MARINA DE GUERRA DEL PERÚ

ESCUELA SUPERIOR DE GUERRA NAVAL

PROGRAMA COMANDO Y ESTADO MAYOR

MAESTRÍA EN ESTRATEGIA MARÍTIMA

Tesis

Para optar el grado académico de

Maestro en Estrategia Marítima

"Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú"

Presentado por:

Maestro, Capitán de Corbeta, Donna Melody Silva Gurrionero

https://orcid.org/0000-0001-7187-5267

Asesor Metodológico:

Doctor, Capitán de Navío (r), Arturo Guillermo Arriarán Schaffer

https://orcid.org/0000-0002-8496-7897

Asesor Técnico:

Maestro, Capitán de Corbeta, Luis Andrés Meza Medina

https://orcid.org/0009-0004-6019-9370

La Punta, 2024

Acta de sustentación

ESCUELA SUPERIOR DE GUERRA NAVAL
DEPARTAMENTO DE INVESTIGACIÓN
DIVISIÓN DE TRABAJOS DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS Nº 013

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN ESTRATEGIA MARÍTIMA

La Punta, 13 Diciembre 2024

En cumplimiento de lo establecido en la Resolución Directoral Nº 063-2024-MGP/DIRESUVAL de fecha 10 de diciembre del 2024, se reúne el Jurado integrado por:

1. Doctor, Carl Johan BLYDAL (Presidente)
2. Maestro, Calm. (r) Andrés ARRIARÁN Schaffer (Miembro)
3. Maestro, C. de C. Alfredo MIRANDA Capurro (Miembro)

Para evaluar la sustentación del trabajo de investigación tipo tesis titulado: **"Análisis Comparativo de las Políticas de Ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú"**, presentado por el Capitán de Corbeta Donna Melody SILVA Gurrionero.

Después de escuchar la exposición y defensa de la Tesis, y como resultado de la deliberación, se acuerda conceder la calificación cualitativa de:

- ☐ Aprobado por Unanimidad, con calificación de Sobresaliente y recomendación a publicación, con la denominación de "Summa cum laude".
- ☐ Aprobado por Unanimidad, con calificación de Muy Bueno y recomendación a publicación, con la denominación de "Magna cum laude".
- ☒ Aprobado por Unanimidad, con calificación de Bueno, con la denominación de "Cum laude".
- ☐ Aprobado por Mayoría
- ☐ Desaprobado

En mérito de lo cual el Jurado le declara: **Apto** ☒ **No Apto** ☐

Para que se le otorgue el Grado Académico de Maestro en Estrategia Marítima.

En fe de lo expuesto firman la presente:

Presidente
Doctor
Carl Johan BLYDAL
C.E. 000876227

Integrante
Maestro, Contralmirante (r)
Andrés ARRIARÁN Schaffer
DNI: 43419519

Integrante
Maestro, Capitán de Corbeta
Alfredo MIRANDA Capurro
DNI: 44325449

Declaración jurada de originalidad

ESCUELA SUPERIOR DE GUERRA NAVAL
DEPARTAMENTO DE INVESTIGACIÓN
DIVISIÓN DE TRABAJOS DE INVESTIGACIÓN

DECLARACIÓN JURADA DE ORIGINALIDAD Y NO PLAGIO DEL AUTOR DEL INFORME FINAL DE TESIS

La Punta, 11 de setiembre de 2025

Yo, Maestro, Capitán de Corbeta, Donna Melody Silva Gurrionero, identificado con 45800906, del programa de Maestría en Estrategia Marítima, declaro bajo juramento, que el presente trabajo de investigación tipo tesis titulado "Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú" es original, elaborado por el suscrito, no vulnera los derechos intelectuales de terceros y no contiene plagio de ninguna naturaleza.

Dejo formal constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no he asumido como mías, las opiniones, ideas, textos, figuras, tablas o cualquier otra información vertida por terceros, ya sea de fuentes encontradas en medios escritos, digitales o de Internet.

Declaro que soy plenamente consciente de todo el contenido del trabajo de investigación presentado y asumo total responsabilidad de cualquier error u omisión en el documento y soy consciente de las connotaciones éticas y legales que ello implica.

Asimismo, me hago responsable ante la Escuela Superior de Guerra Naval o terceros, de cualquier irregularidad o daño que pudiera ocasionar, por el incumplimiento de lo declarado.

De identificarse falsificación, plagio, fraude, asumo las consecuencias y sanciones que de mi acción se deriven, responsabilizándome por todas las cargas pecuniarias o legales que se deriven de ello, sometiéndome a las normas establecidas por la Escuela Superior de Guerra Naval, la Marina de Guerra del Perú y los dispositivos legales vigentes.

Sin otro particular, quedo a la espera de la aceptación de mi propuesta.

Atentamente,

Maestro, Capitán de Corbeta, Donna Melody
Silva Gurrionero
45800906

N - II - 1

Informe de similitud

ESCUELA SUPERIOR DE GUERRA NAVAL
DEPARTAMENTO DE INVESTIGACIÓN
DIVISIÓN DE TRABAJOS DE INVESTIGACIÓN

INFORME DE SIMILITUD DEL ASESOR METODOLÓGICO

Yo, **Arturo Guillermo ARRIARÁN Schaffer**, con DNI **43317937**, en mi condición de asesor metodológico del trabajo de investigación del Programa de Maestría en **Estrategia Marítima** de la Escuela Superior de Guerra Naval.

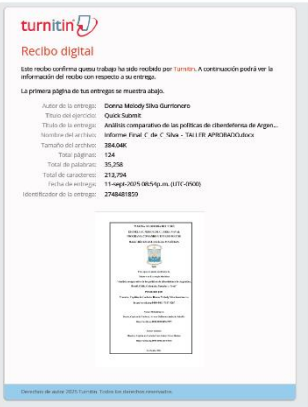
DECLARO:
Que la Tesis titulada **"Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú"**, presentada por el **Maestro, Capitán de Corbeta, Donna Melody SILVA Gurrionero**, para el otorgamiento del grado académico de **Maestro en Estrategia Marítima**, ha sido revisada con la aplicación autorizada por la Escuela Superior de Guerra Naval (Sistema Antiplagio Turnitin), utilizando los filtros autorizados; habiéndose obtenido un reporte con un índice de similitud de **20%**.

Se ha revisado con detalle dicho reporte y no se advierte indicios de plagio en las coincidencias detectadas, atribuyéndose la autoría a las fuentes de información utilizadas.

A mi leal saber y entender la Tesis Completa cumple con todas las normas para el uso de citas y referencias establecidas por la Escuela Superior de Guerra Naval.

La Punta, 11 de setiembre de 2025

Doctor, Capitán de Navío (r), Arturo Guillermo ARRIARÁN Schaffer
DNI 43317937


turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Donna Melody Silva Gurrionero
Título del ejercicio:	Quick Submit
Título de la entrega:	Análisis comparativo de las políticas de ciberdefensa de Argen...
Nombre del archivo:	Informe Final_C. de C. Silva - TAI LTE APROBADO.docx
Tamaño del archivo:	384.04K
Total páginas:	124
Total de palabras:	35,258
Total de caracteres:	213,794
Fecha de entrega:	11-sept-2025 08:51p.m. (UTC-0500)
Identificador de la entrega:	2748481859

Derechos de autor 2025 Turnitin. Todos los derechos reservados.


turnitin Página 2 de 144 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3336633301

20% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Autorizacion de publicación

ESCUELA SUPERIOR DE GUERRA NAVAL
DEPARTAMENTO DE INVESTIGACIÓN
DIVISIÓN DE TRABAJOS DE INVESTIGACIÓN

AUTORIZACIÓN DE PUBLICACIÓN DEL INFORME FINAL DE TESIS

La Punta, 11 de septiembre de 2025

Yo, Maestro, Capitán de Corbeta, Donna Melody Silva Gurrionero, identificado con 45800906, del programa de Maestría en Estrategia Marítima.

Atendiendo al carácter: ☒ PÚBLICO ☐ CLASIFICADO ☐ CERRADO

Del trabajo de investigación tipo tesis titulado "Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú"

Dejo formal constancia de autorización, para que se publique en los repositorios de la Escuela Superior de Guerra Naval y del SUNEDU, el referido trabajo, de forma:

☒ TOTAL

☐ PARCIAL ..... (indicar las secciones o páginas que no se autorizan a ser publicadas)

☐ SÓLO EL RESUMEN

Atentamente,

Maestro, Capitán de Corbeta, Donna Melody
Silva Gurrionero
45800906

N – III - 1

DEDICATORIA

A Zoila, una de las personas más importantes en mi vida, quien enfrentó con valentía una dura enfermedad, siendo un faro de fortaleza y esperanza. Su apoyo incondicional y sus palabras llenas de sabiduría me brindaron la fuerza necesaria para avanzar en los momentos más difíciles en los primeros años de mi vida.

Su presencia y espíritu estarán siempre reflejados en cada página de esta tesis. Este logro también es tuyo, aunque no puedas compartir este momento conmigo, sé que de alguna manera estás aquí, siempre vivirás en mi corazón y en mis recuerdos.

AGRADECIMIENTO

A Dios, por ser mi guía y fortaleza en todo momento, iluminando mi camino con su sabiduría y amor infinito. A mi familia, mi mayor tesoro, por su incondicional apoyo, amor y sacrificios, quienes con su ejemplo y fe me han acompañado siempre. A mi asesor metodológico, cuya paciencia, dedicación y valiosas enseñanzas han sido fundamentales en este proceso. A mi asesor técnico, por su constante comunicación, disposición y asesoramiento, contribuyendo de manera decisiva al éxito de este trabajo.

ÍNDICE

Pág.

ÍNDICE DE TABLAS

Pág.

RESUMEN

Esta investigación tiene como objetivo presentar los resultados que se desprenden del análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

Respecto a la metodología, se adoptó un enfoque cualitativo con un diseño basado en el análisis documental. La investigación fue de tipo básica, con un carácter descriptivo y un alcance temporal transversal. La muestra estuvo constituida de documentos en relación con la ciberdefensa, seleccionados principalmente del Portal de Política Cibernética y que tuvieron la mayoría de los componentes de las políticas empleadas para el desarrollo de la investigación. También se tuvo en cuenta a especialistas de cada Estado menos de Brasil.

Para la recolección de datos, se empleó como instrumentos las fichas de registro bibliográfico, fichas de análisis y fichas de resumen, para ubicar la información y hacer las referencias, establecer los componentes de las políticas y su contenido. Además, se empleó una guía de entrevista semiestructurada para reforzar los hallazgos documentales desde la opinión de los especialistas. Para el procesamiento de la información recopilada, se empleó el análisis de contenido y el análisis del discurso.

Entre los resultados más destacados, se identificaron tanto similitudes como diferencias en la estructura y el contenido de las políticas analizadas. Ante esto, los Estados concuerdan en algunos aspectos de interés para Perú, como el reforzamiento y desarrollo continuo de las capacidades de ciberdefensa, principios como la cooperación internacional, la gestión y prevención de incidentes, así como la resiliencia. Además, los Estados poseen componentes exclusivos, concluyendo que hay elementos distintivos que pueden ser útiles para el Estado Peruano.

Palabras clave: Ciberdefensa, comparación de políticas.

ABSTRACT

This research aims to present the results that emerge from the comparative analysis of the cyberdefense policies of Argentina, Brazil, Chile, Colombia, Ecuador, and Peru.

Regarding the methodology, a qualitative approach was adopted with a design based on documentary analysis. The research was of a basic type, with a descriptive nature and a cross-sectional temporal scope. The sample consisted of documents related to cyber defense, selected mainly from the Cyber Policy Portal and which had most of the components of the policies used for the development of the research. Specialists from each state except Brazil were also taken into account.

For data collection, bibliographic record sheets, analysis sheets and summary sheets were used as instruments, to locate the information and make references, establish the characteristics of the policies and their content. In addition, a semi-structured interview guide was used to reinforce the documentary findings from the opinion of the specialists. For the processing of the information collected, content analysis and discourse analysis were used.

Among the most outstanding results, both similarities and differences were identified in the structure and content of the policies analyzed. In view of this, the States agree on some aspects of interest to Peru, such as the reinforcement and continuous development of cyber defense capabilities, principles such as international cooperation, incident management and prevention, as well as resilience. In addition, the States have exclusive characteristics, concluding that there are distinctive elements that can be useful for the Peruvian State.

Keywords: Cyber Defense, comparison of policy

INTRODUCCIÓN

Las nuevas tecnologías en el mundo facilitan la transmisión de datos, exigen un control riguroso sobre lo que se puede compartir y quién tiene acceso a esos datos, especialmente cuando se trata de información clasificada como secreto nacional. La exposición de estos datos a otros Estados o individuos puede representar un grave riesgo, particularmente en el caso de secretos militares que podrían ser utilizados en perjuicio del Estado. Además, la protección de la tecnología operacional (OT), que abarca sistemas críticos en el ámbito militar como infraestructuras de comunicaciones, sistemas de armas, comando y control, sistemas de armas, se ha convertido en una prioridad, ya que estas tecnologías son esenciales para garantizar la operatividad y seguridad del Estado. Por ello, es indispensable implementar acciones de ciberdefensa que, a través de políticas bien definidas, establezcan protocolos eficaces para prevenir, mitigar y saber responder prontamente a cualquier amenaza cibernética.

En este aspecto, diversos Estados pueden tener distintas políticas que aborden las amenazas cibernéticas, reconociendo que hay algunos que tienen mejores capacidades. Por tal motivo, el análisis de dichas políticas de los Estados como Argentina, Brasil, Chile, Colombia, Ecuador ayudaría al aprendizaje del Estado peruano para poder establecer mejoras en un futuro que puedan incrementar la eficacia de la ciberdefensa en el ámbito militar del contexto peruano, reforzar la seguridad y favorecer la tranquilidad social.

Por tal motivo, se tiene como objetivo, hacer un análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú, para comprender cómo otros Estados plantean sus normativas y aprender sobre los demás y mejorar los lineamientos existentes, siendo beneficioso para optimizar la seguridad digital, proteger los activos y recursos digitales del Estados peruano.

De este modo, para resolver el objetivo principal, se desarrolla la siguiente estructura en el informe de investigación:

El Capítulo I presenta la situación problemática, determinando el contexto del estudio y el propósito de este, luego se hizo la formulación del problema general y de los específicos, los objetivos, prosiguiendo con la justificación destacando su relevancia y culminando con las limitaciones.

El Capítulo II detalla los aspectos teóricos en relación con el tema de investigación, por medio de una revisión profunda de la literatura. Primero se exponen estudios previos o antecedentes tanto a nivel internacional como nacional que también pueden tener resultados similares los cuales contrastar. Luego se desarrollan las bases teóricas indicando conceptos, teorías, características referentes a las unidades temáticas, las bases normativas que se tienen en cuenta, finalizando con los conceptos claves que se abordan en la presente investigación.

El Capítulo III se hace mención del diseño metodológico que involucra el enfoque, tipo, método y diseño de investigación. Luego se señala la población y la muestra considerada, las categorías o unidades temáticas de interés, la hipótesis general, las técnicas e instrumentos de recolección de datos, las técnicas de procesamiento de información y los aspectos éticos, indicando en cada caso por qué se ha utilizado dichos métodos, técnicas, herramientas y procesos.

Luego, en el Capítulo IV se expone la información que se ha recopilado mediante los resultados, en base a los objetivos específicos para finalizar dando respuesta al objetivo general, en cada uno de ellos se describe según las tablas y figuras que se encuentran al final, realizando a su vez el análisis y discusión respectiva.

Por último, en el Capítulo V se establecen las conclusiones, resumiendo los principales hallazgos del estudio y consecuentemente las recomendaciones de acuerdo con los resultados.

Los hallazgos presentados, podrán ser considerados por el Ministerio de Defensa en la toma de decisiones pertinentes que mejoren las normativas con relación a la ciberdefensa, reforzando la seguridad nacional. Además, otros investigadores podrán ampliar este estudio para el incremento del conocimiento en este tema.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Situación problemática

Actualmente, gran parte del conocimiento se encuentra digitalizado y se comparte a nivel mundial. Sin embargo, cada Estado resguarda cierta información estratégica para su beneficio. Como señala Capi (2003 citado en Vargas et al., 2017) los datos confidenciales, al igual que la información personal, pueden ser almacenados y recopilados con el propósito de generar ventajas económicas y políticas que impulsen su desarrollo nacional. No obstante, esta información es susceptible de ser vulnerada, lo que evidencia que persisten conflictos relacionados con la obtención de datos, especialmente en el entorno virtual (Vargas et al., 2017).

De este modo, se comprende que el conflicto es algo común y aún se mantiene en los seres humanos (Feliu 2013, citado en Vargas et al., 2017). Con el avance tecnológico, estos conflictos han evolucionado, dando lugar a nuevas formas, como los ataques en el ámbito virtual. Estos ataques, conocidos como ciberataques, pueden ser perpetrados por individuos o grupos contra los Estados, generando graves consecuencias, como pérdidas económicas o la paralización de infraestructuras críticas, tal como ocurrió en Estonia en 2007 (Klimburg, 2012).

Esto evidencia que, si el bienestar de una sociedad y su economía dependen del manejo de la información y del mercado digital, la seguridad también debe alinearse con estas necesidades. En este sentido, las medidas destinadas a protegerse de amenazas y riesgos deben contribuir a generar confianza y tranquilidad ya sea en la virtualidad y en el mundo real (Vargas et al., 2017). Por ello, cada Estado que aspire a garantizar su seguridad debe identificar los aspectos clave para su defensa, los cuales deben ser coherentes con su nivel de desarrollo y capacidades (De Vergara, 2009, citado en Vargas et al., 2017).

Este fenómeno que ocurre en el ciberespacio es requerido para que las naciones se desarrollan, ya que forma parte integral de sus estrategias de crecimiento y es fundamental para la obtención de poder frente a otros Estados (The Economist, 2010). La intromisión en los datos informáticos de un Estado se clasifica como un ciberataque, definido como cualquier intento de acceder, exponer, inutilizar, alterar o utilizar información de forma no autorizada. Estos ataques pueden ser perpetrados por otros Estados, entidades o individuos.

De este modo, la ciberseguridad un elemento necesario para la defensa, ya que garantiza un ciberespacio protegido contra daños y amenazas (ISO/IEC27032, 2012).

La ciberdefensa, se refiere a las medidas tomadas por un Estado para salvaguardar y gestionar cualquier tipo de amenaza o riesgo de origen cibernético. Su objetivo es asegurar que se use el ciberespacio de manera segura y adecuada, fortaleciendo las infraestructuras críticas de información. Además, apoya al defender el control del territorio y su soberanía. Es importante tener en cuenta, que los desafíos novedosos que presenta el entorno cibernético son capaces de influir en la definición de estrategias viables, para cumplir con la variedad de situaciones militares de ciberdefensa (Virilio, 1995, citado en Vargas et al., 2017). De acuerdo con la Ley de Ciberdefensa (2023), la ciberdefensa se trata de aquella capacidad militar, para poder actuar sobre los ataques o amenazas presentadas en y por medio del ciberespacio, los cuales pueden afectar negativamente a la seguridad del Estado.

Los gobiernos, entidades regionales, organismos de seguridad y defensa han comenzado a modificar sus estrategias, para poder combatir cualquier amenaza dentro del ciberespacio o en lo posible disminuir sus efectos. Algunas naciones en América Latina han seguido este camino; no obstante, a pesar de todas estas iniciativas, gran parte de los Estados hasta ahora no han conseguido adaptarse por completo a este entorno, probablemente debido a que cada Estado tiene diferentes habilidades, presupuestos, recursos, infraestructuras y políticas de gestión (Vargas et al., 2017). Ante esto, Mariano y Núñez (2023) mencionan que en entre los años 2020 a 2022 hubo 82 incidentes que afectaron a 10 países de Latinoamérica, generalmente enfocados a bancos. Por su parte, Robledo (2023) refiere que América Latina y el Caribe su índice es del 33.85 referente a ciberseguridad global a comparación de otros continentes y Estados Unidos presenta el índice máximo (100.0), lo que demuestra que esta región aún posee falencias y es la que menor índice posee.

Sobre ello, Paredes y Ángelo (2024) indica que Ecuador muestra una capacidad emergente para gestionar y tomar medidas que fortalezcan la ciberseguridad y la ciberdefensa. Sin embargo, su capacidad aún es limitada, lo que resulta en su posición en el último lugar en el ranking de ciberseguridad de la Unión Internacional de Telecomunicaciones, con un porcentaje del 26.3%, siguiéndole Argentina con un 50.12%, Perú con un 55.67%, Colombia con un 63.72%, Chile con 68.83% y encabeza Brasil con un 96.6% de índice de ciberseguridad. Siendo de interés la ciberseguridad, respecto a defender los intereses de cada Estado, resaltan los problemas que se encontraron referente a los ataques a diversos Estados, como, por ejemplo, la web de Forbes (2021) señala que los

ataques más importantes fueron en el año 2021, en donde una compañía (*Solarwinds*) fue atacada y de ella se robaron información del gobierno de los Estados Unidos, demorando en ser descubierto.

Por otra parte, en Colombia, si bien se destacó la reducción de los ataques cibernéticos al gobierno, aún intentan derribar sus servidores y sus páginas web (Noticias RCN, 2022). En Costa Rica, el grupo Conti empleó un *ransomware* que secuestró información de 30 entidades del país, entre ellos sus ministerios siendo el más perjudicado el de hacienda, secuestrando datos fiscales y de comercio con otros Estados, perdiendo millones de dólares (BBC Noticias, 2022). También, el Gobierno de México (2020) señala que hay un incremento cuatro veces mayor de ataques a instituciones gubernamentales y a personas mundialmente.

Referente a Perú en la ciberseguridad, ha quedado atrás, sobre todo por la falta de inversión en esta. Durante el 2021, Perú sufrió numerosos ciberataques, lo que lo posicionó como el Estado más atacado de América Latina, evidenciando la fragilidad de su infraestructura de seguridad cibernética (Quevedo, 2023). Perú muestra una carencia en cuestiones de ciberseguridad y ciberdefensa, ya que no se han implementado de manera efectiva, los procesos que ayudan a fortificar la seguridad de la información pública y privada. Esta insuficiencia, es explicada por la poca amenaza a gran escala, generando bajo interés en los gobernantes. En este contexto, esta falta de motivación constituye uno de los desafíos más significativos para alterar el curso de esta situación (Quevedo, 2023). Los ciberataques realizados en Perú fueron diversos, registrándose para el año 2021 más de 4.7 mil millones, entre ellos ataques al gobierno (Fortinet, 2021).

Ante esto, es importante comprender que posiblemente los lineamientos en ciberdefensa del Estado no son los adecuados y que otros Estados podrían tener diferentes normativas, que, mediante un análisis comparativo, se podría entender qué aspectos son diferentes e importantes para poder considerarlos, debido a que falta profundizar en estos temas. En este aspecto, Robledo (2023) refiere que sólo un pequeño número de Estados, han declarado claramente sus políticas de ciberseguridad, pero casi ninguno lo ha hecho en términos de ciberdefensa. Además, en la mayoría de los Estados, no se conocen o simplemente no existen posturas oficiales sobre aquellos procedimientos, para tomar decisiones que favorezcan a la construcción de la gobernanza global de internet y la ciberseguridad.

De este modo, comprender esta problemática y analizar cómo otros Estados estructuran sus normativas resulta fundamental para el Estado peruano y las entidades encargadas de estos temas. Este aprendizaje permite mejorar los lineamientos existentes, lo que beneficia la optimización de toda protección y seguridad en el entorno virtual, así como de los recursos digitales del país, fortaleciendo la disposición a responder de manera activa ante amenazas en el ciberespacio. La carencia de dicho conocimiento incrementa la vulnerabilidad frente a posibles ataques y representa un riesgo significativo para la seguridad nacional. Por ello, este estudio se enmarca en la realidad peruana y el contexto latinoamericano, abarcando el análisis de los Estados de Argentina, Brasil, Chile, Colombia, Ecuador y Perú respectivamente.

