Año 2024, Vol. 21, Nº 2, pp. 72 - 89.
DOI: https://doi.org/10.35628/resup.v16i2.150

Implementación de la Especialidad de Ciberdefensa en el Modelo Educativo de la Marina de Guerra del Perú, como Factor de Fortalecimiento de sus Capacidades Militares

Implementation of Cyber Defense Specialty in the Educational Model of the Peruvian Navy, as a Factor in Strengthening its Military Capabilities

Recibido: 13 de noviembre del 2024 | Aceptado: 25 de noviembre del 2024

Jonny Herrera Romero
https://orcid.org/0009-0009-7739-2867

Ingeniero Electrónico por la Universidad Nacional de Ingeniería y MBA por ESAN. Cuenta con más de 30 años de experiencia en Dirección General y Comercial de Unidades de Negocios en Marcas Transnacionales de Tecnología de Consumo como Sony, Samsung, KODAK y CANON, enfocados principalmente en el diseño y ejecución de Redes de Distribución Comercial basados en procesos seguros y rentables y Transporte Multimodal eficiente (marítimo, aéreo y terrestre) en el ámbito nacional e internacional con alta confiabilidad y predictibilidad.

Email:jherrerar96@gmail.com

Resumen: Una de las preocupaciones cardinales de la Marina de Guerra del Perú (MGP) para ejecutar los roles asignados por ley es el fortalecimiento de sus Capacidades Militares, dentro de las cuales se considera para fines de este artículo, el Tamaño y Calidad de la Fuerza (incluida la captación, capacitación y retención de la misma), el Comando y Control, y finalmente la Seguridad de la Información.

Se revisa en este artículo la relación entre la Ciberdefensa y los roles y funciones de la MGP en el marco de la política de Defensa Nacional al 2030, sus implicancias y rol decisivo en el desarrollo tecnológico de un país, y cómo su implementación a nivel educativo en la MGP puede colaborar decisivamente en concretar esos objetivos. Propongo en esta línea de análisis, la implementación de la especialidad de CIBERDEFENSA, tanto en la DIRCAPEN como en la DIRESPROM, para

imbuir la importancia de esta capacidad a todo nivel de la Marina de Guerra del Perú. Asimismo, en los tiempos actuales, en los que la Defensa es tarea de todos, esbozo cómo la colaboración con la educación privada puede hacer que los cuadros de la Marina se nutran de conocimientos, necesidades, oportunidades y retos del mundo privado/civil en este campo, lo cual les dará una visión holística de la Defensa del Perú.

Finalmente, creo que este escenario de oportunidades servirá como un imán para garantizar el compromiso de nuestros cuadros, atraer el mejor talento a todo nivel y por qué no, pensar en que con el tiempo y un adecuado patrocinio, se forme una red de conocimientos y expertos público/privado, que de acuerdo a una visión renovada de la doctrina, esté presta a entrar en movilización inmediata si las necesidades de defensa nacional así lo exigen.

Palabras clave: Ciberseguridad, ciberdefensa, activos críticos nacionales, transformación digital, dominio marítimo, prospectiva.

Abstract: *One of the Peruvian Navy's cardinal concerns in carrying out the roles assigned by law is the strengthening of its Military Capabilities, among which the following are considered for the purposes of this article: Size and Quality of the Force (including recruitment, training, and retention), Command and Control, and finally Information Security.*

This article goes through the relationship between Cyberdefense and the roles and tasks of the Peruvian Navy within the framework of the National Defense policy for 2030, its implications and decisive role in the technological development of a country, and how its implementation in the Peruvian Navy education can make a substantial contribution to achieving these objectives. In this line of analysis, I propose the implementation of the CYBERDEFENSE specialty, both in DIRCAPEN and DIRESPROM, to imbue the importance of this capability throughout the Peruvian Navy. In current times, when Defense is everyone's task, I also outline how collaboration with private education can ensure that Navy personnel are nourished by knowledge, needs, opportunities, and challenges of the private/civilian world in this field, which will give them a holistic vision of the Defense of Peru.

Finally, I believe that this scenario of opportunities will serve as a magnet to guarantee the commitment of our staff, allure the best talent at all levels, and, why not think about how, over time and with adequate sponsorship, we can establish a knowledge and public/private experts network, who, according to a renewed

vision of the doctrine, is ready to enter into immediate mobilization if the needs of national defense so demand.

Keywords:*Cyber Security, cyber defense, national critical assets, digital transformation, maritime domain, foresight.*

1. INTRODUCCIÓN

Una de las preocupaciones cardinales de la MGP para ejecutar los roles asignados por ley es el fortalecimiento de sus Capacidades Militares, dentro de las cuales se considera para fines de este artículo: el Tamaño y Calidad de la Fuerza (incluida la captación, capacitación y retención de la misma), el Comando y Control, y finalmente la Seguridad de la Información.

