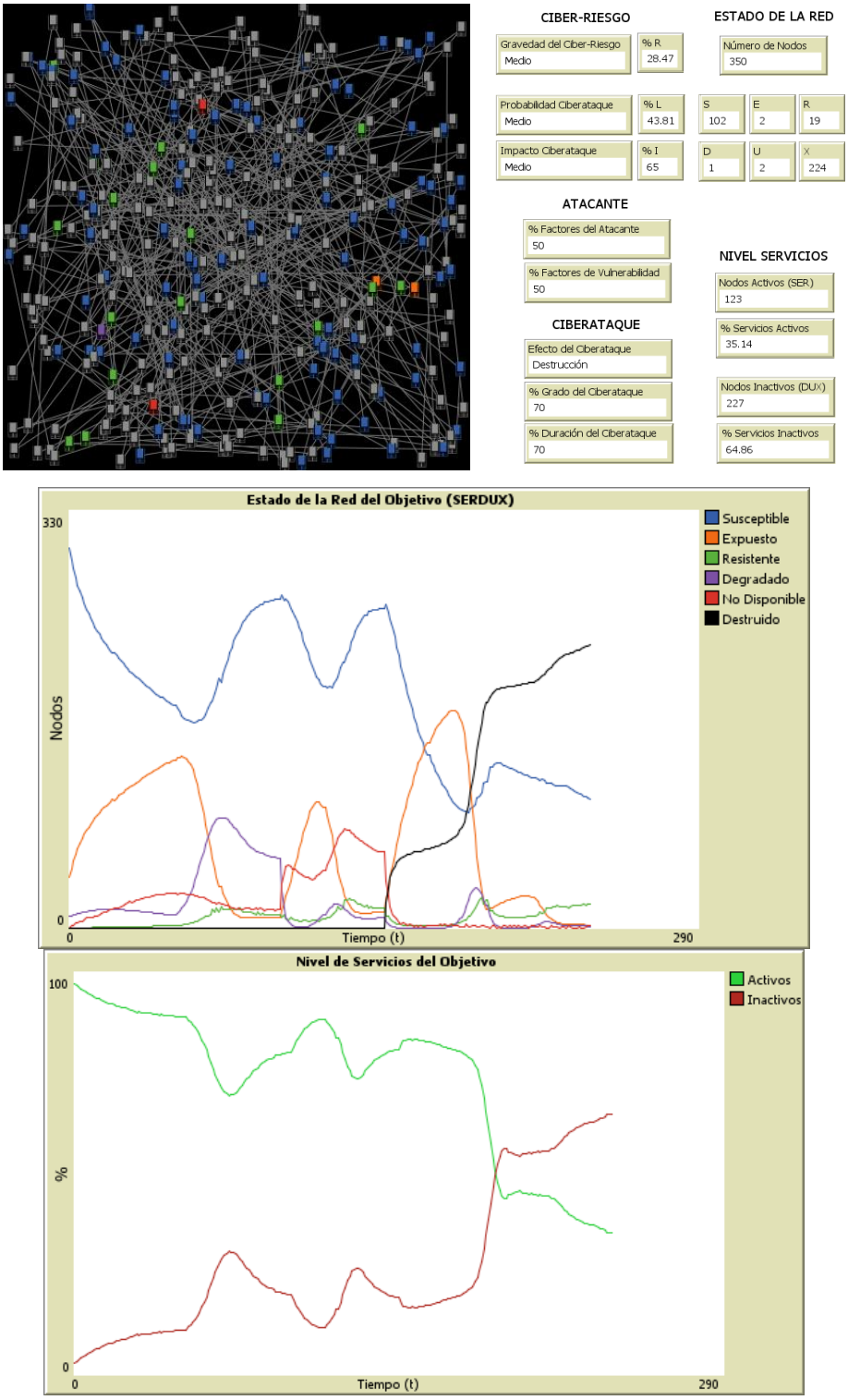
Cada escenario mantiene la misma narrativa general del escenario, pero varía en la forma de enfrentar la crisis. Para cada uno se presenta una tabla con la configuración inicial, decisiones adoptadas y resultados de simulación, así como tres figuras: evolución de estados de los nodos, nivel de servicios y estado final de la red. Estas validaciones permiten evaluar la coherencia del juego y su alineación con los objetivos formativos.

4.1. Escenario 1 – Configuración Pesimista

Este escenario representa una trayectoria en la que el jugador, aun contando con recursos y acciones estratégicas, toma decisiones incorrectas o ineficaces frente a la evolución de la crisis cibernética. Se caracteriza por una Conciencia Situacional Cibernética (CSA) deficiente en sus tres niveles (percepción, comprensión y proyección), reflejada en una gestión táctica y estratégica desarticulada.

A continuación, se presentan los resultados de la simulación (Figura 6, Tabla 8 y Tabla 9), junto con el análisis por ronda:

Figura 6. Resultados simulación en Netlogo – Escenario pesimista



Fuente: elaboración propia usando el software MARCIM-WG en Netlogo

Tabla 8. Información y resultados de la simulación – Escenario pesimista – Parte 1

PARÁMETRO O VARIABLE DE SIMULACIÓN	RONDA									
	1		2		3		4		5	
	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA
CONFIGURACIÓN INICIAL DE LA RED										
Número de conexiones por nodo	2	2		2		2		2		2
Cantidad total de nodos	350	350		350		350		350		350
nodos susceptibles	300	176		260		253		116		102
nodos expuestos	40	133		9		13		15		2
nodos resistentes	0	2		11		16		22		19
nodos degradados	10	11		55		8		18		1
nodos no disponibles	0	28		15		60		1		2
nodos destruidos	0	0		0		0		178		224
Servicios Activos	97.14%	88.86%		80.00%		80.57%		43.71%		35.14%
Servicios Inactivos	2.86%	11.14%		20.00%		19.43%		56.29%		64.86%
Gravedad del Ciber-Riesgo		3.52% Insignificante		14.27 Medio		21.65% Medio		29.74% Medio		28.47% Medio
Probabilidad Ciberataque		39.06% Bajo		37.56 Medio		46.06% Medio		45.06% Medio		43.81% Medio
Impacto Ciberataque		9% Bajo		38% Medio		47% Medio		66% Medio		65% Medio
ATACANTE										
factores-atacante-ATF	0.4		0.4		0.5		0.5		0.5	
vulnerability-factors-VUF	0.4		0.4		0.5		0.5		0.5	
CIBERATAQUE										
grado-ciberataque-ADE	0.1		0.4		0.5		0.7		0.7	
duración-ciberataque-ADU	0.1		0.4		0.5		0.7		0.7	
Efecto ciberataque	Disrupción		Disrupción		Denegación		Destrucción		Destrucción	
CAPACIDADES-OBJETIVO										
capacidades-ciberdefensa-obj-TCD	0.1		0.3		0.4		0.5		0.6	
capacidades-soporte-sostenibilidad-obj-TSS	0.1		0.2		0.4		0.5		0.6	
capacidades-ciberinteligencia-obj-TCI	0.1		0.3		0.5		0.6		0.8	
CONTROLES SEGURIDAD - OBJETIVO										
controles-compensatorios-obj-CCM	0.1		0.2		0.3		0.4		0.5	
controles-disuasorios-obj-CDE	0.1		0.2		0.3		0.4		0.5	
controles-detectivos-obj-CDV	0.1		0.2		0.3		0.4		0.5	
controles-preventivos-obj-CPR	0.1		0.2		0.3		0.4		0.5	
controles-correctivos-obj-CCR	0.1		0.2		0.3		0.4		0.6	
SISTEMA DE ECUACIONES DIFERENCIALES										
tasa-propagacion-inicial-PRO0	0.25		0.5		0.75		1		1	
tasa-no-disponibilidad-otras-causas-UOC	0.0025		0.0025		0.0025		0.0025		0.0025	
parámetro-tiempo-ciberataque-D-tf	240		240		240		240		240	
stregth-damping-loss-resistance-LOR-a	0.01		0.01		0.01		0.01		0.01	
time-damping-loss-resistance-LOR-m	120		48		12		120		120	
pasos-sim	48		48		48		48		48	
Días	2		2		2		2		2	

Fuente: elaboración propia

Tabla 9. Información y resultados de la simulación – Escenario pesimista – Parte 2

USO CARTAS ESPECIALES												
CARTA (ACCIÓN) ESPECIAL	1	2	3	4	5	6	7	8	9	10	11	12
	Planeación y preparación	Detección y Reporte (Interno)	Evaluación y Análisis del Incidente	Declaración de la Crisis	Cooperación	Plan de Recuperación de Desastres	Plan de Continuidad del Negocio	Ciberataque	Pago del Ransomware	Reporte del Incidente	Revisión	Mejora
Fase en la ISO 27035:2023	Planeación y Preparación	Detección y Reporte	Evaluar y Decidir		Responder						Lecciones Aprendidas	
Etapa Crisis	Etapa Estable	Precrisis		Crisis						Poscrisis		Etapa Estable
Ronda	1	2		3	4					5		
Selección			X	X							X	

DISTRIBUCIÓN DE FICHAS PARA ENTRAR A LA SIMULACIÓN DE LA RONDA												
	Entrada Simula. Ronda	1		2		3		4		5		Total
	Origen Fichas	Fichas Entregadas	Cartas Especiales	Fichas Entregadas	Cartas Especiales	Fichas Entregadas	Cartas Especiales	Fichas Entregadas	Cartas Especiales	Fichas Entregadas	Cartas Especiales	
Capacidades	TCD	1		1	1	1		1		1		6
	TSS	1		1		1	1	1		1		6
	TCI	1		1	1	1	1	1		1	1	8
Controles	CCM	1		1		1		1		1		5
	CDE	1		1		1		1		1		5
	CDV	1		1		1		1		1		5
	CPR	1		1		1		1		1		5
	CCR	1		1		1		1		1	1	6
Total		8	0	8	2	8	2	8	0	8	2	46
		8		10		10		8		10		

Fuente: elaboración propia

Ronda 1 – Etapa Estable Funcional

- **Decisiones del jugador:** no se activa la carta especial 1 (Planeación y Preparación), lo cual refleja un bajo nivel de percepción y proyección estratégica inicial. La falta de activación de esta carta indica omisión en la preparación institucional ante un entorno de amenaza latente.
- **Resultados de la simulación:** el sistema pasa del 91.71 % al 88.86% de servicios activos y presenta solo un nodo degradado. La red se conserva estable, aunque 39 nodos se encuentran entre los estados degradado y no disponible, lo cual evidencia que el entorno permanece expuesto y vulnerable. El impacto cibernético aún es bajo, pero se configura un escenario propenso a escalamiento sin intervención oportuna.

Ronda 2 – Precrisis

- **Decisiones del jugador:** se activa la carta 3 (Evaluación y Análisis del Incidente), pero no la carta 2 (Detección y Reporte Interno), lo que limita la capacidad de comprensión situacional y debilita la respuesta sistémica. No se observa una estrategia estructurada en el uso de fichas: no se priorizan capacidades clave para el momento de la crisis, ni se refuerzan mecanismos de alerta temprana.
- **Resultados de la simulación:** El ciberataque comienza a intensificarse. Aumentan los nodos en estado degradado y no disponibles (de 39 a 70), mientras los servicios activos caen al 80 %. Aunque el impacto aún se clasifica como "medio", la evolución del sistema sugiere un deterioro funcional progresivo, sin acciones que mitiguen esta tendencia.

Ronda 3 – Crisis

- **Decisiones del jugador:** se activa la carta 4 (Declaración de la Crisis), lo cual evidencia cierto reconocimiento de la situación, pero se omite la carta 5 (Cooperación), fundamental en esta etapa. La distribución de fichas continúa siendo débil en controles disuasivos y compensatorios, elementos críticos para enfrentar ataques en fase de denegación. La CSA proyectiva sigue siendo baja.
- **Resultados de la simulación:** el sistema mantiene su nivel de servicios, pero se reportan 60 nodos destruidos, en este sentido el comportamiento del sistema sugiere que no se ha logrado contener el ciberataque y podría desencadenar un colapso gradual del sistema.

Ronda 4 – Poscrisis

- **Decisiones del jugador:** no se activan cartas clave como la 6 (Plan de Recuperación de Desastres) ni la 7 (Plan de Continuidad del Negocio), que serían esenciales en esta etapa. La inversión de fichas es insuficiente y no se reorienta la estrategia. La comprensión de la evolución de la crisis es nula, y la capacidad de proyección está completamente deteriorada.
- **Resultados de la simulación:** el nivel de servicios cae abruptamente al 43.71 %, y se configura un punto de inflexión hacia una posible disfunción estructural de la red. El comportamiento del ciberataque, con efectos destructivos, supera la capacidad defensiva.

Ronda 5 – Etapa Estable Degradada

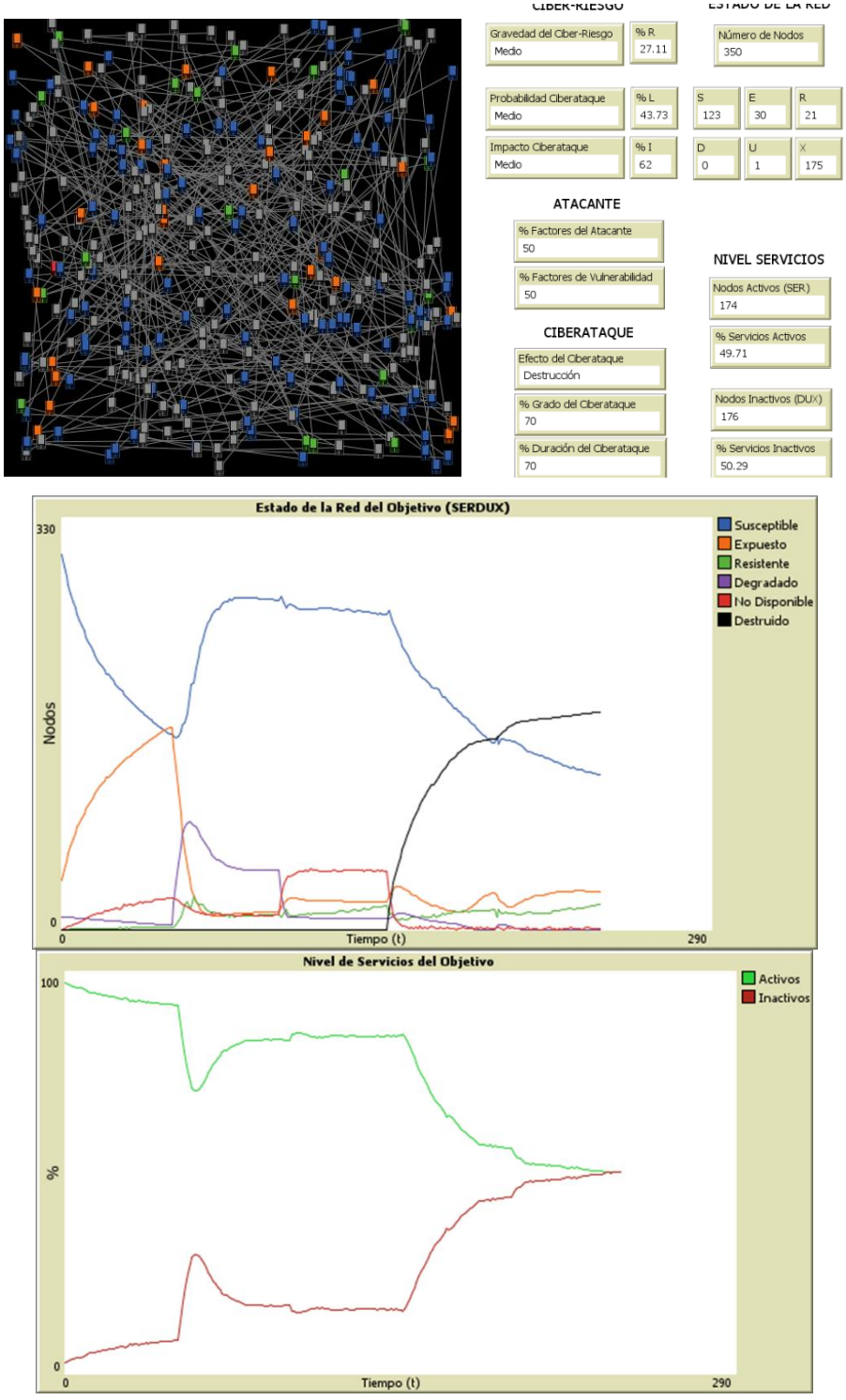
- **Decisiones del jugador:** Solo se activa la carta 11 (Revisión), cuyo efecto es limitado debido a la gravedad acumulada. La inversión de fichas se hace de forma uniforme y no orientada a una estrategia de defensa o recuperación concreta.
- **Resultados de la simulación:** el modelo refleja que el sistema se encuentra en colapso operativo, fracaso estratégico. Se alcanza un 64.86 % de nodos inactivos (DUX), y los nodos destruidos ascienden a 224. El nivel de servicios cae al 35.14 %, marcando un deterioro irreversible de la red. Las decisiones tardías o inefectivas, junto con la gestión errática, desarticulada y carente de CSA conduce al colapso total ante un ciberataque sostenido.

4.2. Escenario 2 – Configuración Neutral

Este escenario representa una postura institucional intermedia, caracterizada por una distribución equilibrada pero no estratégica de recursos. El jugador toma decisiones básicas, sin priorización clara de capacidades críticas ni una lectura adecuada de la evolución del riesgo. Las cartas especiales, aunque disponibles, se emplean en algunos casos de manera tardía, subóptima o con efectos limitados. Este enfoque busca simular una respuesta institucional rutinaria y no contextualizada ante una amenaza emergente, permitiendo establecer un punto de comparación base con los escenarios extremos.

A continuación, se presentan los resultados de la simulación (Figura 7, Tabla 10 y Tabla 11), junto con el análisis por ronda:

Figura 7. Resultados simulación en Netlogo – Escenario neutral



Fuente: elaboración propia usando el software MARCIM-WG en Netlogo.

Tabla 10. Información y resultados de la simulación – Escenario neutral – Parte 1

PARÁMETRO O VARIABLE DE SIMULACIÓN	RONDA									
	1		2		3		4		5	
	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA
CONFIGURACIÓN INICIAL DE LA RED										
Número de conexiones por nodo	2	2		2		2		2		2
Cantidad total de nodos	350	350		350		350		350		350
nodos susceptibles	300	157		264		253		150		123
nodos expuestos	40	162		14		22		30		30
nodos resistentes	0	2		12		19		16		21
nodos degradados	10	4		48		9		0		0
nodos no disponibles	0	25		12		47		1		1
nodos destruidos	0	0		0		0		153		175
Servicios Activos	97.14%	91.71%		82.86%		84.00%		56.00%		49.71%
Servicios Inactivos	2.86%	8.29%		17.14%		16.00%		44.00%		50.29%
Gravedad del Ciber-Riesgo		3.10% Bajo		13.71% Medio		20.66% Medio		28.52% Medio		27.11% Medio
Probabilidad Ciberataque		38.81% Medio		37.66% Medio		45.90% Medio		45.42% Medio		43.73% Medio
Impacto Ciberataque		8.00% Bajo		36.40% Medio		45.00% Medio		62.80% Medio		62.00% Medio
ATACANTE										
factores-atacante-ATF	0.4		0.4		0.5		0.5		0.5	
vulnerability-factors-VUF	0.4		0.4		0.5		0.5		0.5	
CIBERATAQUE										
grado-ciberataque-ADE	0.1		0.4		0.5		0.7		0.7	
duración-ciberataque-ADU	0.1		0.4		0.5		0.7		0.7	
Efecto ciberataque	Disrupción		Disrupción		Denegación		Destrucción		Destrucción	
CAPACIDADES-OBJETIVO										
capacidades-ciberdefensa-obj-TCD	0.1		0.2		0.4		0.4		0.6	
capacidades-soporte-sostenibilidad-obj-TSS	0.1		0.2		0.4		0.4		0.6	
capacidades-ciberinteligencia-obj-TCI	0.1		0.2		0.4		0.4		0.6	
CONTROLES SEGURIDAD - OBJETIVO										
controles-compensatorios-obj-CCM	0.2		0.4		0.4		0.6		0.7	
controles-disuasorios-obj-CDE	0.2		0.3		0.5		0.6		0.7	
controles-detectivos-obj-CDV	0.2		0.4		0.5		0.8		0.8	
controles-preventivos-obj-CPR	0.2		0.4		0.5		0.8		0.8	
controles-correctivos-obj-CCR	0.2		0.3		0.5		0.6		0.8	
SISTEMA DE ECUACIONES DIFERENCIALES										
tasa-propagacion-inicial-PRO0	0.25		0.5		0.75		1		1	
tasa-no-disponibilidad-otras-causas-UOC	0.0025		0.0025		0.0025		0.0025		0.0025	
parámetro-tiempo-ciberataque-D-tf	240		240		240		240		240	
stregth-damping-loss-resistance-LOR-a	0.01		0.01		0.01		0.01		0.01	
time-damping-loss-resistance-LOR-m	120		48		12		120		120	
pasos-sim	48		48		48		48		48	
Días	2		2		2		2		2	

Fuente: elaboración propia.

Tabla 11. Información y resultados de la simulación – Escenario neutral – Parte 2

USO CARTAS ESPECIALES												
CARTA (ACCIÓN) ESPECIAL	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
	Planeación y preparación	**Detección y Reporte (Interno)**	**Evaluación y Análisis del Incidente**	**Declaración de la Crisis**	**Cooperación**	**Plan de Recuperación de Desastres**	**Plan de Continuidad del Negocio**	**Ciberataque**	**Pago del Ransomware**	**Reporte del Incidente**	**Revisión**	**Mejora**
Fase en la ISO 27035:2023	**Planeación y Preparación**	**Detección y Reporte**	**Evaluar y Decidir**		**Responder**						**Lecciones Aprendidas**	
Etapa Crisis	**Etapa Estable**	**Precrisis**		**Crisis**						**Poscrisis**		**Etapa Estable**
Ronda	**1**	**2**		**3**		**4**				**5**		
Selección	**X**	**X**	**X**		**X**		**X**				**X**	

DISTRIBUCIÓN DE FICHAS PARA ENTRAR A LA SIMULACIÓN DE LA RONDA												
	Entrada Simula. Ronda	**1**		**2**		**3**		**4**		**5**		**Total**
	Origen Fichas	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	
Capacidades	**TCD**	1			1	1	1			2		6
	TSS	1			1	1	1			2		6
	TCI	1			1	1	1			1	1	6
Controles	**CCM**	1	1	2				1	1	1		7
	CDE	1	1	1		1	1	1		1		7
	CDV	1	1	2		1		3				8
	CPR	1	1	2		1		2	1			8
	CCR	1	1	1		2		1		1	1	8
Total		**8**	**5**	**8**	**3**	**8**	**4**	**8**	**2**	**8**	**2**	56
		13		**11**		**12**		**10**		**10**		

Fuente: elaboración propia.

Ronda 1 – Etapa Estable Funcional

- **Decisiones del jugador:** el jugador activa correctamente la carta especial 1 (Planeación y Preparación), demostrando un nivel adecuado de percepción situacional. Esta acción refleja una actitud proactiva frente a la amenaza latente.
- **Resultados de la simulación:** la red cae ligeramente a un 91.71 % de servicios activos, con 29 nodos entre degradados y no disponibles, evidenciando un entorno vulnerable. La situación de base se conserva funcional, pero frágil, con indicadores que anticipan posibles disrupciones.

Ronda 2 – Precrisis

- **Decisiones del jugador:** se activan correctamente las cartas especiales 2 (Detección y Reporte Interno) y 3 (Evaluación y Análisis del Incidente), lo que fortalece la comprensión del entorno cibernético y permite anticipar parcialmente la evolución del ciberataque. La distribución de fichas muestra cierta coherencia. La percepción mejora, pero la proyección aún es limitada.
- **Resultados de la simulación:** la red empieza a reflejar el avance del ataque. Se incrementa el número de nodos degradados y no disponibles (de 29 a 60) y la proporción de servicios inactivos se eleva a 17.14 %. Aunque el sistema mantiene 82.86 % de servicios activos, se vislumbra una trayectoria negativa si no se toman decisiones correctivas. La fase de disrupción se consolida.

Ronda 3 – Crisis

- **Decisiones del jugador:** se activa la carta especial 5 (Cooperación), pero no la 4 (Declaración de la Crisis), lo que genera un desfase estratégico frente a la etapa en

curso. Además, aunque se priorizan fichas hacia controles compensatorios (CCM) y correctivos (CCR), se descuida la inversión en recuperación o continuidad operativa. El jugador toma unas medidas reactivas apropiadas, pero no demuestra una comprensión total de la gravedad ni proyecta adecuadamente la evolución de la amenaza.

- **Resultados de la simulación:** el nivel de servicios se recupera un poco, llegando al 84 %. Aunque la red experimenta una transición hacia la etapa de denegación, las medidas reactivas han sido efectivas, pero no parece haberse consolidado una respuesta estratégica sólida. La combinación de decisiones tardías en las primeras rondas y uso parcial de las cartas evidencia una CSA intermedia, con capacidad de contención limitada.

Ronda 4 – Crisis

- **Decisiones del jugador:** se activa únicamente la carta 7 (Plan de Continuidad del Negocio), sin aplicar la carta 6 (Plan de Recuperación de Desastres), lo cual afecta directamente la capacidad del sistema para restablecer servicios críticos. La inversión en fichas es estable, pero se concentra en capacidades ya reforzadas, sin diversificación estratégica. La comprensión de la etapa en curso es parcial y la proyección, deficiente.
- **Resultados de la simulación:** la red entra en una fase crítica llegando a un nivel de servicios del 56 %. Aunque no se colapsa completamente, la recuperación se torna inviable sin una estrategia clara. El ciberataque mantiene su trayectoria destructiva, y la respuesta institucional resulta insuficiente para revertir la tendencia.