1.2 Formulación del problema

1.2.1 Problema general

¿Qué resultados se desprenden del análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?

1.2.2 Problemas específicos.

PE1: ¿Qué políticas de ciberdefensa tienen Argentina, Brasil, Chile, Colombia, Ecuador y Perú?

PE2: ¿Qué componentes se pueden identificar de la estructura de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?

PE3: ¿Cuáles son las similitudes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?

PE4: ¿Cuáles son las diferencias de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?

1.3 Objetivos de la investigación

1.3.1 Objetivo general.

Presentar los resultados que se desprenden del análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

1.3.2 Objetivos específicos.

OE1: Identificar las políticas de ciberdefensa que tienen Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

OE2: Especificar los componentes de la estructura de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

OE3: Determinar las similitudes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

OE4: Determinar las diferencias de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

1.4 Justificación de la investigación

La seguridad de un Estado es un pilar fundamental, sobre todo en los tiempos actuales en donde la globalización y digitalización van de la mano. La información con la que cuentan los Estados, crucial para su seguridad y desarrollo, suele mantenerse como un secreto frente a terceros. Sin embargo, esta información es susceptible de ser vulnerada, lo que hace que la ciberdefensa sea indispensable. A pesar de ello, no siempre se cuenta con políticas adecuadas para garantizar su plena efectividad, mientras que otros Estados pueden disponer de políticas más avanzadas que sirvan como referencia para fortalecer la protección de información sensible.

Esta investigación proporciona un beneficio al identificar estrategias efectivas y fallas comunes, ayudando a optimizar las políticas nacionales. Esto es especialmente útil para entidades gubernamentales, al ofrecerles información fundamentada sobre la implementación de políticas aplicadas en otros contextos gubernamentales, según los resultados obtenidos.

Por otro lado, el estudio también beneficiará a la población en general y al gobierno peruano, ya que elevará el nivel de ciberseguridad y ciberdefensa, permitiendo resguardar las infraestructuras críticas de información de la nación, que son activos críticos nacionales (ACN) importantes. Estos activos son esenciales para el desarrollo y seguridad del Estado, con especial énfasis en sectores estratégicos, como el militar, que son fundamentales para la defensa nacional.

Además, otros sectores del Estado, tras los resultados del estudio, podrán desarrollar prácticas y proyectos para adoptar acciones para la seguridad de la información con potencial riesgo de ser vulnerada. Por último, favorece a los investigadores de estos temas a tener un antecedente que pueda servir para futuros estudios, pudiendo comparar otras realidades fuera del continente, empleando los mismos pasos o metodologías consideradas en la presente.

1.5 Limitaciones de la investigación

Debido a que los datos se obtuvieron de manera libre mediante la web y las estrategias de análisis de dicha información son adecuadas, no se presentaron inconvenientes ni limitaciones para el presente estudio. Por otro lado, los entrevistados al ser de entidades internacionales y del ámbito militar, tuvieron tiempo limitado y en el caso de Brasil, no pudo otorgar información debido a políticas internas que requieren autorización para hablar sobre el tema y limitó la obtención de datos por su parte.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Internacionales.

Estudios previos que abordan el tema de investigación, es posible encontrar a nivel internacional, como el de Paredes y Ángelo (2024) procedente de Ecuador, titulado "El ciberterrorismo y la seguridad nacional" tuvieron como objetivo, determinar la sinergia de la estrategia de ciberseguridad del Estado y la guía de la ciberdefensa para minimizar el impacto del ciberterrorismo. Concluyeron, que Ecuador aún se encuentra en inicio respecto a la implementación de varios lineamientos como lo es la gestión de crisis, la consideración de ciberdefensa, la redundancia en la comunicación, confianza y seguridad en internet, el rol de los medios para difundir la educación en ciberseguridad y en la calidad de software que emplean para este propósito. También, en los aquellos controles criptográficos, técnicos de seguridad, así como el mercado en este ámbito y revelación responsable de datos; por lo que requieren la definición precisa de la infraestructura crítica del Estado, incremento de la capacidad de ciberdefensa y participación conjunta de la sociedad y el Estado, para alcanzar una sinergia que permita tener la resiliencia mínima requerida para evitar que estos ataques causen efectos críticos o catastróficos en el país, promoviendo el desarrollo tecnológico y reduciendo la dependencia tecnológica en un índice razonable.

Mosquera (2021) en su estudio en Ecuador, titulado "Experiencias de seguridad cibernética en Estados europeos y latinoamericanos. Apuntes hacia la defensa nacional", tuvo como objetivo analizar las experiencias relacionadas con la seguridad cibernética en Estados europeos y latinoamericanos, para la formulación de lineamientos que ayuden a una mejor defensa para el país. Concluyó que, haciendo la comparación con los lineamientos de otros países, Ecuador requiere de una ampliación de elementos jurídicos para la seguridad en el mundo virtual de las Infraestructuras Críticas en el Estado; para ello necesitarán de especialistas en este rubro, así como emplear los instrumentos legales pertinentes para garantizar la ciberseguridad.

Huamani y Aparecida (2024) en Brasil en su artículo titulado "Política y Estrategias de la Seguridad Cibernética: Argentina, Perú y Brasil", buscó comprender los elementos y agentes que influyen en el empleo de métodos de ciberseguridad de dichos Estados en

mención. Concluyeron que el aspecto sociocultural y organizacional tiene una importancia significativa para los objetivos de ciberseguridad, sin embargo, el aspecto geopolítico y diplomático tiene una relevancia menor para estos tres Estados de estudio.

Kosevich (2020) en Rusia, realizó un estudio titulado "Estrategias de seguridad cibernética en los países de América Latina", con el objetivo de presentar una visión amplia de las estrategias de ciberseguridad que adoptaron sólo siete países latinoamericanos. Según los hallazgos, varios países se destacan en diferentes aspectos de la ciberseguridad. Colombia ha desarrollado cronogramas detallados y esquemas de financiamiento, estableciendo cinco ejes principales: desarrollo coordinado, cooperación público-privada, cultura ciudadana de ciberseguridad, desarrollo de potencial en manejo de riesgos y generación de un fundamento de ciberseguridad estatal. Chile busca crear una infraestructura de TIC robusta para enfrentar incluso los ataques virtuales más complejos. Brasil se enfoca en mejorar la protección de su infraestructura crítica y las instituciones gubernamentales, con objetivos clave como aumentar el presupuesto de seguridad cibernética y garantizar un alto nivel de protección para las instituciones gubernamentales. Brasil aspira a ser un actor global en seguridad cibernética, planeando lograr esto a través de un aumento rápido de las inversiones internas en tecnología de la información, la creación de empleo y el trabajo mutuo entre el sector privado y público.

El estudio de Jarufe (2020) en Chile titulado "Políticas de ciberseguridad en la experiencia internacional", tuvo como objetivo describir las políticas de ciberseguridad en la experiencia internacional. Argentina, Corea del Sur, Nueva Zelanda y Singapur han establecido Estrategias Nacionales de Ciberseguridad para responder a las ciberamenazas, proteger su infraestructura crítica y promover la cooperación internacional en el ciberespacio. Colombia ha implementado una Política Nacional de Seguridad Digital que promueve un uso responsable de la red en todos los sectores sociales. Ecuador ha implementado un Plan Nacional de Gobierno Electrónico desde 2015, que establece una serie de sistemas tecnológicos gestionados por el Ministerio de Telecomunicaciones y de la Sociedad de la Información. En España, el Instituto Nacional de Ciberseguridad, subordinado al Ministerio de Economía y Empresa, se encarga del desarrollo de la ciberseguridad en relación con la sociedad en general, entidades privadas, el sector académico y aquellos sectores estratégicos del país. En Uruguay, una entidad con autonomía técnica se encarga de aprovechar al máximo las TIC, con énfasis en la inclusión digital de sus habitantes y el fortalecimiento de las habilidades de la sociedad en este ámbito.

El Centro de Estudios de Derecho e Investigaciones Parlamentarias (CEDIP, 2022) de México, en su estudio titulado “La ciberseguridad: un estudio comparado”, tuvo el propósito de desarrollar una guía coherente y práctica sobre cómo la ciberseguridad, puede ser interpretada como un fenómeno de estudio, mientras se formulan enfoques para entender sus desafíos. Concluyó que, los elementos comunes respecto a ciberseguridad en los países de Estados Unidos, Argentina, Brasil, Estonia, Singapur, son el hecho de haber implementado una Estrategia Nacional de Ciberseguridad (ENCS), uso de ciberseguridad, programas educativos, catálogos sobre infraestructuras críticas de información, además de programas educativos para concientizar sobre el empleo del internet y la navegación en línea para todo tipo de personas y entidades.

Odebade y Benkhelifa (2023) en Reino Unido en su artículo titulado “Un estudio comparativo de las estrategias nacionales de seguridad cibernética de diez naciones”, consideró como objetivo, comparar las ENCS de documentos disponibles públicamente de diez países de distintas partes del continente como Europa (Reino Unido, Francia, Lituania, Estonia, España y Noruega), Asia del Pacífico (Singapur y Australia) y la región de América (Estados Unidos de América y Canadá). El estudio observó que no existe una comprensión unificada del término “Ciberseguridad”; sin embargo, una trayectoria común de los ENCS muestra que la lucha contra el delito cibernético es un esfuerzo conjunto entre varias partes interesadas, de ahí la necesidad de una fuerte cooperación internacional. Además, la investigación encuentra similitudes en la protección de ACN, el compromiso con la investigación y el desarrollo, así como una mejor colaboración nacional e internacional; por lo que la falta de un marco unificado de ciberseguridad subyacente conduce a una disparidad en la estructura y el contenido de las estrategias.

Song et al. (2021) en Corea con el estudio “Análisis comparativo de las estrategias nacionales de ciberseguridad mediante modelos temáticos”, consideró como objetivo caracterizar las ENCS de los principales países, considerando cuantitativamente las series temporales e identificar otras agendas de ciberseguridad en beneficio de la revisión de las ENCS en Corea del Sur, aplicando modelos temáticos al análisis de ocho ENCS de Estados Unidos, Reino Unido, Japón, y UE. Concluyeron que, el enfoque de cada Estado hacia la ciberseguridad era diferente y entre los lineamientos establecidos, propusieron agendas adicionales que son un gran aporte para futuras revisiones de la ENCS en Corea del Sur.

Kshetri y Miller (2021) en Estados Unidos realizaron una investigación titulada “Un estudio sobre la ética de la defensa cibernética y las iniciativas de los gobiernos de los países

en desarrollo: un estudio de países seleccionados", su objetivo fue comprender los principios éticos de la ciberdefensa, las prácticas cibernéticas y diversas estrategias de defensa adoptadas por los gobiernos de varios Estados y su propuesta de ciberdefensa, para combatir los desafiantes problemas en el ciberespacio o los dominios cibernéticos. Concluyeron que muchos Estados subdesarrollados (así como Estados en desarrollo) alrededor del mundo, son el pilar de la economía y la seguridad en línea. El estudio de la economía del Estado, la ciberdefensa y las iniciativas cibernéticas de varios países analizados (China, India, Pakistán, Bangladesh y Nepal), difieren en naturaleza, tipo, presupuesto, relaciones internacionales e influencia gubernamental (ya sea el gobierno del Congreso o el gobierno comunista). Además, destaca la variedad y complejidad de las técnicas utilizadas por muchos Estados para combatir las ciberamenazas y salvaguardar activos digitales vitales.

Pranesh et al. (2024) procedentes de la India, realizaron una investigación titulada "Un estudio comparativo de las estrategias de ciberseguridad entre varios países", la cual tuvo como objetivo, realizar una comparación de las estrategias de ciberseguridad en varias dimensiones tales como objetivos de políticas, marcos legales, capacidades técnicas y cooperación internacional, entre los países seleccionados. Concluyeron destacando las estrategias de ciberseguridad de varios países; Estados Unidos y China se centran en proteger su infraestructura vital y desalentar la actividad maliciosa en línea. India se enfoca en desarrollar capacidades cibernéticas y fortalecer las leyes de ciberseguridad. El Reino Unido prioriza la prevención de ciberataques y el fomento del crecimiento económico. Israel promueve las asociaciones público-privadas y la innovación en ciberseguridad, mientras que Japón busca fomentar la colaboración internacional y mejorar las capacidades de ciberseguridad.

2.1.2 Nacionales.

Quevedo (2023) en su estudio titulado "Ciberdefensa y ciberseguridad en Perú: realidad y retos en torno a la capacidad de las FFAA para neutralizar ciberataques que atenten contra la Seguridad Nacional", buscó comprender la realidad sobre Ciberdefensa y ciberseguridad en Perú y la capacidad que tienen las Fuerzas Armadas para afrontarlo, mediante una revisión documental. Concluyó que, Perú enfrenta problemas en ciberdefensa, por la falta de implementación adecuada de tecnologías y procesos para fortalecer la protección de datos. Aunque hay cierta iniciativa, la inversión no es la requerida para su actualización permanente. Las Fuerzas Armadas (FFAA) peruanas, poseen limitaciones para contrarrestar importantes ataques cibernéticos, por el poco equipamiento y tecnología

necesaria. Se necesita una forma adecuada de gobierno en este tema, que incluya efectivamente el esfuerzo de los distintos sectores estatales. El estudio proporciona una visión clara y concisa de los desafíos que enfrenta el Estado en este aspecto. Destaca la necesidad de invertir y de hacer actualización continua en tecnologías de seguridad.

Rossi (2021) en su estudio "La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades de Perú en materia de ciberdefensa y amenazas híbridas", tuvo como objetivo, analizar los elementos de defensa y seguridad de Perú para plantear una propuesta que mejore las capacidades de ciberdefensa en el País. Llegó a concluir, que Perú ha reconocido que existen amenazas cibernéticas y ha establecido una base normativa inicial, para guiar la ciberdefensa y ciberseguridad en el Estado. Sin embargo, no hay entidad que haga una coordinación integral de los esfuerzos del estado en este contexto, así como faltan capacidades operativas, que aseguren un estado ideal. Aunque, el Ministerio de Relaciones Exteriores, debería poner en desarrollo una estrategia de política exterior, que refuerce la dentro del entorno cibernético, la defensa y seguridad del mismo, a través de la colaboración estratégica con otros entes internacionales, para formar profesionales capaces, obtener tecnología y desarrollarla.

Por último, Ormachea (2020) en su estudio "Estrategias integradas de ciberseguridad para el fortalecimiento de la Seguridad Nacional", buscó generar una propuesta para el fortalecimiento de la ciberseguridad en Perú, empleando para la observación y el análisis documental para obtener sus datos. Concluyó que el Estado y la sociedad en general, todavía están en proceso de ser más conscientes sobre la ciberseguridad y en desarrollar en el ámbito militar las capacidades de ciberdefensa, por lo que su mejora requiere de una colaboración entre ambos sectores, el privado y el público, lo cual no se ha logrado en Perú, siendo urgente una ENCS.

2.2 Bases teóricas

2.2.1 Ciberseguridad.

2.2.1.1 Conceptos.

La ciberseguridad comprende una serie de protocolos, directrices y estructuras destinadas a identificar, evitar y contrarrestar los ciberataques, garantizando al mismo tiempo, la solidez y precisión de la infraestructura digital y los sistemas de información (Pranesh et al., 2024). De acuerdo con la Organización Internacional de Normalización

(ISO, 2012) se conceptualiza como la capacidad para preservar la confidencialidad, mantener íntegro y disponible todos los datos del ciberespacio (Organización Internacional de Normalización, 2012).

Por otro lado, de acuerdo con Fuentes et al. (2023) la IBM señala que la ciberseguridad, es considerada como una práctica que consiste en la protección de los sistemas fundamentales y datos confidenciales ante cualquier ataque digital; a su vez, menciona que las medidas de ciberseguridad deben diseñarse con base en los tipos de amenazas que se están previendo, dado que cada una requiere de un tratamiento especial. También, de acuerdo con el Decreto de Urgencia que Aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento (2020) se entiende a la ciberseguridad como cuán capaz tecnológicamente es un sistema para que desempeñe una adecuada función de equipo, redes informáticas y activos, para protegerlos de cualquier amenaza o vulnerabilidad dentro del entorno digital.

De acuerdo c on Arreola (2019) la ciberseguridad en un Estado se comprende como un compendio de conceptos, políticas, herramientas de seguridad, medidas de protección, normas, manejo de riesgos, acciones, entre otros, que ayuden a salvaguardar los recursos informáticos del país, proteger la infraestructura crítica o activos estratégicos, implementar la seguridad cibernética pública, organizar la defensa cibernética, proteger la información y cuidar a los usuarios en el entorno cibernético contra cualquier amenaza. Esto establece la división de lo que respecta a la seguridad cibernética nacional en dos ramas: la seguridad cibernética pública (cibercrimen), que está a cargo de las agencias policiales, y la defensa cibernética (seguridad cibernética nacional), que es responsabilidad de las fuerzas armadas.

2.2.1.2 Características.

Las estrategias de creación de capacidad cibernética abordadas hasta ahora han identificado vías similares para proteger la infraestructura crítica contra amenazas, así como defender la seguridad nacional, la económica y a su vez respetar los derechos de los individuos. Existe un acuerdo general en que la capacidad cibernética, consiste en lograr resiliencia contra las amenazas basadas en Internet, mediante una variedad de políticas que incluyen la creación de estrategias nacionales de ciberseguridad, equipos de respuesta a incidentes de seguridad informática (CSIRT), el fortalecimiento de las leyes contra el delito cibernético, la promoción de la protección públicas y privadas,

así como la mejora de la educación y la sensibilización sobre este asunto (Calderaro & Craig, 2020).

Cuando existe una adecuada ciberseguridad, las Infraestructuras Crítica de Información (ICI), resultan seguras y confiables. No obstante, en situaciones en donde hay una carencia de control de ciberseguridad, son insuficientes o están mal delimitados, el entorno cibernético es visto como un territorio sin ley. Por lo tanto, los objetivos actuales de la ciberseguridad son prevenir, detectar, responder y recuperarse, aunque lo común era evitar que se lleve a cabo un ataque exitoso (Leiva, 2015).

2.2.1.3 Estrategia Nacional de Ciberseguridad (ENCS)

Las ENCS o NCSS (en inglés), son los documentos más concisos para comprender el enfoque nacional de protección del ciberespacio. Al menos 100 Estados han establecido estrategias nacionales para proteger su ciberespacio (Song et al., 2021). Una Estrategia Nacional de Ciberseguridad, puede ser vista como un componente esencial para un país, ya que tiene el potencial de fortalecer la resiliencia de las infraestructuras nacionales de información y sus servicios (Leiva, 2015).

Una ENCS, es un documento que refleja la dirección y la postura de la política de ciberseguridad ante las amenazas cibernéticas a nivel nacional. Debido a que, la ENCS establece objetivos y prioridades estratégicos nacionales para un período específico, es esencial considerar la evolución del entorno de amenazas cibernéticas y el enfoque nacional de la ciberseguridad de manera oportuna (Song et al., 2021). El análisis de los ENCS es esencial para determinar las posturas de respuesta a nivel nacional y para comprender las tendencias internacionales en ciberseguridad. Sin embargo, las ENCS incluyen endógenamente agendas multidimensionales, lo que dificulta realizar un análisis consistente y sistemático de las ENCS, para descubrir qué agenda debe abordarse en el desarrollo o revisión de una ENCS. Para los Estados que quieran establecer o revisar adecuadamente sus ENCS, es importante el análisis de los ENCS de Estados que tienen liderazgo en el ciberespacio o enfoques similares de ciberseguridad (Song et al., 2021).

La estructuración de una ENCS puede realizarse en áreas tales como inversión en investigación y desarrollo, concientización y capacitación, colaboración e intercambio de información, y asociación dentro de organizaciones gubernamentales, dependiendo de la necesidad y percepción del Estado (Min et al., 2015). En

consecuencia, se deben definir las metas, objetivos, alcance y prioridades de una estrategia nacional, para fomentar asociaciones entre las partes interesadas y comunicar los objetivos de un Estado a otros Estados (Sabillon et al., 2016). Las ENCS deben ser actuales, adecuadas y apropiadas para evitar poner en riesgo las TIC y la vida de los ciudadanos (Mori & Goto, 2018). Por lo tanto, se podría afirmar que una ENCS, es una herramienta para potenciar la seguridad y la resiliencia de la ICI, así como la sostenibilidad de los servicios nacionales informáticos. En términos generales, los propósitos de una ENCS incluirán la coordinación de acciones para trabajar de forma coherente, facilitar la colaboración pública y privada, comunicar directrices, obligaciones y formar vínculos entre todos los actores involucrados (Leiva, 2015).

La elaboración de Políticas o Estrategias de Ciberseguridad no es un proceso sencillo, y no está limitada únicamente a la implementación de normas la administración y la tecnología, sino que demanda un enfoque consensuado y armónico de acción y subraya la necesidad de innovación. Los participantes en el marco de una ENCS incluyen a todo el estado y sus agentes, además de los negocios, industrias, Pymes, universidades y la comunidad en su conjunto (Leiva, 2015).

2.2.1.4 Necesidad de ciberseguridad

En el entorno altamente conectado de hoy, es esencial tener una estrategia para maximizar los beneficios y minimizar los perjuicios, en las operaciones cotidianas en el ciberespacio. Esta necesidad estratégica ha surgido debido a que, en los últimos años, el número de incidentes que amenazan la ciberseguridad de los Estados ha aumentado, poniendo en riesgo los datos, la fiabilidad de la red, la seguridad de los usuarios y la ciberseguridad nacional (Arreola, 2019).

La Comisión Económica para América Latina y el Caribe (CEPAL, 2020), indica que la ciberseguridad, implica coordinar de manera enérgica en el país, las bases legales en donde se establezcan directrices claras para proteger la información. Para lograr esto, es esencial cooperar con otros Estados, debido a que es fundamental para combatir cualquier amenaza cibernética. Además, también favorece la alianza pública y privada de tal forma que sea efectiva la ciberseguridad. Además, la institución señala la necesidad de un marco legal, así como una política definida que garantice la ciberseguridad con efectiva gobernanza, esto en base a una entidad centralizada de gestión de la ciberseguridad, esto para favorecer a una respuesta pronta con acciones

operativas ante las amenazas, con el soporte de otras entidades nacionales e internacionales. En este aspecto, la entidad refiere que resulta muy importante tener una agenda integral de ciberseguridad, especificando los sectores más importantes a defender y sobre ello, los ataques pueden darse en distintos niveles de gobierno, lo que hace priorizar la inversión para afrontar los riesgos. Por otra parte, recomienda tener un efectivo sistema de datos para proteger a los civiles de robo de identidad y fraudes a entidades públicas, desarrollando tecnología y habilidades de ciberseguridad para estos fines.

2.2.2 Ciberdefensa.

2.2.2.1 Conceptos.

Consta de actividades ejecutadas por el Estado, para tener un mayor alcance de la defensa ante posibles amenazas, en un entorno de interconectividad en donde participan actores estatales y aquellos no lo son (Vargas et al., 2017; CEDIP, 2022). También, se entiende según el CONPES mencionado por Cabuya y Castaneda (2024) que la ciberdefensa, se refiere a la aplicación de habilidades militares para enfrentar cualquier tipo de amenaza, ataques o acciones hostiles de carácter cibernético que puedan perjudicar a un grupo social, el Estado, el orden, los intereses, el control del territorio y la independencia de un Estado. En este aspecto, la Junta Interamericana de Defensa (2020) refiere que la ciberdefensa, es la habilidad sistematizada y lista para luchar dentro del ciberespacio. Incluye acciones de defensa, ofensiva e inteligencia. De acuerdo con la Ley de Ciberdefensa (2023), la ciberdefensa se trata de aquella capacidad militar, para poder actuar sobre los ataques o amenazas presentadas en y por medio del ciberespacio, los cuales pueden afectar negativamente a la seguridad del Estado.