Se revisa en este artículo la relación entre la Ciberdefensa y los roles y funciones de la MGP en el marco de la política de Defensa Nacional al 2030, sus implicancias y rol decisivo en el desarrollo tecnológico de un país, y cómo su implementación a nivel educativo en la MGP puede colaborar decisivamente en concretar esos objetivos. Propongo en esta línea de análisis, la implementación de la especialidad de CIBERDEFENSA, tanto en la DIRCAPEN como en la DIRESPROM, para imbuir la importancia de esta capacidad a todo nivel de la Marina de Guerra del Perú. Asimismo, ya que la Defensa es tarea de todos, esbozo cómo la colaboración con la educación privada haría que los cuadros de la MGP capten los conocimientos, necesidades, oportunidades y retos del mundo privado en ciberseguridad, capacidad tecnológica definida en el marco de la Seguridad Digital para proteger actividades críticas (D.U. 007-2020 que aprueba el Marco de Confianza Digital, artículo 3, incisos d y h) y que tiene a la Secretaría de Gobierno Digital como ente rector (Ley 30999, Ley de Ciberdefensa, artículo 13), encargando a esta entidad los protocolos para la seguridad digital, lo cual abre espacio para una visión integral/holística de la Defensa del Perú.

2. CIBERSEGURIDAD EN EL MUNDO Y EN EL PERÚ

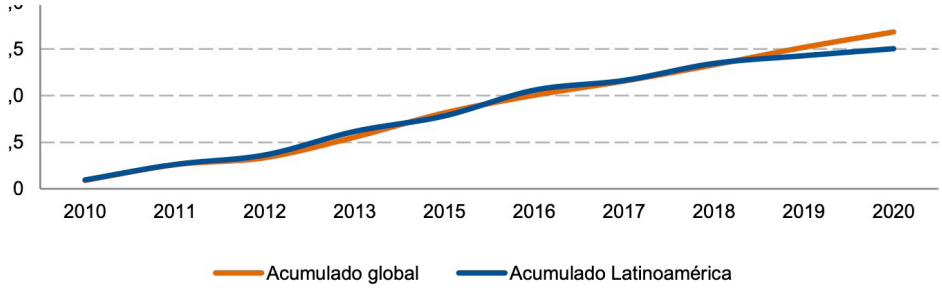
Con el propósito de entender el impacto del tema planteado para el logro de los Objetivos de Desarrollo Económico e Intereses de Integridad Territorial del Perú, haré una revisión del estado de la ciberseguridad en el mundo, la región y el Perú, para lo cual se presenta información de tendencias globales, para luego repasar lo desplegado para el caso peruano, siguiendo elementos de la Dirección del Análisis Estratégico clásico FODA.

a. Tecnologías de Información y el Ciberespacio

El impacto de las tecnologías de información, inicialmente con la expansión de la computación personal durante los años 70 y 80, se vio catapultado en perspectivas y realidad al caer el Muro de Berlín en 1989. En esos tiempos, la apertura de la red ARPANET (con su versión DARPANET, de uso estratégico y militar sólo en los EEUU) dio paso a la Internet (World Wide Web inicialmente o Ciberespacio, que es el término usual de hoy), haciendo que el flujo de información y de servicios digitales (financieros, información, datos, etc.) creciera a niveles exponenciales. En el Gráfico N.º1 (Díaz, R., pág. 8, 2021) se puede apreciar un incremento regional en Latinoamérica de usuarios de Internet en los últimos 10 años de casi 150%, como una idea de un escenario futuro de similar o mayor crecimiento en la región y el Perú.

GRÁFICO N.º 1

Crecimiento de usuarios conectados a Internet (en porcentajes, 100%)



Fuente: Díaz, Rodrigo. Estado de la Ciberseguridad en la Logística de América Latina y Caribe, CEPAL, 2021

b. Riesgos y Amenazas en el Ciberespacio

Sin embargo, junto a las oportunidades producto del conocimiento tecnológico adquirido y su impacto en el bienestar económico surgieron también los riesgos y amenazas, de manera que copiaban el mundo real, como por ejemplo la infestación de redes de computadoras con los llamados virus de todo tipo (destinados a entorpecer la performance de redes y equipos, ingresando mediante técnicas de ingeniería social, hacking, ransomware, etc.), haciendo que en una sociedad cada vez más dependiente de la información y equipos automatizados se ponga en riesgo continuo la producción de bienes y servicios, vitales para los intereses, objetivos y la economía de países, empresas y familias. Por esta razón la ciberseguridad es una de las tareas que el Perú debería priorizar, considerando marcos de gobierno digital referentes como los de EEUU o Australia *(Secure*

Connections, 2022. Cibersecurity in The Philippines: Global Context and Local Challenges, chapter 3).

He incluido el término ciberdefensa junto al de ciberseguridad, para hacer precisiones sobre qué establece cada uno de ellos. Al hablar de ciberseguridad, lo asociamos operativamente con las acciones para preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (Vargas, Recalde y Reyes, 2017, p.34), así como el D.U. 007-2020, Marco de Confianza Digital, la considera una capacidad, un estado, que protege de amenazas y vulnerabilidades. Para ciberdefensa, Vargas et al. afirman:

> " se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros (…), con el fin de permitir el uso del ciberespacio con normalidad¨ (p. 35); y también: "los Estados serán los encargados de decidir en el ámbito de la ciberdefensa, llegando a definir si un ataque (…) puede comprometer el desarrollo y la supervivencia de la nación." (p. 35).

En el Perú, la Ley 30999 define la ciberdefensa como: "la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional" (artículo 4).