Ronda 5 – Poscrisis

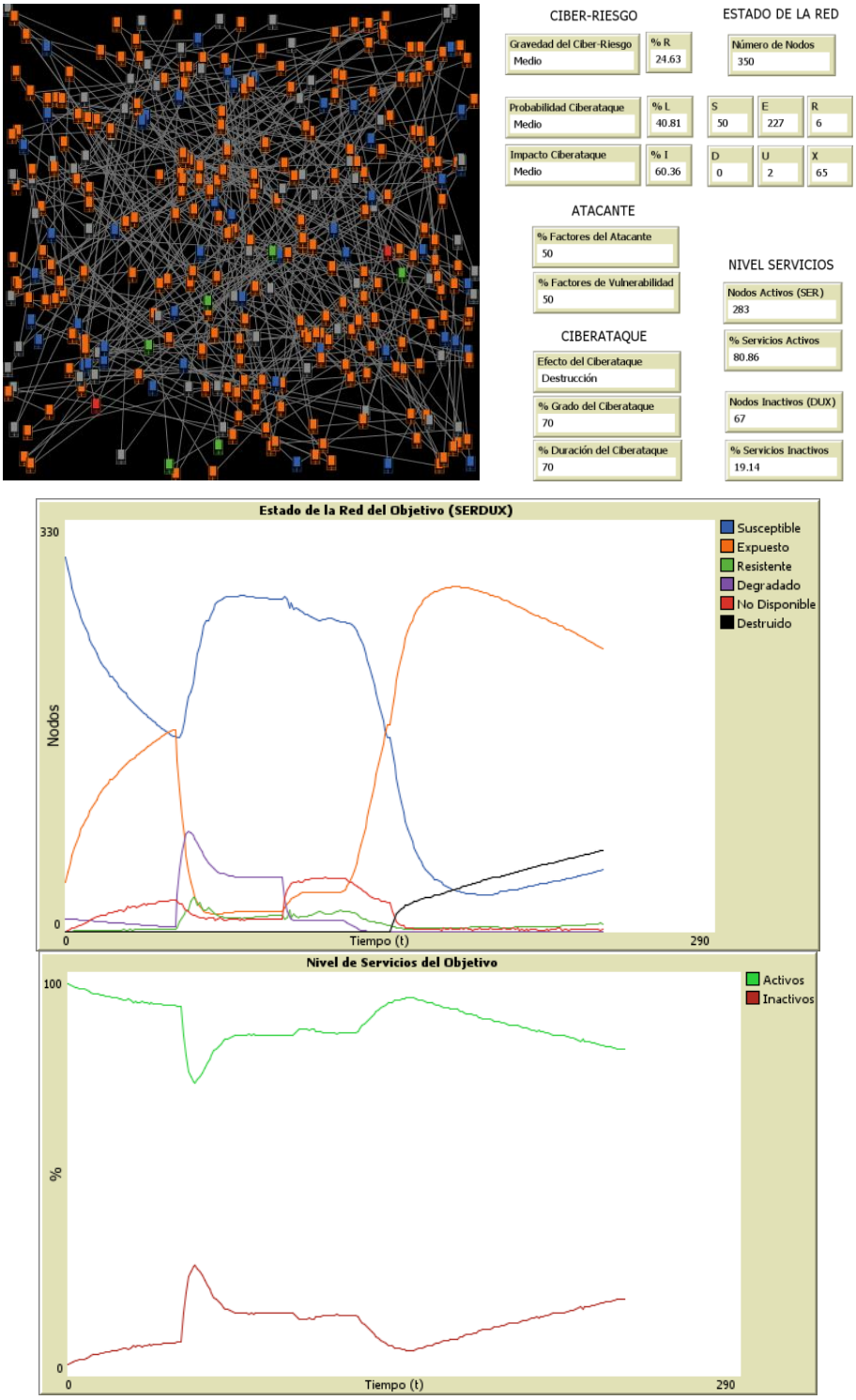
- **Decisiones del jugador:** se activa la carta 11 (Revisión), lo cual demuestra intención de generar lecciones aprendidas, aunque con poco impacto práctico en este punto. No se toman decisiones adicionales ni se corrige la estrategia.
- **Resultados de la simulación:** el sistema termina con 175 nodos destruidos. El nivel de servicios se estabiliza en 49.71%, reflejando una degradación permanente de la red. A pesar de decisiones aceptables en etapas iniciales, la falta de respuesta proactiva en momentos clave impidió una recuperación efectiva. La CSA institucional fue funcional, pero no suficiente para contener un ataque de carácter destructivo.

4.3. Escenario 3 – Configuración Optimista

En este escenario, el jugador despliega una estrategia proactiva, integral y sincronizada. Las capacidades se asignan de forma priorizada, y las cartas especiales se utilizan estratégicamente en la ronda adecuada según su efecto esperado. Esta configuración representa una organización con alto nivel de CSA, capaz de interpretar señales tempranas, anticipar escenarios críticos y tomar decisiones coherentes con la evolución de la amenaza. Se espera que bajo este enfoque se mantenga la operatividad del sistema por encima del umbral de estabilidad (70%).

A continuación, se presentan los resultados de la simulación (Figura 8, Tabla 12 y Tabla 13), junto con el análisis por ronda:

Figura 8. Resultados simulación en Netlogo – Escenario optimista



Fuente: elaboración propia usando el software MARCIM-WG en Netlogo

Tabla 12. Información y resultados de la simulación – Escenario optimista – Parte 1

PARÁMETRO O VARIABLE DE SIMULACIÓN	RONDA									
	1		2		3		4		5	
	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA	ENTRADA	SALIDA
CONFIGURACIÓN INICIAL DE LA RED										
Número de conexiones por nodo	2	2		2		2		2		2
Cantidad total de nodos	350	350		350		350		350		350
nodos susceptibles	300	157		267		156		31		50
nodos expuestos	40	162		16		166		269		227
nodos resistentes	0	2		13		5		4		6
nodos degradados	10	4		44		0		0		0
nodos no disponibles	0	25		10		23		2		2
nodos destruidos	0	0		0		0		44		65
Servicios Activos	97.14%	91.71%		84.57%		93.43%		86.86%		80.86%
Servicios Inactivos	2.86%	8.29%		15.43%		6.57%		13.14%		19.14%
Gravedad del Ciber-Riesgo		3.10% Bajo		13.41% Medio		19.47% Medio		26.63% Medio		24.63% Medio
Probabilidad Ciberataque		38.81% Medio		37.24% Medio		44.56% Medio		43.40% Medio		40.81% Medio
Impacto Ciberataque		8.00% Bajo		36.00% Medio		43.70% Medio		61.36% Medio		60.36% Medio
ATACANTE										
factores-atacante-ATF	0.4		0.4		0.5		0.5		0.5	
vulnerability-factors-VUF	0.4		0.4		0.5		0.5		0.5	
CIBERATAQUE										
grado-ciberataque-ADE	0.1		0.4		0.5		0.7		0.7	
duración-ciberataque-ADU	0.1		0.4		0.5		0.7		0.7	
Efecto ciberataque	Disrupción		Disrupción		Denegación		Destrucción		Destrucción	
CAPACIDADES-OBJETIVO										
capacidades-ciberdefensa-obj-TCD	0.1		0.3		0.6		0.8		1	
capacidades-soporte-sostenibilidad-obj-TSS	0.1		0.2		0.5		0.5		0.9	
capacidades-ciberinteligencia-obj-TCI	0.1		0.3		0.5		0.6		0.9	
CONTROLES SEGURIDAD - OBJETIVO										
controles-compensatorios-obj-CCM	0.2		0.3		0.6		0.8		0.9	
controles-disuasorios-obj-CDE	0.2		0.3		0.6		0.7		0.9	
controles-detectivos-obj-CDV	0.2		0.4		0.6		0.8		0.9	
controles-preventivos-obj-CPR	0.2		0.4		0.7		0.9		1	
controles-correctivos-obj-CCR	0.2		0.4		0.6		0.9		1	
SISTEMA DE ECUACIONES DIFERENCIALES										
tasa-propagacion-inicial-PRO0	0.25		0.5		0.75		1		1	
tasa-no-disponibilidad-otras-causas-UOC	0.0025		0.0025		0.0025		0.0025		0.0025	
parámetro-tiempo-ciberataque-D-tf	240		240		240		240		240	
stregth-damping-loss-resistance-LOR-a	0.01		0.01		0.01		0.01		0.01	
time-damping-loss-resistance-LOR-m	120		48		12		120		120	
pasos-sim	48		48		48		48		48	
Días	2		2		2		2		2	

Fuente: elaboración propia

Tabla 13. Información y resultados de la simulación – Escenario optimista – Parte 2

USO CARTAS ESPECIALES												
CARTA (ACCIÓN) ESPECIAL	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
	Planeación y preparación	**Detección y Reporte (Interno)**	**Evaluación y Análisis del Incidente**	**Declaración de la Crisis**	**Cooperación**	**Plan de Recuperación de Desastres**	**Plan de Continuidad del Negocio**	**Ciberataque**	**Pago del Ransomware**	**Reporte del Incidente**	**Revisión**	**Mejora**
Fase en la ISO 27035:2023	**Planeación y Preparación**	**Detección y Reporte**	**Evaluar y Decidir**		**Responder**						**Lecciones Aprendidas**	
Etapa Crisis	**Etapa Estable**	**Precrisis**		**Crisis**						**Poscrisis**		**Etapa Estable**
Ronda	**1**	**2**		**3**		**4**				**5**		
Selección	**X**	**X**	**X**	**X**	**X**	**X**	**X**			**X**	**X**	**X**

DISTRIBUCIÓN DE FICHAS PARA ENTRAR A LA SIMULACIÓN DE LA RONDA												
	Entrada Simula. Ronda	**1**		**2**		**3**		**4**		**5**		**Total**
	Origen Fichas	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	
Capacidades	**TCD**	1			2	2	1	1	1	1	1	10
	TSS	1			1	1	2			2	2	9
	TCI	1			2		2	1		2	1	9
Controles	**CCM**	1	1	1		3		1	1	1		9
	CDE	1	1	1		3	1	1		2		10
	CDV	1	1	2		2		1	1		1	9
	CPR	1	1	2		2		1	1		1	9
	CCR	1	1	2		2		2	1		1	10
Total		**8**	**5**	**8**	**5**	**15**	**6**	**8**	**5**	**8**	**7**	75
		13		**13**		**21**		**13**		**15**		
						Cambio de 03 BMC por fichas de capacidad (9)						

Fuente: elaboración propia

Ronda 1 – Etapa Estable Funcional

- **Decisiones del jugador:** se activa la carta especial 1 (Planeación y Preparación) en la ronda correcta, lo que evidencia un nivel alto de percepción del entorno y de las condiciones iniciales del sistema.
- **Resultados de la simulación:** con un 91.71 % de servicios activos y sin nodos destruidos, el sistema permanece en estado funcional, aunque vulnerable. Los 157 nodos susceptibles y 162 expuestos reflejan una amenaza latente que, de no ser gestionada, puede escalar rápidamente. El entorno es estable, pero en tensión inicial.

Ronda 2 – Precrisis

- **Decisiones del jugador:** el jugador activa las cartas 2 (Detección y Reporte Interno) y 3 (Evaluación y Análisis del Incidente), fortaleciendo significativamente la comprensión de la situación. La distribución de fichas muestra priorización en los controles de seguridad, evidenciando lectura adecuada del entorno y orientación hacia la contención temprana. La estrategia refleja proyección efectiva frente al avance del ciberataque.
- **Resultados de la simulación:** aunque el sistema registra un descenso a 84.57 % en servicios activos, se mantiene dentro del umbral estratégico, lo cual sugiere efectividad en los controles. El sistema entra en la fase de disrupción, pero con condiciones favorables para la contención si se mantiene el enfoque estratégico.

Ronda 3 – Crisis

- **Decisiones del jugador:** se activa correctamente la carta 4 (Declaración de la Crisis), seguida de la carta 5 (Cooperación). Adicionalmente, el jugador decide transformar dos BitMarCoins en ocho fichas de capacidad adicionales, que se invierten en esta ronda, priorizando controles compensatorios (CCM), disuasivos (CDE) y correctivos (CCR). Estas decisiones demuestran una proyección altamente efectiva y capacidad de adaptación frente al incremento de la amenaza.
- **Resultados de la simulación:** el sistema responde positivamente: el nivel de servicios aumenta a 93.43 %. Se observa una disminución en los nodos en estados degradados o no disponibles. El ciberataque, a pesar de su evolución a fase de denegación, empieza a ser contenido. La tendencia muestra señales de recuperación anticipada.

Ronda 4 – Crisis

- **Decisiones del jugador:** el jugador activa la carta 6 (Plan de Recuperación de Desastres) y la carta 7 (Plan de Continuidad del Negocio) de forma oportuna. Se mantiene una distribución coherente de fichas, reforzando todas las capacidades críticas. Esta ronda consolida un alto nivel de CSA, tanto en comprensión como en proyección, alineando acciones con las condiciones del entorno simulado.
- **Resultados de la simulación:** aunque el ataque alcanza su punto máximo (grado y duración del ciberataque en 70 %), la red se mantiene con 86.86 % de servicios activos y los efectos destructivos se contienen. La resiliencia estructural del sistema se fortalece, resistiendo con solidez la ofensiva cibernética.

Ronda 5 – Poscrisis / Etapa Estable Recuperada

- **Decisiones del jugador:** se activan correctamente las cartas 10 (Reporte del Incidente), 11 (Revisión) y 12 (Mejora), promoviendo procesos de lecciones aprendidas y retroalimentación estratégica. Se conserva el impulso positivo en la dinámica institucional.
- **Resultados de la simulación:** el sistema finaliza con 80.86 % de servicios activos. Los indicadores muestran una red parcialmente degradada pero plenamente funcional, con clara transición hacia una etapa estable. La validación confirma que decisiones informadas y coordinadas pueden contener e incluso revertir ciberataques severos.

4.4. Análisis comparativo de los escenarios

La validación conceptual de MARCIM-WG mediante tres escenarios —pesimista, neutral y optimista— permitió evidenciar el impacto directo de las decisiones estratégicas del jugador sobre la evolución de una crisis cibernética en el ámbito marítimo. Cada escenario reflejó un nivel distinto de Conciencia Situacional Cibernética (CSA), ilustrando los efectos de distintos enfoques frente a la misma amenaza.

En el escenario pesimista, la falta de planificación y el uso errático o tardío de cartas especiales impidieron contener el ataque. El modelo SERDUX-MARCIM registró una rápida degradación del sistema, con una caída del nivel de servicios por debajo del 35 % y 224 nodos destruidos, sin posibilidad de recuperación. Este escenario evidenció una CSA fragmentada y puramente reactiva.

El escenario neutral simuló una respuesta táctica sin articulación estratégica. Aunque se utilizaron cartas especiales, su aplicación fue descoordinada. El sistema mantuvo alrededor del

50 % de servicios activos, pero con 175 nodos destruidos y una red degradada. La CSA fue media, con limitada capacidad de proyección.

En el escenario optimista, la combinación de planificación estructurada, uso oportuno de cartas especiales e inversión coherente de fichas permitió contener y revertir la crisis. La red conservó más del 80 % de servicios activos, con solo 50 nodos destruidos. Se evidenció una CSA elevada, con percepción, comprensión y proyección efectivas.

En conjunto, los tres escenarios prueban que MARCIM-WG es sensible a las decisiones del jugador y simula dinámicas realistas de ciberdefensa marítima. Además, reafirman que la integración entre narrativa operativa, recursos físicos y simulación computacional constituye una herramienta formativa sólida, coherente con los principios doctrinales. El comportamiento del sistema valida la lógica de adjudicación del juego y su utilidad para la formación estratégica en entornos de incertidumbre.

4.5. Validación de competencias y resultados de aprendizaje

4.5.1. Propósito y diseño de la validación

Con el fin de responder de manera precisa a la necesidad de verificar el impacto formativo del juego de guerra MARCIM-WG en el desarrollo de competencias y resultados de aprendizaje relacionados con la Conciencia Situacional Cibernética (CSA), se estructuró una estrategia de validación comparativa con grupo de control. Esta estrategia tuvo como propósito contrastar el nivel de apropiación de conceptos clave entre participantes que no habían jugado y aquellos que sí experimentaron el juego, utilizando como referencia el instrumento de evaluación previamente diseñado y descrito en la Sección 2.3.4 y Anexo 5.

Para tal fin, se aplicó el instrumento de evaluación de competencias y resultados de aprendizaje a un grupo de ocho (8) oficiales con un perfil específico, quienes no habían participado

previamente en el juego MARCIM-WG. Esta medición constituyó el **Grupo de Control**. Posteriormente, se seleccionaron cuatro (4) participantes con el mismo perfil, quienes participaron en una sesión controlada del juego de guerra MARCIM-WG. Al finalizar la experiencia, estos últimos respondieron el mismo instrumento de evaluación aplicado al grupo de control, lo que permitió realizar una comparación directa entre ambos grupos.

Este diseño experimental básico, de tipo cuasi-experimental con medición postest entre grupos equivalentes, permitió aislar el efecto del juego como variable independiente y evaluar su contribución directa al desarrollo de las competencias formuladas. La estructura y formato del instrumento de medición utilizado para esta validación corresponden a los resultados de aprendizaje establecidos para las tres competencias del juego y se alinean con el instrumento consignado en el Anexo 5.

4.5.2. Perfil de los participantes

Tanto el grupo de control como el grupo de intervención estuvieron conformados por oficiales activos de las Fuerzas Militares de Colombia, seleccionados bajo un perfil técnico-operacional común, que garantizara condiciones de equivalencia para la comparación entre ambos grupos. Este perfil fue definido para asegurar la pertinencia de los resultados obtenidos en la validación.

Los participantes cumplieron con los siguientes criterios específicos:

- **Vinculación institucional:** oficiales activos de la Armada Nacional, Ejército Nacional o la Fuerza Aeroespacial Colombiana.
- **Experiencia profesional:** mínimo 20 años de trayectoria laboral en funciones operacionales, estratégicas o de apoyo institucional en defensa nacional.
- **Formación previa:** formación formal, de cualquier nivel, en áreas relacionadas con ciberseguridad, ciberdefensa o estrategia militar.

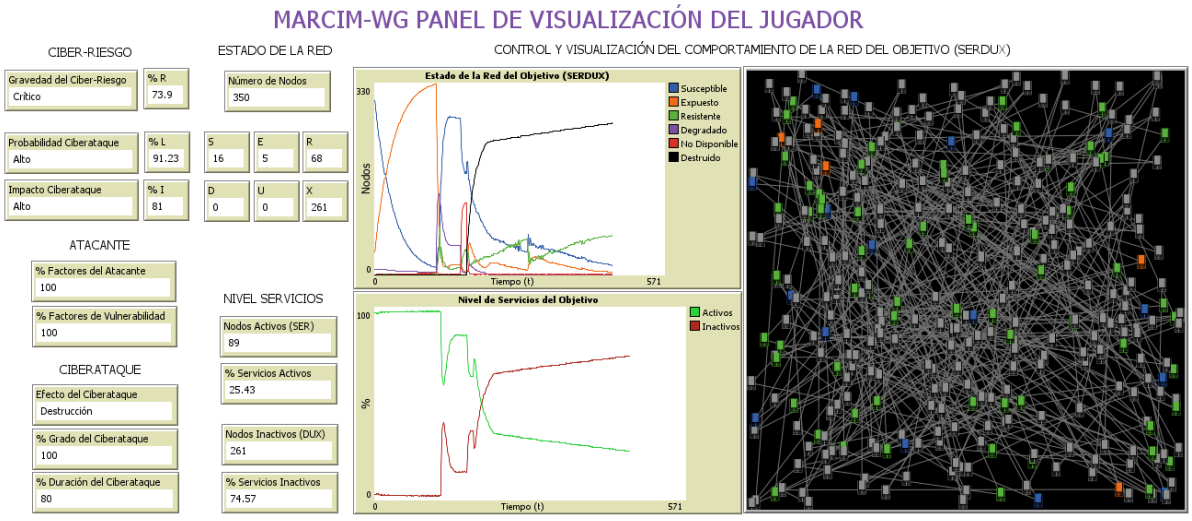
- **Conocimiento funcional:** Comprensión y experiencia directa en aspectos relacionados con el poder marítimo, ya sea desde la teoría, doctrina, planificación o experiencia profesional.

Este perfil fue clave para asegurar que los participantes contaran con la base conceptual y estratégica necesaria para interactuar con los contenidos del juego MARCIM-WG, permitiendo así una validación fundamentada en criterios de idoneidad, relevancia y aplicabilidad operativa.

4.5.3. Resultados

La aplicación de los instrumentos de medición se llevó a cabo el jueves 10 de julio de 2025, en las instalaciones de la Escuela Superior de Guerra "General Rafael Reyes Prieto". En primer lugar, se aplicó el instrumento de medición a un grupo de control conformado por ocho (8) oficiales que no habían participado en el juego de guerra MARCIM-WG. Posteriormente, cuatro (4) oficiales del mismo perfil participaron en una sesión completa del juego (Figura 9 y Figura 10), y respondieron el mismo instrumento de medición al finalizar. Los resultados obtenidos se presentan detalladamente en los Anexo 6 (grupo de control) y Anexo 7 (grupo de intervención).

Figura 9. Resultado de simulación de la sesión de validación de competencias y RA.



Fuente: sesión de juego utilizando MARCIM-WG EN Netlogo

Figura 10. Sesión de validación de competencias y resultados de aprendizaje.

La Tabla 14 resume los resultados obtenidos, evidenciando diferencias significativas entre ambos grupos. A nivel general, el grupo de intervención —que participó en el juego de guerra MARCIM-WG— alcanzó un 91.2 % de respuestas correctas, frente al 57.2% del grupo de control, lo cual representa una mejora del 34 % atribuible directamente a la experiencia lúdico-estratégica.

Tabla 14. Resultados validación de competencias y resultados de aprendizaje

Competencia / Resultado de Aprendizaje (RA)	**Grupo de Control (%)**	**Grupo de Intervención (%)**	**Diferencia (%)**
Resultado general	57.2 %	91.2 %	+34.0 %
Competencia 1 – Percepción estratégica del entorno	66.6 %	88.8%	+29.2 %
RA1.1 Identifica activos críticos	70 %	100 %	+30%
RA1.2 Reconoce amenazas activas	54.3%	100 %	+45.7%
RA1.3 Valora nivel de riesgo cibernético	54.6%	66.6%	+12%
Competencia 2 – Comprensión integrada de cibercrisis	61.9 %	97,5 %	+35.54 %
RA2.1 Analiza evolución del ataque	71.8%	100%	+28.2 %
RA2.2 Evalúa capacidades cibernéticas	44 %	100%	+56 %
RA2.3 Reconoce fases de crisis	71.5 %	100 %	+28.5 %
RA2.4 Aplica norma ISO/IEC 27035	60%	100 %	+40 %
RA2.5 Analiza implicaciones estratégicas	62.5%	87,5 %	+25 %
Competencia 3 – Proyección estratégica de escenarios futuros	78.3%	89.5%	+11.2 %
RA3.1 Formula hipótesis estratégicas	87.5%	100%	+12.5 %
RA3.2 Evalúa efectos de decisiones	59.3%	68.7%	+9.3 %
RA3.3 Reflexiona sobre implicaciones	88 %	100%	+12 %

Fuente: elaboración propia

En términos de competencias específicas, la Competencia 1 (Percepción estratégica del entorno cibernético) mostró una mejora de 22,2 puntos porcentuales; la Competencia 2 (Comprensión integrada de escenarios de cibercrisis), una mejora de 35,6 puntos; y la Competencia 3 (Proyección estratégica de escenarios futuros), una mejora de 11,2 puntos. Estos resultados

indican un desarrollo significativo y transversal en las tres fases de la Conciencia Situacional Cibernética (CSA): percepción, comprensión y proyección.

El análisis por resultado de aprendizaje (RA) confirma esta tendencia. Todos los RA evaluados presentan una mejora individual que oscila entre 9,3 % y 56 %, siendo especialmente relevantes los avances en aspectos conceptuales complejos como la evaluación de capacidades cibernéticas (RA2.2), la aplicación de la norma ISO/IEC 27035 (RA2.4), y la identificación de amenazas activas (RA1.2).

Estos hallazgos permiten sustentar que el juego de guerra MARCIM-WG contribuye significativamente al fortalecimiento de la CSA en contextos estratégicos, validando empíricamente las competencias y resultados de aprendizaje propuestos.

4.5.4. Conclusión de la validación de competencias y resultados de aprendizaje

La validación realizada mediante la comparación entre el grupo de control y verificación demostró que el juego de guerra MARCIM-WG tiene un impacto formativo significativo en el desarrollo de competencias y resultados de aprendizaje relacionados con la Conciencia Situacional Cibernética (CSA). El grupo de intervención superó en promedio al grupo de control en un 34 %, con mejoras en todas las competencias y resultados, especialmente en la valoración del riesgo, la gestión de incidentes y la proyección estratégica. Estos hallazgos confirman que la experiencia lúdico-estratégica facilita una apropiación más profunda y aplicada del conocimiento en escenarios de cibercrisis. Se valida así empíricamente que quienes participan en el juego desarrollan capacidades diferenciales en comparación con quienes no lo hacen.