2.2.2.2 Características.

La ciberdefensa se aplica al escenario del ciberespacio, que de acuerdo con Mosquera (2021), se trata de un dominio de naturaleza militar, siendo necesario desarrollar capacidades militares para este propósito, representando un tema de debate en la defensa nacional. Este entorno virtual que no es físico tiene sus propias reglas y medios, además de no tener un lugar en específico.

Por lo tanto, la Ciberdefensa es un aspecto de la Seguridad Nacional, donde los Estados tienen que establecer la estrategia pertinente, la cual debe implementarse en

colaboración con las entidades privadas y públicas, tienen que estar ajustadas a los derechos humanos y establecer otras acciones que ayuden a identificar diversas amenazas, para afrontarlas con respuestas oportunas y de recuperación de la información ante los posibles incidentes. También, es fundamental promover la cooperación con otros Estados, lo cual es un elemento crucial para tener apoyo externo (Leiva, 2015).

La ciberdefensa es un campo con bastante complejidad, en donde interactúan la tecnología avanzada y los seres humanos, necesitando instrumentos de planificación, implementación, evaluación y optimización de los procesos que se desarrollen, para minimizar los efectos de los ataques cibernéticos. Se sustenta en diversas teorías, el enfoque de sistemas, el modelado y la simulación de la dinámica entre quien ataque y defiende (Cabuya & Castaneda, 2024).

2.2.2.3 Origen de la Ciberdefensa en Perú.

El Comando Conjunto de las Fuerzas Armadas (CCFFAA), puso en marcha el Comando Operacional de Ciberdefensa (COCID), cuyas instalaciones fueron inauguradas el 20 de enero de 2020 por el ministro de Defensa de aquel entonces, Walter Martos Ruiz. Este se encuentra ubicado dentro de la 6.ª División del Estado Mayor Conjunto de las Fuerzas Armadas (6.ª. DIEMCFFAA) (Rivero, 2023). De igual manera, el COCID se compone de tres elementos: terrestre, naval y aéreo. El componente terrestre, está bajo la responsabilidad del Centro de Ciberdefensa del Ejército, que fue inaugurado el 29 de octubre de 2018. El componente naval está a cargo de la Comandancia de Ciberdefensa de la Marina de Guerra, creada el 2 de agosto 2018 que se inauguró el 21 de febrero de 2019. Por último, el componente aéreo está representado por el Grupo de Operaciones en el Ciberespacio de la Fuerza Aérea, que se inauguró el 21 de diciembre de 2019 (Ministerio de Defensa, 2019).

2.2.2.4 Teorías o modelos teóricos que sustentan la ciberdefensa.

La mayoría de las teorías de relaciones internacionales, adoptadas para reaccionar ante los desafíos emergentes en materia de ciberseguridad, se inspiran en enfoques que tradicionalmente asocian la seguridad con iniciativas militares (Calderaro & Craig, 2020). Por otro lado, de acuerdo con Cabuya y Castaneda (2024) la teoría de juegos es un adecuado marco para examinar la dinámica de los ataques y métodos de defensa cibernética, sugiriendo una arquitectura de defensa según esta. El

enfoque metodológico es integral, empleando los principios de un juego estocástico de datos imperfectos. Para Tavares y Penha (2020), la manera más moderna y dispuesta para proceder y entenderlo es interpretarlo tal cual un juego, en donde se requiere tácticas y movimientos estratégicos de ambas partes, para conseguir un resultado legal. Esta teoría, es parte de un campo de las matemáticas aplicadas que estudia eventos estratégicos, en el que los jugadores, tienen que seleccionar sus estrategias en el intento de conseguir una victoria, obteniendo en lo posible el mayor rendimiento.

En este aspecto Fraile (2018), menciona que la teoría de juegos describe el escenario considerándolo como un juego compuesto por jugadores, donde cada jugador, elige acciones que resultan en las mejores recompensas posibles para uno mismo, mientras anticipa las acciones racionales de otros jugadores. La teoría de juegos proporciona herramientas poderosas que permiten modelar a un adversario avanzado, que sabe cómo y qué estrategias de defensa se usan, el cual puede ajustar sus estrategias de ataque en consecuencia. Por tanto, antes de ir a la solución del problema, lo principal es encontrar cómo son los creadores de amenazas y por qué (Fraile, 2018).

2.2.3 Políticas de ciberdefensa.

La política de acuerdo con Jiménez (2012) se trata de un ideal humano que se materializa en diversas actividades para establecer objetivos con metas sociales, por medio del debate de propuestas. Los Estados consideran principios, normativa y procesos característicos de otros Estados, incorporándose dentro de sus propias políticas. Como resultado, los lineamientos se fundamentan en mecanismos multilaterales de cooperación, para conseguir metas colectivas basadas en los intereses de cada Estado, lo que fomenta el apoyo entre los Estados. En este contexto, tanto la Organización de los Estados Americanos como el Banco Interamericano de Desarrollo, han sido los protagonistas más destacados para formular criterios y directrices para crear una política global orientada hacia la ciberdefensa y la ciberseguridad (Montenegro et al., 2022).

2.2.3.1 Objetivos

De acuerdo con la Junta Interamericana de Defensa (2020), las políticas de ciberdefensa deben tener bien claro sus propósitos, siendo uno de estos salvaguardar los datos personales y perjudicar al oponente, aunque posee otras metas adicionales. Durante la generación de la fuerza ciberespacial, es posible hacer planes de más de un

año, que especifiquen los recursos, las líneas de acción y estrategias para conseguir dichos objetivos. Cuando se ha consolidado, es posible formular otros planes con más duración; no obstante, debido a que el ciberespacio cambia constantemente, no es recomendable trazar planes de más de cinco años (Junta Interamericana de Defensa, 2020).

2.2.3.2 Principios

Para Pérez (2021), se refiere a los principios fundamentales, que deben dirigir cualquier acción destinada a garantizar la información y los servicios informáticos. Conforme a la Junta Interamericana de Defensa (2020) estos principios son, por ejemplo, los del arte militar como la capacidad de ejecución, libertad de acción y voluntad de vencer, así como también se considera principios operativos como la perseverancia, sencillez, sorpresa, economía de recursos, flexibilidad, esfuerzo, objetividad entre otros.

2.2.3.3 Capacidades

Se trata de aquellas fortalezas que permiten a las unidades superiores, organizar las habilidades militares para determinados fines, en este caso el ejército posee tres componentes básicos: el estado mayor, responsable de asesorar al mando y planificar las operaciones; la fuerza, que se encarga de llevar a cabo apoyo a la fuerza y operaciones, que se encargan de proporcionar toda la ayuda (operativa, logística y técnica) necesaria para realizar las operaciones (JID, 2020).

2.2.3.3.1 Capacidades principales. De acuerdo con la JID (2020) se pueden dividir en tres capacidades:

Capacidades operativas. Estas se basan en el soporte técnico al mando y operaciones cibernéticas tales como pueden ser la criptografía, auditorías, seguridad de datos, arsenal, desarrollo de tecnología y el área de maniobras (JID, 2020).

Capacidades de mando. La fuerza ciberespacial, debe contar con habilidades dirigidas a hacer más práctico el tomar decisiones, como la planificación y asesorías, colaboración, servicio jurídico, financiero, manejo del conocimiento, representación y lecciones aprendidas (JID, 2020).

Capacidades de técnicas. La fuerza ciberespacial, debe contar con habilidades dirigidas al soporte técnico y operaciones cibernéticas, como por ejemplo el desarrollo

de auditorías en este aspecto, criptografía, seguridad de datos, arsenal, análisis y desarrollo de la tecnología y campo de maniobras (JID, 2020).

También, es posible observar dentro de las capacidades, medidas que acción que toman los Estados para diversos fines. Las medidas de acción en ciberdefensa se refieren al conjunto de medidas destinadas a la protección ante posibles riesgos, que afectan a los sistemas de información, garantizando de este modo los objetivos en ciberseguridad. Estas pueden ser de tipo preventivas, disuasivas, protectoras, detectoras y de respuesta o recuperación (Pérez, 2021). Estas medidas corresponden a la administración del ciberriesgo, los cuales evolucionan constantemente, por lo que identificar y evaluar amenazas nuevas, aspectos vulnerables y activos, tiene que ser constante. Por tanto, de haber cambios, es necesario realizar un análisis nuevo (JID, 2020).

2.2.3.3.2 Medidas de acción. Estas son las siguientes:

Medidas preventivas. Es el primer paso, lo que facilita evitar un posible riesgo, teniendo en consideración ciertas acciones, como tener una lista de webs a las que no se debe acceder, así como medidas para evaluar que se estén desarrollando las acciones correctas, frente al cumplimiento de la seguridad (Unión Internacional de Telecomunicaciones, 2011).

Medidas de detección. Pueden ser acciones orientadas a la verificación de archivos de registro, así como la instauración de un sistema que detecte intrusiones basadas en red y host. Medidas de reacción. Se refiere a que una vez que se detecta y valida un incidente, se deben tomar medidas. Las acciones incluyen: (a) detener un incidente en curso; (b) identificar el alcance/escala del incidente; c) limitar los daños; (d) tomar medidas para investigar el curso de los acontecimientos y (e) evitar que el incidente se repita (Unión Internacional de Telecomunicaciones, 2011).

Medidas de disuasión. Corresponde a medidas activas para rechazar los ataques, que pueden ser sistemas de prevención de intrusiones (IPS) que sean capaces de reaccionar, en tiempo real, para bloquear o prevenir intrusiones. Los IPS, descartan los paquetes ofensivos al detectar actividad maliciosa, pero permiten que pase el resto del tráfico. Los IPS modernos combinan capacidades de firewall, detección de intrusiones, antivirus y evaluación de vulnerabilidades (Unión Internacional de Telecomunicaciones, 2011).

Medidas de protección. Busca resguardar los datos o gran parte de estos, que están siendo vulnerados por las amenazas cibernéticas. Finalmente, las acciones o medidas de recuperación conllevan mitigar el daño y volver al estado principal al que estuvo la información o el sistema informático antes del ataque, en el mejor caso posible (Unión Internacional de Telecomunicaciones, 2011).

2.2.3.4 Activos críticos nacionales (ACN)

De acuerdo con la Dirección Nacional de Inteligencia (DINI, 2018) se trata de cualquier tipo de sistema, infraestructura o recurso necesario a resguardar y que favorecen al desarrollo de la nación. Su alteración o eliminación, complica una solución inmediata, causando un enorme problema al país. En Perú, de acuerdo con Rivero (2023) según lo que estipula la Ley de Ciberdefensa (2023), dentro de los ACN se consideran tres elementos, Software y/o Programas, Sistemas Informáticos y las Infraestructuras Críticas, para el Funcionamiento de Equipos y Sistemas Militares. En el aspecto de la ciberdefensa, su seguridad depende únicamente de los sistemas y tecnologías de control cibernético, que pueden ser propensos a la vulnerabilidad (Kshetri & Miller, 2021).

2.2.3.5 Órganos ejecutores

Dentro de las características de interés en el presente estudio, son los órganos ejecutores, que de acuerdo con el Gobierno de Perú (2021) los organismos públicos ejecutores, son entidades que no están centralizadas con personería jurídica de Derecho Público, ligada a un Ministerio y creada por una ley mediante el Poder Ejecutivo. Según Ley Orgánica del Poder Ejecutivo (2007) su creación surge de la necesidad de las diversas actividades específicas y significativas que debe realizar, se sujetan a determinadas normas técnicas para que se conforme como tal. Las políticas de gasto se aprueban por la institución a la que se sujetan, generalmente no tienen funciones normativas, a no ser que se especifique.

2.2.4 Importancia.

Es evidente la gran importancia que posee la ciberdefensa para un Estado, ya que, al tener un sistema de ciberdefensa y ciberseguridad sólido para la protección de información o datos oficiales del Estado, manteniendo la estabilidad de estos, sobre todo en el aspecto militar, que comprende que el entorno cibernético existe amenazas potenciales que pueden generar gran perjuicio y sobre todo que esto ocurre a menudo por el avance de la tecnología

(Quevedo, 2023). En ese sentido, la ciberdefensa es una cuestión importante debido a su impacto en la sostenibilidad de los Estados (Noreña, 2022).

Por otro lado y de acuerdo al propósito de estudio, es importante comprender y comparar las estrategias de seguridad cibernética en diferentes Estados, ya que proporciona información importante sobre las diferentes estrategias, que los Estados han elegido para combatir las amenazas cibernéticas, de tal forma que se pueda discernir enfoques eficaces y conocimientos valiosos para guiar el desarrollo de políticas y procesos para tomar decisiones a futuro (Pranesh et al., 2024).

2.2.5 Principales amenazas que justifican la ciberseguridad y ciberdefensa

La acelerada expansión del entorno digital ha incrementado de manera exponencial la superficie de exposición de los Estados frente a actores hostiles, tanto estatales como no estatales. Dichos actores llevan a cabo ciberataques, los cuales se manifiestan, por ejemplo, en la vulneración de datos sensibles, la degradación de infraestructuras críticas, la extorsión económica mediante ransomware y la generación de efectos psicológicos y estratégicos de gran magnitud. La evidencia proveniente de estudios comparados demuestra que estos ciberataques incluyen la sustracción y manipulación de información estratégica, así como la capacidad de paralizar servicios esenciales, lo que evidencia que su frecuencia y sofisticación continúan en ascenso a nivel regional y global (Arreola, 2019; CEPAL, 2020; Vargas et al., 2017). En consecuencia, se constata que el conjunto de estas prácticas, claramente identificadas como ciberataques, ha convertido tanto a la ciberseguridad como a la ciberdefensa en capacidades imprescindibles para la protección del Estado, el fortalecimiento de la resiliencia social y la sostenibilidad del poder nacional (Montenegro et al., 2022; Quevedo, 2023).

2.2.5.1 Ataques a infraestructuras críticas de información (ICI) y servicios esenciales

Los ciberataques dirigidos contra infraestructuras críticas como las comunicaciones, la energía, las redes gubernamentales, los sistemas militares, los servicios financieros, el transporte y la salud tienen el potencial de interrumpir funciones esenciales tanto del Estado como de la sociedad. Un caso emblemático es el de Estonia en 2007, donde campañas coordinadas de denegación de servicio distribuida (DDoS) lograron degradar los servicios bancarios, gubernamentales y mediáticos, generando consecuencias políticas y económicas significativas (Klimburg,

2012). En este contexto, la protección de infraestructuras críticas ha sido reconocida como parte de los intereses vitales del Estado, y su resguardo se ha incorporado en diversos marcos estratégicos bajo la categoría de “activos críticos nacionales”, cuya alteración, perturbación o destrucción podría provocar daños graves e irreversibles, al no contar con sustitutos inmediatos (Dirección Nacional de Inteligencia DINI, 2018; Jarufe, 2020; Leiva, 2015).

2.2.5.2 Ciberespionaje y exfiltración de información estratégica

Los datos confidenciales de carácter militar, diplomático, industrial o personal representan fuentes relevantes de poder político, económico y tecnológico. El acceso no autorizado a dicha información tiene el potencial de alterar equilibrios estratégicos, facilitar mecanismos de coerción o habilitar operaciones subsiguientes. Un ejemplo ilustrativo es el ataque a la cadena de suministro del software de SolarWinds, detectado en 2020 aunque con actividad previa, el cual permitió la intrusión en redes gubernamentales de los Estados Unidos y evidenció tanto la escala como la sofisticación de las actuales operaciones de ciberespionaje (Forbes Staff, 2021). La literatura especializada ha enfatizado que la recopilación ilícita de datos estratégicos puede ser utilizada para obtener ventajas económicas o políticas, lo que refuerza la necesidad de proteger esta información frente a actores hostiles (Capi, 2003, citado en Vargas et al., 2017; CEPAL, 2020).

2.2.5.3 Ciberdelincuencia organizada y ransomware de alto impacto estatal

La criminalidad en línea ha experimentado una evolución hacia modelos de carácter industrial, tales como el ransomware as a service, el alquiler de botnets y los ataques dirigidos a las cadenas de pagos, afectando tanto al sector privado como a organismos gubernamentales. Además, informes regionales reportan un total de 82 incidentes significativos registrados entre 2020 y 2022 en América Latina, con un énfasis particular en el sector bancario. Un caso emblemático fue el ataque perpetrado por el grupo Conti contra Costa Rica en 2022, que paralizó más de treinta entidades estatales, incluido el Ministerio de Hacienda, y resultó en el secuestro de datos fiscales y de comercio exterior, lo que motivó la declaratoria de emergencia nacional (BBC Noticias, 2022). A nivel global, reportes industriales evidencian un crecimiento acelerado del ransomware, con un incremento de diez veces en tan solo un año (Fortinet, 2021), afectando también a diversos gobiernos de la región (Gobierno de

México, 2020; Noticias RCN, 2022). En este contexto, Perú figuró entre los Estados más atacados de América Latina en 2021, lo que puso de manifiesto las fragilidades estructurales de su ciberseguridad pública (Quevedo, 2023).

2.2.5.4 Ciberterrorismo y operaciones de impacto estratégico

El terrorismo convencional emplea medios cinéticos (por ejemplo, atentados suicidas o artefactos explosivos improvisados) y opera de diversas maneras. Acompañado de muertes, lesiones y destrucción de bienes, el terrorismo genera miedo y ansiedad en la población objetivo. Los terroristas pueden, por tanto, utilizarlo para desmoralizar a la población civil con el fin de presionar a su gobierno a adoptar o abstenerse de implementar una política específica (Gross, et al., 2018).

Al igual que el terrorismo convencional, el ciberterrorismo busca promover los objetivos políticos, religiosos o ideológicos de los perpetradores mediante el daño físico o psicológico a la población civil. A diferencia del terrorismo convencional, el ciberterrorismo emplea tecnologías informáticas maliciosas en lugar de fuerza cinética. La ciberguerra utiliza malware y virus para inhabilitar objetivos militares, mientras que el cibercrimen persigue un beneficio económico o causar un daño personal a otros (como la venganza o el acoso), sin relación con un conflicto político (Gross, et al., 2018).

En ocasiones, estas categorías se superponen y las diferencias resultan difíciles de distinguir. Los ciberterroristas y los Estados-nación pueden, al igual que los criminales, robar dinero, datos o identidades o, como los hacktivistas, realizar ataques distribuidos de denegación de servicio (DDOS) para paralizar sistemas de gran envergadura. Mucho depende de la intención y la identidad de los actores, que no siempre se conocen (Gross, et al., 2018).

Frente a la creciente amenaza del ciberterrorismo, Gross, et al. (2018) señalan que surge de manera prioritaria la interrogante: "¿De qué manera el ciberterrorismo letal y no letal afecta psicológicamente a los individuos? Primero, el ciberterrorismo agrava la ansiedad y la inseguridad personal. Segundo, el terrorismo letal y no letal exacerba las percepciones de amenaza y la inseguridad personal. Tercero, muchas personas, particularmente aquellas con altos niveles de percepción de amenaza, están dispuestas a apoyar políticas gubernamentales fuertes. Estas políticas se dividen en dos líneas e incluyen la política exterior (por ejemplo, respuestas militares cibernéticas y

cinéticas a los ciberataques) y la política interna (por ejemplo, la tolerancia a la vigilancia gubernamental y el control de internet). A medida que aumenta la percepción de amenaza, los individuos adoptan puntos de vista políticos cada vez más estrictos. Al igual que el terrorismo convencional, el ciberterrorismo endurece las actitudes políticas: los individuos están dispuestos a intercambiar libertades civiles y privacidad por seguridad y a apoyar la vigilancia gubernamental, una mayor regulación de internet y respuestas militares contundentes en respuesta a los ciberataques (Gross, et al., 2018).

2.3 Bases normativa

Respecto a las leyes sobre ciberseguridad en general o la importancia de establecer dichas normativas, aunque no haya alguna establecida como tal, las ISOs de la serie 27000 dan un alcance respecto a lo que es la seguridad de datos. Dentro de ellas, la 27001 es la norma insignia de esta serie, que detalla los requerimientos para un adecuado sistema de gestión de seguridad para los datos. Por su parte, la ISO 27002 proporciona un conjunto de mejores acciones para manejar la seguridad de los datos y la ISO 27005 suministra normativas para el manejo de riesgos de vulneración de la información (International Standard Organization, 2018).

Por su parte, la Organización de Estados Americanos establece la Estrategia Interamericana Integral de Seguridad Cibernética propuesta en junio del 2004, desempeñando un papel de líder sobre la implementación de bases normativas en ciberseguridad y ciberdefensa. Dicho organismo, nace en el escenario de la Guerra Fría, construyendo el Tratado Interamericano de Asistencia Recíproca y se conforma la Junta Interamericana de Defensa, que ayudará a establecer las normativas de ciberdefensa para la región (Montenegro et al., 2022). En este sentido, ambas instituciones, son protagonistas en otorgar las bases para la generación de una política de ciberseguridad y ciberdefensa.

También, la JID otorga un modelo operativo estratégico para la ciberdefensa, con un enfoque militar, siendo un referente para comprender la ciberdefensa en la seguridad de los Estados con soporte de otros Estados, poniendo en evidencia que se requiere de un adecuado manejo en ciberdefensa, así como la implementación del modelamiento y simulación, que optimice tomar decisiones adecuadas en el espacio cibernético (Cabuya & Castaneda, 2024). Aun así, resulta complicado aplicar los lineamientos en otros Estados, por ser jurisdicciones

con independencia, las cuales tienen que reconocer que otras pueden aportar a sus normativas o son merecedoras de apoyo (Leiva, 2015).

Si bien se han establecido normativas generales que se pueden tomar en cuenta para la ciberseguridad y ciberdefensa, los Estados de estudio, establecieron sus políticas o normativas, mediante leyes, decretos y documentos estratégicos que son desarrollados de acuerdo con sus necesidades, los cuales se muestran con mayor detalle en el Capítulo IV.

2.4 Definiciones conceptuales

Activo crítico nacional: Se trata de sistemas, entornos y recursos cruciales para el mantenimiento y desarrollo de las capacidades de una nación. Su alteración o perjuicio, desfavorece una actuación rápida, causando un grave daño a una nación (DINI, 2018).

Alcance y ámbito de aplicación: Se refiere a quién aplica el documento normativo relacionado a la ciberdefensa hacia todo ámbito del organismo ejecutor de la ciberdefensa, sus procesos y recursos, que se relacionan con la entidad por medio de contratos (Dirección Nacional de Ciberseguridad, 2022).

Capacidades: Se trata de aquellas fortalezas que permiten a las unidades superiores, organizar las habilidades militares para determinados fines (JID, 2020).

Ciberamenaza: Conocido también como amenaza cibernética, es un elemento con la potencialidad de perjudicar a algún activo importante de una entidad la cual se manifiesta en el ciberespacio (JID, 2020).

Ciberataque: Se trata del uso intencionado de una ciberarma por un individuo o un programa desarrollado por una persona, que funciona de modo automático para generar un daño a algún componente importante dentro del ciberespacio, que puede incidir indirectamente en entornos convencionales (JID, 2020).

Ciberdefensa: Se trata de una capacidad para el combate en el ciberespacio, la cual es organizada y realiza acciones de defensa, ofensa e inteligencia (JID, 2020).

Ciberdelincuencia: Se conoce también como delincuencia cibernética, que son comportamientos criminales, que se desarrollan por medio de un ordenador y que llegan a afectar los sistemas informáticos pertenecientes a la víctima, incidiendo negativamente en sus derechos y libertades individuales (Piña, 2019).