En ese sentido, se puede establecer como conclusión que:

1. La ciberseguridad se asocia con la protección contra amenazas y/o ataques,
2. La ciberdefensa se orienta no sólo a proteger sino a accionar contra amenazas (ataques potenciales), con un enfoque más proactivo, de eliminación, pudiendo incluir la prospección de escenarios, pensando en la Soberanía e Integridad Nacional.

c. La ciberseguridad en Latinoamérica y el dominio marítimo en el Perú

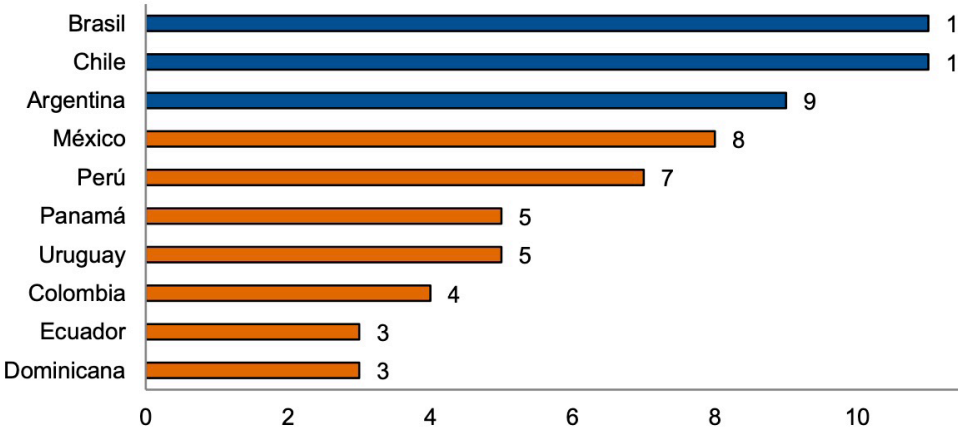
En cuanto a las amenazas a la Soberanía e Integridad Territorial, para nuestro país encontramos en el Observatorio CEPLAN, que es la entidad encargada de generar el Plan de Desarrollo del Perú con visión estratégica, que uno de los escenarios de riesgo considerados es justamente el de *ruptura generalizada de ciberseguridad* (Observatorio CEPLAN, 2022). Este enfoque es correcto si consideramos un futuro desarrollo de nuestro país siguiendo la línea trazada en el escenario de prospectiva del mismo CEPLAN, *Perú próspero, equitativo y pacífico* (Observatorio CEPLAN, 2021).

En este último documento de prospectiva, notamos un correcto análisis de lo que sería la red peruana de puertos, destacando El Callao y Salaverry, aunque se echa de menos una mención al impacto del puerto de Chancay por el análisis incluido sobre el potencial de la minería, cuya mayor demanda es en Asia-Pacífico y donde el puerto de Chancay es el llamado a ser el protagonista en pocos años.

A pesar de este vacío en el análisis, es importante recordar que son funciones de la MGP (Decreto Legislativo N.º 1641, 2024): "Ejercer el control, la vigilancia y la defensa del dominio marítimo, (…), así como del ciberespacio y con la capacidad de ciberdefensa en el ámbito de sus competencias" (artículo 4). Es así que se han considerado los desafíos tecnológicos y sus impactos económicos (oportunidades y riesgos), pues el dominio marítimo y el ciberespacio son ámbitos claves para el desarrollo de nuestro país.

Adentrando en el análisis del dominio marítimo y buscando determinar el impacto económico de las ciber amenazas, me centraré en el ámbito portuario, citando de nuevo el análisis hecho por la CEPAL sobre cadenas logísticas (Díaz, R., pág. 11), que dice que los casos de ciberataques en Latinoamérica se han incrementado en el 2020 en 175% versus el 2019, impactando empresas de primer orden como Maersk. En el Gráfico N.º 2, comparto las incidencias 2020 reportadas por país (Díaz, R., pág. 17), con el Perú sobre el promedio, preocupante si se considera el desarrollo portuario futuro y el hecho de estar muy cerca en número de ocurrencias versus países como Chile o México, cuyos comercios marítimos son mayores. Cabe resaltar que el mayor impacto de estos forados en la ciberseguridad se dio en la disponibilidad de los sistemas informáticos (77%), paralizando las operaciones con el consecuente daño económico por atrasos en las entradas, almacenajes y salidas de mercaderías (Díaz, R., pág. 17).

GRÁFICO N.º 2
Países afectados por la cantidad de incidentes.



Fuente: Díaz, Rodrigo. Estado de la Ciberseguridad en la Logística de América Latina y Caribe, CEPAL, 2021

Para estimar entonces un probable impacto económico de estos ciberataques en el Perú, tomemos en cuenta el nivel de exportaciones: en 2022 se cerró con un valor de USD 63MM (Mincetur, Promperú, Exportaciones 2022). Si consideramos que no menos del 70% es por la vía marítima (Revista Ganamás, 2015), podemos estimar el promedio de exportaciones diarias en el valor de USD 120M. Considerando que el número de ciberataques fueron 7 en 2019, podríamos afirmar que casi USD 1,000 millones estarían en juego de ser impactados por estos ataques y que estarían dentro del dominio del ciberespacio, responsabilidad del Comando de Ciberdefensa del CCFFAA y su componente naval en la MGP. La cifra no considera el crecimiento de las exportaciones ni de los ciberataques al día de hoy, que haría la cifra aún mayor.

d. La ciberseguridad en el Perú y el marco legal del rol de la Marina de Guerra

El Perú es un país que, a pesar del complejo entorno socio-político por el cual está pasando, ha generado, mediante el Centro Nacional de Planeamiento Estratégico (CEPLAN) y luego de una amplia prospección con los actores relevantes en los ámbitos público y privado, un marco de visión a futuro (Plan Estratégico de Desarrollo Nacional al 2050, PEDN). Una revisión de dicho documento, en lo pertinente a este trabajo, nos lleva al Objetivo N.º 3 que dice: “Elevar los niveles

de competitividad y productividad con empleo decente (…), el uso intensivo de la ciencia y tecnología, y la transformación digital del país" (pág. 357).