Conclusiones y recomendaciones

La estructuración del juego MARCIM-WG, fundamentada en los principios metodológicos del *NATO Wargaming Handbook* y alineada con el modelo computacional SERDUX-MARCIM, permite operacionalizar un entorno de simulación estratégica robusto que responde directamente a la necesidad de fortalecer la apropiación de procedimientos de respuesta ante crisis cibernéticas en el dominio marítimo. Esta integración metodológica asegura coherencia entre los objetivos formativos del juego y las dinámicas simuladas, facilitando el desarrollo de competencias clave en toma de decisiones a nivel estratégico.

La incorporación de elementos de fricción, adjudicación analíticamente asistida, narrativa realista y roles especializados dentro del equipo de juego, consolida una arquitectura de diseño que trasciende el enfoque tradicional, posicionando a MARCIM-WG como una herramienta avanzada de aprendizaje experiencial y evaluación estratégica en ciberdefensa marítima. Este enfoque potencia el desarrollo progresivo de la Conciencia Situacional Cibernética (CSA) y sienta las bases para futuras aplicaciones operativas y académicas del juego.

El diseño de MARCIM-WG como juego de aprendizaje estratégico en ciberdefensa marítima constituye una innovación pedagógica al traducir la complejidad del modelo SERDUX-MARCIM en dinámicas accesibles mediante recursos físicos y simulación asistida. Su sistema de adjudicación analíticamente asistido garantiza que las decisiones generen consecuencias fundamentadas en lógica computacional y datos cuantificables, fortaleciendo la formación en contextos de alta incertidumbre y facilitando su aplicación en procesos de entrenamiento y validación doctrinal.

El escenario de crisis diseñado para MARCIM-WG, construido a partir de una narrativa estratégica ficticia con actores, eventos y amenazas técnicamente plausibles, constituye un

referente metodológico para la formulación de contextos realistas en ejercicios de ciberdefensa marítima, permitiendo evaluar la toma de decisiones frente a vectores de ataque complejos.

La validación conceptual de MARCIM-WG, sustentada en su alineación con el modelo SERDUX-MARCIM y principios doctrinales de ciberdefensa, demostró ser exitosa. Su integración de simulación, componentes físicos y narrativa de crisis consolida un modelo replicable para diseñar juegos de guerra aplicables a otros sectores estratégicos, contribuyendo a la resiliencia cibernética nacional.

Se proponen las siguientes líneas de desarrollo para fortalecer y ampliar el alcance:

- Desarrollar nuevos escenarios que aborden amenazas emergentes, ataques multinivel o contextos multinacionales, incrementando la versatilidad y aplicabilidad del juego en distintos dominios de ciberdefensa.
- Implementar el modelo computacional en contenedores Docker, facilitando su despliegue en diversas plataformas sin requerimientos técnicos adicionales.
- Realizar pruebas con usuarios estratégicos en contextos reales de formación y entrenamiento, para evaluar la eficacia de MARCIM-WG en el desarrollo de conciencia situacional y habilidades decisionales en ciberdefensa marítima.

Finalmente, la validación de competencias del juego MARCIM-WG evidenció un impacto formativo positivo en el desarrollo de la Conciencia Situacional Cibernética. Los participantes que vivenciaron el juego mejoraron en promedio un 34 %, con avances en identificación de riesgos, comprensión normativa y toma de decisiones estratégicas. Estos resultados confirman la eficacia del modelo como herramienta pedagógica para fortalecer capacidades en ciberdefensa marítima, aportando evidencia empírica sobre su pertinencia, aplicabilidad y valor en contextos estratégicos de seguridad nacional.

Referencias

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Allied Command Transformation. (2023). *NATO wargaming handbook*. https://paxsims.wordpress.com/wp-content/uploads/2023/09/nato-wargaming-handbook-202309.pdf

Baezner, M., & Cordey, S. (2019). National cybersecurity strategies in comparison-challenges for Switzerland. En *Center for Security Studies (CSS)*. www.css.ethz.ch

Bjørnstad, O. N., Shea, K., Krzywinski, M., & Altman, N. (2020a). Modeling infectious epidemics. *Nature methods*, *17*(5), 455–457. https://doi.org/10.1038/s41592-020-0822-z

Bjørnstad, O. N., Shea, K., Krzywinski, M., & Altman, N. (2020b). The SEIRS model for infectious disease dynamics. *Nature Methods*, *17*(6), 557–558. https://doi.org/10.1038/s41592-020-0856-2

Bodeau, D. J., Mccollum, C. D., & Fox, D. B. (2018). *Cyber wargaming: framework for enhancing cyber wargaming with realistic business context*. http://www.mitre.org/HSSEDI

Cabuya Padilla, D. E. (2024). *Marco de Referencia para el Modelamiento y Simulación de la Ciberdefensa Marítima a Nivel Estratégico – MARCIM* [Tesis Doctoral]. Escuela Naval de Cadetes "Almirante Padilla".

Cabuya Padilla, D. E., Alvarado Carvajal, C. F., Carrascal Ortiz, R. A., Riola Rodríguez, J. M., Fajardo-Toro, C. H., & Escandon Bernal, S. P. (2022). Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990 – 2021. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *49*, 197–210. https://www.risti.xyz/issues/ristie49.pdf

Cabuya-Padilla, D., & Castaneda-Marroquin, C. (2025). Modelo Estratégico de Ciberdefensa Marítima: Protección de Infraestructuras Críticas Cibernéticas en el Entorno Marítimo Colombiano. *Revista Científica General José María Córdova*, *51*.

Cabuya-Padilla, D., Díaz-López, D., & Castaneda-Marroquin, C. (2025). Hybrid Tabletop Exercise (TTX) based on a Mathematical Simulation-based Model for the Maritime Sector. *Actas de las X Jornadas Nacionales de Investigación en Ciberseguridad: Zaragoza, 4 a 6 de junio de 2025*, 37–44. https://2025.jnic.es/

Cabuya-Padilla, D., Díaz-López, D., Martínez-Páez, J., Hernández, L., & Castaneda-Marroquin, C. (2025). SERDUX-MARCIM: Maritime Cyberattack simulation using Dynamic Modeling, Compartmental Models in Epidemiology and Agent-based Modeling. *International Journal of Information Security*, *24*(3), 122. https://doi.org/10.1007/s10207-025-00985-6

Cabuya-Padilla, D. E., & Castaneda-Marroquin, C. A. (2024). Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología. *DYNA*, *91*(231), 169–179. https://doi.org/10.15446/dyna.v91n231.109774

Cornaglia, S., & Vercelli, A. H. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 46. https://doi.org/10.17141/urvio.20.2017.2601

Curry, J., & Drage, N. (2018). Developments in state level cyber wargaming. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3264437.3264468

Damodaran, S. K., & Wagner, N. (2020). Modeling and simulation to support cyber defense. En *Journal of Defense Modeling and Simulation* (Vol. 17, Número 1, pp. 3–4). SAGE Publications Inc. https://doi.org/10.1177/1548512919856543

Departamento Nacional de Planeación. (2011). *Documento CONPES 3701 -lineamientos de política para ciberseguridad y ciberdefensa.* https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf

Departamento Nacional de Planeación. (2017). *Documento CONPES 3854 - política nacional de seguridad digital*. Consejo Nacional de Política Económica y Social. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995 - política nacional de confianza y seguridad digital*. Consejo Nacional de Política Económica y Social. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Dormand, J. R., & Prince, P. J. (1980). A family of embedded Runge-Kutta formulae. *Journal of Computational and Applied Mathematics*, *6*(1), 19–26. https://doi.org/https://doi.org/10.1016/0771-050X(80)90013-3

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, *37*(1), 32–64.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & security*, *46*, 18–31.

Ganuza, N. (2020). *Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*. JID - Junta Interamericana de Defensa. https://jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf

Harguindéguy, J.-B., Hernández Hernández, M. E., Huete García, M. Á., Merinero Rodríguez, R., & Velasco González, M. (2023). Gamificación y políticas públicas ¡Que empiece el juego! *Gestión y Análisis de Políticas Públicas*, *31*, 43–55. https://doi.org/10.24965/gapp.11135

Hurtado de Barrera, J. (2010). *El proyecto de investigación* (E. Quirón, Ed.). Sypal.

International Telecommunication Union. (2024). Global Cybersecurity Index. En *Measuring the Digital Transformation*. https://doi.org/10.1787/5d87fa05-en

ISACA. (2016). *Certified in Risk and Information Systems Control (CRISC)*.

Izaguirre Olmedo, J. (2018). Vista de análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal*, *3*, 172–181. http://201.159.222.115/index.php/innova/article/view/837/779

Jacq, O., Brosset, D., Kermarrec, Y., & Simonin, J. (2019, junio 1). Cyber attacks real time detection: towards a cyber situational awareness for naval systems. *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA*. https://doi.org/10.1109/CyberSA.2019.8899351

Junta Interamericana de Defensa. (2020). *Informe II conferencia de ciberdefensa*. https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, *143*, 105138. https://doi.org/https://doi.org/10.1016/j.marpol.2022.105138

Katsantonis, N. M., Kotini, I., Fouliras, P., & Mavridis, I. (2019). Conceptual framework for developing cyber security serious games. *IEEE Global Engineering Education Conference, EDUCON*, *April-2019*, 872–881. https://doi.org/10.1109/EDUCON.2019.8725061

MathWorks. (1994). *MATLAB & Simulink*. https://la.mathworks.com/products/matlab.html

Mayer, I., Warmelink, H., & Zhou, Q. (2016). The utility of games for society, business, and politics. *The Wiley Handbook of Learning Technology*, 406–435. https://doi.org/10.1002/9781118736494.ch22

Méndez Álvarez, C. E. (2020). *Metodología de la investigación: diseño y desarrollo del proceso de investigación en ciencias empresariales*. Alpha Editorial.

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis – how to reduce threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

National Institute of Standards and Technology - NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

North Atlantic Council. (2012). *NATO modelling and simulation master plan* (Número September, pp. 1–10).

Onduto, B. (2021). Gamification of cyber security awareness – A systematic review of games [Master of Science in Technology Thesis, University of Turku]. En *Computing, Faculty of Technology*. https://www.utupub.fi/bitstream/handle/10024/152929/Onduto_Barack_Thesis_Final.pdf

Ovallos Gazabon, D., Villalobos Toro, B., De la Hoz Escorcia, S., & Maldonado Perez, D. (2016). Gamificación para la gestión de la innovación a nivel organizacional. Una revisión del estado del arte. *Revista Espacio*, *37*(8), 2–10. https://www.revistaespacios.com/a16v37n08/16370803.html

OWASP Foundation. (2017). *OWASP Risk Rating Methodology*. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Paul, C. L., & Whitley, K. (2013). A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness. En *LNCS* (Vol. 8030, pp. 145–154). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39345-7_16

Python Software Foundation. (2023). *Python*. https://www.python.org/

Ramírez-Cabrales, F., Pedroza Nieto, W. T., & Forero Hauzeur, J. C. (2021). *Intereses marítimos colombianos* (Vicepresidencia de la República, Ed.). Vicepresidencia de la República-Comisión Colombiana del Océano-Armada de Colombia.

Rosen, A. M., & Kerr, L. (2024). Wargaming for learning: How educational gaming supports student learning and perspectives. *Journal of Political Science Education*, *20*(2), 318–335.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering (IJCSSE)*, *5*(5), 67–81. www.IJCSSE.org

Sarjakivi, P., Ihanus, J., & Moilanen, P. (2024). Using wargaming to model cyber defense decision-making: observation-based research in Locked Shields. En *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.23.1.2270

Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cyber security. *CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1–4. https://doi.org/DOI: 10.1145/1852666.1852704

Shukla, G., & Gochhait, S. (2020). Cyber security trend analysis using web of science: a bibliometric analysis. *European Journal of Molecular and Clinical Medicine*, *7*(6), 2567–2576.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. En *Technical report*. The MITRE Corporation.

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the maritime sector: a literature review. *Journal of Marine Science and Application*, 1–18.

Till, G. (2007). *Poder marítimo: una guía para el siglo XXI*. Instituto de Publicaciones Navales del Centro Naval.

United Nations Conference on Trade and Development - UNCTAD. (2024). Review of maritime transport 2024. En *United Nations Conference on Trade and Development*. UNCTAD. https://unctad.org/system/files/official-document/rmt2024_en.pdf

Valencia Quecano, L. I. (2022). Gamification Strategies at the Service of Knowledge Management: Gestión del conocimiento y gamificación organizacional. *International Humanities Review*, *13*, 1–12. https://historicoeagora.net/revHUMAN/article/view/4093

Valencia-Arias, A., Giraldo, M., Acevedo-Correa, Y., Garcés-Giraldo, L., Quiroz-Fabra, J., Benjumea-Arias, M., & Patiño-Vanegas, J. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *E29*(05), 225–239.

Valente, J., & Reith, M. (2024). Cyber game-based learning for DoD CEs. *European Conference on Cyber Warfare and Security*, *23*(1), 795–802.

Von Clausewitz, C., & Naville, P. (1977). *De la guerra*. Diógenes.

Weiner, M. G. (1959). *War gaming methodology*. https://doi.org/10.1163/9789087903107_006

Wilensky, U. (2016). *NetLogo*. https://ccl.northwestern.edu/netlogo/

Wilensky, U., & Rand, W. (2015). An Introduction to Agent-Based Modeling: Modeling Natural, Social, and Engineered Complex Systems with NetLogo (MIT Press). En *MIT Press* (Número January).

Anexos

Anexo 1. Guía del Juego de Guerra MARCIM-WG.

I. REGLAS

A. Chatham House Rule

"*Cuando una sesión, o parte de ella, se realiza bajo la Chatham House Rule, los participantes están autorizados a utilizar la información discutida, siempre que no revelen la identidad ni la afiliación institucional de quienes la compartieron, ni la de ningún otro participante. Esta norma está orientada a fomentar la libertad de expresión, proteger la confidencialidad de los aportes y propiciar un entorno seguro para el análisis estratégico*".

Su aplicación en MARCIM-WG tiene como propósito principal incentivar la participación abierta y el intercambio honesto de ideas, sin que ello conlleve implicaciones personales o institucionales. En consecuencia, las opiniones que surjan durante el ejercicio no representan posturas oficiales ni políticas de ninguna entidad gubernamental o privada, sino que son responsabilidad exclusiva de los organizadores y participantes en calidad académica.

Este documento y sus contenidos son confidenciales, y se encuentran destinados exclusivamente a fines académicos y de formación estratégica. Está expresamente prohibida su reproducción, cita, difusión o cualquier otro uso no autorizado que exceda los objetivos del ejercicio.

B. Generales

- Todas las opiniones son válidas y deben ser escuchadas y respetadas sin excepción.
- Ningún participante debe ser interrumpido durante su intervención, salvo que el facilitador lo estime necesario para el adecuado desarrollo de la actividad.
- Dado que el tiempo es limitado, las intervenciones deberán ser claras, concisas y pertinentes, permitiendo la participación equitativa de todos los actores.
- Se debe evitar la repetición innecesaria de argumentos ya tratados, a fin de mantener un flujo dinámico de la discusión y fomentar la construcción progresiva del conocimiento.
- Las diferencias de criterio y los argumentos contrapuestos enriquecen el debate y fortalecen el análisis estratégico. Se anima su expresión con respeto y rigor.
- Cada participante deberá actuar conforme al rol asignado dentro del grupo, manteniendo coherencia con sus responsabilidades simuladas.
- Se deben seguir en todo momento las orientaciones e instrucciones del facilitador, quien garantizará el cumplimiento de la dinámica metodológica del juego.
- Los participantes se comprometen a no divulgar los resultados, dinámicas internas o decisiones adoptadas durante el ejercicio fuera del espacio designado, salvo autorización expresa del equipo organizador.
- Cada participante debe asumir un rol protagónico en el desarrollo del ejercicio, aportando activamente en la toma de decisiones y en las discusiones grupales.
- Las decisiones y aportes deben estar alineados con la narrativa del escenario y las atribuciones del rol asignado, evitando anacronismos o desviaciones metodológicas.

II. CARACTERÍSTICAS GENERALES DEL JUEGO DE GUERRA

Característica		Descripción
Temática	Ciberdefensa Marítima	Entendida como la capacidad estratégica y operativa del Estado para proteger, prevenir y contrarrestar incidentes de naturaleza cibernética que afecten al poder marítimo nacional.
	Planteamiento	Entorno simulado de toma de decisiones estratégicas en escenarios de crisis cibernética marítima,
Tipo de Juego de Guerra	Juego de Aprendizaje	Diseñado para la formación y el entrenamiento estratégico, permite a los participantes tomar decisiones en contextos desafiantes, evaluar sus efectos y recibir retroalimentación significativa sobre sus acciones.
Elementos Esenciales de Diseño	Decisiones	Los jugadores tienen la capacidad de elegir cómo responder ante los desafíos introducidos por el juego.
	Fricción	Se introducen elementos con el objetivo de condicionar las decisiones de los jugadores y generar nuevas perspectivas.
	Consecuencias	Cada decisión de los jugadores impacta directamente el desarrollo del juego. Este efecto se operacionaliza mediante el proceso de adjudicación, que traduce las decisiones en resultados cuantitativos a través del modelo SERDUX-MARCIM.
	Narrativa	El diseño del escenario incorpora una narrativa creíble y contextualizada en ciberdefensa marítima, en el marc o de una crisis cibernética.
Método de Adjudicación	Analíticamente asistido	Las decisiones de los jugadores no se resuelven únicamente por juicio experto o consenso, sino que son ingresadas en un modelo computacional, SERDUX-MARCIM, que simula sus efectos y genera salidas cuantitativas para ser interpretadas en el contexto del juego.
Fuerzas y elementos de ejecución	Objetivo	Representa una organización marítima vulnerable, considerada como el objetivo del ciberataque.
	Atacante	Individuo, grupo organizado o actor estatal que busca afectar la disponibilidad, integridad o confiabilidad de los activos del objetivo.
	Ciberataque	Es la herramienta o ciberarma que puede utilizar el Atacante para generar efectos sobre el Objetivo.

III. OBJETIVOS

A. Ejercicio

Objetivo General

Evaluar los procesos de toma de decisiones estratégicas y las respuestas ante incidentes cibernéticos en el contexto de la ciberdefensa marítima, fortaleciendo en los participantes el desarrollo integral de los tres niveles de la Conciencia Situacional Cibernética (CSA): percepción, comprensión y proyección.

Objetivos específicos

- **Percepción:** identificar hitos críticos, anomalías y cambios relevantes en el entorno durante el desarrollo de una crisis cibernética marítima.
- **Comprensión:** analizar e interpretar la información disponible para determinar su relevancia estratégica, evaluar vulnerabilidades y reconocer amenazas emergentes.
- **Proyección:** anticipar la evolución del incidente cibernético, estimar su impacto en la red crítica y definir estrategias de respuesta proactiva y mitigación adaptativa.

B. Participante

El objetivo específico de cada jugador consiste en **mantener el nivel de servicios operativos de la red Objetivo por encima del 70 % durante toda la simulación**, enfrentando diversas configuraciones de ciberataques que escalan en complejidad y alcance en cada ronda.

- Para alcanzar este objetivo, los participantes deberán:
- Optimizar el uso de capacidades y recursos limitados disponibles.
- Formular estrategias adaptativas ante la evolución dinámica del ciberataque.
- Tomar decisiones en tiempo real, basadas en la retroalimentación entregada por el sistema de adjudicación computacional.
- Equilibrar la defensa proactiva, la recuperación resiliente y la gestión de la incertidumbre en un entorno operacional simulado de alta fricción.

Este objetivo promueve la reflexión crítica, la toma de decisiones fundamentadas y el fortalecimiento de competencias estratégicas para la gestión de crisis cibernéticas en entornos marítimos.

IV. ROLES DEL JUEGO

Rol	Descripción
Patrocinador	Representa a la entidad que impulsa el ejercicio, encargada de definir el propósito estratégico del juego y los objetivos de aprendizaje esperados. Su participación garantiza el alineamiento institucional, la relevancia temática y la orientación de los resultados hacia el fortalecimiento de capacidades.
Director del juego	Supervisa la correcta ejecución metodológica del ejercicio, asegurando la fidelidad al diseño establecido. Actúa como puente entre los jugadores y el equipo técnico, manteniendo la coherencia estructural del juego, resolviendo contingencias y validando que las decisiones se tomen dentro del marco simulado propuesto.
Gestor del evento	Es responsable de la gestión logística, conectividad, soporte técnico y protección de la información durante toda la jornada del ejercicio. Su función garantiza que el entorno de simulación y sus componentes físicos y digitales estén disponibles y operativos, favoreciendo la continuidad del juego sin interrupciones.
Jugadores	Son los actores principales del ejercicio. Representan al Objetivo dentro del escenario, y tienen la responsabilidad de tomar decisiones estratégicas frente a una crisis cibernética progresiva. Su desempeño se evalúa con base en la resiliencia de la red simulada, el uso eficiente de capacidades y la proyección de respuestas ante escenarios inciertos..
Jugador Líder	Dentro del grupo de jugadores, el Jugador Líder asume el rol de coordinador interno. Es responsable de representar el consenso del grupo, introducir las decisiones en el tablero físico y administrar los elementos del juego (fichas, cartas, etc.). Su liderazgo facilita la consolidación de posturas estratégicas y la traducción operativa de las decisiones..
Adjudicador	Tiene una función técnica central: recibe las decisiones del jugador líder, las traduce en parámetros del sistema de adjudicación (modelo computacional), ejecuta la simulación computacional y actualiza el estado del tablero con base en los resultados generados. Asimismo, apoya la interpretación de los efectos del ataque y la respuesta del sistema, proporcionando retroalimentación objetiva a los jugadores.
Facilitador	Modera la dinámica general del juego. Administra el tiempo, entrega los elementos físicos y guía la interacción entre los jugadores y el sistema. Adicionalmente, realiza una interpretación continua del escenario, apoyando a los jugadores en la comprensión de la situación actual y estimulando una discusión estratégica coherente. También vela por el cumplimiento de las reglas, interviniendo cuando sea necesario para resolver dudas o asegurar el correcto desarrollo del ejercicio.
Equipos no jugadores	Representados funcionalmente por el adjudicador, comprenden el atacante y el ciberataque. Aunque no son controlados directamente, su configuración inicial y evolución son gestionadas por el equipo de control y afectan el desarrollo del juego.
Analista	Recoge, procesa e interpreta la información del ejercicio. Evalúa el desarrollo de la Conciencia Situacional Cibernética (CSA), analiza el comportamiento de los jugadores y los efectos del modelo computacional, y gestiona evaluaciones y datos para consolidar el informe técnico.