Ciberespacio: Entendido también como el espacio cibernético, que se trata de un entorno desarrollado por la electrónica, en donde se puede crear, alterar, guardar,

intercambiar y explorar información por medio de sistemas que interconecta a las personas a través de internet y se accede a ellas mediante aparatos electrónicos (Montenegro et al., 2022).

Ciberguerra: Se refiere a un conjunto de tácticas y técnicas específicas en donde se utiliza el ciberespacio como medio principal, por lo que, en lugar de emplear fuerza física directa, se utiliza ciberoperaciones para atacar sistemas de información, causar disrupciones significativas, o influir en los adversarios mediante sabotaje, espionaje o manipulación; no son lo suficientemente letales para ser consideradas como guerra en términos tradicionales, pero se caracteriza por su capacidad para afectar infraestructuras críticas, sistemas de defensa, y operaciones nacionales sin recurrir necesariamente a la violencia física inmediata (Gómez, 2017).

Ciberseguridad: Se entiende también como seguridad cibernética, que conlleva la capacidad de protección de un conjunto de elementos informáticos que se consideran como activos, implementando estrategias que favorezcan a la prevención, detección, recuperación integridad y confidencialidad frente a las amenazas dentro de un entorno cibernético (Leiva, 2015).

Ciberterrorismo: Sería entendido también como el terrorismo cibernético, que se trata de situaciones en las que se emplean los sistemas informáticos con una finalidad terrorista (Pérez, 2021).

Componentes sistémicos subsidiarios: Se trata del diseño de defensa del ciberespacio desde un enfoque multidimensional, en donde interactúan diversos componentes sistémicos, que contribuyen a la capacidad operacional de la ciberdefensa, propiciando su aseguramiento, enfatizando las interconexiones de las distintas dimensiones o componentes sistémicos. ya que no deben estar pensados para ser desplegados de manera separada o secuencial (Ministerio de Defensa, 2022).

Defensa: Se trata de las medidas de acción que ayudan a resguardar a las personas, elementos o entidades de algún riesgo o daño potencial, gracias a una respuesta oportuna (Vargas et al., 2017).

Detección: Acciones orientadas a la verificación de archivos de registro y el establecimiento de un sistema de detección de instrucciones basadas en red y host (Unión Internacional de Telecomunicaciones, 2011).

Disuasión: En el contexto militar de la ciberdefensa, se trata de una estrategia de defensa en el ciberespacio, que busca disuadir a un atacante de intentar vulnerar la seguridad de una red o sistema y de este modo, el atacante no realice una acción determinada para vulnerar la seguridad de una red o sistema que puede ser perjudicial para las infraestructuras críticas de información, demostrando ser una defensa activa que genera un entorno de riesgo para dichos atacantes, haciéndolos más propensos a reconsiderar sus acciones (Kinast, 2021).

Ejes temáticos: Se trata de un modo de abordar un tema desde un enfoque o un cúmulo de contenidos y disciplinas afines, los cuales se consideran de manera transversal (Estrategia Nacional de Seguridad Cibernética - E-Ciber, 2020).

Enfoque de seguridad: Se trata de estrategias y medidas adoptadas para la protección de los individuos, las organizaciones y sistemas de información contra amenazas y riesgos (Gonzales, 2023).

Enfoque sistémico: Se refiere a identificar a un sistema el cual se explica por la suma de sus partes, así como comprender el rol de un objeto y cómo funciona en el sistema (Nieto, 2013). Respecto a la ciberdefensa, posee un cúmulo de componentes que funcionan de manera dinámica y contribuyen al desarrollo y la capacidad de esta (Ministerio de Defensa, 2022) .

Estado: Es una organización política que tiene el poder y autoridad para administrar un territorio o espacio determinado, siendo un ente regulador de relaciones entre los individuos, donde comparten una cultura, historia y tradiciones (Córdova & Hernández, 2019).

Estructura de la política: Consta de los elementos o áreas que corresponden al diseño de la política, el cual puede tener pilares, líneas de acción, dimensiones, ejes, etc… (Secretaría Distrital de Planeación, 2012).

Financiamiento: Se trata de los costos generados por la instauración de las normativas emitidas por la entidad correspondiente respecto a ciberdefensa y ciberseguridad (Consejo Nacional de Política Económica y Social, 2011).

Infraestructura crítica de información (ICI): Se trata de un cúmulo de elementos computacionales, de información y redes de comunicación que, si se destruyen, pueden impactar negativamente en la seguridad de un país (Leiva, 2015).

Infraestructura crítica. Cualquier componente o elemento, que puede ser una red, sistema, equipo, instalación o ambiente fundamental para la prestación de servicios estatales, siendo necesario para mantener el funcionamiento de la sociedad, la economía, la seguridad y salud de la población (Jarufe, 2020).

Instrumentos: Se trata de las herramientas normativas que contribuyen a la protección de sistemas y redes gubernamentales (Estrategia Nacional de Seguridad Cibernética - E-Ciber, 2020).

Modelo de gobernanza: Se trata de un esquema de actividades con un cúmulo de lineamientos, principios, normativas y procesos para tomar decisiones y programas compartidos por diversas partes interesadas en seguridad (Decreto 338 de 2022, 2022).

Operacionales militares: Son acciones estratégicas que se planifican y ejecutan en el ciberespacio con el objetivo de lograr resultados militares específicos para proteger la seguridad nacional desde el Ministerio de Defensa (Reglamento Ley de Ciberdefensa, 2023).

Organismos ejecutores: Son entidades que no están centralizadas con personería jurídica de Derecho Público, ligada a un Ministerio y creada por una ley mediante el Poder Ejecutivo (Gobierno de Perú, 2021).

Plan de acción: Se trata de un conjunto de acciones ordenadas y concretas determinadas por actividades para la ejecución de la ciberdefensa (Consejo Nacional de Política Económica y Social, 2011).

Políticas de seguridad: Se trata del cúmulo de lineamientos plasmados en documentos formales, los cuales establecen una manera en que una entidad protege y maneja la información, así como la gestión de los servicios considerados como críticos (Pérez, 2021).

Prevención: Es el primer paso, lo que facilita evitar un posible riesgo, teniendo en consideración ciertas acciones, como tener una lista de webs a las que no se debe acceder, así como medidas para evaluar que se estén desarrollando las acciones correctas, frente al cumplimiento de la seguridad (Unión Internacional de Telecomunicaciones, 2011)

Principio: Se trata de aspectos fundamentales, que deben dirigir cualquier acción destinada a garantizar la información y los servicios informáticos (Pérez, 2021).

Protección: Se trata de resguardar los datos o gran parte de estos, que están siendo vulnerados por las amenazas cibernéticas (Unión Internacional de Telecomunicaciones, 2011).

Reacción: Proceso en el que se toma medidas de acción, luego de detectar y validar un incidente en curso (Unión Internacional de Telecomunicaciones, 2011).

Recuperación: Conllevan mitigar el daño y volver al estado principal al que estuvo la información o el sistema informático antes del ataque, en el mejor caso posible (Unión Internacional de Telecomunicaciones, 2011).

Rol del Ministerio de Defensa: Se trata de las actividades del Ministerio de Defensa, según su competencia y función, en cuanto a la dirección, normatividad, supervisión y evaluación las disposiciones en materia de ciberdefensa (Reglamento Ley de Ciberdefensa, 2023).

***Softwares* maliciosos:** Es un tipo de software, que busca hacer daño o introducirse sin ningún consentimiento en un sistema informático, los cuales pueden ser programas maliciosos como los gusanos, virus, troyanos, *spyware*, entre otros (Fuentes et al., 2023).

Uso de la fuerza: En el contexto de la ciberdefensa, se trata de las acciones de las FFAA, en y mediante el ciberespacio, con las estrategias correspondientes (Reglamento Ley de Ciberdefensa, 2023).

CAPÍTULO III

METODOLOGÍA

3.1 Diseño metodológico

3.1.1 Enfoque de la investigación.

La presente investigación tiene un enfoque cualitativo, de acuerdo a la clasificación metodológica de Hernández-Sampieri y Mendoza (2018) este tipo de estudios analizan los fenómenos obteniendo información desde las narrativas escritas, verbales, visuales o auditivas, para así conseguir conclusiones de acuerdo con los objetivos propuestos; además de poder estudiar dichos fenómenos de manera sistemática, examinando los hechos existentes, comprendiendo la realidad de los mismos e incrementar las teorías al respecto.

3.1.2 Tipo de investigación.

Según su finalidad, es de tipo básica, porque incrementó los conocimientos o entendimiento de un tema del cual poco se conoce, aportando información para estudios posteriores (Li et al., 2018). Por consecuencia, se llenó un vacío de conocimiento, actualizando el tema respecto a las políticas de ciberdefensa de los Estados a analizar, sobre cómo se estructura, qué componentes según su estructura tienen y qué describen estos, para hacer una comparación y comprender sus diferencias y similitudes.

También, de acuerdo con su carácter es descriptivo que según Manjunatha (2019), es un tipo de estudio que busca describir los componentes de algún fenómeno. De este modo, se hizo una descripción de los hallazgos referentes a las políticas de ciberdefensa y sus similitudes y diferencias entre los Estados, gracias al análisis del contenido de la información para comprender el estado sobre este tema.

Por su alcance temporal es transversal, debido a que la información se recolectó en un sólo momento en el tiempo (Sánchez et al., 2018). Por tanto, la información fue recolectada y analizada en un lapso temporal, que corresponde al desarrollo del presente proyecto de investigación entre junio y noviembre.

3.1.3 Método.

Se emplea el método de análisis e inductivo, en este caso el análisis conlleva realizar comparaciones de los elementos de estudio, por lo que se trata de investigaciones, en las cuales se puede obtener distintos grados de evidencia dependiendo del contexto en el que se

encuentra (Manterola et al., 2018); además es inductivo, porque conlleva un procedimiento meticuloso para obtener conclusiones generales, a partir de la información de casos particulares (Hernández-Sampieri & Mendoza, 2018). De este modo, se indagó en datos de diversos documentos, para buscar patrones de clasificación (tipos) recurrentes, utilizando codificaciones y comparaciones, para así tener una comprensión general del fenómeno que se presente estudiar.

3.1.4 Diseño.

Tuvo un diseño de análisis documental, el cual conlleva la realización de un proceso sistematizado y de síntesis de información cualitativa, la cual permite poder triangular la documentación encontrada en forma de texto, haciendo una combinación de distintas fuentes que brindan la información necesaria, realizando un análisis del contenido (Guevara, 2019).

3.2 Población y muestra

3.2.1 Población de estudio.

La totalidad de la información de registros bibliográficos y audiovisuales acerca de las unidades temáticas de estudio, sobre las políticas de ciberdefensa de los Estados considerados, los cuales son Argentina, Brasil, Chile, Colombia, Ecuador y Perú, seleccionados de manera conveniente y así como a personas con amplio conocimiento del tema sobre las unidades temáticas de estudio, quienes brindaron información en base a sus experiencias, tras años de labor en rubros asociados a la ciberseguridad y ciberdefensa.

3.2.2 Muestra.

Todos los documentos normativos, bibliografía científica y fuentes audiovisuales referentes a las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú, según la pertinencia de la información de dichas fuentes documentales, con un alcance de 15 documentos principales sobre normativas, políticas o documentos estratégicos referidos a la ciberdefensa, los cuales se obtuvieron principalmente del Portal de Política Cibernética del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) (2024), seleccionando los Estados de análisis y ubicando sus normativas más recientes y que contengan las principales componentes de políticas establecidos en el presente estudio que son de mayor interés. Así es como se tuvieron datos actualizados respecto al tema y 69 fuentes bibliográficas para sustento del presente estudio con un total de 84 registros bibliográficos.

Los especialistas fueron solo cinco de ellos en materia de ciberdefensa, uno de Perú y uno de cada Estado considerado, menos de Brasil, con el que no se pudo contar debido a que declaró que no pudo proporcionar información debido a políticas internas que requieren autorización para tratar sobre temas relacionados a la ciberdefensa, a pesar de ser solo una consulta con fines académicos, no permite compartir este tipo de información. El detalle de los especialistas se aprecia en la siguiente tabla:

Tabla 1

Especialistas entrevistados

Estado	Especialista	Experiencia relacionada a la investigación	Codificación de siglas
Argentina	Capitán de Fragata Anselmo Omar Herrera	Director de Ciberdefensa de la Armada y Director de Comunicaciones de la Armada	E-A
Chile	Capitán de Fragata Roberto Siña Lazo	Jefe Departamento de Planes del CSIRT de la Defensa Nacional del Estado Mayor Conjunto de las Fuerzas Armada de Chile	E-CH
Colombia	Capitán de Fragata Francisco José Jaraba Hadechiny	Comandante del Comando Cibernético Naval de la Armada de la República de Colombia	E-CO
Ecuador	Capitán de corbeta Vivanco Toala Danny	Jefe de TICs, Oficial de Grupo de Defensa y Auditor TICs del Comando de Ciberdefensa	E-E
Perú	Coronel Fuerza Aérea Luigui Aurelio Rivas Guevara	Comandante de Operaciones Ciberespaciales (COPCE)	E-P

Todos estos especialistas, aportaron a encontrar la información relevante sobre el tema que en algunos casos brindaron algunas fuentes actualizadas para este propósito, además de reforzar y aseverar la existencia de las características que poseen las políticas de ciberdefensa de los Estados en estudio.

Sobre el muestreo, este fue de manera no probabilística por conveniencia del investigador, debido a que fueron escogidos según la pertinencia de datos que pueden brindar y que son de interés para el estudio. Además, los documentos estuvieron sujetos a su elección al contener la mayoría de información para el desarrollo de las categorías de análisis, tal como se muestra en la tabla 2, siendo estas las de interés en el presente estudio.

3.3 Tema, categorías y unidades de análisis

3.3.1 Tema

Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.

3.3.2 Categorías o unidades temáticas

1. Políticas de ciberdefensa: Identificación de las Normativas y directrices relacionadas al desarrollo de la ciberdefensa plasmado en documentos oficiales y actualizados de los Estados en estudio.
2. Componentes de la estructura de las políticas de los Estados: Se trata de los apartados o subtítulos presentes en la estructura de los documentos normativos de los Estados en estudio. Los componentes estudiados fueron los siguientes:

   Componentes preestablecidos

   - Objetivos (general y específicos)
   - Principios
   - Capacidades
   - Activos críticos nacionales
   - Organismos ejecutores

   Componentes emergentes

   - Componentes sistémicos subsidiarios
   - Enfoque sistémico
   - Alcance y ámbito de aplicación
   - Instrumentos
   - Ejes temáticos
   - Plan de acción
   - Financiamiento
   - Modelo de gobernanza
   - Enfoque de seguridad
   - Rol del Ministerio de Defensa
   - Operacionales militares
   - Uso de la fuerza

3. Similitudes de las políticas de ciberdefensa: Semejanzas o aspectos parecidos entre los componentes de las políticas encontradas en los documentos normativos de todos Estados en estudio.
4. Diferencias de las políticas de ciberdefensa: Componentes diferentes entre los componentes de las políticas encontradas en los documentos normativos de los Estados en estudio.

Los componentes preestablecidos detallados en la segunda categoría de análisis (que figuran también en la Tabla 2), se basaron en los componentes de la estructura de la Ley de Ciberdefensa de Perú, que luego se afinó por criterio del investigador, considerando los más importantes y recurrentes en las normativas de otros Estados. Los componentes emergentes fueron resultado de la investigación, tratando de agrupar las diferentes partes de las políticas de ciberdefensa que presentaban los otros Estados, agrupándolos bajo una tecnología según su contenido.

3.3.3 Unidades de análisis

Las unidades de análisis están constituidas por normativas y directrices relacionadas a las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú, así como segmentos obtenidos de la entrevista a especialistas de los Estados seleccionados.

A continuación, se muestra la tabla resumen:

Tabla 2

Tema, categorías y unidades de análisis

Tema	Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.
Categorías de análisis	
1. Políticas de ciberdefensa	
2. Componentes de la estructura de las políticas	**Componentes preestablecidos** – Objetivos (principal y específicos) – Principios – Capacidades – Activos críticos nacionales – Organismos ejecutores **Componentes emergentes** – Componentes sistémicos subsidiarios – Enfoque sistémico – Alcance y ámbito de aplicación – Instrumentos – Ejes temáticos – Plan de acción – Financiamiento – Modelo de gobernanza – Enfoque de seguridad – Rol del Ministerio de Defensa – Operacionales militares – Uso de la fuerza
3. Similitudes de las políticas de ciberdefensa	
4. Diferencias de las políticas de ciberdefensa	
Unidades de Análisis	Las normativas y directrices relacionadas a las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú, así como segmentos obtenidos de las entrevistas realizados a los especialistas de los diversos países.

3.4 Formulación de hipótesis

Al inicio del estudio se estableció como hipótesis:

El análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú muestran similitudes en cuanto a objetivo, capacidades y activos

críticos. Sin embargo, también poseen diferencias en el contenido de sus componentes, especialmente en los principios y objetivos específicos o estratégicos.

3.5 Técnicas e instrumentos

3.5.1 Técnicas de recolección de datos.

La primera técnica fue el análisis documental, siendo un método para organizar la información que se requiere, desde documentos, registros audiovisuales y cualquier otra fuente documental ya sea virtual o física, las cuales pueden brindar dicha información (Bernal, 2016).

Como segunda técnica, se usó la entrevista que, de acuerdo con Ryan et al. (2009), ayudó a recolectar datos para estudios cualitativos, obteniendo información sobre las perspectivas y creencias de las personas sobre algún asunto de interés.

3.5.2 Instrumentos de recolección de datos.

Para recolectar la información, el primer instrumento fueron las fichas de trabajo, que según Garcés (2000) es la herramienta para la investigación bibliográfica. Dentro de ellas se encuentran las fichas bibliográficas, que permiten anotar la información de artículos, libros, normativas y fuentes institucionales que servirán de referencia para el trabajo. También, se usaron las fichas de análisis y resumen, en donde se plasmó la información resumida de los documentos consultados, de acuerdo con cada categoría, lo cual es equivalente a una guía de análisis documental (Bernal, 2016). Las fichas que fueron de elaboración propia se usaron durante la recolección de la información para conseguir las referencias como es el caso de la ficha bibliográfica (Ver Anexo E), la información de los componentes de las políticas de ciberdefensa gracias a la ficha de análisis (Ver Anexo F) y el contenido de dichas componentes con la ficha de resumen (Ver Anexo G) por cada Estado en cuestión.

El segundo instrumento fue la guía de entrevista semi estructurada, que es un formato en donde se planifica de manera previa, aquello que se va a preguntar en concreto, esperando ciertas respuestas por parte de los entrevistados, pero con mayor libertad y siendo orientado por el entrevistador (Garcés, 2000). Tal como se muestra en el Anexo C, la entrevista fue elaborada con cinco preguntas, las cuales parten de los problemas de estudio establecidos como preguntas generales y específicas.

3.6 Técnicas para el procesamiento de la información

Para poder hacer una comparación de la información, sobre las políticas de ciberdefensa de los Estados en estudio, se tuvo que sintetizar los datos mediante dos técnicas principal. La primera fue el análisis de contenido que de acuerdo con Sánchez et al. (2021), corresponde con examinar las fuentes bibliográficas y/o audiovisuales, de donde se obtuvo datos actualizados sobre el tema en estudio, analizando, además, el contenido de las entrevistas que se realizaron.

Luego de haber obtenido la información de los entrevistados, se recurrió a otra técnica, el análisis del discurso que, según Sánchez et al. (2021), es la interpretación y comprensión del discurso para tener ideas concisas que sean de aporte para una investigación. Con esta información, se respondió a cada objetivo de estudio, dando solución a su vez al objetivo general, tras describir qué hallazgos se obtienen de la comparación de dichas políticas entre los Estados seleccionados. Los hallazgos se presentaron de manera ordenada, en tablas y figuras acorde con los objetivos de estudio.

3.7 Aspectos éticos

Se ha considera los aspectos éticos, que parten de lo estipulado por la Escuela Superior de Guerra Naval (2024) siendo los más importantes el de honestidad, presentando datos tal cual la revisión proporcione sin alterar información, respetando a su vez el principio de veracidad y transparencia, al buscar la verdad que responda a la pregunta de investigación, entregando datos confiables y reales sobre la comparación de las políticas de ciberdefensa de los Estados considerados.

Además, el principio de imparcialidad se reflejó en que la información analizada, se hizo sin ninguna discriminación o prejuicio alguno, que podría alterar la perspectiva y finalidad de la presente investigación, sin denotar favoritismos o exclusividades en algún aspecto. Por último, el principio de respeto se logró mediante la citación en las normas APA séptima edición, reconociendo el trabajo y aporte de los autores que proporcionaron la información y sustento del tema de estudio.

CAPÍTULO IV

RESULTADOS Y ANÁLISIS

Los resultados se presentan según los documentos que manifiestan los componentes de la estructura de las políticas de ciberdefensa o que lo incluyan en sus textos en resoluciones, decretos, guías, manuales, propuestas, entre otros; pero todos formalmente establecidos por las entidades gubernamentales de cada Estado. A su vez, se presenta lo expuesto por los especialistas entrevistados que, para facilitar el entendimiento, se codifican con la sigla "E" seguida de la inicial del Estado en cuestión: "A", "B", "Ch", "Co", "E", "P". Aunque, para el caso de Brasil, no se contó con su participación y en algunos casos, como el especialista de Ecuador, se abstuvo de responder a algunas preguntas (ver Anexo D).

4.1 Políticas de ciberdefensa de los Estados

Argentina: Los documentos más recientes que estipulan lineamientos referentes a la ciberdefensa en Argentina son cuatro: en el año 2022 concretamente el 1 de febrero, se publicó el documento "Modelo Referencial de Política de Seguridad de la Información" (Dirección Nacional de Ciberseguridad, 2022), documento el cual tiene un abordaje un poco más amplio en relación con la ciberdefensa. Meses más tarde, el 24 de agosto de 2022 se desarrolló la "Política de Ciberdefensa" (Ministerio de Defensa, 2022) con lineamientos más específicos sobre este tema. Luego se desarrolla en el mismo año, pero para el 13 de diciembre, una Segunda Estrategia Nacional de Ciberseguridad (Gobierno de Argentina, 2022), siendo la primera la desarrollada en el año 2019 por la Secretaría de Gobierno de Modernización (2019) mediante Resolución 829/2019, llamada "Estrategia Nacional de Ciberseguridad de la República Argentina". Un mes más adelante, el 30 de enero de 2023, se estipula crear el Centro de Supervisión y Control de Gestión de Ciberdefensa y el Comité de Infraestructura Crítica de la Información de la Defensa (Gobierno de Argentina, 2023), para adicionar nuevos aspectos relativos a la ciberdefensa (ver Tabla 3). En este aspecto, el especialista **E-A** señala que es el documento de política de ciberdefensa del año 2022, el que rige y da origen a la directiva de políticas de ciberdefensa nacional, las cuales las establece el Ministerio de Defensa a través de la Subsecretaría de Ciberdefensa, que es el órgano que conduce la ciberdefensa y deriva las directivas de acuerdo con las políticas nacionales, al comando conjunto de ciberdefensa que es la parte operativa (ver Anexo D).