Este último concepto, TRANSFORMACION DIGITAL, junto con los riesgos y escenarios descritos en el PEDN, se refleja en gran medida en los esfuerzos normativos que han venido generando las autoridades de turno, para proteger el rol vital de la sociedad de la información y sus tecnologías en el desarrollo de nuestro país y que mencionamos a continuación.

En primer lugar, tenemos el marco de Gobierno Digital (Decreto Legislativo N.º 1412, 2018, Ley de Gobierno Digital). En su Capítulo VI, sobre SEGURIDAD DIGITAL, se definen los conceptos de *entorno digital* y su confiabilidad (estado de confianza), gestión y aplicación de medidas *proactivas y reactivas*, riesgos y afectaciones a la prosperidad económica y *seguridad nacional*, en línea con el Objetivo N.º 3 del PEDN antes citado.

Asimismo, en el artículo 32, inciso a, sobre la Gestión del Marco de Seguridad Digital, encarga al MINDEF la dirección, supervisión y evaluación de las normas en materia de ciberdefensa, en el marco de sus *funciones y competencias*. Cabe resaltar que ese encargo se amplía o aclara con la ya citada Ley N.º 30999, artículo 14, Ley de Ciberdefensa, que añade la tarea de *normar* lo tocante a Ciberdefensa, haciendo aún más importante el rol de las FFAA en este campo.

Pero más importante, la Ley N.º 30999 en su Título I, artículos 1 y 2, establece las operaciones militares en el ciberespacio, relacionándolas con los Activos Críticos Nacionales (ACN), mientras que el artículo 10 establece el ejercicio de la legítima defensa como sigue:

> " Toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa".

Desde mi punto de vista, si bien la frase Seguridad Digital del Decreto Legislativo N.º 1412 puede traducirse literalmente al inglés como Cibersecurity (Ciberseguridad en español), no es menos cierto que en la definición de conceptos de la Ley 30999, se habla tanto de medidas proactivas (acciones para *proteger o actualizar* la protección del entorno digital o *actuación sobre amenazas* entendidas como ataques inminentes), como de medidas reactivas (acciones de respuesta para mitigar o eliminar los efectos de ataques al entorno digital), reforzadas por lo establecido en el artículo 10 explicado en el párrafo anterior.

Finalmente, son la Directiva de Protección de los Activos Críticos Nacionales – ACN (Decreto Supremo 005-2021-IN, 2021) y su Reglamento de Identificación (Decreto Supremo 106-2017-PCM, 2017), los que definen aquellos ACN que están directamente relacionados con el ámbito de la Marina de Guerra del Perú, tal cual se definió anteriormente, en su rol de preservar las Capacidades Nacionales y que se presentan en la Tabla N.º 1 abajo.

TABLA N.º 1
Capacidades Nacionales

CAPACIDADES NACIONALES	**CLASIFICACION DE ACN**	**ACTIVOS**
SEGURIDAD Y DEFENSA NACIONAL (11)	SEGURIDAD Y DEFENSA NACIONAL	SEGURIDAD DIGITAL (DEL ENTORNO DIGITAL)
TRANSPORTE MARITIMO, FLUVIAL Y LACUSTRE (13)	TRANSPORTE MARITIMO INFRAESTRUCTURA PORTUARIA NAVES DE TRANSPORTE EMBARQUE	PUERTOS PRINCIPALES COMO CALLAO, SALAVERRY, CHANCAY, PAITA INCLUYENDO SU FLUJO DE ENTRADA, ESTADIA Y SALIDA DE NAVES, MERCANCIAS Y PERSONAS
TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES TIC (12)	TECNOLOGIAS DE LA INFORMACION COMUNICACIONES	SERVICIOS WEB SERVICIOS DE BASES DE DATOS
INDUSTRIA (7)	INDUSTRIAS CRITICAS	SIMA Y SU CLUSTER INDUSTRIAL

Fuente: elaboración propia

Como se aprecia en la Tabla N.º 1, si se considera que en los actuales tiempos, donde las tecnologías de información están presentes como parte indispensable del funcionamiento de casi cualquier industria, producto o servicio, público o privado, se puede establecer que para cada una de las tres Capacidades Nacionales 7, 12, 13 y sus ACN respectivos, el Entorno Digital constituye un elemento inseparable, complementario y clave de esos ACN, cayendo por tanto en el ámbito de responsabilidad de la Seguridad Digital y por ende del CCFFAA, su unidad COCID (Comando Operacional de Ciberdefensa), y por extensión la MGP como actor directo en su ámbito incluyendo el ciberespacio, por las normas que regulan su intervención en el ACN 11.