V. TIPOS DE ACTORES EN LA NARRATIVA DEL JUEGO DE GUERRA

Actor	Tipo	Actores asociados
OBJETIVO Corresponde a la entidad simulada cuya red crítica debe ser protegida. Representa el sistema bajo ataque, gestionado por los jugadores, quienes toman decisiones estratégicas para mantener su operatividad y resiliencia durante la crisis cibernética.	Marítimo	Autoridades marítimas Terminales y operadores portuarios Buques, carga e instalaciones Industria marítima Información y comunicaciones marítimas Proveedores de servicios Operadores de sistemas de transporte marítimo Proveedores de servicios de gestión marítima Proveedores y socios intermodales
	Defensa y Seguridad	Fuerzas Militares Fuerza Naval Unidad Cibernética Naval Comando Conjunto Cibernético Policía Nacional Centro de Policía Cibernética CERT Nacional / CSIRT CSIRT Sectorial
	Coordinación y Cooperación	Instituciones del Gobierno Nacional Agencias y Organizaciones Internacionales Instituciones Academia Sector privado Sindicatos y Asociaciones Profesionales Otros no formales
ATACANTE Es un actor simulado, no controlado por jugadores, que representa a un adversario con capacidades cibernéticas ofensivas. Su comportamiento está modelado computacionalmente y evoluciona en función del escenario, introduciendo presiones tácticas y estratégicas.	Amenaza Cibernética	Estados-nación Servicios de inteligencia extranjeros Ciberdelincuentes Espías industriales Hacktivistas Grupos tistas Amenazas internas Organizaciones ilegales Individuos Amenazas Persistentes Avanzadas (APT)

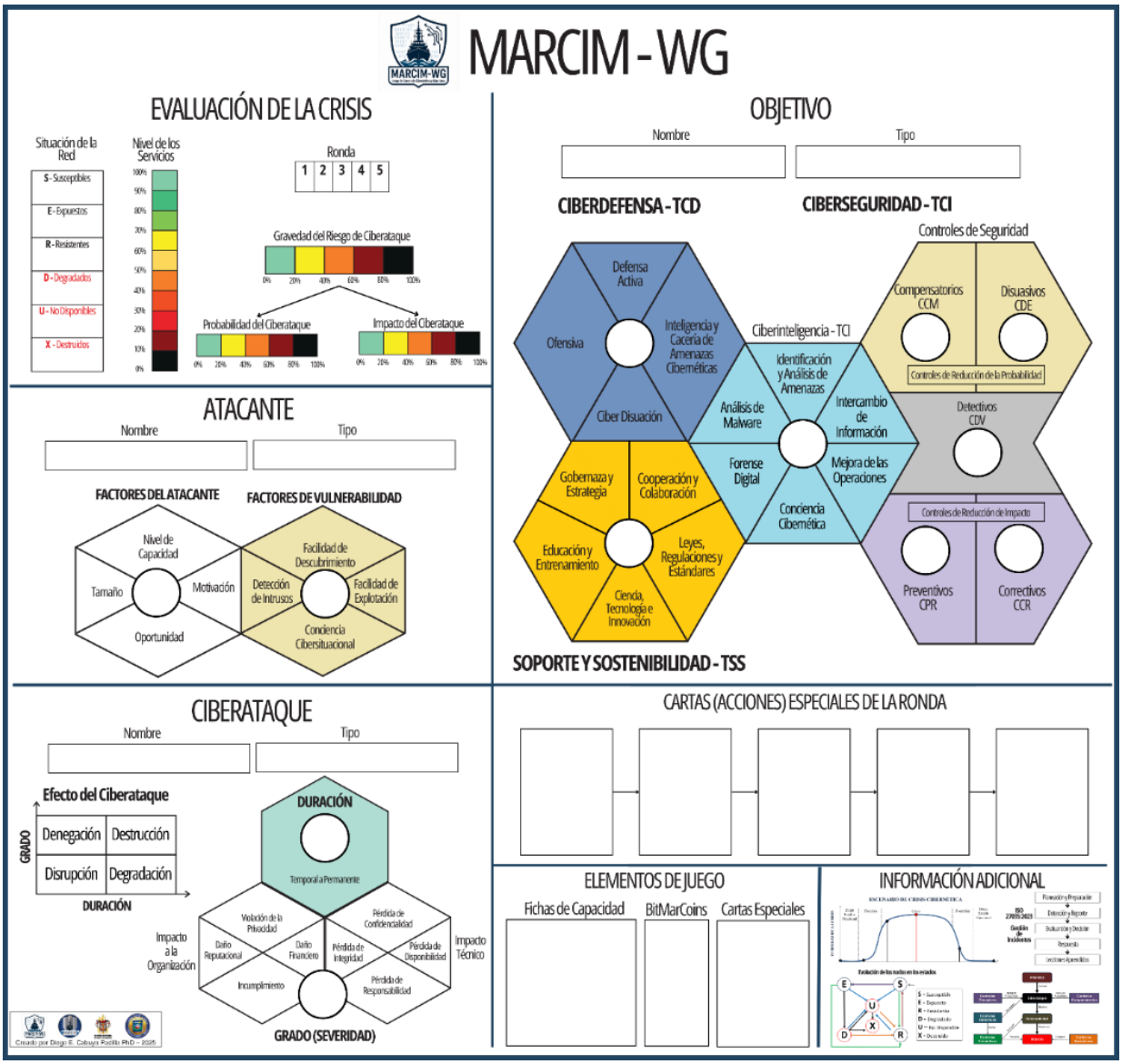
VI. ELEMENTOS DEL JUEGO Y ACCIONES

A. Tablero de Juego

El tablero de juego es el centro visual y operativo de MARCIM-WG. Representa un entorno estratégico simulado donde convergen todos los elementos críticos del ejercicio: el objetivo, el atacante y el ciberataque. Incluye de forma estructurada la red del objetivo, compuesta por nodos y conexiones, cuyos estados se visualizan según la lógica del sistema de adjudicación (Susceptible, Expuesto, Resistente, Degradado, Indisponible, Destruido). También permite monitorear el nivel de servicios, la evolución de la crisis por rondas y la gravedad del riesgo de ciberataque mediante escalas gráficas. Además, es el espacio donde se despliegan las cartas especiales, las fichas de capacidad y los BitMarCoins.

El tablero integra áreas específicas para registrar la información y los factores del atacante, caracterizar el ciberataque (nombre, tipo, duración, efectos y severidad), y visualizar su impacto sobre la red. También representa las capacidades del objetivo, organizadas en tres dominios: Ciberdefensa (TCD), Ciberseguridad (TCI) y Soporte y Sostenibilidad (TSS), junto con los controles de seguridad clasificados como compensatorios, disuasivos, detectivos, preventivos y correctivos. Es sobre estas capacidades y controles donde el jugador debe enfocar su toma de decisiones, invirtiendo fichas de capacidad de manera estratégica para mejorar la resiliencia del objetivo.

En síntesis, el tablero constituye la herramienta central del juego: refleja las decisiones tomadas, activa la interacción con el sistema de adjudicación y fortalece la comprensión del entorno de amenaza, promoviendo el desarrollo de la Conciencia Situacional Cibernética (CSA).



B. Fichas de Capacidad

Las fichas de capacidad representan los recursos que el jugador puede asignar para fortalecer al objetivo. Cada ficha equivale a una inversión en capacidades específicas de ciberseguridad, ciberdefensa, ciberinteligencia o en controles de seguridad. En términos del sistema de adjudicación, cada ficha tiene un valor de 0.1 unidades en la variable correspondiente, con un máximo acumulable de 1.0 por capacidad o control. Esto significa que el valor máximo permitido por cada capacidad o control es de 10 fichas. Dado su carácter limitado, el jugador debe tomar

decisiones estratégicas sobre qué capacidades priorizar, según el estado de la red y la evolución de la crisis cibernética.

Estas fichas pueden ser entregadas por el facilitador, ya sea por asignación en la ronda respectiva, o por el correcto uso de las cartas especiales. También pueden adquirirse o intercambiarse utilizando BitMarCoins, una criptomoneda ficticia que simula restricciones presupuestales. El jugador debe decidir si destina sus recursos a reforzar la defensa, mantener reservas o asumir riesgos mediante acciones ofensivas contra el atacante, con el fin de mitigar el impacto del ciberataque y mantener el nivel de servicios por encima del umbral crítico.

C. Fichas indicadoras de nivel

Estas fichas permiten monitorear elementos clave de la situación estratégica en el tablero. Representan el número de la ronda en curso, el nivel de riesgo cibernético, la potencia ofensiva del atacante y las características del ciberataque activo. Su visibilidad constante brinda al jugador una referencia clara del estado del juego, facilitando decisiones oportunas y fundamentadas.

Además de orientar la toma de decisiones, estas fichas permiten construir una narrativa visual del progreso del conflicto, reflejando tanto el deterioro como la recuperación de la red. En contextos formativos, funcionan como apoyo pedagógico al condensar de manera accesible la evolución del escenario, favoreciendo el análisis conjunto entre jugadores y facilitadores.

D. BitMarCoins (BMC)

Los BitMarCoins (BMC) son una criptodivisa ficticia del juego que introduce una dimensión económico-estratégica en la simulación. Cada jugador recibe una cantidad inicial de BMC en la Ronda 1, y debe gestionar este recurso limitado para tomar decisiones clave durante la crisis cibernética. Los BMC pueden utilizarse para:

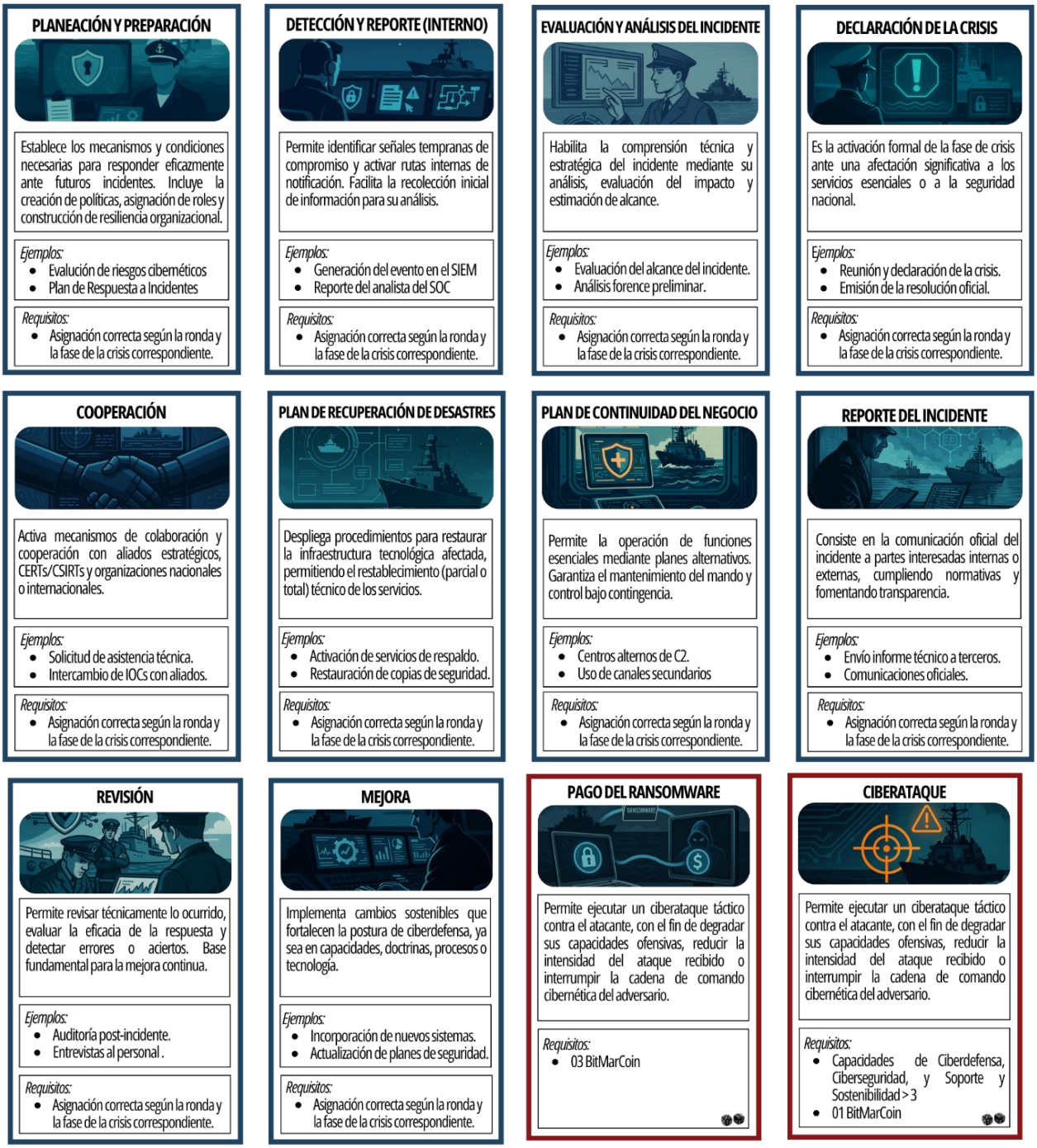
- Adquirir fichas de capacidad, mediante su venta directa.
- Comprar BMC adicionales, intercambiando fichas de capacidad.
- Financiar ciberataques, activando la carta especial correspondiente (01 BMC).
- Pagar rescates por *ransomware*, activando la carta especial de (03 BMC).

Esta mecánica obliga al jugador a establecer prioridades entre defensa, respuesta ofensiva y negociación bajo presión. Así, los BMC replican las restricciones financieras del mundo real, introduciendo un componente crítico de gestión de recursos.

E. Cartas (Acciones) Especiales

Las cartas especiales permiten ejecutar acciones extraordinarias que pueden modificar de forma decisiva el curso del juego. Cada una está vinculada a condiciones específicas de activación: ronda, y fase de la crisis. Su correcta utilización genera beneficios adicionales, como la entrega de fichas de capacidad en dominios o controles de seguridad determinados. Algunas cartas requieren el lanzamiento de dados para definir su resultado, incorporando una dimensión de incertidumbre que simula la fricción característica de los juegos de guerra. Además, su uso puede implicar el gasto de BitMarCoins, lo que obliga al jugador a tomar decisiones estratégicas entre invertir en capacidades, ejecutar acciones tácticas o reservar recursos.

A continuación, se presentan las cartas especiales disponibles en el juego, junto con su descripción, ejemplos de acciones y requerimientos de uso.



F. Dados

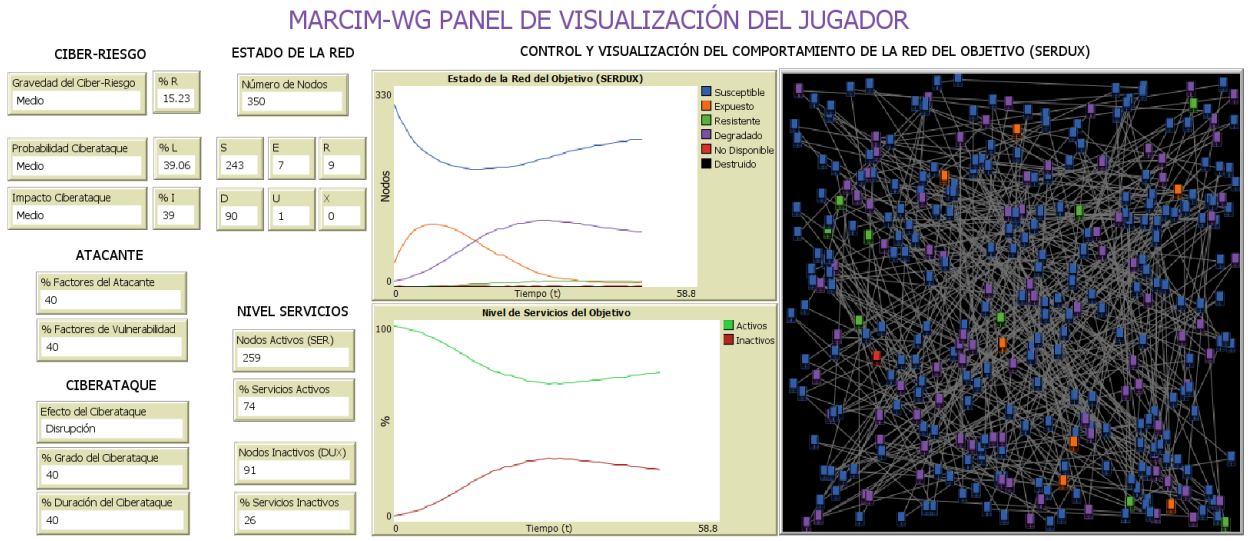
Los dados introducen incertidumbre en el desarrollo del juego, simulando condiciones impredecibles propias de los entornos reales de cibercrisis. Su uso está asociado a cartas especiales que requieren resolución probabilística, como los ciberataques ofensivos o los pagos de rescate por *ransomware*. Cada lanzamiento representa la fricción inherente a los juegos de guerra, donde incluso las mejores decisiones pueden verse afectadas por factores externos no controlables. Este mecanismo obliga al jugador a ponderar el riesgo antes de actuar, añadiendo realismo y complejidad al proceso de toma de decisiones estratégicas en el marco de la ciberdefensa.

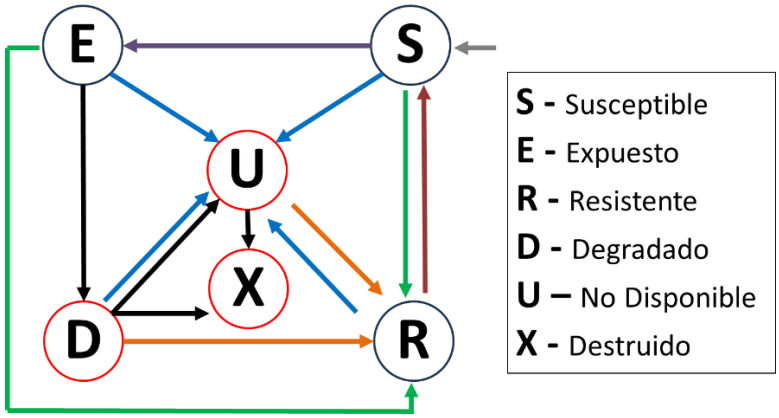
G. Sistema de Adjudicación (Modelo computacional)

El sistema de adjudicación del juego está respaldado por un modelo computacional basado en el esquema SERDUX-MARCIM. Este modelo emplea ecuaciones diferenciales y simulaciones estocásticas para calcular rigurosamente el impacto de las decisiones del jugador y la evolución del ciberataque. A diferencia de una resolución manual, incorpora parámetros técnicos realistas —como tasas de propagación, degradación y recuperación— que otorgan solidez analítica a cada ronda. Las decisiones estratégicas, por tanto, no solo alteran la narrativa del juego, sino que generan efectos cuantificables que modifican el estado del tablero.

Este sistema garantiza la coherencia interna del juego, asegura la trazabilidad entre acciones y resultados, y permite al jugador percibir con claridad la relación causa-efecto, lo cual es clave para generar aprendizajes válidos. En conjunto, el modelo se convierte en el eje técnico que articula el juego como una herramienta pedagógica, analítica y formativa, alineada con las recomendaciones metodológicas de la doctrina de juegos de guerra de la OTAN.

A continuación, se presenta la vista general del sistema de adjudicación de MARCIM-WG, centrada en el panel de visualización del jugador. Este panel está dividido en cuatro bloques de información clave: (i) nivel de ciber riesgo, (ii) características del atacante y del ciberataque, (iii) estado actual de la red según la distribución de nodos en los estados SERDUX, y (iv) nivel de servicios junto con la evolución temporal de la red. Esta estructura permite al jugador comprender de forma integrada el impacto de sus decisiones y anticipar la progresión del conflicto cibernético.





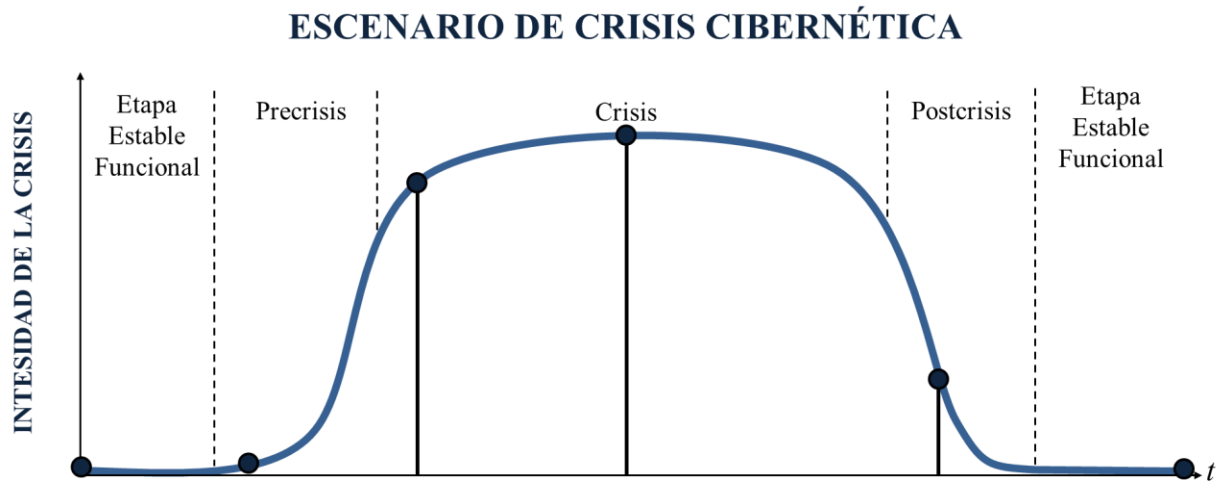
VII. ESCENARIO

El escenario del juego es completamente ficticio y ha sido diseñado con fines académicos en el contexto de la ciberdefensa marítima. Su propósito es ofrecer un entorno simulado que permita al jugador tomar decisiones estratégicas alineadas con los objetivos del ejercicio.

La simulación representa la evolución de una crisis cibernética que afecta a un actor marítimo, estructurada en cinco fases: estabilidad funcional, precrisis, crisis, postcrisis y retorno a la estabilidad. Estas etapas reflejan la progresión típica de un incidente complejo y sirven como marco para contextualizar las acciones del jugador.

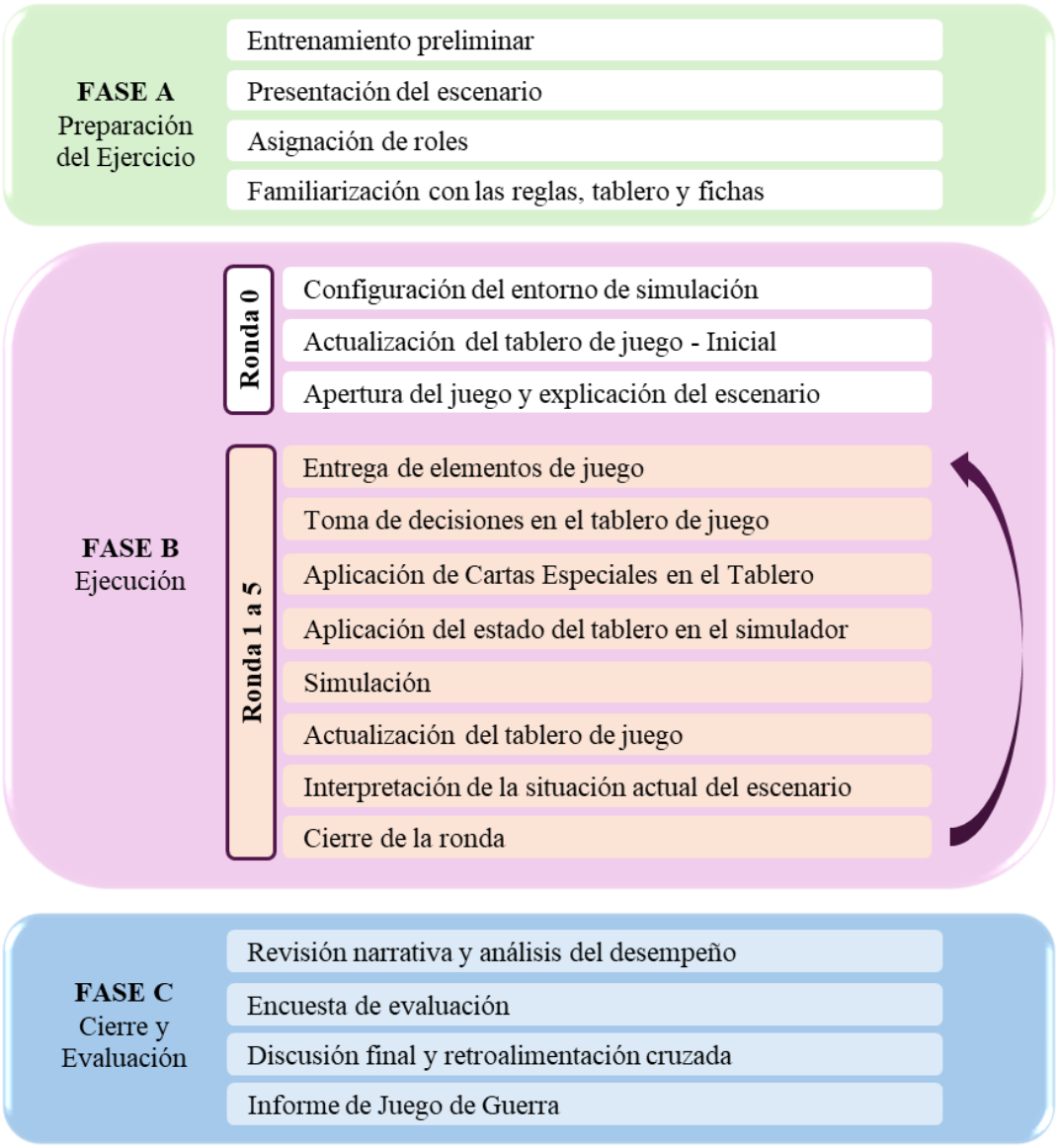
El desarrollo del escenario no es lineal ni predeterminado, ya que depende directamente de las decisiones adoptadas durante el juego. Si las acciones implementadas son inadecuadas, es posible que la red permanezca en estado de crisis o incluso empeore. Esta dinámica refuerza el carácter formativo del ejercicio y la importancia de evaluar riesgos, priorizar capacidades y anticipar consecuencias.

La figura a continuación ilustra la progresión típica de una crisis cibernética en el contexto simulado de MARCIM-WG.



VIII. DESARROLLO Y EJECUCIÓN DEL JUEGO DE GUERRA

El juego de guerra MARCIM-WG se estructura en tres fases metodológicas secuenciales: preparación, ejecución y cierre, tal como se muestra en la figura siguiente.



Esta organización permite desarrollar una simulación iterativa, controlada y dirigida de escenarios de crisis en ciberdefensa marítima, donde las decisiones estratégicas de los participantes se articulan con la evolución dinámica del ciberataque, modelada computacionalmente mediante el sistema de adjudicación.

En la **fase de preparación** se configura el escenario base, se asignan los roles, se entregan los insumos del juego y se familiariza a los participantes con la dinámica operativa. La **fase de ejecución** se desarrolla por rondas sucesivas. En cada una, los jugadores toman decisiones, gestionan recursos, interactúan con el tablero físico y reciben retroalimentación del sistema. Esta fase representa la evolución de la crisis cibernética en tiempo simulado, y es el núcleo dinámico del ejercicio. Finalmente, la **fase de cierre** permite analizar los resultados obtenidos, aplicar instrumentos de evaluación, consolidar observaciones y entregar retroalimentación estructurada a los participantes; sus resultados nutren el informe final del ejercicio.

Adicionalmente, la figura siguiente muestra la relación entre las fases y actividades del juego con las jornadas y tiempos previstos para su desarrollo.

Cronograma de eventos

	Fase	Actividad	Tiempo en minutos	
Jornada 1	**Fase de Preparación del Ejercicio**	Entrenamiento preliminar (FASE 1)	60	
		Descanso	15	
		Entrenamiento preliminar (FASE 2)	60	
		Descanso	15	
		Familiarización con las reglas, tablero y fichas	30	60
		Asignación de roles	10	
		Presentación del escenario	20	
		Total	**210 (3h 30m)**	

	Fase	Actividad	Tiempo en minutos	
Jornada 2	**Fase de Ejecución**	Ronda 0	10	70
		Ronda 1	30	
		Ronda 2	30	
		Descanso	10	
		Ronda 3	30	90
		Ronda 4	30	
		Ronda 5	30	
		Descanso	15	
	Fase de Cierre	Revisión Narrativa y análisis de desempeño	10	45
		Encuesta de evaluación	10	
		Discusión final y retroalimentación cruzada	25	
		Informe de juego de guerra	N/A	
		Total	**230 (3h 50m)**	

A. FASE A – Preparación del ejercicio

Esta fase establece las condiciones necesarias para la ejecución exitosa del juego de guerra.