Brasil: Según la documentación encontrada, Brasil desde el año 2012 está vigente el "Livro Branco de Defesa Nacional" que sería el primer documento oficial en incluir la

ciberseguridad en la defensa del Estado (Ministerio de Defensa, 2012), sin embargo, este aún no estipulaba lineamientos claros específicos relativos a la ciberdefensa, por tanto, no se considera parte del análisis de sus componentes. Dicho esto, como se observa en la Tabla 3, ya en el año 2020 se aprueba el documento normativo del Decreto N°10.222, de 5 de febrero de 2020, Estrategia Nacional de Seguridad Cibernética - E-Ciber (2020) el cual es una actualización, del documento Estrategia de Seguridad de la Información y las Comunicaciones y Seguridad Cibernética Administración Pública Federal que fue válido solo hasta el 2018. Años más tarde, en el 2023, la Presidencia de la República de Brasil establece la Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad (2023).

Chile: El Ministerio de Defensa Nacional aprobó el documento "Política de Ciberdefensa" (Ministerio de Defensa Nacional, 2018). Aunque posteriormente se aprobó la "Ley Marco de Ciberseguridad" por el Ministerio del Interior y Seguridad Pública (2024), en donde se hace un abordaje general sobre la ciberseguridad, pero su Título V menciona la ciberdefensa (ver Tabla 3). El especialista **E-Ch** manifiesta que Chile estableció su Política de Ciberdefensa, pero no ha realizado cambios hasta ahora que sean significativos y que todavía se incluye en los planes a futuro del Estado (ver Anexo D).

Colombia: En Colombia, el documento principal relacionado a la ciberdefensa es el Documento Conpes 3701 del Consejo Nacional de Política Económica y Social (CONPES, 2011) titulado "Lineamientos de Política para Ciberseguridad y Ciberdefensa". A partir de allí, se busca con mayor determinación la seguridad tanto para el ámbito público como militar, incluyendo dicho aspecto como parte de su necesidad de defensa nacional, siendo el documento base para este propósito. El documento principal (3701) no ha tenido modificaciones, hasta el año 2022, en donde se expone en el Decreto 338 (2022), la adición del Título 21 en la Parte 2 del Libro 2, mediante Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078, el cual se formuló considerando el documento Conpes 3701 (ver Tabla 3). **E-Co** señala que Colombia ha tenido una buena actualización en materia de ciberseguridad, siendo corroborados en los documentos encontrados en el análisis documental, como parte de los lineamientos para formular políticas estratégicas en materia de ciberdefensa y ciberseguridad, que son el Conpes 3701 y 3854.

Ecuador: En Ecuador, el documento que establece la iniciativa formal para la ciberdefensa fue el Plan Específico de Defensa 2019 – 2030 (Ministerio de Defensa

Nacional, 2019), sin embargo, este documento no se considerará como parte del análisis, ya que dos años más tarde, como se especifica en la tabla 3, plantean el documento de Política de Ciberseguridad en marzo de 2021 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021), con la finalidad de tener lineamientos generales para el Estado, que busquen la mejora de la ciberseguridad en el mismo, mencionando la ciberdefensa. Luego, en el mismo año se establece la "Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia" (Asamblea Nacional República del Ecuador, 2021), para ser un poco más específica. También, en dicho año, se publica el documento de Estrategia de Ciberdefensa (Ministerio de Defensa, 2021). Luego, para el año 2022, se realiza el documento Estrategia Nacional de Ciberseguridad del Ecuador (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022), también con un abordaje general, pero que incluye aspectos a rescatar al indicar algunas acciones relativas a la ciberdefensa (ver Tabla 3). **E-E** indica que el proceso para establecer lineamientos claros en materia de ciberdefensa ha sido paulatino y reciente, modificándose constantemente para mejorar sus propuestas. Aunque, menciona también que se ha creado una Política de Ciberdefensa, que establece la base para la estructura de apoyo en el desarrollo de estas capacidades (ver Anexo D).

Perú: Ya en el año 2021, se establece la Ley de Ciberdefensa (2021) con número 30999, que fue aprobada el 26 de febrero de 2019. No obstante años después se plantea el Reglamento de la Ley N° 30999, Ley de Ciberdefensa (2023) (ver Tabla 3), aprobado mediante Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa (2024). En este caso el especialista, **E-P** indica que, en efecto, se tiene una ley en concreto respecto a la ciberdefensa, pero indica que no es una política como tal y que otros Estados están más adelantados en este aspecto (ver Anexo D).

Sobre lo expuesto, como se observa en la tabla 3, todos los Estados poseen documentos que dentro de los mismos hacen el respectivo abordaje de la ciberdefensa. Varios de ellos poseen en sus títulos precisamente la ciberdefensa y otros solo ciberseguridad, pero que en sus lineamientos se especifica la ciberdefensa. Además, la generación de estos documentos o leyes precisamente sobre ciberdefensa ha sido de cierta forma reciente, entendiendo que fueron las necesidades del Estado las que impulsaron su desarrollo. Tal como indican Huamani y Aparecida (2024), los Estados de Argentina, Perú y Brasil, para sus métodos de ciberseguridad y ciberdefensa, toman en cuenta el contexto sociocultural y organizacional,

más no el geopolítico y diplomático, pudiendo ser por tal motivo, la falta de actualización y demora en el establecimiento de lineamientos claros en ciberdefensa.

Por otro lado, como se observa en la tabla 3, sólo Argentina, Chile, Colombia y Perú, poseen documentos individuales y específicos que destacan normativas o políticas en ciberdefensa. Para el caso de Brasil, sólo tienen decretos y documentos estratégicos sobre ciberseguridad o seguridad digital. Además, Ecuador tiene un documento de estrategia de ciberdefensa, pero no se ubica una normativa o ley específica sobre este. Es así, como se comprende que no todos los Estados en estudio contemplan de manera concreta políticas de ciberdefensa; sin embargo, sí lo toman en cuenta y lo incluyen en sus documentos sobre ciberseguridad, pero que esto, como lo demuestra Brasil, no es un impedimento para las acciones técnicas adecuadas para enfrentar las amenazas cibernéticas. De manera similar a lo expuesto, Mosquera (2021) y Paredes y Ángelo (2024) identifican que a Ecuador aún le falta implementar mejores lineamientos para la ciberdefensa.

En este aspecto, tal como se muestra en la Tabla 3, se encuentran los documentos seleccionados para el análisis posterior, debido a que son los documentos más actualizados en relación con la ciberdefensa y que en muchos casos, sí son leyes o normativas en ciberdefensa.

Tabla 3

Políticas de ciberdefensa de los Estados

Estado	Políticas de ciberdefensa
Argentina	- Modelo Referencial de Política de Seguridad de la Información (Dirección Nacional de Ciberseguridad, 2022). Link: https://www.boletinoficial.gob.ar/detalleAviso/primera/257620/20220216 - Política de Ciberdefensa (Ministerio de Defensa, 2022). - Segunda Estrategia Nacional de Ciberseguridad (Gobierno de Argentina, 2022). Link: https://www.argentina.gob.ar/sites/default/files/anexo_6777529_1.pdf - Crear el Centro de Supervisión y Control de Gestión de Ciberdefensa y el Comité de Infraestructura Crítica de la Información de la Defensa (Gobierno de Argentina, 2023)
Brasil	- Estrategia Nacional de Seguridad Cibernética - E-Ciber (2020). Link: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf - Política Nacional de Ciberseguridad (Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad, 2023). Link: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11856.htm
Chile	- Política de Ciberdefensa (Ministerio de Defensa Nacional, 2018). Link: https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf - Ley Marco de Ciberseguridad (Ministerio del Interior y Seguridad Pública, 2024). Link: https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf
Colombia	- Documento Conpes 3701 (Consejo Nacional de Política Económica y Social, 2011). Link: https://sherloc.unodc.org/cld/uploads/res/lessons-learned/col/lineamientos-de-politica-para-ciberseguridad-y-ciberdefensa_html/Lineamientos_de_politica_para_ciberseguridad_y_ciberdefensa.pdf - Decreto 338 de 2022 (2022) Adición del Título 21 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Link: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866
Ecuador	- Política de Ciberseguridad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021). Link: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf - Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia" (Asamblea Nacional República del Ecuador, 2021). Link: https://asobanca.org.ec/wp-content/uploads/2021/10/Proyecto-de-Ley-Organica-de-Seguridad-Digital-Ciberseguridad-Ciberdefensa-y-Ciberinteligencia.pdf - Estrategia de Ciberdefensa (Ministerio de Defensa, 2021) - Estrategia Nacional de Ciberseguridad del Ecuador (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). Link: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf
Perú	- Ley de Ciberdefensa (2021). Link: https://cdn.www.gob.pe/uploads/document/file/1671813/Ley%20N%C2%B030999%2C%20Ley%20de%20Ciberdefensa.pdf?v=1613166516 - Reglamento de la Ley N° 30999 (2023). Link: https://cdn.www.gob.pe/uploads/document/file/4933153/Proyecto%20de%20Reglamento%20Ley%2030999.pdf

4.2 Componentes de la estructura de las políticas de ciberdefensa de los Estados en estudio

4.2.1 Descripción de los componentes de las políticas de ciberdefensa

Los componentes que contemplan los documentos seleccionados y relacionados a la ciberdefensa o la ciberseguridad expresado en las siguientes Tablas (4-9), se manifiestan según la estructura de éstos en base a sus subtítulos, teniendo en cuenta que fueron escogidos luego del subtítulo de "Introducción" que es común en los documentos y comenzando su selección a partir de su propósito u objetivo. A continuación, se describen dichos componentes por cada Estado.

Argentina: El documento de Modelo Referencial de Política de Seguridad de la Información de la Dirección Nacional de Ciberseguridad (2022) señala entre sus componentes: objetivo, alcance, principios básicos y lineamientos específicos. Luego, en el documento Política de Ciberdefensa del Ministerio de Defensa (2022), se pueden identificar los siguientes componentes que abordan la ciberdefensa: planeamiento estratégico, un marco conceptual, objetivos específicos y componentes sistémicos subsidiarios. Por otra parte, en el documento de Segunda Estrategia Nacional de Ciberseguridad del Gobierno de Argentina (2022) se observan como componentes: objetivo principal, principios rectores y objetivos específicos (ver Tabla 4). Por otro lado, de acuerdo con **E-A**, considera que el documento de Política de Ciberdefensa tiene lo necesario, aunque se subdivide de manera sencilla, pero posee los diversos componentes detallados para abordar la ciberdefensa. El entrevistado destaca que la protección de las infraestructuras críticas de información es fundamental para la seguridad nacional. Indica también, que es positivo que se esté monitoreando las redes de las Fuerzas Armadas a través del Comando Conjunto de Ciberdefensa, pero que necesita definir mejor una política de ciberdefensa a nivel estatal para establecer directrices claras y estrategias efectivas (ver Anexo D).

En este aspecto, se aprecia que Argentina posee componentes que son similares entre los documentos explorados, como objetivos y principios, denotando la importancia que tienen estos elementos. En este aspecto Jarufe (2020) indica que Argentina emplea Estrategias Nacionales de Ciberseguridad para responder a las ciberamenazas, proteger su infraestructura crítica y promover la cooperación internacional en el ciberespacio. Huamani y Aparecida (2024) encontraron que posee componentes sobre el abordaje de amenazas y riesgos, capacidad y respuesta, entre otros que se reflejan en sus políticas. Por su parte,

concuerda con el CEDIP (2022) que señala que Argentina tiene una diversa gama de normativas sobre ciberseguridad, aunque tienen un enfoque administrativo.

Brasil: En el documento Estrategia Nacional de Seguridad Cibernética - E-Ciber (2020) se detectan varios componentes en su estructura como objetivos estratégicos, acciones estratégicas, ejes temáticos (protección y seguridad), ejes temáticos (transformadores). Por otra parte, en el documento Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad (2023) se pueden observar varios componentes en la Política Nacional de Ciberseguridad como principios, objetivos, instrumentos y organismos ejecutores (ver Tabla 5). En este caso Kosevich (2020) refuerza el hecho de que Brasil aspira a ser un actor global en seguridad cibernética, planeando lograr esto a través de un aumento rápido de las inversiones internas en tecnología de la información, la creación de empleo y la promoción de la cooperación interinstitucional. Estos aspectos estarían dentro de sus políticas, las cuales pueden ser las más adecuadas ya que han demostrado ser el número 1 en materia de ciberdefensa. Así lo reforzaría también el CEDIP (2022) al indicar que Brasil posee normativa variada y amplia para regular la ciberseguridad. Aunque en este caso se ha podido determinar algunos documentos actuales que hablan de la ciberdefensa y que reflejan las necesidades que requieren.

Chile: En el documento normativo de Política de Ciberdefensa del Ministerio de Defensa Nacional (2018), se pueden identificar los siguientes componentes: objetivo principal, principios, políticas, instrumentos. Por su parte, en el documento Ley Marco de Ciberseguridad del Ministerio del Interior y Seguridad Pública (2024) se identifican objeto, principios rectores, ámbito de aplicación, operadores, Equipo de Respuesta a Incidentes de Seguridad Informática y funciones (ver Tabla 6). El especialista **E-Ch** indica que la normativa que aborda los componentes de la ciberdefensa tiene los aspectos fundamentales, pero que se necesita mucha mayor especificación y consideración de otros componentes como capacidades específicas de defensa y la infraestructura crítica de información, destacando que su enfoque en la colaboración internacional y la creación de Equipos de Respuesta ante Incidentes Informáticos demuestra una postura proactiva (ver Anexo D). Algunos antecedentes indican que en estos componentes en algunos Estados han ido mejorando en las que todavía falta especificar o adicionar, por ejemplo, Mosquera (2021) indica que hace 2 años atrás, en Chile aún faltaba ampliar herramientas jurídicas e institucionales que garanticen la ciberseguridad. Aunque en este caso Chile se actualizó mediante la Ley Marco de Ciberseguridad del Ministerio del Interior y Seguridad Pública

(2024) para sus necesidades de ciberseguridad y ciberdefensa, pero aun así **E-Ch** señaló que falta un mejor detalle en sus políticas, sobre todo de sus capacidades. Por su parte, Kosevich (2020) refuerza estos componentes al indicar que Chile busca crear una infraestructura de TIC robusta para enfrentar incluso los ataques virtuales más complejos, lo cual se evidenciaría en todos los componentes de sus políticas establecidas.

Colombia: En el documento 3701 del Conpes (2011) se observan los componentes: objetivo central, objetivos específicos, plan de acción y financiamiento. Aunque el Decreto 338 de 2022 (2022), adiciona el Título 21, complementa los componentes anteriores considerando, además: objetivo, ámbito de aplicación, lineamientos generales, principios, modelo de gobernanza, identificación de las infraestructuras críticas, atención y gestión de incidentes (ver Tabla 7). En este caso **E-Co** indica que, dentro de los elementos o componentes importantes, está el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), que es un grupo que proporciona asistencia técnica en caso de incidentes cibernéticos y coordina la respuesta a emergencias a nivel nacional. También, señala que tienen al Consejo Nacional de Seguridad Informática (CNSI), que formula políticas y estrategias en materia de ciberseguridad, asegurando la protección de la infraestructura crítica del país. Por último, indica un Marco de Seguridad de la Información, el cual desarrolla estándares y procedimientos para proteger la información en las entidades estatales y en el sector privado (ver Anexo D). Esto se refuerza con lo que manifiesta Kosevich (2020) al indicar que Colombia ha desarrollado cronogramas detallados y esquemas de financiamiento, estableciendo cinco ejes principales: desarrollo coordinado, cooperación público-privada, cultura ciudadana de ciberseguridad, desarrollo de potencial en manejo de riesgos y generación de un fundamento de ciberseguridad estatal.

Ecuador: Ecuador posee el documento Política de Ciberseguridad del Ministerio de Telecomunicaciones y de la Sociedad de la Información (2021) se destacan los siguientes componentes: pilares, objetivos y líneas de acción (objetivo general y específico), responsabilidades de las áreas de operación, seguimiento y monitoreo de las líneas de acción. Por otro lado, dentro de la Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia de la Asamblea Nacional República del Ecuador (2021) se destacan objeto y ámbito, definiciones, principios, Sistema Nacional de Seguridad Digital, Subsistemas de seguridad y organismos. En el documento de Estrategia de Ciberdefensa del Ministerio de Defensa (2021), se observan aspectos fundamentales como alcances de la estrategia, objetivos, seguimiento y evaluación. Finalmente, el documento Estrategia

Nacional de Ciberseguridad del Ecuador del Ministerio de Telecomunicaciones y de la Sociedad de la Información (2022) establece en su estructura: visión, principios y objetivos estratégicos, pilares, implementación, seguimiento y evaluación (ver Tabla 8). Sobre lo mencionado **E-E**, confirma que los componentes más importantes que dan forma a los lineamientos de ciberdefensa en las políticas existentes son los objetivos y principios, las cuales deben armonizar las políticas estatales y las estrategias sectoriales en materia de seguridad digital y defensa, aunque los recursos puedan ser limitados (ver Anexo D). A pesar de poseer estos componentes se reconoce como menciona Paredes y Ángelo (2024), que a Ecuador todavía le falta mejorar en sus políticas, y como señala el autor requiere de especificaciones mayores referentes a la gestión de riesgos.

Perú: El principal documento que expone diversos componentes que tratan la ciberdefensa está en Reglamento de la Ley N° 30999 (2023), en la cual se observa en su estructura lo siguiente: objeto de la política, finalidad, principios rectores, rol del Ministerio de Defensa, órganos ejecutores y responsabilidades, capacidades, operaciones militares, uso de la fuerza y seguridad de activos críticos (ver Tabla 9). **E-P** indica que dentro de los componentes o aspectos que menciona la Política de Ciberdefensa, se encuentra la Estrategia Nacional de Ciberdefensa, la protección de las infraestructuras críticas, la gestión de incidentes, las especificaciones de la legislación y normativas, la educación y concientización, la colaboración o cooperación internacional, así como la investigación y desarrollo (ver Anexo D). A pesar de considerar estos componentes, parece que a Perú aún le falta una mejora de sus políticas, como refiere Quevedo (2023) aún falta una adecuada implementación de las tecnologías para la ciberdefensa y que la inversión es pobre para que se actualice, existiendo una capacidad limitada por parte de las FF.AA., lo que denotaría una falta de precisión de ello, a diferencia de Colombia que especifica un apartado de "financiamiento".

De lo expuesto, se observa en las Tablas 4 a la 9, los componentes de los diferentes documentos que advierten lineamientos relacionados a la ciberdefensa o, en su defecto, ciberseguridad que incluye la ciberdefensa.

Tabla 4

Identificación de los componentes de las políticas de ciberdefensa en Argentina

Documento	Componentes de su estructura
Modelo Referencial de Política de Seguridad de la Información (Dirección Nacional de Ciberseguridad, 2022).	Objeto/objetivo, alcance, principios básicos, revisión y actualización, lineamientos específicos.
Política de Ciberdefensa (Ministerio de Defensa, 2022)	Planeamiento estratégico, marco conceptual, enfoque sistémico, misión principal, componentes sistémicos subsidiarios.
Segunda Estrategia Nacional de Ciberseguridad (Gobierno de Argentina, 2022)	Introducción, principios rectores de la ciberseguridad, objetivos de la estrategia nacional de ciberseguridad.
Crear el Centro de Supervisión y Control de Gestión de Ciberdefensa y el Comité de Infraestructura Crítica de la Información de la Defensa (Gobierno de Argentina, 2023)	Actualización en: Creación del Centro de Supervisión y Control de Gestión de Ciberdefensa, El Comité de Infraestructuras Críticas de la Información de la Defensa (órganos ejecutores).

Nota: Información tomada del análisis documental

Tabla 5

Identificación de los componentes de las políticas de ciberdefensa de Brasil

Documento	Componentes de su estructura
Decreto N° 10.222 de 5 de febrero de 2020 (Estrategia Nacional de Seguridad Cibernética - E-Ciber, 2020)	Objetivos estratégicos, acciones estratégicas, ejes temáticos (protección y seguridad), ejes temáticos (transformadores)
Política Nacional de Ciberseguridad (Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad, 2023).	Principios, objetivos, instrumentos, organismos ejecutores, competencias

Nota: Información tomada del análisis documental

Tabla 6

Identificación los componentes de las políticas de ciberdefensa de Chile

Documento	Componentes de su estructura
Política de Ciberdefensa (Ministerio de Defensa Nacional, 2018)	Introducción, objetivo principal, principios, políticas, instrumentos.
Ley Marco de Ciberseguridad (Ministerio del Interior y Seguridad Pública, 2024)	Objeto, principios rectores, ámbito de aplicación, operadores, Equipo de Respuesta a Incidentes de Seguridad Informática, funciones.

Nota: Información tomada del análisis documental

Tabla 7

Identificación los componentes de las políticas de ciberdefensa de Colombia

Documento	Componentes de su estructura
Documento Conpes 3701 (Consejo Nacional de Política Económica y Social, 2011)	Objetivo central, objetivos específicos, plan de acción, financiamiento.
Decreto 338 de 2022 (2022)	Actualización mediante Título 21 en la Parte 2 del Libro 2: Objeto, ámbito de aplicación, definiciones, lineamientos generales, principios, modelo de gobernanza, instancias, identificación de infraestructuras críticas cibernéticas, servicios esenciales, modelo nacional de atención y gestión de incidentes

Nota: Información tomada del análisis documental

Tabla 8

Identificación los componentes de las políticas de ciberdefensa de Ecuador

Documento	Componentes de su estructura
Política de Ciberseguridad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).	Pilares, objetivos y líneas de acción (objetivo general y específico), responsabilidades de las áreas de operación, seguimiento y monitoreo de las líneas de acción.
Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia" (Asamblea Nacional República del Ecuador, 2021)	Objeto y ámbito, definiciones, principios, Sistema Nacional de Seguridad Digital, Subsistemas de seguridad, organismos
Estrategia de Ciberdefensa (Ministerio de Defensa, 2021)	Objetivos y líneas de acción, seguimiento y evaluación.
Estrategia Nacional de Ciberseguridad del Ecuador (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).	Visión, principios y objetivos estratégicos, pilares, implementación, seguimiento y evaluación.

Nota: Información tomada del análisis documental

Tabla 9

Identificación de los componentes de las políticas de ciberdefensa de Perú

Documento	Componentes de su estructura
Ley de Ciberdefensa (2021)	Objeto, finalidad, ámbito de aplicación, organismos ejecutores, rol del Ministerio de Defensa, operaciones militares, uso de la fuerza, seguridad de los activos críticos nacionales.
Reglamento Ley de Ciberdefensa (2023)	Objeto, finalidad, principios, rol del Ministerio de Defensa, organismos ejecutores, capacidades, operaciones militares, uso de la fuerza, seguridad de los activos críticos nacionales.

Nota: Información tomada del análisis documental

4.2.2 Comparación de las políticas de ciberdefensa

De acuerdo con lo que se pudo comparar entre los componentes encontrados de las políticas de ciberdefensa de los Estados, tal como se aprecia en la Tabla 10, es posible distinguir aquellos que se encuentran de manera explícita e implícita, aunque en varios casos también hay ausencia de éstos componentes que no se mencionan en algunos Estados; esto quiere decir, que no en todos los casos se comparten los componentes de las políticas de ciberdefensa en su estructura o apartado, pero sí se puede observar que se habla de ello al hacer una lectura minuciosa.

De esta manera, se puede describir según la Tabla 10 entre los componentes de objetivo principal, principios, capacidades, activos críticos nacionales y organismos ejecutores, cerca de la mitad poseen un subtítulo explícito, por otra parte, la otra mitad también existe, pero de manera implícita sin un subtítulo, pero se encuentran en el contenido de los documentos. Por otro lado, los demás componentes indicados en la Tabla 10, poseen un subtítulo explícito, pero en baja frecuencia como un apartado en los documentos. Haciendo un conteo general, se puede determinar que el 32.4% de los componentes, poseen un subtítulo explícito en las políticas de los seis Estados analizados, por otro lado, el 36.3% se encuentra de manera implícita sin un subtítulo en los documentos y el otro 31.3% no se mencionan (ver Tabla 10).