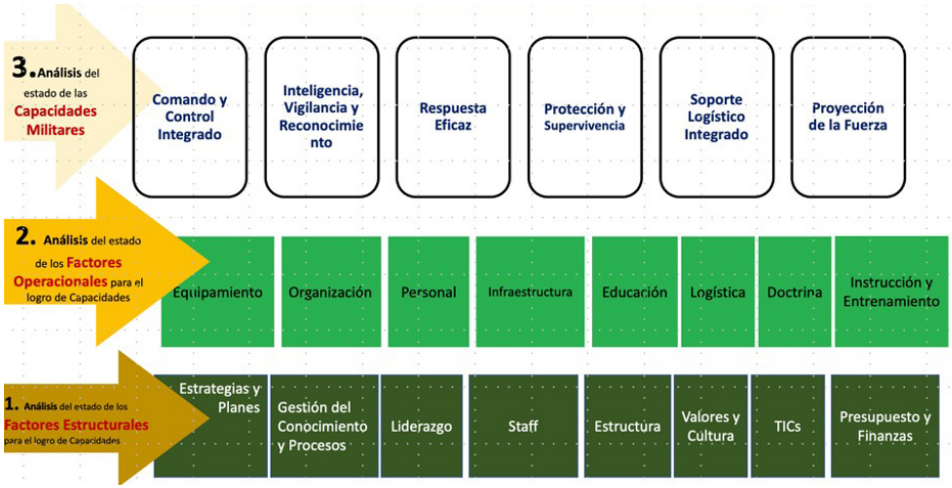
3. ANÁLISIS

a. Análisis interno para capacidades militares

Habiendo comprobado el rol de la Marina de Guerra del Perú en la protección del dominio marítimo y del ciberespacio, que incluye los ACN, pasaré a analizar el interior de la institución, enfocándome en aquellos factores relacionados a la formación del personal, que permitan construir las capacidades necesarias para el rol de ciberdefensa y ciberseguridad. Para tal efecto, usaré como marco de referencia un modelo conceptual de análisis interno para alcanzar las Capacidades Militares (Gráfico N.º 3), que presenta un punto de vista de cómo se construyen dichas capacidades.

GRÁFICO N.º 3

Análisis Interno para Capacidades Militares – Modelo Conceptual



Fuente: Universidad ESAN

De este modelo se desprende que para lograr la implementación de la especialidad de ciberdefensa y ciberseguridad deben analizarse y relacionarse ciertos factores. Analizando todos estos factores en los dos primeros niveles, y luego de una revisión identificamos los siguientes (Tabla N.º 2, abajo), como claves para el desempeño del personal, incluyendo la instrucción, alcanzando ejemplos de acciones de ciberdefensa y ciberseguridad:

TABLA N.º 2
Análisis Interno para Capacidades Militares – Modelo Conceptual

Nivel	Factor	Acciones
Estructural	Estrategia y Planes	Escenarios de Ciberdefensa
	Gestión del Conocimiento	Inteligencia, Formación en Ciberdefensa
	Valores y Cultura	Respuesta militar acorde a ley
Operacional	Personal	Tamaño y perfil de la fuerza en Ciberdefensa
	Doctrina	Respuesta ante ciberataques o ciber amenazas
	Instrucción, Entrenamiento, Educación	Capacitación en Ciberseguridad/Ciberdefensa

Fuente: Elaboración propia

Del cuadro anterior, se concluye que las capacidades a lograr con el personal ya formado incluyen Comando y Control Integrado, Inteligencia, Vigilancia y Reconocimiento y Respuesta Eficaz.

Realizaré el análisis revisando las entidades educativas que, dentro de la Marina de Guerra del Perú, son las encargadas de instruir al personal en las capacidades de ciberseguridad y ciberdefensa, tanto a nivel técnico (Oficiales de Mar), como Superior de Mando (Oficiales). Se tiene entonces al CITEN, la ENP y la ESUP como fuentes de ese personal.

Junto con esto, a modo de comparación, se revisarán los avances en capacitación de recursos humanos en el ámbito civil. Para tal efecto, se ha revisado lo disponible en la UNI y el SENATI. Empezaré primero con el nivel técnico de capacitación, para luego pasar al superior.

b. CITEN (Instituto de Educación Superior Tecnológico Público Naval)

En la declaración de Visión y Misión de esta entidad (CITEN, Web Institucional, Visión y Misión, 2024), destacamos el compromiso con la formación académica en su Misión: "Formar militar, profesional, técnico y físicamente a los Alumnos (…) se desempeñen eficientemente en el Servicio Naval" y su Visión: "Al 2025, ser un Instituto de Educación Superior (…) para actuar con éxito donde lo requiere la Marina de Guerra del Perú".

Al revisar las Carreras Profesionales y Áreas Técnicas de Formación (CITEN, Web Institucional, 2024), de 3 años de duración, se nota dos de interés al presente análisis: Sistemas y Administración de Redes (CITEN, Carreras Profesionales, Administración de Redes, SAR) y Telemática con mención en Servicio Naval

(CITEN, Carreras Profesionales, Telemática, TEL). En la primera se incluyen tópicos de formación para desarrollar soluciones en seguridad informática, virtualización, gestión de bases de datos y redes informáticas y ciberseguridad, entre otros. La segunda, si bien no declara la ciberseguridad, su orientación a gestión de equipos y sistemas de telecomunicaciones tiene relación con ésta, pues esta infraestructura es objetivo de los ciber delincuentes.