- **Entrenamiento preliminar**: se realiza una capacitación inicial en la cual se introducen los fundamentos del modelo SERDUX-MARCIM, el contexto de ciberdefensa marítima y las reglas generales del juego. Esto asegura un nivel homogéneo de conocimiento técnico y estratégico entre los participantes.
- **Presentación del escenario**: se expone la narrativa general, incluyendo los actores principales (Objetivo, Atacante, Ciberataque), la red objetivo, y los elementos geopolíticos y tecnológicos del entorno. Se explican las condiciones iniciales, los riesgos latentes y la lógica del modelo computacional.
- **Asignación de roles**: se asignan los roles bajo las consideraciones del Equipo de Juego de Guerra.
- **Familiarización con las reglas, el tablero físico y fichas**: se explican las mecánicas del tablero, las fichas de capacidad, las cartas especiales, y su relación con las variables del modelo.

B. FASE B – Ejecución del juego de guerra

La fase de ejecución de MARCIM-WG se basa en una estructura híbrida que combina un entorno físico —representado por el tablero de juego y sus elementos— con un entorno computacional —sustentado en el modelo de simulación SERDUX-MARCIM—. Esta integración permite que las decisiones estratégicas del jugador generen efectos observables y medibles en una simulación dinámica de crisis cibernética.

El entorno de ejecución está conformado por cinco componentes esenciales: jugadores, facilitador, adjudicador, modelo de simulación y elementos físicos de juego. Cada grupo,

conformado por entre 6 y 10 participantes, desarrolla el ejercicio en una sala independiente con acceso completo a los elementos del juego, bajo la guía directa del facilitador y el adjudicador.

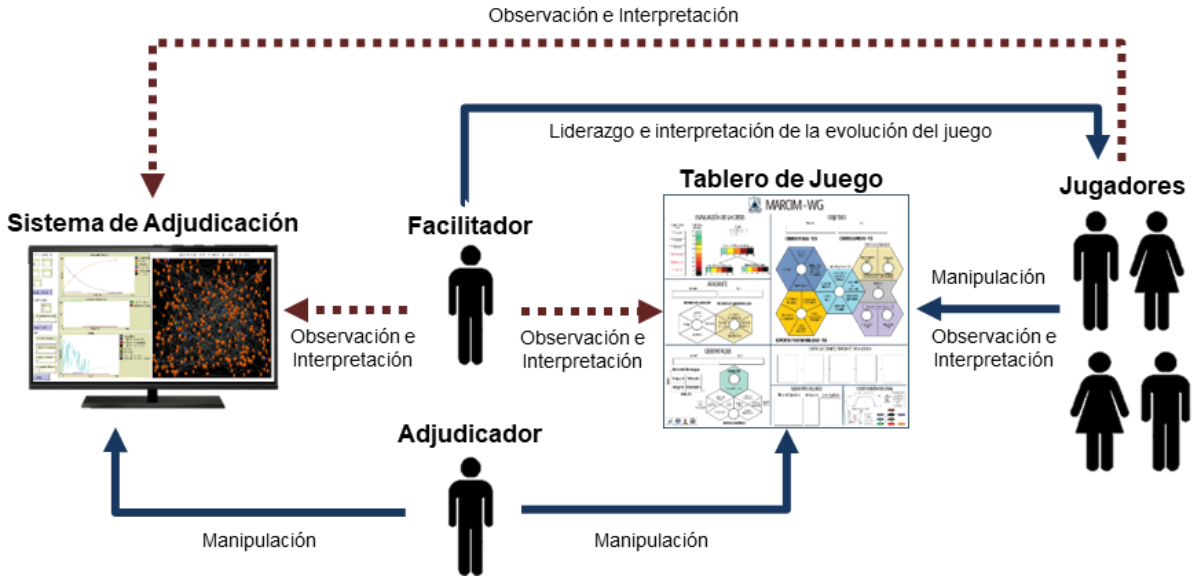
El juego se desarrolla en cinco rondas secuenciales, que simulan la evolución progresiva de una crisis cibernética en el ámbito marítimo. Cada ronda representa una fase del conflicto y permite al jugador evaluar el impacto de sus decisiones, reajustar su estrategia y experimentar la lógica causa-efecto del entorno simulado.

El ciclo metodológico de cada ronda sigue la siguiente secuencia:

- El **jugador** analiza el estado del tablero y los resultados del sistema de adjudicación.
- **Toma decisiones estratégicas** con base en las condiciones del escenario y los recursos disponibles (fichas de capacidad, cartas especiales y BitMarCoins).
- El **adjudicador** ingresa las decisiones en el modelo computacional, ejecuta la simulación y actualiza el tablero físico conforme a los resultados obtenidos.
- El **facilitador** interpreta la situación con los jugadores, orienta el análisis y promueve ajustes en las decisiones.

Este ciclo se repite en cada ronda, permitiendo observar la evolución del sistema ante distintos patrones de comportamiento del atacante, niveles de escalamiento y capacidades defensivas. Cada ronda cumple una función específica dentro de la estructura del juego y se desarrolla siguiendo un orden predeterminado que articula toma de decisiones, adjudicación y retroalimentación estratégica.

La figura siguiente ilustra esta dinámica de ejecución, destacando la interacción continua entre el jugador, el tablero, el modelo computacional y los roles de apoyo.



A continuación, se detallan las especificaciones procedimentales y la lógica de ejecución correspondiente a cada ronda.

Ronda 0 – Configuración inicial

La Ronda 0 establece las condiciones de base del ejercicio y alista el entorno simulado para el inicio de la dinámica. Comprende los siguientes pasos:

- **Configuración del entorno de simulación**: el adjudicador inicializa el modelo MARCIM-WG desde el panel de control, configurando el estado base de la red objetivo, el atacante y el ciberataque.
- **Actualización inicial del tablero de juego:** se reflejan en el tablero físico las condiciones iniciales del entorno simulado.
- **Explicación del escenario y apertura formal:** el facilitador presenta el escenario, explica las condiciones iniciales y declara abierta la fase de ejecución.
- Cierre de la ronda.

Rondas 1 a 5 – Iteración estratégica y adaptación

Estas rondas representan la evolución progresiva del ciberataque, el posible deterioro de la red objetivo y la capacidad del jugador para responder estratégicamente. Cada ronda sigue un ciclo operativo estructurado, en el que se articulan la asignación de recursos, la toma de decisiones, la ejecución de la simulación y la retroalimentación de resultados. El procedimiento es el siguiente:

- **Entrega de elementos de juego**: El facilitador entrega a los jugadores un conjunto de fichas de capacidad, que representan cuantitativamente las capacidades defensivas del objetivo. Estas fichas pueden ser distribuidas por el jugador de manera estratégica, considerando el riesgo, la evolución del ciberataque y el impacto operativo. Las fichas se agrupan en tres dimensiones clave: ciberdefensa, ciberinteligencia, soporte y sostenibilidad, y controles de seguridad.

  Adicionalmente, se entregan cartas especiales, diseñadas para introducir eventos inesperados, generar beneficios tácticos o alterar la dinámica del juego. Estas cartas funcionan como mecanismos de fricción que simulan incertidumbre operativa y condiciones de sorpresa estratégica.
- **Toma de decisiones en el tablero de juego**: los jugadores analizan el estado del tablero y definen cómo asignar sus recursos, priorizando dominios estratégicos, activando cartas especiales o gestionando BitMarCoins, con el objetivo de preservar la operatividad de la red y mitigar los efectos del ciberataque.
- **Aplicación de los efectos de las cartas especiales en el tablero de juego**: el facilitador verifica que se cumplan las condiciones de activación de las cartas especiales y aplica sus efectos en el tablero, ajustando los estados del sistema según lo indicado por cada carta.

- **Ingreso de decisiones en el simulador**: el adjudicador transfiere al modelo computacional las decisiones reflejadas en el tablero, actualizando la configuración interna del simulador conforme a las acciones del jugador.
- **Simulación**: se ejecuta la simulación mediante sistema de adjudicación, lo que genera nuevas salidas que reflejan el impacto de las decisiones frente a la evolución del ciberataque.
- **Actualización del tablero de juego:** los resultados del modelo —como el estado de los nodos (SERDUX), el nivel de disponibilidad de servicios, y la evaluación del riesgo— se representan de forma visual y tangible en el tablero mediante fichas, marcadores y elementos gráficos.
- **Interpretación y retroalimentación:** el facilitador presenta e interpreta los resultados de la simulación ante los jugadores, estimulando la reflexión estratégica y la discusión colectiva para preparar la siguiente ronda.
- **Cierre de la ronda:** se da por finalizada la iteración, permitiendo un breve espacio para ajustes antes del inicio de la siguiente fase.

C. FASE C – Cierre y evaluación

La fase final tiene como propósito sintetizar los aprendizajes, evaluar la efectividad del ejercicio y recoger percepciones de los participantes. Incluye:

- **Revisión narrativa y análisis del desempeño**: el facilitador reconstruye la progresión de eventos y el desempeño del jugador en función los resultados y las decisiones tomadas.
- **Instrumento de evaluación**: se aplica un instrumento de evaluación estructurado que mide el desarrollo de competencias en los niveles de CSA (percepción, comprensión

y proyección), así como el grado de satisfacción con el ejercicio, la claridad del modelo y la relevancia del escenario.

- **Discusión final y retroalimentación cruzada**: se discuten las decisiones críticas tomadas, los errores cometidos y los aciertos estratégicos, cerrando con recomendaciones para futuras versiones del juego y posibles mejoras del modelo.
- **Informe del Juego de Guerra:** este informe contendrá los hallazgos clave del ejercicio y será entregado al patrocinador y demás partes interesadas.

IX. Información adicional de uso exclusivo del Facilitador y Adjudicador

A. Proceso detallado de la fase de ejecución de MARCIM-WG

		Jugador	Facilitador	Adjudicador	Mod. Comp.	Tiempo en minutos
RONDA 0 - CONFIGURACIÓN INICIAL						
	Configuración del entorno de simulación			X		**5**
	1. CONDICIONES INICIALES			X	X	
	2. CONFIGURACIÓN			X	X	
	Actualización del tablero de juego con las condiciones iniciales			X		
	Apertura del juego y explicación del escenario		X			**5**
RONDA 1 A 5					**Total**	**10**
	Entrega de elementos de juego (8 fichas por ronda - 03 BMC - 13 Cartas Especiales)		X			**3**
	Toma y ejecución decisiones en el tablero	X				**15**
	Cartas (Acciones) Especiales	X				
	Aplicación de Cartas Especiales en el Tablero			X		**5**
	Aplicación del estado del tablero en el simulador			X	X	
	Ronda 1 a 5			X	X	
	2. CONFIGURACIÓN			X	X	
	3. EJECUTAR			X	X	
	Actualización del tablero de juego con los resultados de la simulación			X		
	Interpretación de la situación actual del escenario (Resultados Simulación)		X			**7**
	Cierre de la Ronda		X			
					Total	**30**

B. Información del Ciberataque y Pago del *Ransomware*.

En las decisiones de ciberataque y pago del *Ransomware* se lanzan dos dados y la suma de ellos define si fue efectiva o no la decisión. En este sentido si la suma es mayor o igual que el rango de probabilidad establecido se aplica el beneficio.

Ciberataque	• El jugador hace mención del uso de la carta (por hasta dos veces) • Lanzamiento de los dados por el jugador • Si la suma de los dados se encuentra entre 2 y 6 el ciberataque es exitoso.
Pago del *Ransomware*	• El jugador hace mención del uso de la carta • Lanzamiento de los dados por el jugador • Si la suma de los dados se encuentra entre 7 y 12 el ciberataque es exitoso.

Suma	Probabilidad	Casos
2	1/36	(1-1)
3	2/36	(1-2) (2-1)
4	3/36	(1-3) (2-2) (3-1)
5	4/36	(1-4) (2-3) (3-2) (4-1)
6	5/36	(1-5) (2-4) (3-3) (4-2) (5-1)
7	6/36	(1-6) (2-5) (3-4) (4-3) (5-2) (6-1)
8	5/36	(2-6) (3-5) (4-4) (5-3) (6-2)
9	4/36	(3-6) (4-5) (5-4) (6-3)
10	3/36	(4-6) (5-5) (6-4)
11	2/36	(5-6) (6-5)
12	1/36	(6-6)

Ciberataque
(2 a 5)
(Probabilidad: 41.6%)

Pago
Ransomware
(6-10)
(Probabilidad: 58.3 %)

C. Información uso de cartas especiales

Cartas (Acciones) Especiales	1	2	3	4	5	6	7	8	9	10	11	12
	Planeación y preparación	Detección y Reporte (Interno)	Evaluación y Análisis del Incidente	Declaración de la Crisis	Cooperación	Plan de Recuperación de Desastres	Plan de Continuidad del Negocio	Ciberataque	Pago del Ransomware	Reporte del Incidente	Revisión	Mejora
ISO 27035:2023	Planeación y Preparación	Detección y Reporte	Evaluar y Decidir		Responder						Lecciones Aprendidas	
EVOLUCIÓN DE LA CRISIS	Etapa Estable	Precrisis		Crisis						Poscrisis		Etapa Estable
RONDA EN EL JUEGO	1	2		3		4				5		

	Total Fichas	Asignación de fichas de capacidad por uso de cartas en la ronda correcta										
CAPACIDADES-OBJETIVO												
capacidades-ciberdefensa-obj-TCD	**5**		1	1		1	1					1
capacidades-soporte-sostenibilidad-obj-TSS	**5**		1		1	1				1		1
capacidades-ciberinteligencia-obj-TCI	**5**		1	1	1	1					1	
CONTROLES SEGURIDAD - OBJETIVO												
controles-compensatorios-obj-CCM	**2**	1						1				
controles-disuasorios-obj-CDE	**2**	1				1						
controles-detectivos-obj-CDV	**3**	1					1					1
controles-preventivos-obj-CPR	**3**	1						1				1
controles-correctivos-obj-CCR	**3**	1					1				1	
ATACANTE												
factores-atacante-ATF								-2	-3			
vulnerability-factors-VUF									-3			
CIBERATAQUE												
grado-ciberataque-ADE								-2	-3			
duracion-ciberataque-ADU								-1	-3			

Total Fichas	28
En juego	40
Venta 03 BMC (Tasa Máxima)	15
Total fichas en juego	83

BITMARCOINS (BMC) - TASAS DE CAMBIO FACILITADOR				
RONDA	**2**	**3**	**4**	**5**
COMPRA / VENTA AL JUGADOR	2	3	4	5

Ciberataque CA	Pago del Ransomware
CAP. OBJ > 3 01 BMC X CA	03 BMC
02 CA	01 Pago R.
Estas cartas se pueden usar en cualquier ronda	

Requerimientos

D. Planilla de registro de juego.

USO CARTAS ESPECIALES												
CARTA (ACCIÓN) ESPECIAL	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
	Planeación y preparación	**Detección y Reporte (Interno)**	**Evaluación y Análisis del Incidente**	**Declaración de la Crisis**	**Cooperación**	**Plan de Recuperación de Desastres**	**Plan de Continuidad del Negocio**	**Ciberataque**	**Pago del Ransomware**	**Reporte del Incidente**	**Revisión**	**Mejora**
Fase en la ISO 27035:2023	**Planeación y Preparación**	**Detección y Reporte**	**Evaluar y Decidir**		**Responder**						**Lecciones Aprendidas**	
Etapa Crisis	**Etapa Estable**	**Precrisis**		**Crisis**						**Poscrisis**		**Etapa Estable**
Ronda	**1**	**2**		**3**		**4**				**5**		
Selección												

DISTRIBUCIÓN DE FICHAS PARA ENTRAR A LA SIMULACIÓN DE LA RONDA												
	Entrada Simula. Ronda	**1**		**2**		**3**		**4**		**5**		**Total**
	Origen Fichas	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	**Fichas Entregadas**	**Cartas Especiales**	
Capacidades	**TCD**											
	TSS											
	TCI											
Controles	**CCM**											
	CDE											
	CDV											
	CPR											
	CCR											
Total												
Observaciones												

Fuente: elaboración propia.

X. GLOSARIO

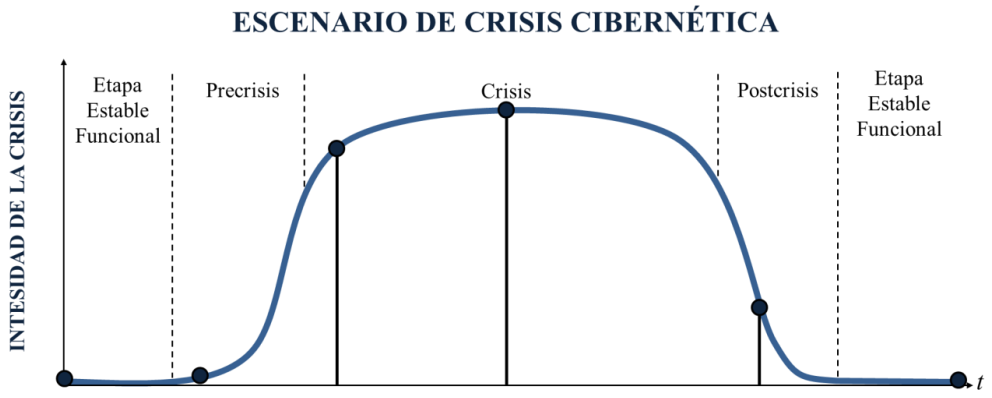
Concepto	Definición
Crisis	Un acontecimiento crítico y a menudo inesperado que amenaza los principales objetivos y operaciones de una organización, requiriendo una toma de decisiones inmediata y estratégica para mitigar los impactos negativos.
Infraestructuras críticas	Sistemas y activos, ya sean físicos o virtuales, que son tan vitales para una nación, de modo que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador sobre la economía nacional, la salud pública, la seguridad nacional, o cualquier combinación de estas cuestiones.
Ciberdefensa	Capacidad organizada y preparada para luchar en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia.
Ciberseguridad	Proceso de protección de la información mediante la prevención, detección y respuesta a los ataques.
Evento sobre ciberseguridad	Un cambio en las condiciones de ciberseguridad que pueda afectar las operaciones de la organización (incluida la misión, las capacidades o la reputación).
Incidente de ciberseguridad	Un suceso de ciberseguridad que se ha determinado que afecta a una organización y que requiere acciones de respuesta y recuperación. Un ciberataque implica generalmente un conjunto de incidentes cibernéticos coordinados y correlacionados.
Ciberespacio	Entorno digital en el que las comunicaciones tienen lugar a través de redes informáticas.
Ciberarma	Software diseñado para causar daños o efectos perjudiciales hacia un elemento del ciberespacio, con la posibilidad de tener consecuencias en el entorno físico.
Ciberataque	El uso deliberado de una ciberarma, por una persona o de forma automática, para causar daños o efectos perjudiciales a un elemento del ciberespacio de un adversario, que pueda tener efectos indirectos en las áreas de operaciones convencionales.
Conciencia cibernética	El conocimiento de los elementos y acontecimientos del ciberespacio en un momento dado, la explicación de su significado y la proyección de su estado.
Ciberriesgos	La probabilidad de que una amenaza cibernética explote una vulnerabilidad, causando daños hacia un activo que tiene un cierto valor y criticidad.
Ciberamenaza	Una fuente potencial de daños externos o internos hacia los activos digitales de una organización.
Malware	Software diseñado para interrumpir, dañar u obtener acceso no autorizado a un sistema informático.
Ransomware	Un *malware* que bloquea permanentemente el acceso a los datos de la víctima a menos que se pague un rescate.

Anexo 2. Escenario del juego de guerra MARCIM-WG.

ESCENARIO MARCIM-WG

I. Introducción

El escenario descrito a continuación es completamente ficticio y ha sido diseñado con fines académicos en el contexto de la ciberdefensa marítima. Su configuración busca que el jugador, mediante la toma de decisiones estratégicas, alcance los objetivos establecidos en el juego. La simulación está estructurada para representar la evolución de una crisis cibernética que afecta a un actor marítimo, atravesando las fases de estabilidad funcional, precrisis, crisis, postcrisis y retorno a la estabilidad, como se muestra en la siguiente figura. No obstante, el desarrollo del escenario dependerá directamente de las decisiones adoptadas por el jugador, pudiendo incluso mantenerse en estado de crisis si las acciones resultan ineficaces. A continuación, se detallan los elementos que conforman el escenario.



II. Contexto temporal, geografía y entorno

AMERIX es uno de los catorce países que conforman la América Insular en el mar Caribe. Está constituido por una isla principal de 230 km de largo por 90 km de ancho, ubicada estratégicamente en el Golfo de México, con cercanía geográfica a Estados Unidos, México y Cuba. **Su capital es Amer**, un nodo logístico y comercial fundamental en la región.

Gracias a su privilegiada ubicación geoestratégica y su elevado nivel de desarrollo portuario —con dos mega puertos al norte y al sur de la isla— AMERIX se ha consolidado como un "**Centro de Operaciones Logístico Regional**", articulando el tránsito marítimo de mercancías de alto valor estratégico para el continente. Esta posición ha traído consigo grandes oportunidades económicas, pero también crecientes amenazas en el dominio marítimo y cibernético.

Las **Fuerzas Militares de AMERIX** cuentan con un alto componente tecnológico en las áreas de Comando, Control, Comunicaciones e Inteligencia (C3I). Su principal fuerza es la Marina de Guerra, considerada de tamaño mediano, pero con proyección regional. A pesar de estos avances, existe una desconexión crítica entre el desarrollo tecnológico y la protección cibernética: la ciberdefensa no ha sido integrada de forma efectiva en la doctrina ni en la estrategia de defensa.

Uno de los principales activos operacionales de AMERIX es **LINKAMERIX**, una red táctica de enlace de datos militares interoperable con sistemas de información propios, aliados y externos. Aunque esta red potencia las capacidades de coordinación multinacional y despliegue de fuerza, su alta conectividad la convierte en un vector de ataque crítico. En particular, su integración con sistemas de armas, plataformas SCADA, sistemas logísticos y de comando embarcados en buques de guerra incrementa la superficie de ataque y compromete su resiliencia cibernética.

En el último año, se han registrado comportamientos anómalos en las redes militares —normalizados como incidentes menores— y se ha identificado un aumento significativo en la exposición a vectores de amenaza persistente avanzada (APT), lo cual anticipa una posible crisis cibernética de gran escala.

Situación base – Etapa estable funcional

A raíz del posicionamiento geoestratégico de AMERIX y su consolidación como potencia marítima regional, las tensiones diplomáticas con el Estado-nación **ADVERSARIX** han escalado rápidamente. Las divergencias se centran en la explotación de recursos marítimos y el control de rutas comerciales críticas, exacerbadas por acusaciones cruzadas en escenarios multilaterales. ADVERSARIX ha denunciado que AMERIX representa una amenaza económica regional y la responsabiliza de provocar una crisis comercial sin precedentes al concentrar de forma desproporcionada el flujo de mercancías por sus puertos y aguas jurisdiccionales.

En este ambiente hostil, los servicios de inteligencia de AMERIX han detectado señales de preparación de un ciberataque coordinado a gran escala contra su principal fuerza naval, con la intención de paralizar capacidades críticas y desestabilizar el equilibrio estratégico en el mar Caribe. Se ha identificado que el grupo atacante conocido como **PIGCYB (APT390)** estaría detrás de esta operación, con apoyo financiero y logístico directo de ADVERSARIX.