Tabla 10

Componentes en las políticas de ciberdefensa entre los Estados

Componentes de las políticas	Argentina	Brasil	Chile	Colombia	Ecuador	Perú
Objetivo Principal	Subtítulo explícito					
Objetivos Específicos o Estratégicos	Subtítulo explícito					No describe
Principios	Subtítulo explícito					
Capacidades	Sin subtítulo, implícito en el contenido					Subtítulo explícito
Activos Críticos	Sin subtítulo, implícito en el contenido			Subtítulo explícito	Sin subtítulo, implícito en el contenido	Subtítulo explícito
Organismos Ejecutores	Sin subtítulo, implícito en el contenido					Subtítulo explícito
Componentes sistémicos subsidiarios	Subtítulo explícito	No describe				
Enfoque Sistémico	Subtítulo explícito	Sin subtítulo, implícito en el contenido	No describe			
Alcance y ámbito de aplicación	Subtítulo explícito	Sin subtítulo, implícito en el contenido		Subtítulo explícito		Sin subtítulo, implícito en el contenido
Instrumentos	Sin subtítulo, implícito en el contenido	Subtítulo explícito	Sin subtítulo, implícito en el contenido			No describe
Ejes temáticos	Sin subtítulo, implícito en el contenido	Subtítulo explícito	No describe		Sin subtítulo, implícito en el contenido	No describe
Plan de acción	No describe	Sin subtítulo, implícito en el contenido		Subtítulo explícito	No describe	
Financiamiento	No describe		Sin subtítulo, implícito en el contenido	Subtítulo explícito	Sin subtítulo, implícito en el contenido	No describe
Modelo de gobernanza	No describe	Sin subtítulo, implícito en el contenido	No describe	Subtítulo explícito	Sin subtítulo, implícito en el contenido	No describe
Enfoque de seguridad	Sin subtítulo, implícito en el contenido	No describe		Sin subtítulo, implícito en el contenido	Subtítulo explícito	No describe
Rol del Ministerio de Defensa	Sin subtítulo, implícito en el contenido	No describe		Sin subtítulo, implícito en el contenido		Subtítulo explícito
Operacionales militares	Sin subtítulo, implícito en el contenido	No describe		Sin subtítulo, implícito en el contenido		Subtítulo explícito
Uso de la fuerza	No describe		Sin subtítulo, implícito en el contenido	No describe		Subtítulo explícito

Nota. Se establecen los componentes encontrados en cada Estado, comparando si se encuentran de manera explícita como un apartado o subtítulo.

Según los hallazgos, se comprende que existe una variabilidad y heterogeneidad en la cantidad y tipo de componentes que abordan las políticas de los Estados respecto a la ciberdefensa. Demostrando a su vez, que faltaría incluir otros componentes en las políticas de otros Estados, que en muchos casos no se abordan, por lo que esta falta puede ser un problema para tener una política más ordenada.

Haciendo más detalle de lo encontrado, si bien Perú no tiene un apartado de objetivos específicos, aún conserva tener uno de objetivo general, al igual que los demás Estados y se comparten los demás componentes de las políticas de ciberdefensa como principios, capacidades, activos críticos, organismos ejecutores, rol del Ministerio de Defensa, operacionales militares y uso de la fuerza. En los demás componentes encontrados, solo algunos comparten el mismo entre algunos Estados, de manera implícita o explícita, demostrando que hay muchos más elementos que podrían ayudar a las políticas actuales de Perú, que, como refiere Quevedo (2023) a Perú aún le falta una adecuada implementación de las tecnologías para la ciberdefensa y la inversión es pobre para que se actualice, existiendo una capacidad limitada por parte de las FF.AA., lo que denotaba una falta de precisión de ello, a diferencia de Colombia que especifica un apartado de “financiamiento”.

Por su parte, Mosquera (2021) indica que hace 2 años atrás, en Chile aún faltaba ampliar herramientas jurídicas e institucionales que garanticen la ciberseguridad. Aunque en este caso Chile se actualizó mediante la Ley Marco de Ciberseguridad del Ministerio del Interior y Seguridad Pública (2024) para sus necesidades de ciberseguridad y ciberdefensa. También, el CEDIP (2022) señala que Argentina posee una normativa diversa respecto a la ciberseguridad, aunque muchas tienen un enfoque administrativo. Siendo el que más componentes describe junto con Colombia Kosevich (2020) al indicar que Colombia ha desarrollado cronogramas detallados y esquemas de financiamiento, estableciendo cinco ejes principales: desarrollo coordinado, cooperación público-privada, cultura ciudadana de ciberseguridad, desarrollo de potencial en manejo de riesgos y generación de un fundamento de ciberseguridad estatal. Así lo reforzaría también el CEDIP (2022) al indicar que Brasil tiene bastante normativa que regulariza la ciberdefensa. Aunque en este caso se ha podido determinar algunos documentos actuales que hablan de la ciberdefensa y que reflejan las necesidades que requieren.

Luego se hizo una comparación del contenido de los componentes de las políticas de ciberdefensa, como se muestra en la Tabla 11, en donde varios Estados comparten entre todos el mismo contenido o descripción de dichos componentes, en otros casos, algunos

Estados comparten ciertos componentes. Por tanto, en ellos es posible distinguir similitudes y diferencias, que son de importancia analizar y comprender para entender que algunos Estados comparten significados similares en sus políticas.

Tabla 11

Contenido de los componentes de las políticas de ciberdefensa entre los Estados

Componentes	Descripción del contenido	Argentina	Brasil	Chile	Colombia	Ecuador	Perú
Objetivo Principal	Protección de la información. Establecer estrategias de gestión de riesgos. Defensa Nacional ante las amenazas cibernéticas	✓	✓	✓	✓	✓	✓
	Proteger los intereses nacionales.	✓					✓
	Reforzamiento de las capacidades para la ciberdefensa			✓	✓	✓	
Objetivos Específicos o Estratégicos	Cooperación internacional	✓	✓	✓	✓	✓	
	Protección de las infraestructuras críticas.	✓	✓			✓	
Principios	Principio de cooperación internacional	✓	✓	✓	✓	✓	
	Gestión de incidentes y riesgos.		✓		✓	✓	
	Principio de resiliencia		✓			✓	
	Protección de derechos fundamentales		✓			✓	
	Principio de legalidad, necesidad militar, proporcionalidad y oportunidad						✓
Capacidades	Gestión de incidentes y riesgos. Capacidad de prevención. Capacidad de respuesta y/o defensa activa.	✓	✓	✓	✓	✓	✓
	Recuperación y resiliencia.	✓	✓			✓	✓
	Seguimiento y evaluación.					✓	✓
Activos Críticos	Infraestructuras Críticas Nacionales de Información como principales activos críticos, donde se almacenan datos y que comprenden sistemas de información y comunicación.	✓	✓	✓	✓	✓	✓
Organismos Ejecutores	Entidades que ejecutan la ciberdefensa	✓	✓	✓	✓	✓	✓
Componentes sistémicos subsidiarios	Diseño de la defensa del ciberespacio desde un enfoque multidimensional.	✓					
Enfoque sistémico	Reúne un conjunto de Componentes contribuyentes al desarrollo de la capacidad, que son las bases del planteo tanto estratégico como operacional, como la evolución dinámica, mejora de talento humano con inversión tecnológica	✓	✓				
Alcance y ámbito de aplicación	Aplicado a todo el ámbito del organismo ejecutor y cualquiera con vínculo contractual o jerárquico. En donde participan entidades obligadas a las disposiciones contenidas en las normativas que conforman la Administración Pública.	✓	✓	✓	✓	✓	✓
Instrumentos	Documentos de estrategia nacional para ciberseguridad y ciberdefensa, así como de planes nacionales, convenios y resoluciones	✓	✓	✓	✓	✓	
Ejes temáticos	Revisión y actualización de normativas para mejorar los objetivos estratégicos, la formulación de acciones de ciberseguridad nacional, y la modificación de estrategias a nivel normativo, tecnológico y de vínculos. Promueven el desarrollo de una infraestructura digital segura y el uso responsable de las TIC, abarcando la protección y seguridad de la información.	✓	✓			✓	
Plan de acción	Se especifican las acciones concretas a desarrollar como la capacitación en ciberseguridad y ciberdefensa, el fortalecimiento de la legislación y la cooperación internacional.			✓	✓		
Financiamiento	Señala el responsable y costo de aquí a varios años del financiamiento para la ciberdefensa.			✓	✓	✓	
Modelo de gobernanza	Se trata de un esquema de actividades con un cúmulo de lineamientos, principios, normativas y procesos para tomar decisiones y programas compartidos por diversas partes interesadas en seguridad.		✓		✓	✓	
Enfoque de seguridad	Se describe diversos sub-enfoques adoptados, como de confianza digital, gobernanza, resiliencia, derechos digitales, multisectorial y multidimensional, sistémico, integral y de planificación estratégica, enfoques que guían las acciones sobre ciberseguridad y ciberdefensa.	✓			✓	✓	
Rol del Ministerio de Defensa	Especifica su rol para dirigir, normar, supervisar y evaluar las disposiciones en ciberdefensa.	✓			✓	✓	✓
Operacionales militares	Menciona acciones estratégicas que se planifican y ejecutan en el ciberespacio con el objetivo de lograr resultados militares específicos para proteger la seguridad nacional.	✓			✓	✓	✓
Uso de la fuerza	Se justifica el empleo de la fuerza, para tomar medidas que debiliten o anulen las habilidades y acciones del oponente en el ciberespacio, señalando las reglas de enfrentamiento.			✓			✓

Nota. Comparación del contenido de los componentes encontrados en las políticas de los Estados provenientes de los datos del anexo G.

Ante los hallazgos, es importante destacar que esta diversidad de contenidos encontrados y poca similitud, refleja también un problema que concuerda con lo que manifiesta el CEDIP (2022), que considera importante tener un consenso respecto al entendimiento de ciertos componentes y términos, que ayude a unificar la comprensión sobre los aspectos que se abordan en la ciberdefensa, teniendo en cuenta que la ciberdefensa como un fenómeno global, es algo cambiante y complejo, siendo de gran interés para los Estados. Los conceptos de ciberseguridad, ciberguerra y cibercrimen no tienen definiciones uniformes. Las doctrinas y entidades de diversos Estados no tienen una definición homogénea debido a que cada una atiende a las amenazas y ataques cibernéticos según su propio contexto (CEDIP, 2022).

De este modo, también como refiere la UIT (2024) los países deben priorizar la ciberseguridad en los pilares jurídico, técnico, organizativo, cooperativo y de desarrollo de capacidades. En lugar de centrarse en documentos superficiales, deben enfocarse en actividades de alto impacto, como implementar medidas legales claras y justas, fomentar esfuerzos interfuncionales, mantener instituciones capacitadas, involucrar a diversas partes interesadas, actualizar la estrategia nacional de ciberseguridad, aplicar medidas de protección infantil en línea, abordar desafíos en infraestructuras críticas, realizar campañas de concienciación, ofrecer capacitación, crear incentivos para el desarrollo de capacidades y promover la cooperación nacional e internacional. La ciberseguridad sigue evolucionando, y los países deben participar en procesos de mejora continua para enfrentar desafíos futuros y proporcionar una conectividad significativa para todos.

4.3 Similitudes en las políticas de ciberdefensa

En este apartado, se establecen las similitudes de los componentes de las estructuras de las políticas de los Estados considerados y también lo que mencionan en su contenido, remarcando que, en varios casos, al tener en sus descripciones similares denominaciones, se unieron a los componentes considerados dentro de una categoría tratada en el presente estudio, por tanto, se reducen dichos componentes que se expusieron en las Tablas 4 a la 9.

De esta manera, se ha podido evidenciar según la Tabla 10, que **todos los Estados** en su estructura poseen un **objetivo principal, principios, capacidades**, **activos críticos de información y los organismos ejecutores y alcance o ámbito de aplicación**. Aunque, resalta que no todos poseen un subtítulo explícito sobre el apartado de capacidades y organismos ejecutores, alcance y ámbito de aplicación, pero sí lo tienen de manera implícita. Estos son los componentes similares que se han podido detectar y demuestra que, a pesar de las diferencias en la estructuración de las políticas en ciberdefensa, comparten estos elementos importantes de similar índole, comprendiendo que para ellos son prácticamente la base para formar y desarrollar los aspectos que necesitan en sus políticas de ciberdefensa.

Ahora, es necesario corroborar las similitudes que existen en el contenido de los componentes similares encontrados. En este aspecto, en la Tabla 11, se puede observar sobre el **objetivo principal,** que se comparte en el contenido, la explicación de la protección de la información en el ciberespacio, teniendo en cuenta estrategias de gestión y la necesidad de defensa nacional contra amenazas cibernéticas. En este aspecto, así como menciona

Respecto a los **principios**, aunque los Estados compartan el componente, no contemplan un tipo de principio similar entre todos dentro de su contenido, lo que sería una diferencia que también se verá en el siguiente apartado. De todas formas, es importante reconocer, que siempre es necesario guiarse por principios que puedan regir o normar la conducta o actuación frente a algo tan importante como es la defensa nacional desde el ámbito cibernético.

Respecto a las **capacidades**, según la Tabla 11, se observa que todos los Estados, concuerdan en la gestión de incidentes y riesgos, capacidad de prevención y capacidad de respuesta y/o defensa activa. En este contexto, se abordan los aspectos técnicos para la ciberseguridad y ciberdefensa, observando por ejemplo como capacidad la de prevención, que sería una medida pasiva para prever que se genere un ataque cibernético. También comparten la capacidad de respuesta y/o defensa activa, que se desarrolla cuando ya existe

el ataque de por medio, siendo una medida activa. También, tienen en cuenta la gestión de incidentes y de riesgo, que conlleva todo el proceso anteriormente mencionado, buscando reportar, resolver, gestionar, detectar y prevenir incidentes, así como riesgos potenciales que atentan o vulneran los datos de secreto militar y del Estado en general. Este hallazgo es de cierta forma similar con lo mencionado por Kshetri y Miller (2021), que destacan la variedad y complejidad de las técnicas utilizadas por muchos Estados para combatir las ciberamenazas y salvaguardar activos digitales vitales. Por tanto, si bien casi todos los Estados tienen en cuenta las mismas capacidades para la ciberdefensa, puede que dentro de sus aspectos más concretos o técnicos sean diferentes, ya que esto estaría demostrado por la efectividad que tienen al enfrentarse a las ciberamenazas.

Sobre los **activos críticos nacionales,** todos los Estados señalan que los activos críticos en materia de ciberdefensa se basan en las denominadas Infraestructuras Críticas Nacionales de Información, importantes para el funcionamiento del Estado y que su vulneración sería un enorme riesgo para este, ya que son vitales el desarrollo social y económico y son estructuras en donde se almacenan datos y comprenden sistemas de información y comunicación (ver Tabla 11). Por tanto, la definición es correcta para el ámbito de la ciberdefensa, debido a que la información es un gran activo, sobre todo si es de secreto militar. El resultado es parecido al de Odebade y Benkhelifa (2023), el cual también concuerda que diversos Estados poseen similitudes, sobre lo que consideran proteger como activos críticos nacionales, por tanto, se denota que es sencillo reconocer para cada Estado, cuáles son sus activos más importantes, siendo sobre todo aquellos que poseen información secreta y que representa un riesgo para el Estado y su defensa. Así también lo señala el CEDIP (2022) al indicar que varios Estados, entre ellos Estados Unidos, Argentina, Brasil, Estonia y Singapur, tienen catálogos de infraestructuras críticas de la información, en donde se especifica un poco más cuáles son esos activos para su defensa nacional, al igual que Perú que tienen señalado sus activos críticos según la DINI la CCFFAA y las FFAA.

Por último, como se muestra en la Tabla 11, todos los Estados señalan sus **organismos ejecutores**, encargados de manera directa de la ciberdefensa (ver Tabla 11). En este aspecto se comprende que cada Estado tiene bien en claro la entidad que debe ejecutar la ciberdefensa. Sin embargo, Paredes y Ángelo (2024), siguen haciendo hincapié en que a Ecuador aún le falta mejorar en ciberdefensa, lo que se puede interpretar que, a pesar de tener un Comando de Ciberdefensa, puede que no esté desarrollando adecuadamente sus labores o no tengan las políticas adecuadas para ello.

La entrevista a **E-Co** señala que es común la presencia de un Centro Nacional de Respuesta Cibernética. Este centro se encarga de orientar a los sectores más regulados, los cuales generalmente incluyen aquellos que involucran infraestructura crítica, como energía, agua, telecomunicaciones y servicios financieros, debido a su impacto crucial en el bienestar de la población y la seguridad del país. **E-A** señala que el comando conjunto de ciberdefensa es la que realiza la parte operativa y que busca proteger las infraestructuras críticas. Esto es algo que se repite en los demás Estados, siendo común la necesidad de protección de los activos críticos gracias a los comandos de ciberdefensa.

Finalmente, sobre el **Alcance y ámbito de aplicación**, todos los **Estados** lo poseen, donde Argentina, Colombia y Ecuador lo expresan de manera explícita como un subtítulo a diferencia de Brasil, Chile y Perú. En todos los casos, explican el alcance de la política hacia todo ámbito del organismo ejecutor de la ciberdefensa; en este caso, se hace responsable el ministerio, los Comando Conjunto, entre otras entidades encargadas para la implementación y evolución del plan nacional de ciberdefensa y que contribuya a este propósito. En este aspecto **E-A**, manifiesta que la ciberdefensa se centra en la parte militar, mientras que, en otros lugares, como Perú, el Comando Conjunto de Ciberdefensa también participa en eventos civiles (ver Anexo D).

De todo lo encontrado, se aprecia que hay diversos componentes que se comparten entre todos los Estados, comprendiendo que los componentes detallados son requeridos en sus políticas. Ante esto, la Unión Internacional de Telecomunicaciones (2024) señala que en los cinco pilares del ICG, la mayoría de los Estados son más fuertes en el pilar jurídico. Lo que sugeriría que incluso los Estados mencionados, poseen aspectos normativos pertinentes o adecuados. Sin embargo, también la UIT (2024) menciona que muchos Estados pueden aclarar aún más sus leyes y regulaciones sobre privacidad, protección de datos y notificación de infracciones. Por ejemplo, no todos los Estados han definido claramente cuál es el período de notificación esperado para las infracciones, o el mandato de las autoridades competentes para monitorear y responder a las infracciones. También, en este aspecto la UIT (2024) de acuerdo con los índices de fuerza relativa y potencial de crecimiento en ciberseguridad, Brasil posee el máximo de puntaje que es 20, siendo calificado como un modelo a seguir en el aspecto legal, seguido de Perú (20) Ecuador (19.21), Argentina (16.96), Chile (14.69) y Colombia (13.37). Esto demuestra, que, si bien de manera legal es posible que varios de los Estados de análisis se encuentren adecuadamente establecidos y compartan componentes similares, la realidad sobre su efectividad puede ser diferente.

4.4 Diferencias en las políticas de ciberdefensa

Debido a que no todos los Estados han compartido similares contenidos entre todos ellos, se han establecido como diferencias en el presente estudio, los cuales son importantes analizar.

En este aspecto, por ejemplo, hay diferencias en el contenido del **objetivo principal,** ya que solo **Colombia, Ecuador y Chile** comparten la necesidad del reforzamiento de las capacidades de ciberdefensa (CONPES, 2011; Ministerio de Defensa, 2021; Ministerio de Defensa Nacional, 2018); **Argentina y Perú** indican que, se tienen que proteger los intereses nacionales (Dirección Nacional de Ciberseguridad, 2022; Ley de Ciberdefensa, 2023) (ver Tabla 11). Además de ello, cada Estado tuvo algo particular que dentro del contenido del **objetivo principal**. **Argentina**, hace hincapié en mejorar continuamente. En este caso **Brasil,** agrega que se busca asegurar el uso confiable del ciberespacio, incrementar la resiliencia ante amenazas cibernéticas y fortalecer actividades de ciberseguridad. **Colombia** busca crear un entorno con circunstancias necesarias para que el ciberespacio esté protegido. **Ecuador** señala mejorar la Ciberinteligencia para tomar decisiones adecuadas (ver Anexo G).

El resultado se asemeja al de Odebade y Benkhelifa (2023), en el aspecto de que, encontraron que, en diferentes Estados, no se tiene una comprensión unificada de lo que es ciberdefensa. Analizando este punto, un objetivo principal, ayuda a comprender la meta a donde se quiere llegar y en este caso, los objetivos principales de las políticas para la ciberdefensa varían en lo que quieren conseguir, algunos indicando más aspectos que otros, por lo que sería importante que se compartiera o tuviera una comprensión unificada del propósito de la ciberdefensa, que sea completa y necesaria para la realidad actual.

Por consiguiente, se tiene que mencionar los **objetivos específicos o estratégicos** que derivan del objetivo principal, que también no todos los Estados los poseen, en donde se diferencia porque Perú no lo posee y **Argentina, Brasil, Chile**, **Colombia** y **Ecuador**, concuerdan en ello y mencionan la importancia de la cooperación internacional y reforzamiento continuo y desarrollo de las capacidades de ciberdefensa (Ministerio de Defensa, 2022: Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad, 2023; Ministerio de Defensa Nacional, 2018; CONPES, 2011; Ministerio de Defensa, 2021). También, **Argentina, Brasil y Ecuador** concuerdan en la protección de las infraestructuras críticas (Gobierno de Argentina, 2022; Estrategia Nacional de Seguridad

Cibernética - E-Ciber, 2020; Ministerio de Defensa, 2021). También, **Brasil, Colombia y** Ecuador, concuerdan a diferencia de otros, la protección de los derechos fundamentales. (Estrategia Nacional de Seguridad Cibernética - E-Ciber, 2020; Decreto 338 de 2022, 2022; Ministerio de Defensa, 2021) (ver Tabla 11).

Además, continuando con los **objetivos específicos o estratégicos**, se observan ciertas particularidades distintas o únicas en cada Estado, por ejemplo, **Argentina** agrega el fomento de la industria de la ciberseguridad. **Brasil**, incluye el desarrollo profesional, investigación e innovación, fortalecimiento de las infraestructuras críticas y mayor concientización de seguridad cibernética. **Chile,** destaca la promoción de transparencia. **Colombia,** señala la capacitación especializada y ampliación de investigación. **Ecuador** indica fortalecer la cultura de ciberdefensa (ver Anexo G).

Es posible apreciar que tanto los objetivos específicos o estratégicos, tienen gran coherencia con los principios que establecen los Estados de estudio. Esto es similar a lo que menciona el estudio de Jarufe (2020), que diversos Estados como Argentina, Corea del Sur, Nueva Zelanda y Singapur, establecen como necesario en sus lineamientos, proteger su infraestructura crítica y promover la cooperación internacional en el ciberespacio, como en el caso de los Estados analizados, aunque difiere con Perú que no especifica el aspecto de la cooperación internacional. También, es similar al estudio de Odebade y Benkhelifa (2023) que, dentro de las similitudes encontradas en otros Estados de Europa, Asia y América, tienen como objetivo la protección de activos críticos, investigar y desarrollarse, además de una mejor colaboración nacional e internacional, infiriendo de este modo que hay muchos Estados, que consideran estos puntos muy importantes dentro de sus políticas y que son aspectos comunes y que no se deben dejar pasar por otros Estados que no lo consideran hasta el momento.

También, se analiza que los Estados se enfocan en sus objetivos, sobre la necesidad de buscar mejoras en la estrategias o capacidades para la ciberdefensa. De similar forma esto se subdivide en los objetivos específicos o estratégicos que se detallan en los demás Estados, como proteger las infraestructuras críticas, desarrollar capacidades, mayor investigación y la necesidad de cooperar entre naciones. Esto es algo realmente importante dentro de las políticas, ya que permite continuar con el avance de nuevas formas de defensa en el ámbito cibernético y estar a la vanguardia de la tecnología. Ante esto, hallazgos similares como el de Paredes y Ángelo (2024) mencionan que, para incrementar la capacidad de ciberdefensa, se necesita mayor desarrollo tecnológico para no depender de otros; de similar forma

concluye Quevedo (2023) que se necesita invertir y hacer actualización continua en tecnologías de seguridad.