Para posterior perfeccionamiento técnico, validamos que la DIRCAPEN (Dirección de Capacitación y Perfeccionamiento del Personal Naval) tiene en su malla de Procesamiento de Datos (PDA) los tópicos de Ciberseguridad y Auditorías informáticas; pero más interesante, en la malla de Telemática (TEL) el tópico de Ciberdefensa tiene un enfoque 100% práctico. Hay entonces una base para escalar a más conocimiento, pero hay que confirmar que la prospectiva de casos prácticos considere los escenarios de nuevas infraestructuras, como el puerto de Chancay y el mayor tráfico ya mencionados.

c. SENATI (Servicio Nacional de Adiestramiento en Trabajo Industrial)

Entidad creada por la Sociedad Nacional de Industrias (SNI), cuenta con amplia reputación en la formación de cuadros técnicos para laborar en el sector privado, su mercado objetivo. Revisando las Especialidades disponibles, se encuentra la de *Ingeniería de Ciberseguridad* (SENATI, Ingeniería de Ciberseguridad, 2024), donde se declara: "El Profesional Técnico en Ingeniería, está preparado para defender las computadoras, los servidores, los dispositivos móviles, (…), las redes y los datos de ciberataques". Como puede verse, el SENATI decidió proponer al sector privado una especialidad *específica* para enfrentar los desafíos de la ciberseguridad.

En ese sentido, considero que la Marina de Guerra del Perú está un paso atrás en el nivel técnico, debido a la falta de una especialidad específica en Ciberseguridad (como mínimo), siendo necesario revisar los factores para incluir un plan educativo que permita generar personal con capacidades más especializadas en Ciberseguridad. Dicho esto, paso a revisar la educación superior.

d. ENP (Escuela Naval del Perú)

Como Alma Mater de la Marina de Guerra del Perú, su formación busca proveer Oficiales Navales en una malla curricular de 5 años, donde se ven estudios en *Ciberseguridad* en el 5º año (ENP, Carrera Naval, 2024), lo que provee la base de conocimientos para que posteriormente, al tomar la segunda especialidad profesional de *Ingeniería de Sistemas*, administrada por la DIRESPROM (Escuela de Especialización Profesional de Oficiales de la Marina, 2024), se amplíen los

conocimientos. No he podido acceder a la malla de estudios de esta especialidad, pero la declaración de capacidades del personal egresado dice: "Dirigir la implementación de esquemas de seguridad en la red para evitar la pérdida y el uso incorrecto de los datos". Al no ver una mención específica a la ciberdefensa, es necesario revisar la malla para validar si la carga en esta área es ampliable para el rol de ciberdefensa y ciberseguridad que tiene la Marina de Guerra del Perú o, caso contrario, considerar una nueva especialidad de *Ciberdefensa y Ciberseguridad* sería lo recomendable.

e. UNI (Universidad Nacional de Ingeniería)

En esta universidad, especializada en carreras de ingeniería para diversos sectores económicos, encontramos en la Facultad de Ingeniería Eléctrica y Electrónica la carrera de Ingeniería de Ciberseguridad (UNI, FIEE, 2024), en cuya descripción se aprecia una fuerte orientación a los aspectos prácticos, proyectos e incluso ciberdefensa, aunque habría que validar si esta parte coincide con la definición establecida según la ley de Gobierno Digital ya comentada previamente.

Es posible que en esta entidad encontremos conocimientos de ciberseguridad que, mediante acuerdos de colaboración, podrían estar también al servicio de la DIRESPROM con adaptaciones, para la segunda especialidad de Ingeniería de Sistemas ya comentada.

f. ESUP (Escuela Superior de Guerra Naval)

Esta entidad, a cargo de formar al oficial superior (ESUP, Escuela Superior de Guerra Naval, 2024), ofrece diversos programas de perfeccionamiento/posgrado, tales como el Programa de Alto Mando (orientado a los oficiales de alta graduación), en cuya estructura curricular, módulo de Estrategia y Seguridad, hay una asignatura de *Fundamentos de Ciberseguridad y Ciberdefensa*, que se estima como una de alcance propedéutico, añadiendo que el módulo está compuesto de 18 horas, sólo de teoría. No se tuvo acceso al resto de programas, pero por las descripciones se estima que se trata de instrucción orientada a la Planificación Estratégica, Administración y Coordinación con niveles políticos decisores.

Analizando esta realidad, considero que podría ser oportuno incluir un Programa o Curso Corto de Ciberdefensa en el Ciberespacio (un trimestre, por ejemplo), de corte eminentemente práctico, donde se plantee a los alumnos, dentro de la Prospectiva de Escenarios, situaciones en las que se incluyan amenazas, detección de amenazas (inteligencia), ciberataques, reducción de vulnerabilidades y las acciones de ciberdefensa o ciberseguridad que se deben tomar, a modo de

estudio de casos. El trabajo coordinado con la Comandancia de Ciberdefensa (COMCIBERDEF) y el aporte por el lado de DIRESPROM será vital para incluir los ajustes que aseguren una formación acorde a las necesidades de defensa.

Entonces, es posible construir una columna o jerarquía de conocimientos que permitan accionar al personal instruido en el entorno digital, sea en ciberdefensa o en ciberseguridad, como se muestra en la Tabla N.º 3.