III. Objetivo

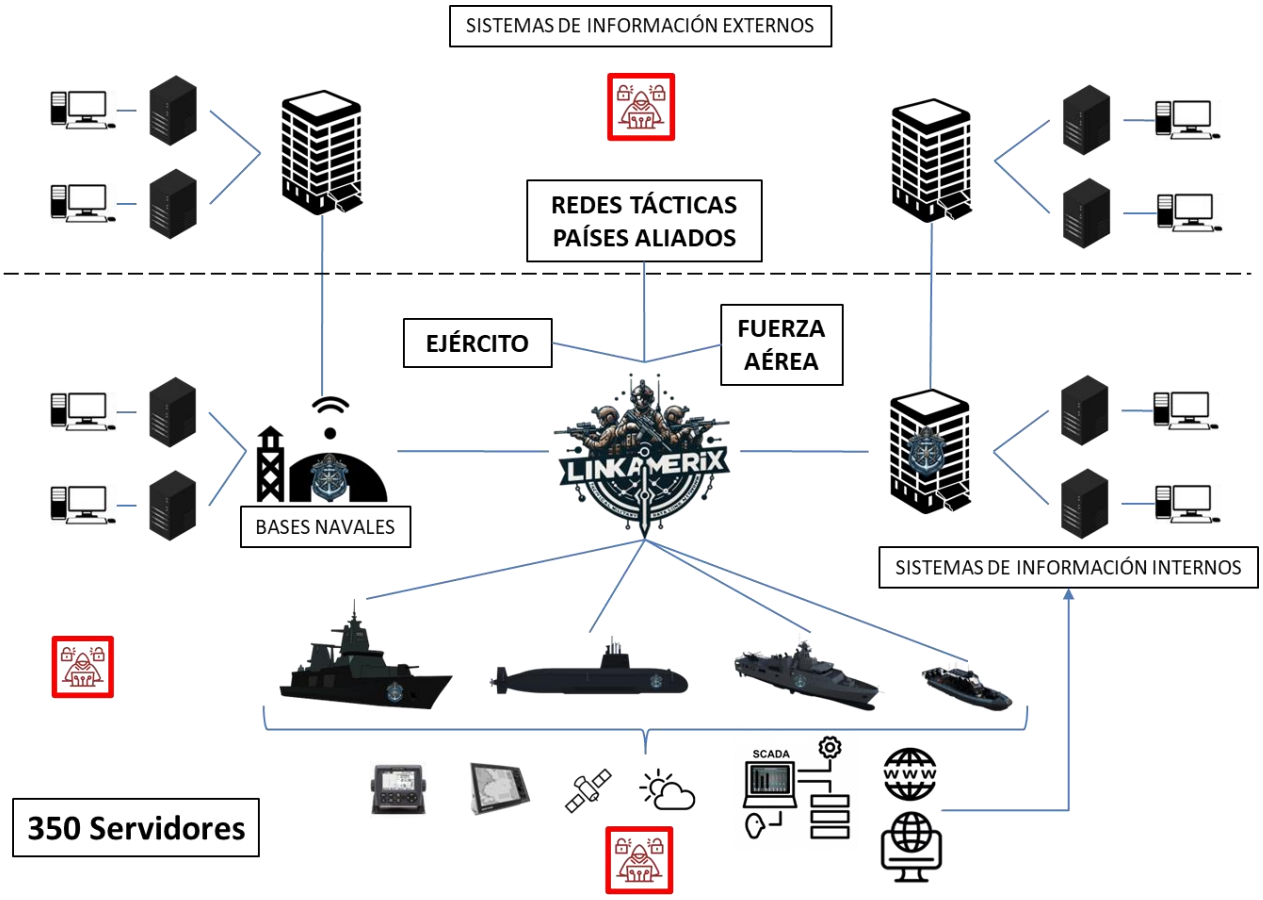
Marina de guerra de AMERIX

La Marina de Guerra de AMERIX constituye el componente central de sus Fuerzas Armadas y es la encargada de garantizar la seguridad del entorno marítimo, proteger las Líneas de Comunicación Marítima (LCM) y combatir amenazas transnacionales en la región. Cumple funciones clave en la lucha contra la piratería, la migración irregular, la pesca ilegal, el narcotráfico, la explotación ilícita de recursos marítimos, y el tráfico de armas, municiones y explosivos. Su efectividad operacional ha generado reconocimiento internacional, siendo frecuente la participación de sus unidades en operaciones navales combinadas con países aliados.

No obstante, la Marina enfrenta desafíos estratégicos relacionados con su **madurez cibernética institucional**. A pesar de contar con una red de plataformas altamente interconectadas y con desarrollos tecnológicos en C3I, **no se considera la ciberseguridad como eje estructural de su doctrina operativa**, lo que genera una marcada vulnerabilidad.

El sistema más crítico bajo su responsabilidad es **LINKAMERIX**, una red táctica interoperable con más de **350 servidores distribuidos**, conectada a sistemas internos y externos, incluyendo bases navales, redes del Ejército y Fuerza Aérea, así como plataformas de países aliados.

Esta red soporta funciones clave en unidades de superficie, submarinos y medios aeronavales. A través de LINKAMERIX se transmiten datos de mando, navegación, sistemas SCADA, redes logísticas, comunicaciones tácticas, inteligencia operativa y sistemas de información transversales, como se observa en la siguiente figura.



Dada esta complejidad y la madurez de la organización, **la seguridad de LINKAMERIX es limitada**. Los buques de guerra de AMERIX —aunque dotados con sistemas TIC modernos— mantienen en sus entornos tecnológicos de operación (TO) **sistemas operativos antiguos, sin soporte técnico vigente**, lo cual ha expuesto a los servidores y terminales de combate a vulnerabilidades críticas ampliamente documentadas.

Asimismo, la red mantiene conexiones activas con múltiples sistemas de información de terceros, incluidos proveedores externos, sistemas SCADA navales y módulos de interoperabilidad. Esto no solo aumenta la superficie de ataque, sino que dificulta los procesos de trazabilidad y contención ante incidentes avanzados.

En síntesis, **la Marina de Guerra de AMERIX es tecnológicamente capaz pero estratégicamente expuesta**, enfrentando una creciente dependencia digital sin un blindaje cibernético equivalente. Esta asimetría entre sofisticación operativa e inmadurez ciberdefensiva la convierte en un blanco de alto valor para amenazas persistentes avanzadas, como las promovidas por actores tipo Estado-Nación.

Teniendo en cuenta lo anterior, la siguiente tabla resume las características y situación de la red del objetivo para el momento de la precrisis.

Característica	Valor
Total de nodos en la red objetivo	**350**
Nodos susceptibles	300
Nodos expuestos	40
Nodos degradados	10
Nodos no disponibles	0
Nodos destruidos	0
Ciber riesgo	Bajo
Probabilidad de ciberataque	Medio
Impacto ciberataque	Bajo
Capacidades	10%
Controles	10%

IV. Atacante

APT390 - PIGCYB

Con base en análisis de inteligencia, se presume con alta probabilidad que el grupo de Amenaza Persistente Avanzada **APT390**, conocido operativamente como **PIGCYB**, es el actor responsable de la operación cibernética que se estaría gestando contra la Marina de Guerra de AMERIX. Este grupo ha sido vinculado reiteradamente a campañas cibernéticas de naturaleza ofensiva en el continente americano, y se le atribuye una relación estrecha con el Estado-nación **ADVERSARIX**, que lo emplearía como instrumento de proyección estratégica indirecta en el ciberespacio.

APT390/PIGCYB ha concentrado su accionar en sectores relacionados con la **defensa, la industria marítima, y las tecnologías operacionales (TO)**, dirigiendo campañas de vigilancia, acceso persistente y, en algunos casos, de interrupción o degradación funcional. Sus capacidades incluyen tanto herramientas de exfiltración y reconocimiento como técnicas avanzadas de intrusión que comprometen servidores críticos y plataformas de comunicación interoperables.

La actividad histórica del grupo revela un patrón de acciones orientadas a:

- Obtener información operativa y de inteligencia de valor geopolítico.
- Interferir con la estabilidad institucional o militar de sus objetivos.

- Preparar el entorno técnico para ataques de mayor envergadura, incluyendo operaciones destructivas o de denegación prolongada.
- Entre las tácticas y técnicas asociadas a APT390 se encuentran:
- Campañas de ***spearphishing*** con archivos adjuntos maliciosos y enlaces disfrazados, usando cuentas previamente comprometidas para ganar legitimidad.
- Registro y uso de **dominios falsificados** que imitan plataformas del sector marítimo.
- Explotación de **servidores web vulnerables** donde instalan *web shells* para mantener persistencia.
- Uso de **credenciales legítimas robadas** para acceder a servicios como Outlook o a redes internas de entidades del sector naval.

Aunque no se ha confirmado de manera concluyente su autoría, la combinación de las evidencias técnicas, el patrón de comportamiento, el interés estratégico demostrado por el grupo, y el contexto diplomático actual, permiten **considerar altamente probable que PIGCYB esté detrás de una campaña cibernética en curso o en preparación**, dirigida contra AMERIX, con objetivos de impacto estratégico en su entorno marítimo, tecnológico y militar.

Teniendo en cuenta lo anterior, la siguiente tabla resume las características y situación estimada del Atacante para el momento de la precrisis.

Característica	Valor
Factores del atacante	40%
Factores de vulnerabilidad	40%

V. Ciberataque

Según informes de inteligencia técnica y cibernética recopilados por agencias aliadas y capacidades propias de contrainteligencia, existe una alta probabilidad de que se esté preparando un ciberataque avanzado de múltiples fases contra la Marina de Guerra de AMERIX. El análisis de indicadores técnicos y patrones de actividad en redes asociadas al sector marítimo sugiere que la operación estaría siendo gestada por el grupo APT390, también conocido como PIGCYB, el cual ha sido vinculado históricamente con ataques al sector defensa y marítimo en América.

El ataque se prevé altamente sofisticado, dirigido a explotar vulnerabilidades ya conocidas en sistemas de Tecnologías de la Información (TI) y Tecnologías de la Operación (TO) embarcadas, muchas de las cuales se encuentran desactualizadas o fuera de soporte técnico. Este panorama de riesgo se ve agravado por el uso de sistemas interoperables con terceros, la elevada conectividad de la red LINKAMERIX, y la presencia de múltiples accesos no controlados.

Se presume que el ataque seguiría un enfoque por fases:

- **Acceso inicial:** mediante técnicas de *spearphishing* con documentos maliciosos y enlaces camuflados, distribuidos desde cuentas de correo previamente comprometidas. Además, APT390 ha sido observado utilizando dominios falsos que imitan organizaciones navales legítimas, explotando así la confianza institucional.
- **Persistencia y reconocimiento:** explotación de servidores web vulnerables en organizaciones asociadas, donde instalan *web shells*, junto con el uso de credenciales robadas para comprometer recursos sensibles (plataformas y sistemas).

En caso de activarse, se prevé que el grupo emplearía un ciberataque llamado MALPIG que contiene al menos dos herramientas clave:

- Un *malware* polimórfico especializado en sistemas TO desactualizados. Su objetivo es asegurar persistencia, recopilar datos de infraestructura crítica y comunicaciones, y preparar el entorno para fases destructivas.
- Una ciberarma de tipo *ransomware,* con efectos destructivos confirmados en pruebas anteriores. Al ejecutarse, inutiliza por completo los servidores afectados, eliminando la posibilidad de recuperación si no se paga un rescate. Su activación sobre sistemas como LINKAMERIX o servidores de gestión operativa supondría un riesgo extremo para la continuidad operativa.

Aunque aún no se ha producido una intrusión confirmada, los comportamientos anómalos recientes en la red de AMERIX, la coincidencia con la infraestructura objetivo de campañas anteriores de APT390, y la intensificación de tensiones con ADVERSARIX, justifican una alerta de amenaza inminente, especialmente sobre los nodos críticos de C3I y soporte naval.

La evaluación estima que, si se materializa, el ataque podría degradar significativamente las capacidades operacionales de la Marina de Guerra de AMERIX, comprometiendo su rol como garante de la seguridad marítima regional y afectando su interoperabilidad con aliado.

Teniendo en cuenta lo anterior, la siguiente tabla resume las características y situación estimada del Ciberataque para el momento de la precrisis.

Característica	Valor
Grado del ciberataque	10%
Duración del ciberataque	10%

VI. Evento inicial – Situación detonante

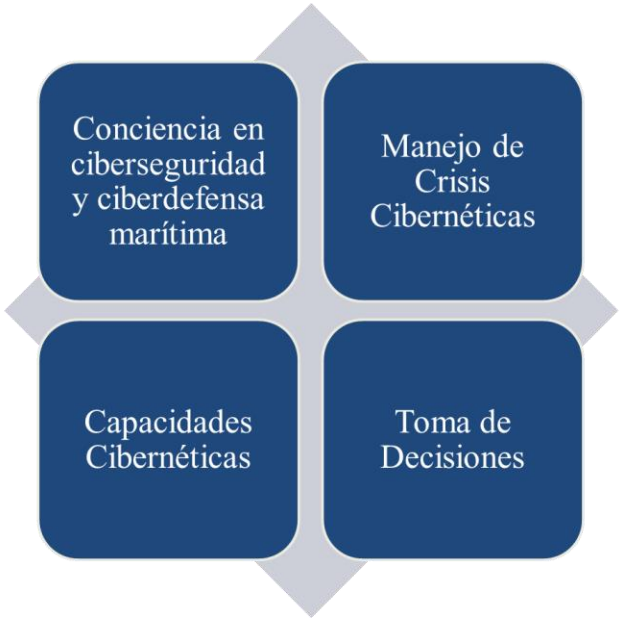
En las últimas 48 horas, la Marina de Guerra de AMERIX ha detectado **una secuencia sostenida de anomalías operacionales** en la red de enlace táctico **LINKAMERIX**, identificadas inicialmente como inconsistencias de comunicación entre nodos navales y bases de comando. Estos eventos, considerados dentro de lo usual por el centro de monitoreo, comenzaron a adquirir patrones repetitivos, afectando la sincronización de datos con aliados y provocando interrupciones intermitentes en los flujos de información táctica.

Simultáneamente, se ha reportado una **actividad inusual en servidores internos conectados a sistemas SCADA**, sensores de control de navegación y sistemas logísticos en unidades navales desplegadas en el sur del país. A través de labores de ciberinteligencia e interoperabilidad con aliados, se obtiene información clasificada que **apunta a una campaña cibernética en preparación por parte de PIGCYB (APT390)**, presuntamente patrocinada por el Estado-nación ADVERSARIX. Aunque no se ha producido un ataque de gran escala, **la probabilidad de ocurrencia es alta y se considera inminente**.

Bajo este panorama de inestabilidad creciente, el Alto Mando Naval de AMERIX declara **alerta cibernética nivel 3**, y convoca a una célula de planeamiento estratégico para coordinar acciones que **eviten la degradación crítica del nivel de servicios** en la infraestructura de defensa marítima nacional.

VII. Objetivo de los jugadores en el escenario

Los jugadores, actuando como asesores estratégicos de la Marina de Guerra de AMERIX, deben analizar el entorno de crisis, interpretar señales tempranas, gestionar las capacidades disponibles y **tomar decisiones tácticas y estratégicas bajo incertidumbre** para garantizar que **el nivel de servicios del sistema LINKAMERIX se mantenga por encima del 70 %** durante la progresión de los eventos. Su desempeño será evaluado en función de su capacidad para prevenir o mitigar el impacto de un ciberataque destructivo en un entorno operacional interconectado, con implicaciones geoestratégicas regionales.



Anexo 3. Registro software MARCIM-WG

DNDA Dirección Nacional de Derecho de Autor
Ministerio del Interior

OFICINA DE REGISTRO

Libro - Tomo - Partida
13-103-397
Fecha Registro
12-May-2025

CERTIFICADO DE REGISTRO DE SOPORTE LOGICO - SOFTWARE

Página 1 de 1

1. DATOS DE LAS PERSONAS

AUTOR

Nombres y Apellidos	DIEGO EDISON CABUYA PADILLA	**No de identificación CC**	80932698
Nacional de	COLOMBIA		
Dirección	CARRERA 16 C # 156-12	**Ciudad:**	BOGOTA D.C.

PRODUCTOR

Nombres y Apellidos	DIEGO EDISON CABUYA PADILLA	**No de identificación CC**	80932698
Nacional de	COLOMBIA		
Dirección	CARRERA 16 C # 156-12	**Ciudad:**	BOGOTA D.C.

2. DATOS DE LA OBRA

Título Original MARCIM-WG
Año de Creación 2025 **País de Origen** COLOMBIA **Año Edición**

CLASE DE OBRA	INEDITA
CARACTER DE LA OBRA	OBRA INDIVIDUAL
CARACTER DE LA OBRA	OBRA DERIVADA
ELEMENTOS APORTADOS DE SOPORTE LOGICO	PROGRAMA DE COMPUTADOR
ELEMENTOS APORTADOS DE SOPORTE LOGICO	DESCRIPCIÓN DEL PROGRAMA

3. DESCRICIPCIÓN DE LA OBRA

ESTE SOFTWARE IMPLEMENTA EN NETLOGO UNA ADAPTACIÓN DEL SOFTWARE SERDUX-MARCIM PARA SU USO EN UN JUEGO DE GUERRA DE CIBERDEFENSA MARÍTIMA LLAMADO MARCIM-WG. EL SOFTWARE SIMULA LA PROPAGACIÓN DE CIBERATAQUES EN INFRAESTRUCTURAS MARÍTIMAS. PERMITE CONFIGURAR ESCENARIOS ESTRATÉGICOS PARA JUEGOS DE GUERRA, PARAMETRIZANDO LA RED, CAPACIDADES DEL OBJETIVO Y ATACANTE, CARACTERÍSTICAS DEL ATAQUE Y LOS PARÁMETROS DEL MODELO, ASÍ COMO VISUALIZAR LOS RESULTADOS MEDIANTE SIMULACIÓN COMPUTACIONAL.

4. OBSERVACIONES GENERALES DE LA OBRA

5. DATOS DEL SOLICITANTE

Nombres y Apellidos	DIEGO EDISON CABUYA PADILLA	**No de Identificación C.C**	80932698
Nacional de	COLOMBIA	**Ciudad**	BOGOTA D.C.
Dirección	CARRERA 16 C # 156-12	**Teléfono**	3115497824
Correo electrónico	DIEGO.CABUYA@GMAIL.COM	**Medio Radicación**	REGISTRO EN LINEA
En representación de	EN NOMBRE PROPIO	**Radicación de entrada**	1-2025-46866

NATHALIE GRANADOS BERMEO
JEFE OFICINA DE REGISTRO

NGB

Descargado a través de www.registroenlinea.gov.co, el 14 de Mayo de 2025 a las 13:02:51

Nota: El derecho de autor protege exclusivamente la forma mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas a las obras . No son objeto de protección las ideas contenidas en las obras literarias y artísticas, o el contenido ideológico o técnico de las obras científicas, ni su aprovechamiento industrial o comercial (artículo 7o. de la Decisión 351 de 1993).

Anexo 4. Explicación entorno visual y código fuente MARCIM-WG.

MARCIM-WG (MODELO COMPUTACIONAL)

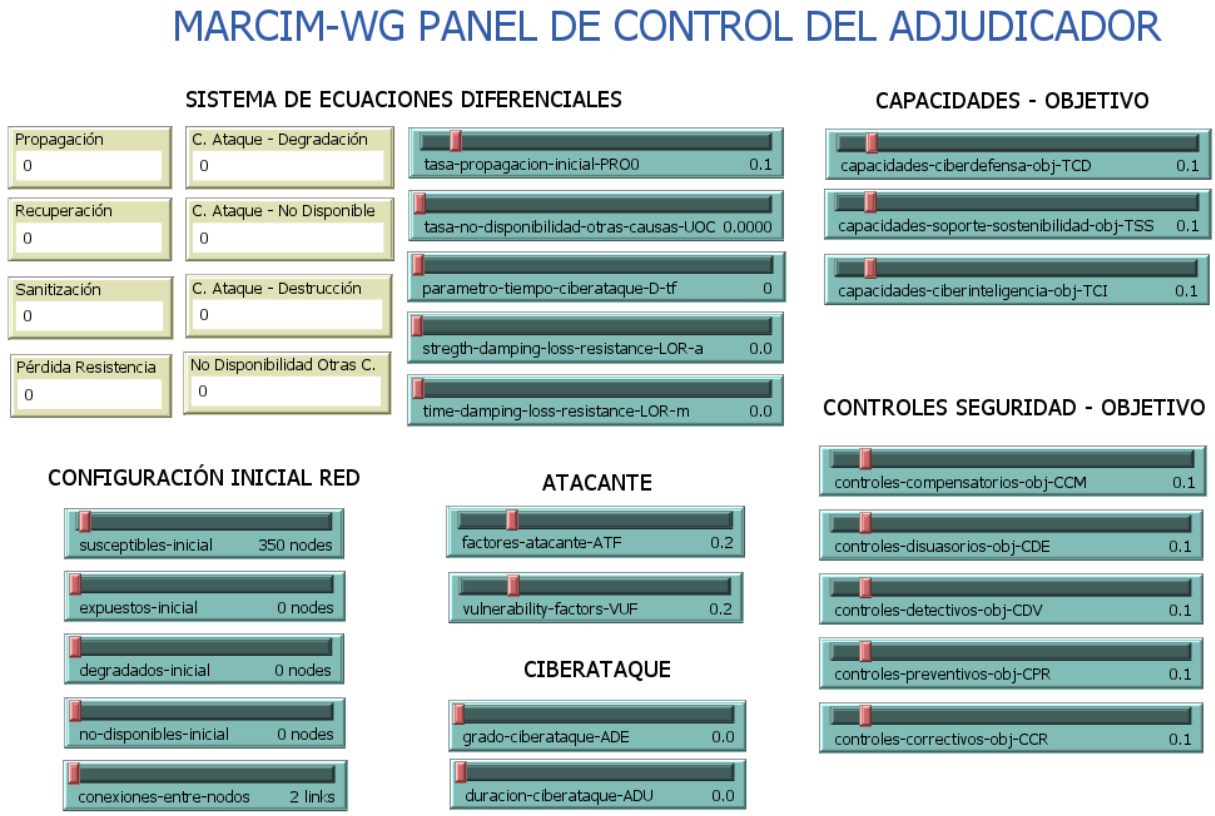
I. Entorno visual

La interfaz de usuario del software MARCIM-WG ha sido diseñada para facilitar la interacción operativa entre el adjudicador, el modelo computacional y el participante del juego de guerra. Se encuentra estructurada en cuatro secciones funcionales principales:

A. Panel de control del adjudicador

En esta sección, el adjudicador configura todos los parámetros necesarios para ejecutar el modelo SERDUX-MARCIM conforme a las condiciones establecidas por el diseño del juego. Este panel está dividido en las siguientes subsecciones (Figura 11):

Figura 11. MARCIM-WG panel de control del adjudicador.



Fuente: elaboración propia utilizando el software Netlogo.

- **SISTEMA DE ECUACIONES DIFERENCIALES:** configuración y control de los valores de las tasas y parámetros iniciales para el sistema de ecuaciones diferenciales.
- **CONFIGURACIÓN INICIAL RED:** configuración del número inicial de nodos en los estados Susceptible (S), Expuesto (E), Degradado (D) y No Disponible (U), junto con el número promedio de conexiones entre nodos.
- **ATACANTE:** Configuración de los factores de atacante y vulnerabilidad.
- **CIBERATAQUE:** Configuración del grado y duración inicial del ciberataque.
- **CAPACIDADES - OBJETIVO:** configuración de las capacidades del objetivo en términos de ciberdefensa, ciberinteligencia y, soporte y sostenibilidad.
- **CONTROLES DE SEGUIRDAD - OBJETIVO:** configuración de los controles de seguridad del objetivo: compensatorios, disuasorios, detectivos, preventivos, y correctivos
- **SISTEMA DE ECUACIONES DIFERENCIALES:** permite configurar las tasas de transición y parámetros técnicos requeridos para la solución del sistema diferencial que gobierna el comportamiento dinámico del modelo.
- **CONFIGURACIÓN INICIAL RED:** define el número inicial de nodos en los estados Susceptible (S), Expuesto (E), Degradado (D) y No Disponible (U), así como el número promedio de conexiones entre nodos dentro de la red objetivo.
- **ATACANTE:** establece los factores asociados al atacante y las condiciones de vulnerabilidad del objetivo.
- **CIBERATAQUE:** permite definir el grado (Ψ) y duración (δ) del ciberataque.
- **CAPACIDADES - OBJETIVO:** configura los niveles de capacidad en tres aspectos principales del objetivo:

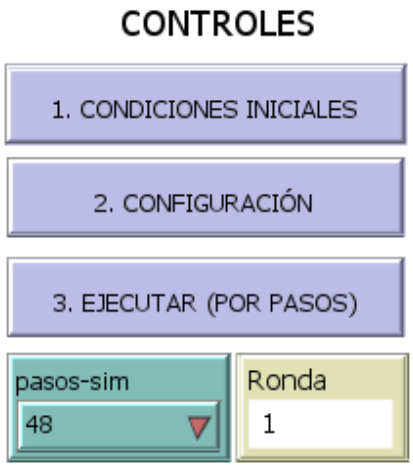
  - Ciberdefensa (TCD),
  - Ciberinteligencia (TCI), y
  - Soporte y sostenibilidad (TSS).

- **CONTROLES DE SEGURIDAD - OBJETIVO:** permite configurar la presencia y nivel de cinco tipos de controles: correctivos, preventivos, detectivos, disuasorios y compensatorios, todos los cuales influyen directamente en la capacidad del objetivo para resistir, responder o mitigar un ciberataque.

B. Controles de la simulación

Esta sección agrupa los controles que permiten la ejecución operativa del modelo. Incluye los siguientes botones y campos (Figura 12):

Figura 12. MARCIM-WG panel de control de la simulación.



Fuente: elaboración propia utilizando el software Netlogo.

- **CONDICIONES INICIALES**: carga una parametrización por defecto adecuada para iniciar una nueva simulación.
- **CONFIGURACIÓN**: registra los valores establecidos en el *PANEL DE CONTROL DEL ADJUDICADOR* y configura los módulos de ejecución del software. En la primera ejecución, inicializa el entorno de Python en segundo plano.

- **EJECUTAR (POR PASOS)**: lanza la simulación por un número determinado de pasos, definidos por el campo "pasos-sim". La ejecución se detiene cuando se cumpla al menos una de las condiciones de parada predefinidas:
  - Todos los nodos están en estado *S*, *E* o *R*.
  - Todos los nodos están en estado *D*, *U* o *X*.
- **pasos-sim**: define el número de pasos por ejecutar en la simulación.
- **Ronda**: registra el número de ronda ejecutada en el marco del juego de guerra.

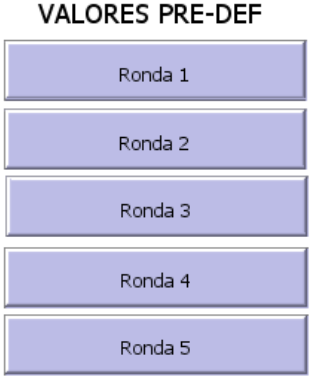
C. Escenario predefinido para el juego de guerra

Esta sección permite cargar configuraciones específicas del modelo que representan situaciones prediseñadas por el Director del Juego de Guerra. Está compuesta por dos bloques funcionales:

VALORES PRE-DEF (Valores predefinidos)

Incluye cinco botones que, al ser activados, cargan en el *PANEL DE CONTROL DEL ADJUDICADOR* valores determinados por la narrativa y estructura del escenario diseñado para el juego de guerra. Cada botón (Ronda #) se utiliza al inicio de una ronda particular y debe ser seguido de la ejecución del botón *EJECUTAR (POR PASOS)* para que la simulación procese dicha configuración y genere los resultados correspondientes (Figura 13).