A pesar de tener bastante descrito los objetivos específicos, en donde se estipulan diversas actividades o requerimientos para la ciberdefensa, al parecer no se están desarrollando adecuadamente, ya que, según algunos datos de la Unión Internacional de Telecomunicaciones (UIT, 2024) a nivel mundial, entre el 14 % y el 35% por ciento de los servicios de correo en el mundo, no utilizan protocolos o cifrados adecuados (SSL/TLS), o utilizan protocolos inseguros o débiles, denotando la carencia de implementación adecuada de las herramientas para la ciberdefensa. No obstante, señala que el desarrollo de capacidades se percibe mejor en Brasil con una puntuación de 19.09 de un máximo de 20, seguido de Perú con 15.16, Colombia con 15.14, Ecuador con 13.78, Chile con 11.52 y Argentina con 1.88, comprendiendo que, Perú todavía podría mejorar en este aspecto, debido a que como refiere Quevedo (2023) Perú enfrenta problemas en ciberdefensa, por la falta de implementación adecuada de tecnologías y procesos para fortalecer la protección de datos, además de que Perú no posee un apartado de objetivos específicos, lo cual sería ideal para adicionar en su política.

Por otro lado, Argentina, aunque tenga como uno de sus objetivos el desarrollo continuo, según el análisis de la UIT (2024), en la práctica esto no se está llevando a cabo por las puntuaciones bajas en desarrollo de capacidades. En este aspecto el **E-A** señala que es necesaria la colaboración y coordinación entre estas entidades, para producir un efecto más significativo al enfrentar a los agresores cibernéticos. También requiere fortalecer la ciberdefensa, con más control y monitoreo. Además, señala que la consolidación en un solo sistema de monitoreo simplificará los esfuerzos y mejorará la seguridad.

Sobre las diferencias encontradas en los **principios, todos los Estados** menos Perú poseen de similar forma el principio de cooperación internacional y **Brasil**, **Colombia y Ecuador** poseen el principio de protección de derechos fundamentales y el principio de gestión de riesgos. (Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad, 2023; Decreto 338, 2022; Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). Por otra parte, **Brasil y Ecuador,** comparten el principio de resiliencia (Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad, 2023; Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022 (ver Tabla 11). Por otro lado, los Estados de manera particular poseen los siguientes principios. **Argentina**, indica el principio de confidencialidad, integridad, disponibilidad, cumplimiento

normativo, paz y seguridad, cultura en ciberseguridad (educación y concientización), desarrollo socioeconómico y soberanía nacional. **Brasil,** adiciona el principio de Educación y Desarrollo Tecnológico en Ciberseguridad, el principio de gobernanza, el principio de Política Nacional, principio de compromiso de alta administración, principio de marco legal, principio de soberanía nacional y principio de integración. **Chile,** destaca el principio de equivalencia, respeto del derecho internacional público y promoción de la democracia. **Colombia,** resalta el principio de confianza, coordinación, colaboración entre partes interesadas, gradualidad, inclusión, proporcionalidad, principio de recursos y uso eficiente de infraestructura para proteger los activos críticos. **Ecuador,** incluye el principio de liderazgo y responsabilidad compartida, visión inclusiva y colaborativa. **Perú,** el principio de legalidad, necesidad militar, proporcionalidad y oportunidad (ver Anexo G).

Por su parte, **E-P**, concuerda en que las políticas y estrategias de ciberseguridad y ciberdefensa, comparten el objetivo de fortalecer la resiliencia cibernética de los Estados. Esto implica garantizar el bienestar de los ciudadanos y su confianza en el uso seguro de los servicios digitales nacionales. Aunque existen similitudes, cada Estado adapta estas políticas según sus contextos y desafíos específicos (ver Anexo D). Se asemeja a lo que encontró Odebade y Benkhelifa (2023) que encontraron, que muchos Estados consideran también de manera similar la colaboración nacional e internacional, para afianzar y reforzar la ciberdefensa con el soporte de otros Estados o de entidades privadas dentro del Estado. Al respecto según la UIT (2024) Argentina es la que menos aplica la cooperación público-privada para la defensa, con un índice de 8.41. En este caso, Brasil es quien lidera con el puntaje máximo (20), seguido de Ecuador con 17.7, luego Perú y Chile con 16.8 y por último Colombia con 10.23. Esto da a entender, que no siempre lo que está en las políticas se lleva a cabo, aunque Brasil, si es coherente con esto.

Por tanto, se observa que a Colombia le falta aplicar mucho más esta cooperación, pero también puede deberse a las capacidades que posee, por lo que ante ataques cibernéticos no consideran mucho el optar por dicha cooperación. Sin embargo, es claro que a Perú le falta definir mejor y de manera más concreta la cooperación internacional, aunque la ejecuta también en la realidad, pero que no lo posee sobre todo como un principio. En este caso, el especialista **E-Ch** señala que sería recomendable que Perú genere una respuesta coordinada sobre las ciberamenazas mediante la integración de la ciberdefensa en la Política Nacional de Ciberseguridad, siguiendo el ejemplo de Chile. Algunos aspectos clave para lograrlo incluyen establecer una estructura organizativa clara, fomentar la cooperación internacional,

proteger las infraestructuras críticas y definir un lenguaje común en términos de ciberdefensa y ciberseguridad; por tanto, adaptar estas recomendaciones a las necesidades específicas de Perú es fundamental.

Ahora respecto a las **capacidades,** se ha encontrado diferencias ya que no todos comparten los mismos contenidos, por ejemplo**, Argentina, Brasil, Ecuador y Perú** comparten la **capacidad** de recuperación, que es similar a la resiliencia (Gobierno de Argentina, 2022; Estrategia Nacional de Seguridad Cibernética - E-Ciber, 2020; Ministerio de Defensa, 2021; Ley de Ciberdefensa, 2023). **Ecuador y Perú** comparten la capacidad de explotación que es el seguimiento y evaluación de las ciberamenazas (Ministerio de Defensa, 2021; Ley de Ciberdefensa, 2023) (ver Tabla 11). Por otro lado, de manera particular **Chile,** adiciona el uso de inteligencia artificial (ver Anexo G).

La necesidad de diversas capacidades para la ciberdefensa es crucial como lo menciona Ormachea (2020), quien menciona que, gracias a la colaboración privada y pública, también es posible reforzar las capacidades de ciberdefensa, esto gracias a una acción más coordinada para responder de manera eficiente ante los ataques y saber cómo disuadir o recuperar la información con dicho apoyo, pero más que todo para prevenir y responder. De acuerdo con la UIT (2024) la mayoría de los países son débiles ante el desarrollo de capacidades y técnicas. Cada región tiene países que están dando ejemplo o están avanzando, y cada región también tiene países que recién construyen sus compromisos en materia de ciberseguridad. En este aspecto, las puntuaciones de los aspectos técnicos de los Estado de análisis según la UIT (2024) demuestran que Argentina poseen la puntuación más baja (12.18), la más alta es la de Brasil (20) luego le sigue Ecuador con 17.89, Colombia con 16.22, Chile con 13.81 y Perú con 13.51. Ante ello, la ciberdefensa puede complementarse con el desarrollo de capacidades, para garantizar que los actores relevantes estén bien capacitados y sean conscientes de las amenazas actuales a la ciberseguridad.

Perú demuestra que, en el aspecto técnico, tampoco es el mejor y Rossi (2021) señala que en Perú se necesita del reforzamiento de la seguridad y defensa en el campo cibernético, a través de la colaboración estratégica con otros entes internacionales, para formar profesionales capaces, obtener tecnología y desarrollarla. Para el especialista **E-Co** Perú necesita desarrollar capacidades específicas según los roles misionales de cada fuerza militar o entidad estatal. Además, es crucial establecer un plan de comunicación sobre incidentes y lecciones aprendidas en ciberdefensa. También debe enfocarse en proteger sus

infraestructuras críticas y considerar la creación de organismos especializados, siguiendo ejemplos de otros Estados como Brasil, Chile y Colombia.

Respecto a los **activos críticos**, si bien todos los estados abordan este tema, hay ciertas diferencias en sus descripciones de contenido, por ejemplo, **Argentina** señala cómo identificarlos teniendo en cuenta varios componentes como datos disponibles, su integridad y confidencialidad, además de funciones que dan soporte al activo y las leyes que lo sustentan. **Chile,** indica especificando algunas como redes de centros de salud y transporte. **Colombia,** indica que son activos y sistemas, tanto virtuales como físicos que las soportan las TICs. **Ecuador,** agrega que comprenden sistemas de información y comunicación (ver Anexo G). De lo descrito, es claro la importancia de saber cuáles son los activos críticos para proteger y sobre todo que hay las entidades correspondientes para ello. De lo mencionado, la identificación de los activos críticos relacionados a la ciberdefensa es crucial para identificar cuáles realmente son los más importantes, destacando que Argentina y Chile son los que detallan un poco más dichos activos, aunque podría ser algo importante imitar esta descripción en su política, podría ser un riesgo el exponer dichos activos en documentos de acceso libre. Aun así, como refiere el especialista peruano, **E-P**, se necesitan marcos legales más sólidos para regular aspectos clave de la ciberseguridad y protección de la información personal, la respuesta a incidentes y la cooperación público-privada. También, menciona que se necesita una mejor coordinación interinstitucional, ya que la eficacia de las políticas de ciberdefensa a menudo depende de la coordinación entre diferentes agencias gubernamentales y sectores privados. Por tanto, a pesar de tener un comando para la ciberdefensa en los distintos Estados como se ha descrito, la cooperación y alianza estratégica resultan óptimas para este propósito.

Ahora, sobre los **organismos ejecutores,** si bien todos los Estados lo poseen, hay ciertas diferencias en las denominaciones de dichas entidades, como por ejemplo **Argentina,** cuenta con el Comando Conjunto de Ciberdefensa (Gobierno de Argentina, 2023); **Brasil** con el Comando de Ciberdefensa (Estrategia Nacional de Seguridad Cibernética - E-Ciber, 2020); **Chile** con el Comando Conjunto de Ciberdefensa (Ministerio de Defensa Nacional, 2018); **Colombia** posee el Comando Conjunto Cibernético (Decreto 338 de 2022, 2022); **Perú** tiene el Comando Operacional de Ciberdefensa (Ley de Ciberdefensa, 2023) y **Ecuador** el Comando de Ciberdefensa (Ministerio de Defensa, 2021) (ver Tabla 11). En la entrevista **E-Co**, destaca que Colombia es el primero en la adopción de una Estrategia Nacional Integral de Ciberdefensa, así como unidades policiales especializadas en

ciberdelitos, así como un comando cibernético para la defensa del Estado, creando además un CNRIC (ver Anexo D).

Por otro lado, se puede observar en los documentos que la finalidad básica es proteger las infraestructuras críticas de información, así como aplicar sus capacidades de defensa cibernética para responder ante los ataques, algunos organismos ejecutores tienen otras particularidades, por ejemplo, de Argentina, el Comando Conjunto de Ciberdefensa, realiza una coordinación con las Fuerzas Armadas, así como lo realiza Perú. De Brasil el Comando de Ciberdefensa, busca el desarrollo y participación en ejercicios internacionales, colaboración con agencias y organizaciones. Chile con el Comando Conjunto de Ciberdefensa, busca generar capacidades que promuevan la ciberseguridad. Colombia con el Comando Conjunto Cibernético, realizar un monitoreo de información en redes sociales y combatir a la desinformación. En Perú, el Comando Operacional de Ciberdefensa busca el desarrollo de operaciones conjuntas de ciberdefensa, de tal forma que se protejan los sistemas de información y redes. Y en Ecuador, el Comando de Ciberdefensa, busca además de la defensa, la exploración de ciberespacio.

Ante todo, esto, es rescatable y muy positivo que los Estados en sus políticas puedan delimitar entidades exclusivas sobre ciberdefensa, demostrando el compromiso que tienen para abordar esta problemática, ya que casi todos cuentan con un "comando" que es capaz de prevenir, reaccionar y recuperar información de secreto militar.

Ahora se procederá a describir los componentes únicos encontrados, que son elementos diferentes de las políticas de ciberdefensa, y representan un aporte en la estructuración de las políticas de ciberdefensa. En este caso, el apartado de **componentes sistémicos subsidiarios** es exclusivo de **Argentina** y se diferencia y destaca por mencionar que se trata del diseño de defensa del ciberespacio desde un enfoque multidimensional (ver Tabla 11). Esto es importante ya que, considerar los diversos elementos que funcionan entre sí, es lo mejor para reconocer que el mal funcionamiento de un aspecto puede afectar a otro, detallando de esta manera cuáles son dichos componentes.

Luego se tiene el componente de **enfoque sistémico**, que lo considera **Argentina y Brasil,** en donde explican que se reúne un conjunto de componentes que funcionan de manera dinámica y contribuyen al desarrollo y la capacidad de ciberdefensa, buscando la inversión tecnológica, con un diseño estratégico nacional sistémico (ver Tabla 11). Y aunque este componente tiene cierta relación con los componentes sistémicos subsidiarios, porque

engloba el aspecto sistémico, su definición tiene ciertas diferencias que es mejor detallar por separado, ya que además son apartados o subtítulos exclusivos de cada Estados en su política. En este aspecto, el especialista **E-A**, señala que cada Estado, puede tener otros enfoques con sus particularidades y desafíos. Sin embargo, aunque **Chile** no habla sobre un enfoque sistémico, el especialista **E-Ch** sustenta que el enfoque que tiene Chile es integral y multidimensional, el cual además busca estar actualizado constantemente y mantener la cooperación internacional (ver Anexo D).

Sobre el componente de **instrumentos,** todos los Estados menos Perú, lo indican, aunque solo Brasil lo posee de manera explícita y el resto implícitamente, diferenciándose de este modo. En estos se especifican los documentos estratégicos a considerar sobre la ciberdefensa, además de planes nacionales, convenios y resoluciones (ver Tabla 11). Considerar un apartado sobre los instrumentos concretos para el abordaje de la ciberdefensa, resulta pertinente para Perú, denotando la manera organizada de tener listado sus documentos más representativos a los cuales acudir para orientarse en ciberdefensa, aunque sí los posea, refiriéndose a documentos normativos y demás guías para el abordaje de la ciberdefensa, no emplea esta terminología como tal para referirse a ello en el documento principal.

También se observó el apartado de **ejes temáticos**, en donde solo Brasil lo posee explícitamente, pero también lo mencionan Argentina y Ecuador implícitamente, en estos se habla de una revisión y actualización de normativas para mejorar los objetivos estratégicos, la formulación de acciones de ciberseguridad nacional, y la modificación de estrategias a nivel normativo, tecnológico y de vínculos. Además, promueven el desarrollo de una infraestructura digital segura y el uso responsable de las TIC, abarcando la protección y seguridad de la información (ver Tabla 11). Esto también puede ser pertinente para Perú, ya que el optar por una visión de mejora constante, es lo que permitirá estar a la vanguardia y prever ataques cibernéticos más complejos. De igual forma, como lo menciona Kosevich (2020) Brasil aspira a ser un actor global en seguridad cibernética, realizando diversas acciones como la implementación de un mayor presupuesto y la colaboración intra e internacional y buscando con esto, cumplir su objetivo principal, que sobre todo es poder prevenir. Por tanto, es rescatable lo que se puede comprender del objetivo planteado por este Estado.

Se observó también el apartado de **plan de acción**, en donde Colombia lo tiene muy detalladamente, aunque Chile también menciona ellos. Sin embargo, en Colombia se detalla

acciones concretas sobre las actividades que se deben realizar en torno a la ciberseguridad y ciberdefensa. Esto también es útil, cuando se requiere saber exactamente qué acciones tomar, ya que, al poseer algo detallado, es más práctico para su uso. Por su parte Chile indica que el plan de acción debe ser informado a un CSIRT cuán pronto sea adoptado (ver Tabla 11).

Otro componente es el **financiamiento**, que explícitamente lo menciona Colombia y que detalla la inversión a realizar a lo largo de los años. También Chile y Ecuador hacen cierta mención de ello, aunque solo mencionan al responsable de ello y las posibles fuentes, pero no detallan cantidades. Aquello también resultaría algo muy útil, debido a la falta de inversión y detalle de este en materia de ciberdefensa en el Perú, que podría comenzar con el establecimiento adecuado del financiamiento pertinente para este propósito (ver Tabla 11).

El siguiente componente es el **modelo de gobernanza**, en donde también Colombia lo tiene de manera explícita, en donde se detallan las normas que se comparten por las partes interesadas en la seguridad digital. Y en este aspecto, también Brasil y Ecuador mencionan el modelo de gobernanza implícitamente, indicando que debe ser centralizado y con planificación multisectorial, involucra a diversos actores (ver Tabla 11).

El otro componente encontrado es el **enfoque de seguridad**, que lo tiene explícitamente Ecuador, y solo Argentina y Colombia lo mencionan de manera implícita. En este caso Ecuador indica sub-enfoques como de confianza y derechos digitales, resiliencia, desarrollo sostenible, sistémico multisectorial y multidimensional, planificación estratégica, enfoques que guían acciones sobre ciberseguridad y ciberdefensa (ver Tabla 11). Resulta llamativo, cómo Ecuador, considera importante señalar estos enfoques que van en consonancia con sus demás principios y objetivos específicos, para guiar las acciones en ciberdefensa. Por tanto, el hecho de tener un enfoque sobre las cosas dice mucho sobre la perspectiva que se tiene sobre algo y facilita la toma de decisiones, por tener una base de la cual partir y orientarse para cuando ocurran situaciones en donde se tiene que actuar frente a los ciberataques. En el caso de Argentina, incluye una perspectiva de seguridad en políticas, priorizando la tecnología y Colombia adopta un enfoque de seguridad multidimensional y multidisciplinario para generar una cultura adecuada en ciberseguridad (ver Tabla 11).

Se observó otro componente explícito en la política de Perú que es el **rol del Ministerio de Defensa**, en donde se señala su responsabilidad para dirigir, normar, supervisar y evaluar las disposiciones en ciberdefensa. Aunque de manera implícita, dicho

rol se cada ministerio se menciona en Argentina, Colombia y Ecuador y el resto no, sin embargo, cada Estado también tiene su Ministerio correspondiente, Argentina el Ministerio de Defensa, Brasil el *Ministério da Defesa*; Chile, Colombia y Ecuador se denominan Ministerio de Defensa Nacional. Sobre ello, deberían los demás Estados, mejorar sus especificaciones sobre el rol de su ministerio, para tener en claro sus capacidades y responsabilidad, con la posibilidad de demanda a la misma ante las necesidades de protección Estatal (ver Tabla 11).

Otro componente explícito de Perú es un apartado de las **operaciones militares**, en donde se mencionan acciones estratégicas que se planifican y ejecutan en el ciberespacio con el objetivo de lograr resultados militares específicos para proteger la seguridad nacional. También lo mencionan de manera implícita Argentina, indicando las fases de protección ante ciberamenazas, también Colombia que especifica lo que hace el Comando Conjunto Cibernético de las Fuerzas Militares, y Ecuador menciona sobre la prevención y respuesta militar ante las ciberamenazas o ataques (ver Tabla 11).

Finalmente, el componente **uso de la fuerza**, explícito en la normativa de Perú, justifica las medidas de acción para contrarrestar los ataques cibernéticos. Estos apartados, si bien no lo poseen los demás Estados, denotan la importancia que le dan a estos temas para abordar la ciberdefensa. También de manera implícita lo menciona Chile, indicando que puede hacer uso de la fuerza dentro del ciberespacio en legítima defensa (ver Tabla 11).

De todo lo mencionado, los componentes descritos poseen distinciones entre los Estados, aunque entre algunos hay ciertas similitudes, sin embargo, dichas similitudes no son totales, por ende, se establecen en este apartado. En este aspecto, el especialista el especialista **E-P**, refuerza los encontrado, por ejemplo, referente al **financiamiento** señala que Brasil y Argentina, gracias a su desarrollo económico, tienen más recursos para la ciberdefensa, a diferencia de Ecuador y Perú, por tener más sofisticadas sus políticas e infraestructura de seguridad cibernética. También, señala que otros Estados, pueden tener mejor coordinación interinstitucional, como se indica en los **principios**, para responder de manera más eficaz ante las ciberamenazas, así como políticas específicas centradas en proteger sectores críticos como energía, finanzas y salud, esto referente a la necesidad de protección de los **activos críticos nacionales**. Otros, en cambio, adoptan un enfoque más amplio, no solamente un **enfoque de seguridad o sistémico,** que abarca una gama diversa de sectores, además de que pueden estar centrados en campañas de concientización pública

sobre seguridad cibernética y ciberdefensa, lo cual puede variar, pero todos los Estados promueven campañas de un buen uso del ciberespacio (ver Anexo D).

En todo lo analizado, se puede identificar tal como se expone en la Tabla 11, que existen varios componentes que se diferencian entre los lineamientos o políticas de los documentos analizados en los Estados de estudio, algunos aportando aspectos importantes que podrían considerarse para Perú y que están de manera explícita e implícita pero no en todos. Las diferenciaciones de los componentes de las políticas de ciberseguridad y ciberdefensa es algo recurrente, que de acuerdo con el estudio de Kshetri y Miller (2021) varios Estados pueden diferir con respecto a la ciberdefensa y las iniciativas cibernéticas en naturaleza, tipo, presupuesto, relaciones internacionales e influencia gubernamental, debido probablemente a las necesidades que va teniendo cada Estado; sin embargo, ahora no resulta factible esperar que suceda un ataque cibernético para recién actuar, ya que el auge de la tecnología hace que su uso sea mayor y generan a su vez mayor riesgo, por lo que éstas necesidades deben ser proyectadas para prevenir de manera adecuada.

Se puede rescatar de todas las demás diferencias, que a Perú le falta especificar y detallar mejor respecto a la actualización y desarrollo constante sobre las competencias necesarias respecto a la ciberseguridad y ciberdefensa como lo tienen los demás Estados, lo que demuestra que, es necesario estipularse para un mejor orden y organización, aunque se realice en la práctica. Además, Perú también podría considerar los componentes sistémicos subsidiarios de Argentina, e identificar el alcance de la política con mayor precisión, así como señalar sus instrumentos de acción como guías o manuales para orientar la actividad de defensa ante las amenazas cibernéticas. Así, también, se requiere planificar tomando en cuenta el ejemplo de Colombia y delimitar el financiamiento requerido para ello. Deben considerar diversos enfoques para un trabajo integral con enfoque de seguridad y componentes que funcionan de manera interconectada.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. Se presentaron los resultados del análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú, comprobando la hipótesis de estudio, revelando similitudes pero sobre todo diferencias en su estructura y contenido, que pueden ser beneficiosas para el Estado peruano, por ejemplo, la necesidad de precisar un apartado de objetivos estratégicos, que incluya el fortalecimiento continuo y el desarrollo de capacidades de ciberdefensa, así como la promoción de principios como la cooperación internacional, la gestión y prevención de incidentes, y la resiliencia. Asimismo, se pueden resaltar componentes específicos de otros Estados: de Argentina, la inclusión de componentes sistémicos subsidiarios; de Ecuador, su enfoque en la seguridad; y, de manera sobresaliente, de Colombia, su plan de acción detallado que abarca financiamiento, modelo de gobernanza y ámbito de aplicación.