TABLA N.º 3

Nivel de estudios/Jerarquía	Capacidades	Acciones
Oficiales Superiores	Gestión, Planificación en Ciberdefensa, Ciberseguridad	Planes Gestión aplicados a Suprimir Amenazas y/o Ataques al ciberespacio, reducción de vulnerabilidades
Oficiales Subalternos	Especialización, Soporte Operacional en Ciberdefensa	Planes Ejecución aplicado a asegurar el ciberespacio de ciberataques, reducción de vulnerabilidades
Personal Técnico	Especialización técnica en Ciberdefensa	Soporte técnico y de sistemas a las acciones de ciberdefensa, ciberataque, supervisión de instalaciones físicas

Fuente: Elaboración propia

Finalmente, haciendo un estimado del costo que traería la implementación de estas iniciativas de formación, se puede hacer, para los fines de la Marina de Guerra del Perú y a modo de Perfil, una equivalencia o promedio con el costo de formación en la educación privada que hemos presentado (Educación al Futuro, 2016). En ese sentido, alcanzo en la Tabla N.º 4 un resumen de costos aproximados para los tres niveles. Suponiendo en un año dado en el futuro se entregue el personal, a promoción completa, con las capacidades requeridas, el costo total involucrado asciende a USD 585,000. Si se consideran los equipos, licencias adicionales y expertos para el empuje inicial, se estima un 20% adicional, haciendo un total de USD 702,000.

TABLA N.º 4

Nivel	Costo por promoción	Equivalencia
ESUP	USD 30,000 Programa Ciberdefensa	1 Trimestre de formación. 10 alumnos por promoción. Equivalencia ESAN
ENP	USD 430,000 Ingeniería de Ciberseguridad	2 años de formación. 10 alumnos por promoción. Equivalencia UNI
CITEN	USD 125,000 Técnico en Ciberseguridad	3 años de formación. 25 alumnos por promoción. Equivalencia SENATI.

Fuente: Elaboración propia

4. CONCLUSIONES

- El concepto de Ciberdefensa incluye acciones proactivas, esto es, accionar para suprimir la amenaza o prepararse para afrontarla, además de actuar remedialmente ante ciberataques, a diferencia de la ciberseguridad que se orienta a asegurar el entorno digital contra ciberataques.
- El conjunto de leyes alrededor de la Ciberdefensa, Confianza y Gobierno Digital, aun siendo de años diversos y con modificaciones, contiene los mecanismos para asegurar los ACN de acuerdo a lo concluido en el punto anterior.
- De acuerdo a cifras estadísticas públicas del 2019, el impacto económico anual estimado a futuro en el ámbito marino portuario del dominio marítimo, responsabilidad de la MGP, tiene una base 2020 de casi USD 1,000 millones por ciberataques, en perjuicio de las exportaciones peruanas.
- En el 2019, el Perú reportó un número de ciberataques concretados, superior a la media de la costa del Pacífico, con tendencia clara a subir debido al tráfico de naves esperado a futuro, considerando el impacto del puerto de Chancay, generando un gran riesgo de no tomarse acciones en ciberdefensa y ciberseguridad.
- Comparado con el sector privado, SENATI, se nota una falencia o retraso en la oferta de estudios en el CITEN en cuanto a ciberseguridad.
- De la información disponible, no se nota énfasis en ciberseguridad y ciberdefensa en la especialidad de Ingeniería de Sistemas de la MGP, a diferencia de la UNI que ya cuenta con una carrera de Ingeniería de Ciberseguridad, que incluso menciona preparación en Ciberdefensa.

- El costo de entregar personal con las capacidades de Ciberdefensa y Ciberseguridad en un año, dado a futuro, es de USD 702,000, que representaría un promedio anual de USD 351,000.
- Considerando las conclusiones arriba expuestas, el costo porcentual estimado de implementar esta iniciativa de instrucción es de sólo 0.12% anual, si se reduce tan solo el 30% de las pérdidas estimadas, atractivo como ROI para ser incluido dentro de la propuesta de presupuesto anual de la MGP.

5. RECOMENDACIONES

- Validar la malla curricular de la especialidad de Ingeniería de Sistemas de la Marina, para evaluar la carga correcta de instrucción en Ciberdefensa y Ciberseguridad, para actualizarla de ser el caso.
- Acercarse a la UNI para validar el contenido curricular orientado a la Ciberdefensa, para buscar replicar al interior de la ENP o ESUP, de tratarse de una buena práctica.
- Buscar acercarse y firmar convenios de intercambio académico con el SENATI y la UNI, con el fin de actualizar la instrucción y reforzar las capacidades, de ser el caso.
- Buscar el acercamiento con empresas privadas y gremios, para impulsar el gobierno digital con leyes promotoras. Concretamente, la SNI ha hecho un planteamiento al Congreso para dar ventajas a sectores claves, como las Tecnologías de Información, donde la MGP puede colaborar para poner en primer lugar el apoyo a la Ciberdefensa y Ciberseguridad. Este sería un primer paso a un real Gobierno Digital, donde el Estado vele por la Seguridad Digital. Se adjunta enlace a video explicativo (SNI, Perú Industria al 2050, 2023), ver del minuto 70 al 73.
- Proponer en el presupuesto del año 2025 el plan de reforzamiento de la instrucción en Ciberdefensa y Ciberseguridad (USD 702,000), de alto ROI versus el daño esperado.