Figura 13. MARCIM-WG panel de valores predefinidos del escenario.

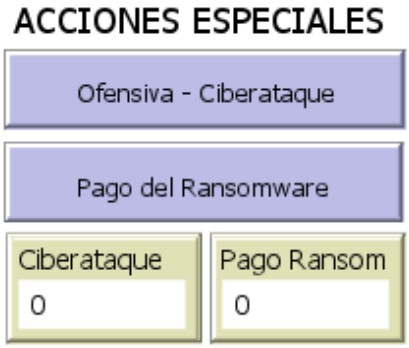


Fuente: elaboración propia utilizando el software Netlogo.

ACCIONES ESPECIALES

Este bloque contiene dos botones que representan eventos especiales dentro de la narrativa del juego de guerra (Figura 14):

Figura 14. MARCIM-WG panel de acciones especiales.



Fuente: elaboración propia utilizando el software Netlogo.

- **Ofensiva – Ciberataque:** al activarse, modifica automáticamente ciertos parámetros del modelo, incrementando la agresividad del atacante o introduciendo condiciones críticas adicionales para el objetivo.
- **Pago del *Ransomware*:** simula la decisión estratégica del objetivo de pagar un rescate ante un ciberataque tipo *ransomware*, lo cual altera determinados valores defensivos o de sostenibilidad de la red.

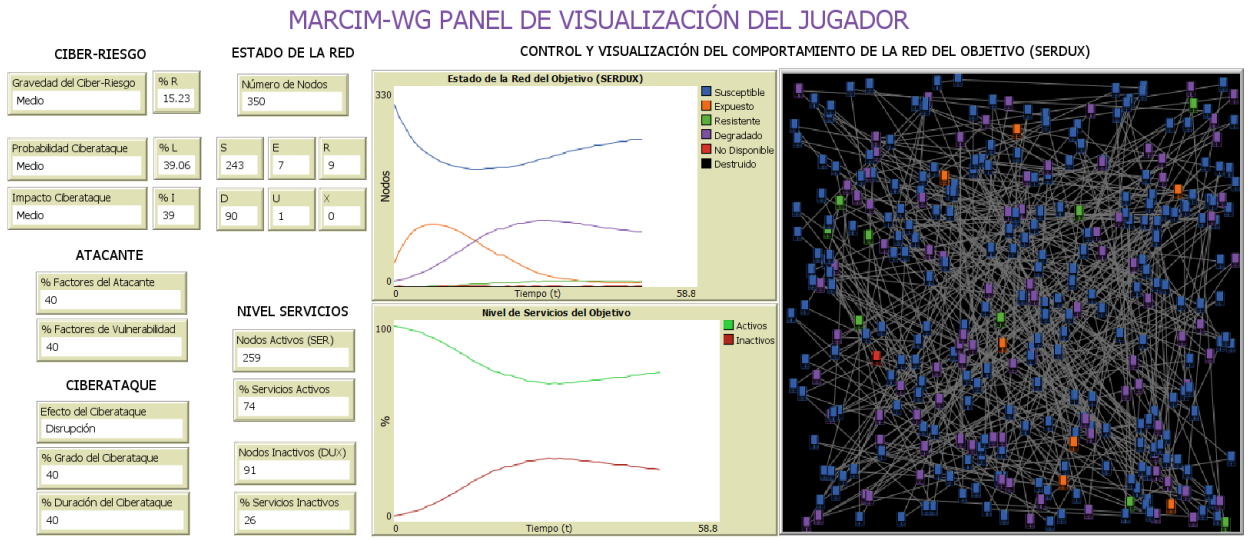
Indicadores de activación:

- **Ciberataque:** variable que indica si la acción de ofensiva cibernética ha sido activada (valores: 0 = no activado, 1 o 2 = activado una o más veces).
- **Pago *Ransom*:** variable que refleja si se ha activado la acción de pago del *ransomware* (valores: 0 = no activado, 1 = activado).

D. Panel de visualización del jugador

Este panel proporciona al participante del juego una representación gráfica y numérica del estado de la simulación, permitiendo monitorear la evolución del ciberataque y evaluar los efectos de sus decisiones. Está compuesto por las siguientes subsecciones (Figura 15):

Figura 15. MARCIM-WG panel de visualización del jugador.



Fuente: elaboración propia utilizando el software Netlogo.

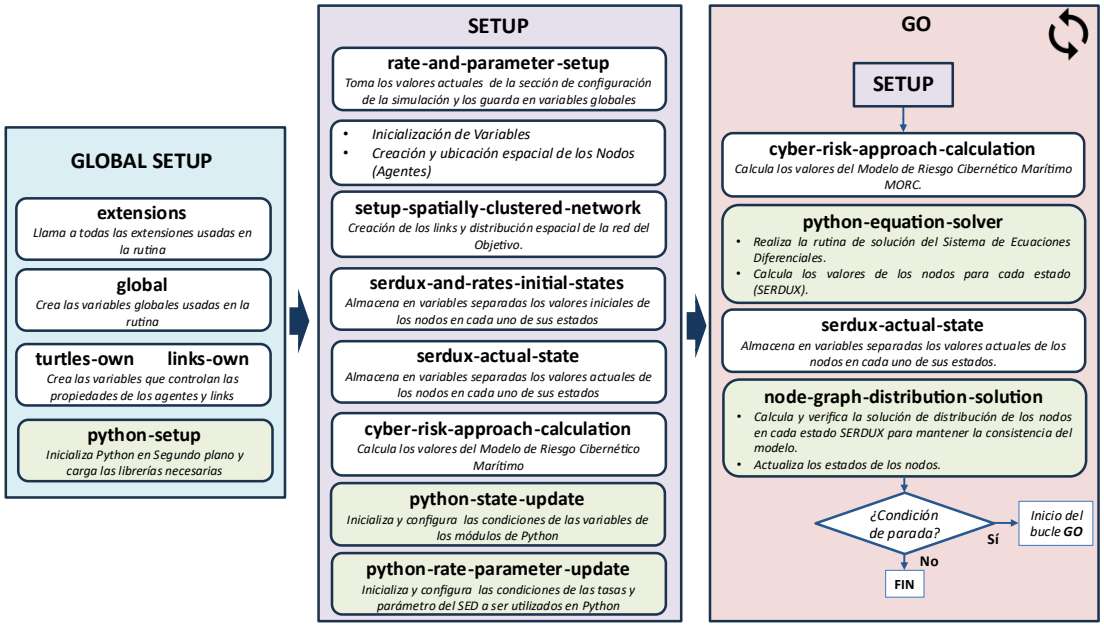
- **CIBER-RIESGO**: muestra los porcentajes y resultados de la evaluación de riesgo cibernético conforme al enfoque propuesto en SERDUX-MARCIM, incluyendo las variables de probabilidad, impacto y gravedad del riesgo.
- **ESTADO DE LA RED**: presenta el número total de nodos en la red y su distribución actual entre los seis estados del modelo SERDUX (S, E, R, D, U, X), con visualización gráfica en el tiempo.
- **NIVEL DE SERVICIOS**: grafica la proporción de nodos activos (estados S, E, R) frente a los inactivos (estados D, U, X), y su evolución a lo largo de la simulación.
- **ATACANTE**: permite visualizar los valores actuales de los factores del atacante y de vulnerabilidad.
- **CIBERATAQUE**: muestra los valores actuales de grado y duración del ciberataque en curso.

- **CONTROL Y VISUALIZACIÓN DE LA RED DEL OBJETIVO (SERDUX)**: ofrece una representación gráfica dinámica de la red de nodos y sus interconexiones, permitiendo observar el cambio de estado individual de cada nodo a lo largo del tiempo, con códigos de color diferenciados por estado.

II. Código Fuente

El flujo general del código, organizado por bloques y módulos, se muestra en la Figura 16. Esta figura representa la adaptación funcional del código del modelo SERDUX-MARCIM (Cabuya Padilla, 2024; D. Cabuya-Padilla, Díaz-López, Martínez-Páez, et al., 2025) orientada específicamente a los requerimientos del entorno simulado de MARCIM-WG.

Figura 16. Estructura del código de programación.



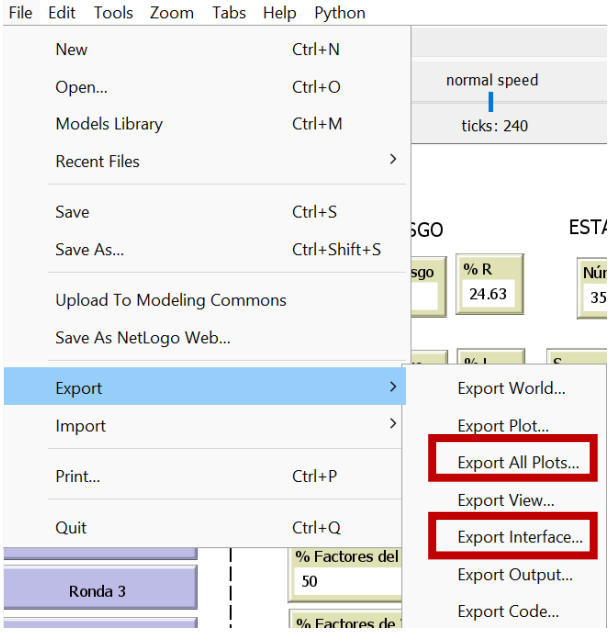
Fuente: elaboración propia basado (Cabuya Padilla, 2024).

El código fuente del software se organiza en tres bloques funcionales principales: GLOBAL SETUP, SETUP y GO. Cada uno de estos bloques agrupa un conjunto de rutinas identificadas por su nombre en el código (resaltado en negrilla), acompañado de una descripción general de su propósito. Las rutinas desarrolladas directamente en NetLogo están representadas en color blanco, mientras que las ejecutadas en segundo plano mediante Python aparecen en verde.

El bloque GLOBAL SETUP se encarga de la inicialización de las variables globales y parámetros propios del entorno de NetLogo, así como de la preparación de los procesos auxiliares que se ejecutan en Python. El segundo bloque, SETUP, establece las condiciones iniciales de la simulación. En esta etapa se generan los nodos (agentes) y los enlaces de red (links), de acuerdo con los valores definidos por el experimentador en la interfaz. Además, se realiza el cálculo inicial del Modelo de Riesgo Cibernético Marítimo, y se preparan todos los componentes necesarios para la ejecución posterior del sistema de ecuaciones diferenciales en Python. El bloque GO ejecuta el bucle principal de la simulación, que puede configurarse para un número fijo de iteraciones o hasta que se cumplan las condiciones de parada preestablecidas. Posteriormente, se recalcula el riesgo cibernético y se resuelve el Sistema de Ecuaciones Diferenciales (SED) utilizando el método numérico de Runge-Kutta de orden 4(5) (Dormand & Prince, 1980). Tras obtener la solución del SED, el sistema almacena los resultados y actualiza los estados de los nodos de acuerdo con la evolución de la simulación. Posteriormente, se ejecuta la rutina *node-graph-distribution-solution*, que garantiza la coherencia de las transiciones entre estados. Finalmente, el sistema actualiza en tiempo real la visualización de los parámetros y variables del modelo SERDUX-MARCIM y repite el ciclo para cada instante t hasta alcanzar el número de pasos definido o hasta que se verifique alguna de las siguientes condiciones de finalización: (1) todos los nodos se encuentren en los estados *S, E* o *R;* o (2) todos los nodos se encuentren en los estados *D, U* o *X*.

III. Almacenamiento de los datos de simulación

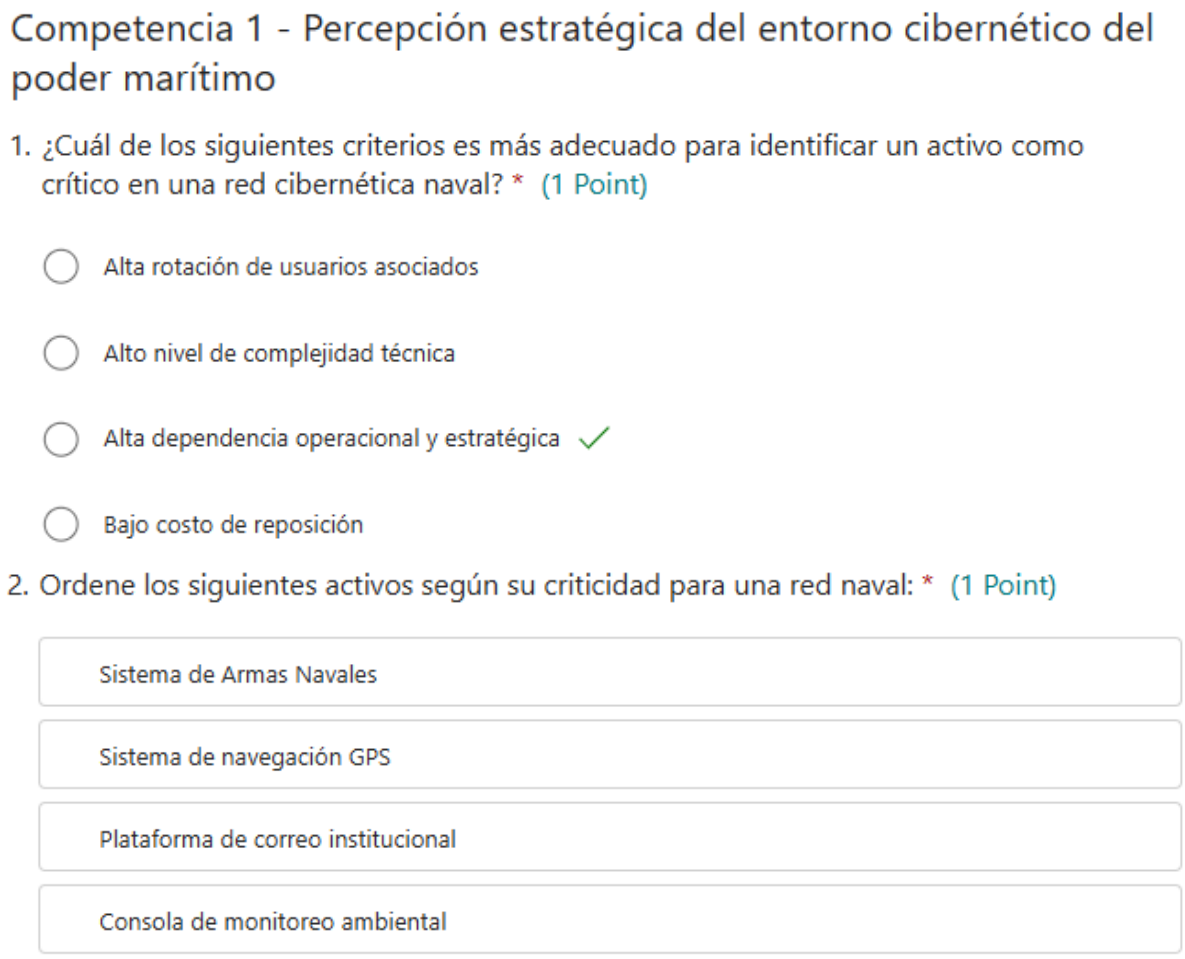
Figura 17. Almacenamiento de los resultados en el simulador.



Fuente: elaboración propia usando Netlogo.

Anexo 5. Instrumento de evaluación de competencias y resultados de aprendizaje.

Competencia 1 - Percepción estratégica del entorno cibernético del poder marítimo	
RA 1.1	Preguntas: 1 - 2 - 3
RA 1.2	Preguntas: 4 - 5 - 6
RA 1.3	Preguntas: 7 - 8 - 9
Competencia 2 - Comprensión integrada de escenarios de cibercrisis en el poder marítimo	
RA 2.1	Preguntas: 10 -11
RA 2.2	Preguntas: 12 - 13
RA 2.3	Preguntas: 14 - 15
RA 2.4	Preguntas: 16 - 17
RA 2.5	Preguntas: 18 - 19
Competencia 3 - Proyección estratégica de escenarios futuros en entornos complejos	
RA 3.1	Preguntas: 20 – 21
RA 3.2	Preguntas: 22 -23
RA 3.3	Preguntas: 24 - 25



3. ¿Cuál de las siguientes afirmaciones describe mejor una vulnerabilidad desde el punto de vista del atacante? * (1 Point)

- ○ Es un objetivo de alto valor
- ○ Es una debilidad explotable del sistema ✓
- ○ Es una amenaza latente en la infraestructura
- ○ Es un evento adverso ya materializado

4. ¿Qué afirmación describe correctamente la relación entre amenaza, vulnerabilidad y ciberataque? * (1 Point)

- ○ Un ciberataque genera una amenaza, y esta crea vulnerabilidades
- ○ Una vulnerabilidad da lugar a una amenaza que puede producir un ciberataque
- ○ Una amenaza puede explotar una vulnerabilidad y provocar un ciberataque ✓
- ○ No hay relación directa entre estos tres conceptos

5. ¿Cuál de los siguientes factores aumenta la severidad de una amenaza? * (1 Point)

- ○ El nivel de exposición mediática de la organización
- ○ La duración del ciclo de vida del atacante
- ○ La capacidad del atacante y el grado de acceso posible ✓
- ○ La antigüedad de la infraestructura tecnológica

6. "La severidad de una amenaza depende solo de la intención del atacante." * (1 Point)

- ○ Verdadero
- ○ Falso ✓

7. ¿Cómo se calcula generalmente el nivel de riesgo cibernético en un sistema? * (1 Point)

- ◯ Grado de criticidad x nivel de exposición
- ◯ Nivel de impacto x probabilidad de ocurrencia ✓
- ◯ Severidad del atacante + cantidad de nodos
- ◯ Vulnerabilidad detectada x número de usuarios

8. ¿Cuál de estos controles reduce directamente la probabilidad de ocurrencia de un ciberataque? * (1 Point)

- ◯ Correctivo
- ◯ Preventivo
- ◯ Detectivo
- ◯ Compensatorio ✓

9. ¿Cuál de estos controles reduce el impacto de un ciberataque? * (1 Point)

- ◯ Preventivo ✓
- ◯ Disuasivo
- ◯ Detectivo
- ◯ Compensatorio

Competencia 2 - Comprensión integrada de escenarios de cibercrisis en el poder marítimo

10. Ordene las siguientes etapas de un ciberataque dirigido (de la primera a la última): * (1 Point)

- Acceso inicial
- Escalamiento de privilegios
- Movimiento lateral
- Exfiltración de datos

11. ¿Cuál de las siguientes condiciones permite afirmar que un nodo ha sido ciberatacado? * (1 Point)

- ◯ Presenta tráfico inusual, pero sigue operativo.
- ◯ Ha sido aislado preventivamente por decisión del administrador.
- ◯ Se encuentra en estado degradado, no disponible o completamente destruido. ✓
- ◯ Fue identificado como activo crítico sin protección completa.

12. ¿Cuál de las siguientes capacidades es del ámbito de la ciberdefensa? * (1 Point)

- ◯ Conciencia cibernética
- ◯ Análisis de malware
- ◯ Defensa activa ✓
- ◯ Mejora de las operaciones

13. ¿Cuál de las siguientes capacidades es propia del ámbito de la ciberinteligencia? * (1 Point)

- ◯ Ciberdisuasión
- ◯ Intercambio de información ✓
- ◯ Ciberofensiva
- ◯ Ciberresiliencia

14. Ordene las fases de una crisis cibernética según su secuencia cronológica * (1 Point)

- Etapa estable funcional (Pre)
- Precrisis
- Crisis
- Postcrisis
- Etapa estable funcional (Pos)

15. ¿Qué caracteriza la fase de **precrisis** en una situación cibernética? * (1 Point)

- ◯ El sistema ha sido restaurado, pero se investiga el origen
- ◯ El ataque se ha confirmado y se ejecutan acciones
- ◯ Se observan indicios de anomalías sin confirmación del ataque ✓
- ◯ Se recopilan lecciones aprendidas y se actualizan protocolos

16. Ordene las fases de la gestión de incidentes cibernéticos según su secuencia cronológica: * (1 Point)

- Planeación y preparación
- Detección y reporte
- Evaluación y decisión
- Respuesta
- Lecciones aprendidas

17. ¿Cuál de las siguientes acciones corresponde a la fase de "evaluación y decisión" en la norma ISO/IEC 27035? * (1 Point)

- ○ Implementar plan de recuperación
- ○ Declarar formalmente una crisis ✓
- ○ Activar monitoreo 24/7
- ○ Restaurar servicios no críticos

18. ¿Qué posible consecuencia estratégica puede derivarse del uso ofensivo de ciberataques contra un actor de tipo amenaza cibernética? * (1 Point)

- ○ Fortalecimiento institucional
- ○ Contención diplomática efectiva
- ○ Escalada del conflicto y daño colateral ✓
- ○ Reducción de ciberriesgos inmediatos

19. ¿Cuál es una consecuencia potencial del pago de un rescate tras un ataque con ransomware? * (1 Point)

- ◯ Se fortalece la ciberresiliencia institucional ante futuras amenazas
- ◯ Se infringen regulaciones nacionales e internacionales sobre financiación de actores ilícitos ✓
- ◯ Se logra contener totalmente el ciberataque y se recupera la información secuestrada
- ◯ Se considera una medida aceptada bajo los principios de continuidad operativa

Competencia 3 - Proyección estratégica de escenarios futuros en entornos complejos

20. Una organización ha sido atacada por ransomware. Se detecta que el mismo grupo ha evolucionado en otros casos previos a ataques destructivos tras 48 horas. ¿Qué hipótesis estratégica sería más razonable? * (1 Point)

- ◯ El grupo probablemente abandonará el sistema una vez cobrado el rescate.
- ◯ El grupo no tomará más acciones mientras se negocia.
- ◯ Existe riesgo de escalamiento destructivo si no se actúa antes del plazo. ✓
- ◯ No se requiere ninguna respuesta hasta una nueva agresión.

21. ¿Cuál de los siguientes elementos se considera esencial para diseñar un curso de acción defensivo efectivo? * (1 Point)

- ◯ Disponibilidad financiera del actor
- ◯ Análisis del riesgo, prioridades y capacidades disponibles ✓
- ◯ Historial de vulnerabilidades de otros países
- ◯ Monitoreo exclusivo del entorno geopolítico

22. Ordene las siguientes acciones según su utilidad estratégica en escenarios poscrisis * (1 Point)

- Activación de plan de recuperación
- Restauración de nodos críticos
- Evaluación del impacto residual
- Revisión de lecciones aprendidas

23. ¿Cuál de los siguientes controles es más apropiado para proteger a una red que está bajo ciberataque por la explotación de una vulnerabilidad? * (1 Point)

- ◯ Control disuasivo
- ◯ Control preventivo ✓
- ◯ Control detectivo
- ◯ Control compensatorio

24. ¿Qué implicación estratégica puede tener el pago de un rescate ante un ataque de ransomware por parte de una fuerza militar? * (1 Point)

- ◯ Ninguna, si se restaura el sistema
- ◯ Legitimar actividades criminales y violar normativas ✓
- ◯ Proteger la reputación institucional
- ◯ Recuperar el control de las capacidades propias

25. En un entorno estratégico naval, ¿cuál podría ser una consecuencia de declarar una crisis cibernética sin verificación suficiente? * (1 Point)

- ◯ Reacción preventiva efectiva sin costos asociados
- ◯ Fortalecimiento automático de la disuasión frente al adversario
- ◯ Pérdida de credibilidad institucional y desgaste de recursos clave ✓
- ◯ Activación de mecanismos de respuesta sin implicaciones tácticas

Anexo 6. Resultados del instrumento de evaluación en el grupo de control.

Responses Overview

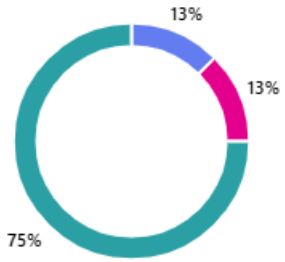
Closed

Responses	Average Score	Average Time
8	14.3	20:51

1. ¿Cuál de los siguientes criterios es más adecuado para identificar un activo como crítico en una red cibernética naval? (1 point) More details

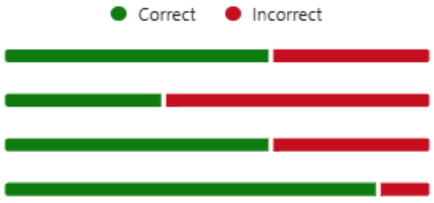
75% of respondents answered this question correctly.

Alta rotación de usuarios asociados	1
Alto nivel de complejidad técnica	1
Alta dependencia operacional y estratégica	6 ✓
Bajo costo de reposición	0



2. Ordene los siguientes activos según su criticidad para una red naval: (1 point) More details

25% of respondents answered this question correctly.

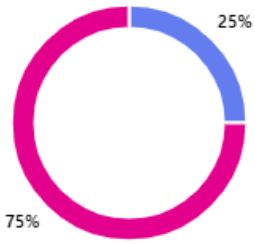


1.	Sistema de Armas Navales	62.5%
2.	Sistema de navegación GPS	37.5%
3.	Plataforma de correo institucional	62.5%
4.	Consola de monitoreo ambiental	87.5%

3. ¿Cuál de las siguientes afirmaciones describe mejor una vulnerabilidad desde el punto de vista del atacante? (1 point) More details

75% of respondents answered this question correctly.

Es un objetivo de alto valor	2
Es una debilidad explotable del sistema	6 ✓
Es una amenaza latente en la infraestructura	0
Es un evento adverso ya materializado	0



4. ¿Qué afirmación describe correctamente la relación entre amenaza, vulnerabilidad y ciberataque? (1 point) More details

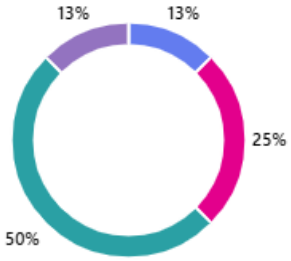
50% of respondents answered this question correctly.

Un ciberataque genera una amenaza, y esta crea vulnerabilidades	0
Una vulnerabilidad da lugar a una amenaza que puede producir un ciberataque	4
Una amenaza puede explotar una vulnerabilidad y provocar un ciberataque ✓	4
No hay relación directa entre estos tres conceptos	0

5. ¿Cuál de los siguientes factores aumenta la severidad de una amenaza? (1 point) More details

50% of respondents answered this question correctly.

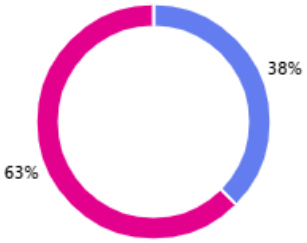
El nivel de exposición mediática de la organización	1
La duración del ciclo de vida del atacante	2
La capacidad del atacante y el grado de acceso posible ✓	4
La antigüedad de la infraestructura tecnológica	1



6. "La severidad de una amenaza depende solo de la intención del atacante." (1 point) More details

63% of respondents answered this question correctly.

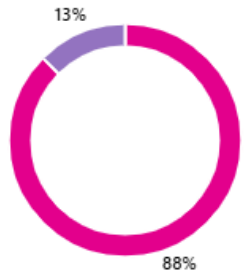
Verdadero	3
Falso ✓	5



7. ¿Cómo se calcula generalmente el nivel de riesgo cibernético en un sistema? (1 point) More details

88% of respondents answered this question correctly.

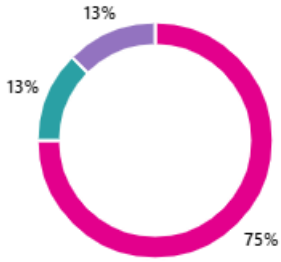
Grado de criticidad x nivel de exposición	0
Nivel de impacto x probabilidad de ocurrencia ✓	7
Severidad del atacante + cantidad de nodos	0
Vulnerabilidad detectada x número de usuarios	1



8. ¿Cuál de estos controles reduce directamente la probabilidad de ocurrencia de un ciberataque? (1 point) More details

13% of respondents answered this question correctly.

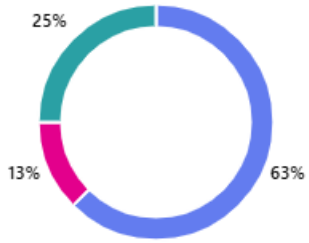
Correctivo	0
Preventivo	6
Detectivo	1
Compensatorio	1 ✓



9. ¿Cuál de estos controles reduce el impacto de un ciberataque? (1 point) More details

63% of respondents answered this question correctly.

Preventivo	5 ✓
Disuasivo	1
Detectivo	2
Compensatorio	0



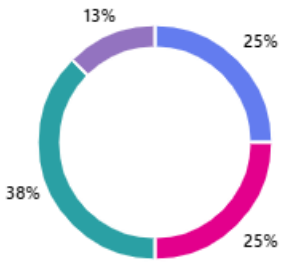
10. Ordene las siguientes etapas de un ciberataque dirigido (de la primera a la última): (1 point) More details

50% of respondents answered this question correctly.

11. ¿Cuál de las siguientes condiciones permite afirmar que un nodo ha sido ciberatacado? (1 point) More details

38% of respondents answered this question correctly.

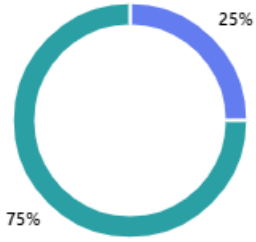
Presenta tráfico inusual, pero sigue operativo.	2
Ha sido aislado preventivamente por decisión del administrador.	2
Se encuentra en estado degradado, no disponible o completamente destruido.	3 ✓
Fue identificado como activo crítico sin protección completa.	1



12. ¿Cuál de las siguientes capacidades es del ámbito de la ciberdefensa? (1 point) More details

75% of respondents answered this question correctly.

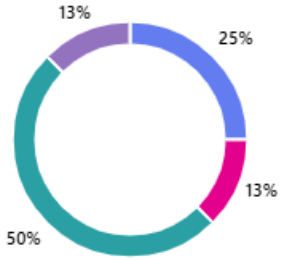
Conciencia cibernética	2
Análisis de malware	0
Defensa activa	6 ✓
Mejora de las operaciones	0



13. ¿Cuál de las siguientes capacidades es propia del ámbito de la ciberinteligencia? (1 point) More details

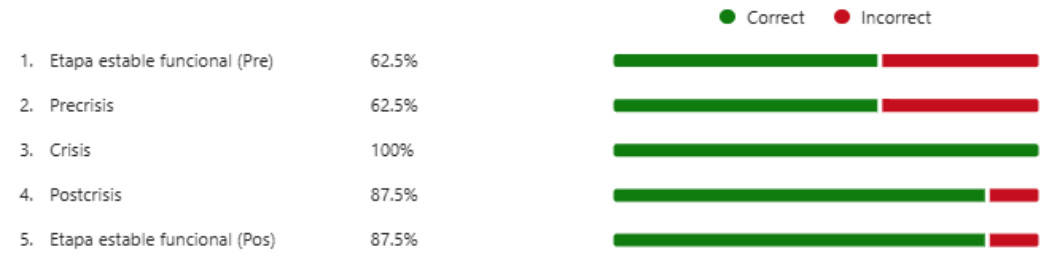
13% of respondents answered this question correctly.

Ciberdisuasión	2
Intercambio de información	1 ✓
Ciberofensiva	4
Ciberresiliencia	1



14. Ordene las fases de una crisis cibernética según su secuencia cronológica (1 point) More details

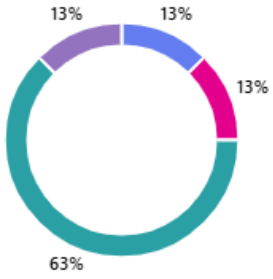
50% of respondents answered this question correctly.



15. ¿Qué caracteriza la fase de **precrisis** en una situación cibernética? (1 point) More details

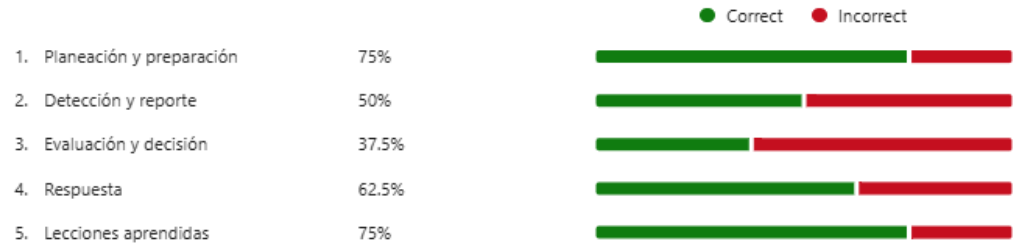
63% of respondents answered this question correctly.

El sistema ha sido restaurado, pero se investiga el origen	1
El ataque se ha confirmado y se ejecutan acciones	1
Se observan indicios de anomalías sin confirmación del ataque	5 ✓
Se recopilan lecciones aprendidas y se actualizan protocolos	1



16. Ordene las fases de la gestión de incidentes cibernéticos según su secuencia cronológica: (1 point) More details

38% of respondents answered this question correctly.

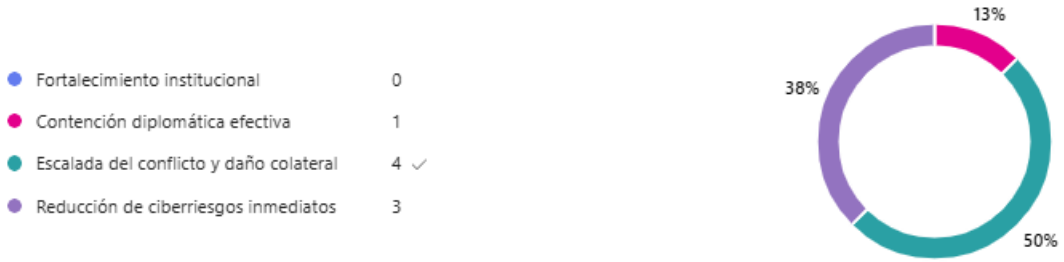


17. ¿Cuál de las siguientes acciones corresponde a la fase de "evaluación y decisión" en la norma ISO/IEC 27035? (1 point) More details

25% of respondents answered this question correctly.

18. ¿Qué posible consecuencia estratégica puede derivarse del uso ofensivo de ciberataques contra un actor de tipo amenaza cibernética? (1 point) More details

50% of respondents answered this question correctly.



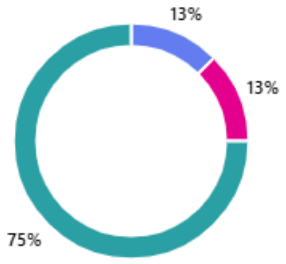
19. ¿Cuál es una consecuencia potencial del pago de un rescate tras un ataque con ransomware? (1 point) More details

75% of respondents answered this question correctly.

20. Una organización ha sido atacada por ransomware. Se detecta que el mismo grupo ha evolucionado en otros casos p revios a ataques destructivos tras 48 horas. ¿Qué hipótesis estratégica sería más razonable? (1 point) More details

75% of respondents answered this question correctly.

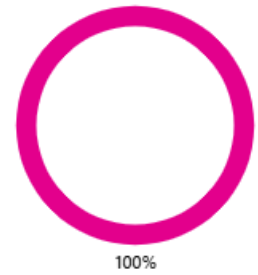
El grupo probablemente abandonará el sistema una vez cobrado el rescate.	1
El grupo no tomará más acciones mientras se negocia.	1
Existe riesgo de escalamiento destructivo si no se actúa antes del plazo. ✓	6
No se requiere ninguna respuesta hasta una nueva agresión.	0



21. ¿Cuál de los siguientes elementos se considera esencial para diseñar un curso de acción defensivo efectivo? (1 point) More details

100% of respondents answered this question correctly.

Disponibilidad financiera del actor	0
Análisis del riesgo, prioridades y capacidades disponibles ✓	8
Historial de vulnerabilidades de otros países	0
Monitoreo exclusivo del entorno geopolítico	0



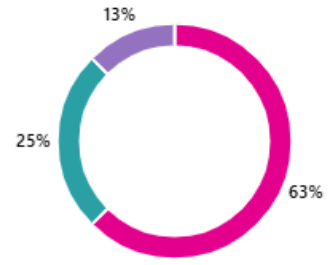
22. Ordene las siguientes acciones según su utilidad estratégica en escenarios poscrisis (1 point) More details

38% of respondents answered this question correctly.

23. ¿Cuál de los siguientes controles es más apropiado para proteger a una red que está bajo ciberataque por la explota ción de una vulnerabilidad? (1 point) More details

63% of respondents answered this question correctly.

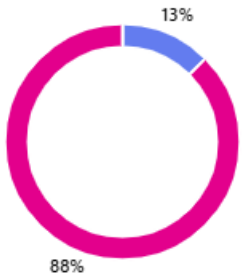
Control disuasivo	0
Control preventivo ✓	5
Control detectivo	2
Control compensatorio	1



24. ¿Qué implicación estratégica puede tener el pago de un rescate ante un ataque de ransomware por parte de una fuerza militar? (1 point) More details

88% of respondents answered this question correctly.

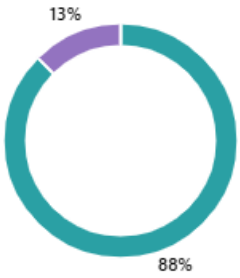
Ninguna, si se restaura el sistema	1
Legitimar actividades criminales y violar normativas	7 ✓
Proteger la reputación institucional	0
Recuperar el control de las capacidades propias	0



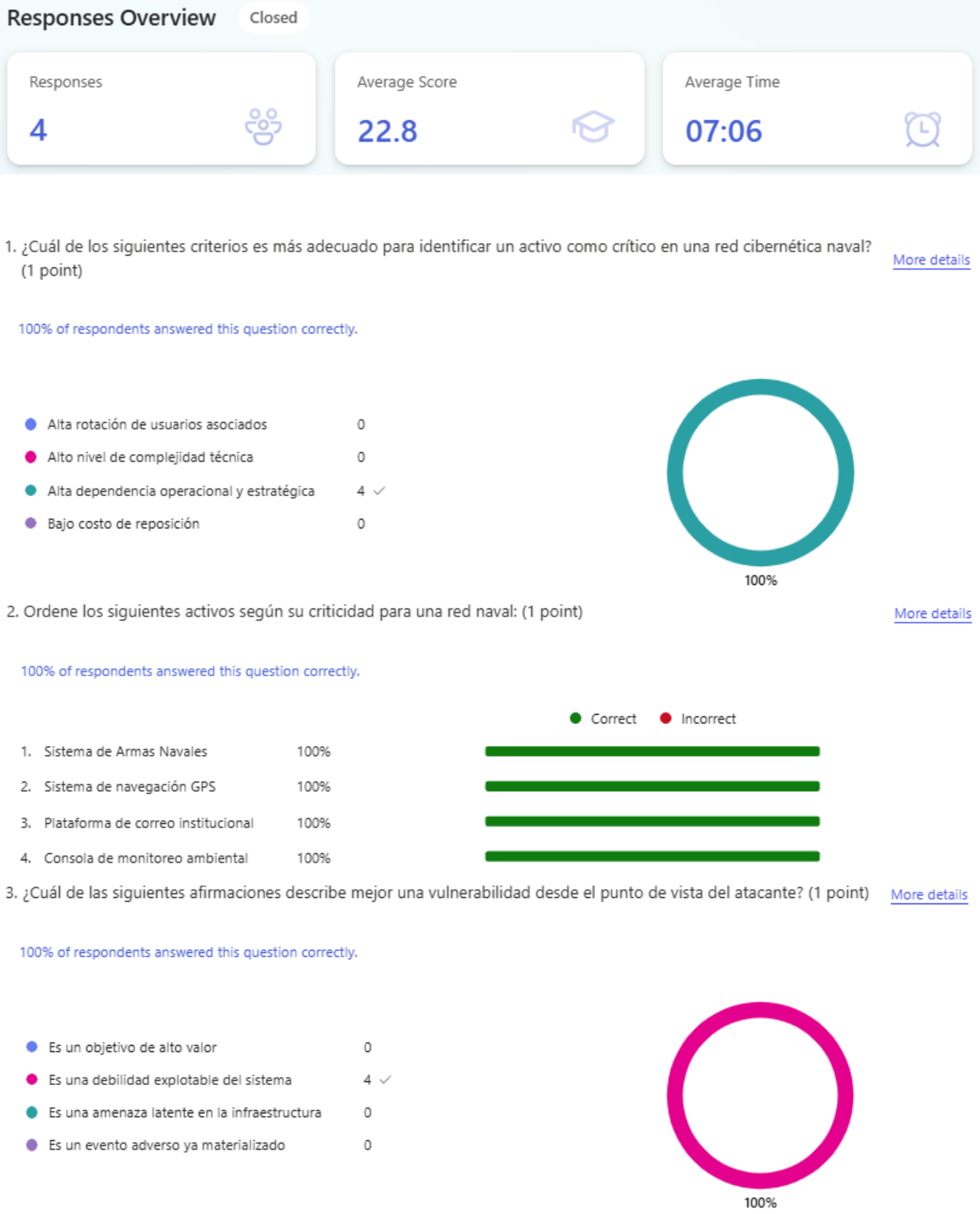
25. En un entorno estratégico naval, ¿cuál podría ser una consecuencia de declarar una crisis cibernética sin verificación suficiente? (1 point) More details

88% of respondents answered this question correctly.

Reacción preventiva efectiva sin costos asociados	0
Fortalecimiento automático de la disuasión frente al adversario	0
Pérdida de credibilidad institucional y desgaste de recursos clave	7 ✓
Activación de mecanismos de respuesta sin implicaciones tácticas	1



Anexo 7. Resultados del instrumento de evaluación en el grupo de intervención.



4. ¿Qué afirmación describe correctamente la relación entre amenaza, vulnerabilidad y ciberataque? (1 point) More details

100% of respondents answered this question correctly.

Un ciberataque genera una amenaza, y esta crea vulnerabilidades	0
Una vulnerabilidad da lugar a una amenaza que puede producir un ciberataque	0
Una amenaza puede explotar una vulnerabilidad y provocar un ciberataque	4 ✓
No hay relación directa entre estos tres conceptos	0

5. ¿Cuál de los siguientes factores aumenta la severidad de una amenaza? (1 point) More details

100% of respondents answered this question correctly.

El nivel de exposición mediática de la organización	0
La duración del ciclo de vida del atacante	0
La capacidad del atacante y el grado de acceso posible	4 ✓
La antigüedad de la infraestructura tecnológica	0

6. "La severidad de una amenaza depende solo de la intención del atacante." (1 point) More details

100% of respondents answered this question correctly.

Verdadero	0
Falso	4 ✓

7. ¿Cómo se calcula generalmente el nivel de riesgo cibernético en un sistema? (1 point) More details

100% of respondents answered this question correctly.

Grado de criticidad x nivel de exposición	0
Nivel de impacto x probabilidad de ocurrencia	4 ✓
Severidad del atacante + cantidad de nodos	0
Vulnerabilidad detectada x número de usuarios	0

8. ¿Cuál de estos controles reduce directamente la probabilidad de ocurrencia de un ciberataque? (1 point) More details

50% of respondents answered this question correctly.

Correctivo	0
Preventivo	2
Detectivo	0
Compensatorio	2 ✓

9. ¿Cuál de estos controles reduce el impacto de un ciberataque? (1 point) More details

50% of respondents answered this question correctly.

Preventivo	2 ✓
Disuasivo	0
Detectivo	0
Compensatorio	2

10. Ordene las siguientes etapas de un ciberataque dirigido (de la primera a la última): (1 point) More details

100% of respondents answered this question correctly.

1.	Acceso inicial	100%
2.	Escalamiento de privilegios	100%
3.	Movimiento lateral	100%
4.	Exfiltración de datos	100%

11. ¿Cuál de las siguientes condiciones permite afirmar que un nodo ha sido ciberatacado? (1 point) More details

100% of respondents answered this question correctly.

Presenta tráfico inusual, pero sigue operativo.	0
Ha sido aislado preventivamente por decisión del administrador.	0
Se encuentra en estado degradado, no disponible o completamente destruido.	4 ✓
Fue identificado como activo crítico sin protección completa.	0

12. ¿Cuál de las siguientes capacidades es del ámbito de la ciberdefensa? (1 point) More details

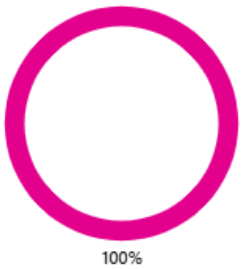
100% of respondents answered this question correctly.

Conciencia cibernética	0
Análisis de malware	0
Defensa activa	4 ✓
Mejora de las operaciones	0

13. ¿Cuál de las siguientes capacidades es propia del ámbito de la ciberinteligencia? (1 point) More details

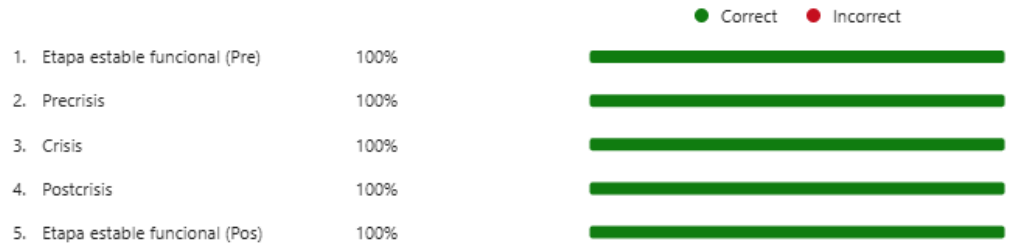
100% of respondents answered this question correctly.

Ciberdisuasión	0
Intercambio de información	4 ✓
Ciberofensiva	0
Ciberresiliencia	0



14. Ordene las fases de una crisis cibernética según su secuencia cronológica (1 point) More details

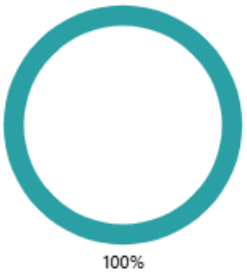
100% of respondents answered this question correctly.



15. ¿Qué caracteriza la fase de **precrisis** en una situación cibernética? (1 point) More details

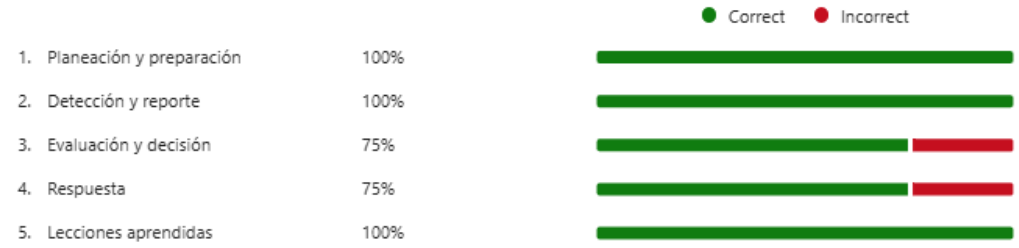
100% of respondents answered this question correctly.

El sistema ha sido restaurado, pero se investiga el origen	0
El ataque se ha confirmado y se ejecutan acciones	0
Se observan indicios de anomalías sin confirmación del ataque	4 ✓
Se recopilan lecciones aprendidas y se actualizan protocolos	0



16. Ordene las fases de la gestión de incidentes cibernéticos según su secuencia cronológica: (1 point) More details

75% of respondents answered this question correctly.



17. ¿Cuál de las siguientes acciones corresponde a la fase de "evaluación y decisión" en la norma ISO/IEC 27035? (1 point) More details

100% of respondents answered this question correctly.

18. ¿Qué posible consecuencia estratégica puede derivarse del uso ofensivo de ciberataques contra un actor de tipo amenaza cibernética? (1 point) More details

75% of respondents answered this question correctly.

19. ¿Cuál es una consecuencia potencial del pago de un rescate tras un ataque con ransomware? (1 point) More details

100% of respondents answered this question correctly.

20. Una organización ha sido atacada por ransomware. Se detecta que el mismo grupo ha evolucionado en otros casos p revios a ataques destructivos tras 48 horas. ¿Qué hipótesis estratégica sería más razonable? (1 point) More details

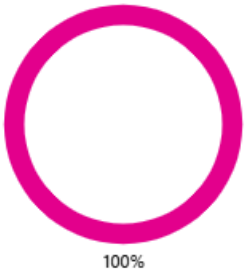
100% of respondents answered this question correctly.

El grupo probablemente abandonará el sistema una vez cobrado el rescate.	0
El grupo no tomará más acciones mientras se negocia.	0
Existe riesgo de escalamiento destructivo si no se actúa antes del plazo.	4 ✓
No se requiere ninguna respuesta hasta una nueva agresión.	0

21. ¿Cuál de los siguientes elementos se considera esencial para diseñar un curso de acción defensivo efectivo? (1 point) More details

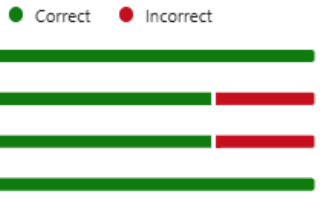
100% of respondents answered this question correctly.

Disponibilidad financiera del actor	0
Análisis del riesgo, prioridades y capacidades disponibles	4 ✓
Historial de vulnerabilidades de otros países	0
Monitoreo exclusivo del entorno geopolítico	0



22. Ordene las siguientes acciones según su utilidad estratégica en escenarios poscrisis (1 point) More details

75% of respondents answered this question correctly.



1.	Activación de plan de recuperación	100%
2.	Restauración de nodos críticos	75%
3.	Evaluación del impacto residual	75%
4.	Revisión de lecciones aprendidas	100%

23. ¿Cuál de los siguientes controles es más apropiado para proteger a una red que está bajo ciberataque por la explota ción de una vulnerabilidad? (1 point) More details

50% of respondents answered this question correctly.

Control disuasivo	0
Control preventivo	2 ✓
Control detectivo	0
Control compensatorio	2

24. ¿Qué implicación estratégica puede tener el pago de un rescate ante un ataque de ransomware por parte de una fuerza militar? (1 point) More details

100% of respondents answered this question correctly.

Ninguna, si se restaura el sistema	0
Legitimar actividades criminales y violar normativas	4 ✓
Proteger la reputación institucional	0
Recuperar el control de las capacidades propias	0

25. En un entorno estratégico naval, ¿cuál podría ser una consecuencia de declarar una crisis cibernética sin verificación suficiente? (1 point) More details

100% of respondents answered this question correctly.

Reacción preventiva efectiva sin costos asociados	0
Fortalecimiento automático de la disuasión frente al adversario	0
Pérdida de credibilidad institucional y desgaste de recursos clave	4 ✓
Activación de mecanismos de respuesta sin implicaciones tácticas	0