Referencias

CITEN, Instituto de Educación Superior Tecnológico Público Naval. (2024). Web Institucional. Carreras Profesionales. Administración y Logística. https://citen.edu.pe/area-administracion-y-logistica/

CITEN, Instituto de Educación Superior Tecnológico Público Naval. (2024). Web Institucional. Carreras Profesionales. Operaciones. https://citen.edu.pe/area-de-operaciones/

CITEN, Instituto de Educación Superior Tecnológico Público Naval. (2024). Web Institucional. Misión y Visión. https://citen.edu.pe/nuestra-mision-vision-y-valores/

Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. (2020). Diario Oficial El Peruano – Normas Legales. https://busquedas.elperuano.pe/dispositivo/NL/1844001-2

Decreto Legislativo N° 1412, Ley de Gobierno Digital. (2018). Diario Oficial El Peruano – Normas Legales. https://busquedas.elperuano.pe/dispositivo/NL/1691026-1

Decreto Legislativo N° 1641 que modifica el Decreto Legislativo N° 1138, Ley de la MGP. (2024). Diario Oficial El Peruano – Normas Legales. https://busquedas.elperuano.pe/dispositivo/NL/2321390-3

Decreto Supremo N° 005-2021-IN, Directiva nacional de Orden Interno para la protección de los ACN. (2021). Ministerio del Interior – Normas Legales. https://www.gob.pe/institucion/mininter/normas-legales/2013064-ds-005-2021-in

Decreto Supremo N° 106-2017-PCM, Aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los ACN. (2021). PCM. El Peruano– Normas Legales. https://busquedas.elperuano.pe/dispositivo/NL/1585361-1

Díaz R., "Estado de la ciberseguridad en la logística de América Latina y el Caribe", Serie Desarrollo Productivo, N° 228, Santiago, CEPAL, 2021. https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

Educación al Futuro, (2024). En una Universidad Peruana ¿Cuánto cuesta estudiar? https://educacionalfuturo.com/noticias/costos-de-estudios-en-universidades-peruanas/

ENP, Escuela Naval del Perú. (2024). Carrera Naval. 4° Año. https://www.escuelanaval.edu.pe/carrera-naval

Escuela de Especialización Profesional de Oficiales de la Marina, DIRESPROM. (2024). Segunda Especialidad Ingeniería de Sistemas. Programa. https://esprom.edu.pe/dirtel/

ESUP, Escuela Superior de Guerra Naval, (2024). Perfeccionamiento. Programa de Alto Mando. https://www.esup.edu.pe/perfeccionamiento/

Ley N° 30999, Ley de Ciberdefensa. (2019). Diario Oficial El Peruano – Normas Legales. https://busquedas.elperuano.pe/dispositivo/NL/1801519-5

MINCETUR - Ministerio de Comercio Exterior y Turismo, PROMPERU (2023). Resultado de Exportaciones Perú 2022. https://recursos.exportemos.pe/resultados-exportaciones-peru-2022.pdf

Observatorio CEPLAN (2021). Perú próspero, equitativo y pacífico. Lima, Perú. CEPLAN. https://observatorio.ceplan.gob.pe/ficha/e1_cp

Observatorio CEPLAN (2022). Ruptura generalizada en las medidas de ciberseguridad. Lima, Perú. CEPLAN. https://observatorio.ceplan.gob.pe/ficha/r48_2022

Plan Estratégico de Desarrollo Nacional 2050, CEPLAN (2023). Diario Oficial El Peruano – Normas Legales. https://www.gob.pe/institucion/ceplan/informes-publicaciones/4637571-peru-plan-estrategico-de-desarrollo-nacional-al-2050

Revista GANAMÁS, (28 Junio, 2015). ADEX: El 72% de las exportaciones peruanas se realiza por vía marítima. https://revistaganamas.com.pe/adex-el-72-de-las-exportaciones-peruanas-se-realiza-por-via-maritima/

Secure Connections & The Asia Foundation. 2022. Cibersecurity in The Philippines: Global Context and Local Challenges. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

SENATI, Servicio Nacional de Adiestramiento en Trabajo Industrial. (2024). Ingeniería de Ciberseguridad. https://www.senati.edu.pe/especialidades/tecnologias-de-la-informacion/ingenieria-de-ciberseguridad

SNI, Sociedad Nacional de Industrias, Semana de la Industria 2023, Perú Industria al 2050 (min 70 a 73). https://www.youtube.com/live/EREdW_yLWvc?feature=share

UNI, Universidad Nacional de Ingeniería. (2024). FIEE. Escuela Profesional de Ingeniería de Ciberseguridad. https://fiee.uni.edu.pe/es/ingenieria_ciberseguridad

Vargas, R., Recalde, L., Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, N° 20, 31-45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571

Secure Connections & The Asia Foundation. 2022. Cibersecurity in The Philippines: Global Context and Local Challenges. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

SENATI, Servicio Nacional de Adiestramiento en Trabajo Industrial. (2024). Ingeniería de Ciberseguridad. https://www.senati.edu.pe/especialidades/tecnologias-de-la-informacion/ingenieria-de-ciberseguridad

SNI, Sociedad Nacional de Industrias, Semana de la Industria 2023, Perú Industria al 2050 (min 70 a 73). https://www.youtube.com/live/EREdW_yLWvc?feature=share

UNI, Universidad Nacional de Ingeniería. (2024). FIEE. Escuela Profesional de Ingeniería de Ciberseguridad. https://fiee.uni.edu.pe/es/ingenieria_ciberseguridad

Vargas, R., Recalde, L., Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, N° 20, 31-45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571