2. Se identificaron las políticas de ciberdefensa vigentes en los Estados estudiados, destacando que cuentan con documentos relacionados a normativas en ciberdefensa. Sin embargo, únicamente Argentina, Chile, y Perú disponen de documentos específicos sobre políticas de ciberdefensa, mientras que Brasil, Colombia y Ecuador cuentan con documentos estratégicos que abordan aspectos de ciberdefensa.

3. Se especificaron y caracterizaron los componentes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú, identificando que, aunque presentan variaciones, la mayoría se encuentran alineadas con las categorías de análisis, encontrando subtítulos o apartados, como objetivos principales, objetivos específicos o estratégicos, principios, capacidades, activos críticos nacionales, organismos ejecutores, componentes sistémicos subsidiarios, enfoque sistémico, alcance y ámbito de aplicación, instrumentos, ejes temáticos, plan de acción, financiamiento modelo de gobernanza, enfoque de seguridad, rol del ministerio de defensa, operacionales militares y uso de la fuerza, aunque un tercio de ellos se encuentran de manera explícita como subtítulo, otro tercio de manera implícita y otro tercio no los abordan, con similitudes y diferencias en el contenido de dichos componentes.

4. Se identificaron todos los Estados concuerdan en componentes similares como objetivos, principios, capacidades, activos críticos, organismos ejecutores y alcance o ámbito de aplicación. Por otro lado, en el contenido también hay similitudes, en donde por ejemplo en el objetivo principal, se habla de la protección de los datos y el establecimiento de estrategias de gestión de riesgos y garantizar la defensa nacional frente a amenazas cibernéticas. En las capacidades todas las políticas abordan la gestión de incidentes y riesgos, así como la capacidad de prevención y respuesta ante amenazas. También, todas identifican los activos críticos nacionales considerados como posibles infraestructuras críticas a proteger y definen claramente los organismos ejecutores responsables de la ciberdefensa. Además, todos indican tener organismos ejecutores. Por último, en el alcance y ámbito de aplicación, mencionan quienes son los responsables o entidades obligadas a ejecutar las disposiciones contenidas en las normativas para la ciberdefensa.

5. Las diferencias identificadas reflejan las fortalezas de la variedad de componentes y contenidos en los Estados de análisis, en donde algunos comparten aspectos similares, pero otros no, distinguiéndose de esta forma de los demás, en donde se puede rescatar la protección de intereses nacionales, reforzamiento de capacidades, cooperación internacional, diversos principios, capacidad de seguimiento, evaluación y resiliencia, la determinación de un enfoque de seguridad con perspectiva sistémica, ejes temáticos, la identificación de instrumentos, plan de acción detallado, financiamiento detallado, un modelo de gobernanza, el rol que cumple el Ministerio de Defensa, sobre las operaciones militares y la justificación del uso de la fuerza.

5.2 Recomendaciones

1. Que la Escuela Superior de Guerra Naval continúe promoviendo investigaciones relacionadas con este tema, involucrando a nuevos investigadores a enfocarse en explorar aspectos operacionales, técnicos y administrativos u otros, que puedan contribuir al fortalecimiento y perfeccionamiento de las políticas de ciberdefensa, con especial énfasis en la prevención y mitigación de amenazas en el ciberespacio.

2. Elevar a la Comandancia de Ciberdefensa este estudio, para que así puedan utilizar sus hallazgos como base para futuras modificaciones a la ley o reglamento de ciberdefensa, así como para respaldar discusiones estratégicas en reuniones de alto nivel en apoyo al COCID.

REFERENCIAS

Arreola, A. (2019). Desafíos a las estrategias de Ciberseguridad en América. *Revista del Centro de Estudios Superiores Navales, 40*(4), 25-53. http://repositorio.uninav.edu.mx/xmlui/handle/123456789/1042

Asamblea Nacional República del Ecuador. (2023). *Informe para primer debate ley Orgánica de Seguridad Digital.* [Memorando Nro. AN-CSIS-2023-0123-M]. https://observatoriolegislativo.ec/wp-content/uploads/2024/06/INFORME-PARA-PRIMER-DEBATE.pdf

BBC Noticias. (2022, 20 de mayo). ″Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia. *BBC.* https://www.bbc.com/mundo/noticias-america-latina-61516874

Bernal, C. (2016). *Metodología de la Investigación: Administración, Economía, Humanidades y Ciencias Sociales* (4ª, ed.). Editorial Pearson.

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

Calderaro, A. & Craig, A. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building [Gobernanza transnacional de la ciberseguridad: desafíos políticos y desigualdades globales en el desarrollo de capacidades cibernéticas]. *Third World Quarterly, 41*(6), 917-938. https://doi.org/10.1080/01436597.2020.1729729

Centro de Estudios de Derecho e Investigaciones Parlamentarias. (2022). *La ciberseguridad: un estudio comparado.* Cámara de Diputados del Honorable Congreso de la Unión. [pdf]. https://www.nodal.am/wp-content/uploads/2023/06/cibersegu.pdf

Comisión Económica para América Latina y el Caribe. (2020). *La seguridad cibernética en América Latina y el Caribe: un esfuerzo multilateral.* [Presentación]. https://www.cepal.org/sites/default/files/events/files/presentation_comtelca.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa* (Documento N° 3701). [pdf]. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Córdova, E. & Hernández, J. (2019). El Estado desde la perspectiva de las ciencias sociales y políticas. *Utopía y Praxis Latinoamericana, 24*(86), 198-209. https://doi.org/10.5281/zenodo.3370719

Decreto N°10.222. (2020). *Estrategia Nacional de Seguridad Cibernética - E-Ciber.* (2020, 5 de febrero).

Decreto 338 de 2022 (2022). *Ministerio de Tecnologías de la Información y las Comunicaciones.* Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Decreto de Urgencia 007- (2020). Que Aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento. Presidencia de la República. https://busquedas.elperuano.pe/dispositivo/NL/1844001-2

Decreto Supremo N.° 017-2024-PCM. (2024). *Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa*. Presidencia de la República https://cdn.www.gob.pe/uploads/document/file/5858763/5192944-ds-n-017-2024-pcm.pdf?v=1716839855.

Dirección Nacional de Ciberseguridad. (2022). *Disposición 1/2022* (DI-2022-1-APN-DNCIB#JGM). *Modelo Referencial de Política de Seguridad de la Información.* https://www.boletinoficial.gob.ar/detalleAviso/primera/257620/20220216

Dirección Nacional de Inteligencia (DINI). (2018). *Guía Metodológica para la Identificación, Análisis y Evaluación de Riesgos de los Activos Críticos Nacionales - ACN.*

Escuela Superior de Guerra Naval. (2024). *Reglamento Interno de Investigación.* Marina de Guerra del Perú. https://www.esup.edu.pe/wp-content/uploads/2020/12/Reglamernto%20Investigaci%C3%B3n%202024.pdf

Forbes Staff. (2021,15 de diciembre). Seis ciberataques que marcaron el 2021. *Forbes.* https://forbescentroamerica.com/2021/12/15/seis-ciberataques-que-marcaron-el-2021

Fortinet. (2021, 15 de setiembre). *Fortinet reporta que los ataques de ransomware se han multiplicado por diez en el último año*. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/fortinet-reporta-ataques-ransomware-multiplicado-diez-ultimo-ano

Fraile, A. (2018, 21 de mayo). *"La Teoría de Juegos" aplicada a la Ciberseguridad* [Imagen adjunta] [Actualización de estado]. LinkedIn. https://www.linkedin.com/pulse/la-teor%C3%ADa-de-juegos-aplicada-ciberseguridad-alvaro-fraile-hern%C3%A1ndez/

Fuentes, A., Gómez, R. & González, J. (2023). La Ciberseguridad en México y los derechos humanos en la era digital. *Espacios Públicos, 24*(61), 119-142. https://doi.org/10.36677/espaciospublicos.v23i61.21083

Garcés, H. (2000). *Investigación Científica.* Abya-Yala. Repositorio UNM. https://digitalrepository.unm.edu/abya_yala/357/

Gobierno de Argentina. (2022). *Consulta Pública: Segunda Estrategia Nacional de Ciberseguridad.* [Documento]. República Argentina - Poder Ejecutivo Nacional. https://www.argentina.gob.ar/sites/default/files/anexo_6777529_1.pdf

Gobierno de México. (2020, 12 de octubre). Ciberataques, la "otra pandemia". *Procuraduría Federal del Consumidor.* https://www.gob.mx/profeco/articulos/ciberataques-la-otra-pandemia?idiom=es

Gobierno del Perú. (2006). *Libro Blanco de la Defensa Nacional Perú.* [Libro Blanco]. https://cdn.www.gob.pe/uploads/document/file/397073/Libro_blanco.pdf

Gómez, H. (2017). Ciberguerra... ¿Dudáis? *Revista de Marina, 1*(959), 34-39. https://revistamarina.cl/revistas/2017/4/hgomeza.pdf

Gonzales, R. (2023). Revisión de los enfoques de seguridad y su caracterización actual. *Revista Científica De La Escuela Superior De Guerra Del Ejército, 2*(2), 82-91. https://doi.org/10.60029/rcesge.v2i2art7

Gross, M., Canetti, D. & Vashdi, D. (2018). Cyber Terrorism. En H. Lin, y A. Zegart, *Bytes Bombs and Spies. The Strategic Dimensions of Offensive Cyber Operations. (Ciberterrorismo. En H. Lin y A. Zegart,* Bytes, bombas y espías: Las dimensiones estratégicas de las operaciones cibernéticas ofensivas.). (pp. 235-264). Brookings Institution Press.

Guevara, G. (2019). Análisis documental: Propuestas metodológicas para la transformación en programas de posgrado desde el enfoque socioformativo. *Atenas, 3*(47), 105-123 https://www.redalyc.org/journal/4780/478060102007/478060102007.pdf

Hernández-Sampieri, R. & Mendoza, C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Huamani, A. & Aparecida, M. (2024). Política y Estrategias de la Seguridad Cibernética: Argentina, Perú y Brasil. *Revista Ibero-Americana de Ciência da Informação, 17*(1), 115-141. https://doi.org/10.26512/rici.v17.n1.2024.51481

International Standard Organization. (2018, febrero). *ISO/IEC 27000:2018*. ISO: https://www.iso.org/standard/73906.html

International Standard Organization. (2012, julio). *Information technology - Security techniques - Guidelines for cybersecurity.* ISO: Information technology — Security techniques — Information security management systems — Overview and vocabulary [Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad. ISO: Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Panorama general y vocabulario]. https://www.iso.org/standard/44375.html

Instituto de las Naciones Unidas de Investigación sobre el Desarme (2024, julio). *Portal de Política Cibernética*. UNIDIR. https://cyberpolicyportal.org/es

Jarufe, J. (2020). *Políticas de ciberseguridad en la experiencia internacional.* Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/30304/1/Politicas_de_ciberseguridad_en_la_experiencia_internacional.pdf

Jiménez, W.G. (2012). El concepto de política y sus implicaciones en la ética pública: reflexiones a partir de Carl Schmitt y Norbert Lechner. *Revista del CLAD Reforma y Democracia, 1*(3), 215-238. https://www.redalyc.org/pdf/3575/357533685008.pdf

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

Klimburg, A. (2012). *National Cyber Security. Framework Manual.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Kinast, R. (2021). Disuasión y Uso de la Legítima Defensa en el Ciberespacio. *Cuadernos de Difusión Pensamiento de Estado Mayor, 1*(45), 103-122. https://publicacionesacague.cl/index.php/cuadernos/article/view/238

Kosevich, E. (2020). Cyber Security Strategies of Latin America Countries. *Iberoamérica, 1*(1), 137-159. https://doi.org/10.37656/s20768400-2020-1-07

Kshetri, N. & Miller, K. (2021). A Study on Cyber-Defense Ethics and Initiatives by Governments of Under Developing Nations: A Study of Selected Countries. *The International journal of analytical and experimental modal analysis, 13*(1), 977-986. https://doi.org/https://www.researchgate.net/publication/349380825_A_Study_on_Cyber-

Defense_Ethics_and_Initiatives_by_Governments_of_Under_Developing_Nations_A_Study_of_Selected_Countries

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software, 3*(4), 161-176. https://doi.org/10.18294/relais.2015.161-176

Ley N° 30999. (2021). *Ley de Ciberdefensa.* https://cdn.www.gob.pe/uploads/document/file/1671813/Ley%20N%C2%B030999%2C%20Ley%20de%20Ciberdefensa.pdf?v=1613166516

Ley N° 29158. (2007). *Ley Orgánica del Poder Ejecutivo.* Presidencia de la República. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29158.pdf

Li, A., Mahoney, A. & Poling, A. (2018). Basic research in behavior analysis. *Behavior Analysis: Research and Practice* (Investigación básica en análisis de la conducta**.** *Análisis de la conducta: Investigación y práctica), 18*(2), 117-118. https://doi.org/10.1037/bar0000134

Llori E. G. (2021), (2021). *Difusión del Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad* [Memorandum Nro. AN-PR-2021-0431-M]. Asamblea Nacional República del Ecuador. https://goo.su/pKtCz

Manjunatha, N. (2019). Descriptive Research. (Investigación descriptiva). *Journal of Emerging Technologies and Innovative Research, 6*(6), 863-867. https://www.jetir.org/papers/JETIR1908597.pdf

Manterola, C., Quiroz, G., Salazar, P. & García, N. (2018). Metodología de los tipos y diseños de estudio más frecuentemente utilizados en investigación clínica. *Revista Médica Clínica Las Condes, 30*(1), 36-49. https://doi.org/10.1016/j.rmclc.2018.11.005

Mariano, R. & Núñez, G. (2023). *Estado de la ciberseguridad en la logística de América Latina y el Caribe.* Naciones Unidas CEPAL. https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

Min, K., Chai, S. & Han, M. (2015). An international comparative study on cyber security strategy. (Un estudio comparativo internacional sobre la estrategia de ciberseguridad). *International Journal of Security and Its Applications, 9*(2), 13-20. https://doi.org/10.14257/ijsia.2015.9.2.02

Ministerio de Defensa. (2012). *Defense White Paper: Livro Branco de Defesa Nacional.* [Libro Blanco de Defensa: Libro Blanco de Defensa Nacional]. https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/livro_branco/lbdna_2013a_inga_net.pdf

Ministerio de Defensa. (2019, 21 de diciembre de 2019). *Fuerza Aérea presentó moderno Data Center y Centro de Monitoreo de Amenazas Cibernéticas*. *gog.pe.* https://www.gob.pe/institucion/mindef/noticias/71274-fuerza-aerea-presento-moderno-data-center-y-centro-de-monitoreo-de-amenazas-ciberneticas

Ministerio de Defensa. (2021). *Estrategia de Ciberdefensa 2021.* República de Ecuador.

Ministerio de Defensa. (2022). *Política de Ciberdefensa.* República de Argentina.

Ministerio de Defensa Nacional. (2018). *Aprueba Política de Ciberdefensa* (CVE 1363153). [Chile]. Presidencia de la República. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Ministerio de Defensa Nacional. (2019). *Plan Específico de Defensa 2019 - 2030* (Ecuador). https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-defensa-web.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Política de Ciberseguridad.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador.* https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Ministerio del Interior y Seguridad Pública. (2024). *Ley Marco de Ciberseguridad.* https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf

Montenegro, H., Pantoja, M., Rojas, A. & García, R. (2022). Políticas públicas de ciberdefensa en Chile y Colombia: un análisis desde el rastreo de procesos. *Brújula. Semilleros de Investigación, 10*(20), 7-16. https://doi.org/10.21830/23460628.118

Mori, S. & Goto, A. (2018, 27 de setiembre). *Review of National Cybersecurity Policies. (*Revisión *de las políticas nacionales de ciberseguridad)*. [Conferencia]. 22nd Pacific Asia Conference on Information Systems (PACIS 2018). https://aisel.aisnet.org/pacis2018/335

Mosquera, S. (2021). Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional. *Polo del Conocimiento, 6*(3), 1251-1273. https://doi.org/10.23857/pc.v6i3.2432

Nieto, L. (2013). Enfoque sistémico en los procesos de gestión humana. *Revista Escuela de Administración de Negocios*, *1*(74), 120-136. https://www.redalyc.org/pdf/206/20628498008.pdf

Noreña, D. (2022). Ciberdefensa y Ciberseguridad: Un Análisis Bibliométrico desde Dimensiones (1989-2023). *Revista de la Escuela Superior de Guerra Naval, 19*(1), 88-99. https://doi.org/10.35628/resup.v16i2.112

Noticias RCN. (2022, de marzo). *Exclusivo: informe de Mindefensa revela aumento de ciberataques en Colombia*. RCN. https://www.noticiasrcn.com/colombia/exclusivo-informe-de-mindefensa-revela-aumento-de-ciberataques-en-colombia-407306

Odebade, A. & Benkhelifa, E. (2023). A Comparative Study of National Cyber Security Strategies of ten nations. *Computers and Society, 1*(1), 1-28. https://doi.org/10.48550/arXiv.2303.13938

Organización Internacional de Normalización. (2012). *ISO/IEC 27032:2012. Information Technology Security techniques – Guidelines for cybersecurity*. (*Tecnología de la información – Técnicas de seguridad – Directrices para la ciberseguridad)* https://www.iso27001security.com/html/27032.html

Ormachea, J. (2020). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. *Revista de Ciencia e Investigación en Defensa-CAEN, 1*(4), 36-48. https://www.recide.caen.edu.pe/index.php/recide/article/download/36/32/29

Paredes, M. & Ángelo, E. (2024). El ciberterrorismo y la seguridad nacional. *Revista Academia de Guerra del Ejército Ecuatoriano, 17*(1), 144-458. https://doi.org/10.24133/AGE.VOL17.N01.2024.11

PCM. (2021). *Procedimiento de evaluación de Continuidad de Organismos Públicos Ejecutores, Programas y Proyectos Especiales del Poder Ejecutivo* (Anexo DS N° 143-2021). Gobierno de Perú. https://goo.su/Ablp

Pérez, F. (2021). *Ciberseguridad.* Francis Lefebvre. https://www.marcialpons.es/media/pdf/ciberseguridad.pdf

Piña, H. (2019). Cibercriminalidad y ciberseguridad en México. *Ius Comitialis, 2*(4), 47-69. https://doi.org/10.36677/iuscomitialis.v2i4.13203

Pranesh, M., Dharun, K. & Sofía, A. (2024). A Comparative Study of Cyber Security Strategies Among Various Countries. (Un estudio comparativo de las estrategias de

ciberseguridad entre varios países). *International Journal of Research Publication and Reviews, 5*(4), 2372-2376. https://ijrpr.com/uploads/V5ISSUE4/IJRPR24884.pdf

Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad. D. N° 11.856. (2023). https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11856.htm

Quevedo, C. (2023). Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF.AA. para neutralizar ciberataques que atenten contra la seguridad nacional. *Revista de Ciencia e Investigación en Defensa - CAEN, 4*(1), 55-76. https://doi.org/10.58211/recide.v4i1.99

Reglamento de la Ley N° 30999, (2023). Ley de Ciberdefensa. https://cdn.www.gob.pe/uploads/document/file/4933153/Proyecto%20de%20Reglamento%20Ley%2030999.pdf

Resolución N°105 (2023). *Ministerio de Desarrollo Social.* Presidencia de la Nación República de Argentina. https://www.boletinoficial.gov.ar/detalleAviso/primera/280426/20230130

Rivero, E. (2023). Ciberdefensa: Los Desafíos del Mundo Virtual. *Revista de Seguridad y Poder Terrestre, 2*(2), 99-105. https://doi.org/10.56221/spt.v2i2.29

Robledo, M. (2023). *América Latina y la gobernanza global y regional sobre ciberseguridad.* Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/bueros/la-seguridad/20662.pdf

Rossi, G. (2021). *La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas* [Tesis de Maestría, Academia Diplomática del Perú Javier Pérez De Cuéllar]. Repositorio Principal de la ADP. http://repositorio.adp.edu.pe/handle/ADP/170

Ryan, F., Coughlan, M. & Cronin, P. (2009). Interviewing in qualitative research: the one-to-one interview. (La entrevista en la investigación cualitativa: la entrevista individual). *International Journal of Therapy and Rehabilitation, 16*(6), 309-314. https://doi.org/10.12968/ijtr.2009.16.6.42433

Sabillon, R., Cavaller, V. & Cano, J. (2016). National Cyber Security Strategies. Global Trends in Cyberspace. (Estrategias nacionales de ciberseguridad: Tendencias globales en el ciberespacio). *International Journal of Computer Science and*

Engineering, 5(5), 67-81. https://www.proquest.com/docview/1868264400?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals

Sánchez, M., Fernández, M. & Diaz, J. (2021). Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo. *UISRAEL Revista Científica, 8*(1), 107-121. https://doi.org/10.35290/rcui.v8n1.2021.400

Sánchez, H., Reyes, C. & Mejía, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística.* Universidad Ricardo Palma. http://repositorio.urp.edu.pe/bitstream/handle/URP/1480/libro-manual-de-terminos-en-investigacion.pdf?sequence=1&isAllowed=y

Secretaría Distrital de Planeación. (2012). *Guía para la Formulación, Implementación y Evaluación de Políticas Públicas Distritales.* Gobierno de Colombia. https://www.alcaldiabogota.gov.co/sisjur/adminverblobawa?tabla=T_NORMA_ARCHIVO&p_NORMFIL_ID=1812&f_NORMFIL_FILE=X&inputfileext=NORMFIL_FILENAME#:~:text=Estructura%20de%20la%20pol%C3%ADtica%3A%20hace,acci%C3%B3n%2C%20pilares%2C%20entre%20otros.

Song, M., Kim, D., Bae, S. & Kim, S. (2021). Comparative Analysis of National Cyber Security Strategies using Topic Modelling. (Análisis comparativo de las estrategias nacionales de ciberseguridad mediante modelado de temas). *International Journal of Advanced Computer Science and Applications, 12*(12), 62-69. https://doi.org/10.14569/IJACSA.2021.0121209

Tavares, R. & Penha, T. (2020). Teoría de los juegos: Una visión práctica, procedimental y normativa del proceso penal. *Revista Derecho Penal y Criminología, 41*(110), 161-175. https://doi.org/10.18601/01210483.v41n110.07

The Economist. (2010, 1 de julio). *Cyberwar: war in the fifth domain.* Economist. www.economist.com/node/16478792

Unión Internacional de Telecomunicaciones. (2011). *ITU National Cybersecurity Strategy Guide.* https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

Unión Internacional de Telecomunicaciones. (2024). *Global Cybersecurity Index 2024 5 th Edition.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Vargas, R., Recalde, L. & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad, 1*(20), 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Anexos

Anexo A: Matriz de consistencia

TÍTULO: ANÁLISIS COMPARATIVO DE LAS POLÍTICAS DE CIBERDEFENSA DE ARGENTINA, BRASIL, CHILE, COLOMBIA, ECUADOR Y PERÚ				
PROBLEMA	**OBJETIVO**	**HIPÓTESIS**	**CATEGORÍA DE ANÁLISIS**	**METODOLOGÍA**
Problema General ¿Qué resultados se desprenden del análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?	**Objetivo General** Presentar los resultados que se desprenden del análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.	El análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú muestran similitudes en el objetivo, capacidades y activos críticos, pero sobre también poseen diferencias entre ellas respecto al contenido de sus componentes como en principios y objetivos específicos o estratégicos.	1. Políticas de Ciberdefensa 2. Componentes de la estructura de las políticas a. Objetivos b. Principios c. Capacidades d. Activos críticos e. Organismos ejecutores f. Componentes sistémicos subsidiarios g. Enfoque sistémico h. Alcance y ámbito de aplicación i. Instrumentos j. Ejes temáticos	**Enfoque:** ▪ Cualitativo **Tipo de investigación:** ▪ Según su finalidad: Básica. ▪ Según su carácter: Descriptiva ▪ Según alcance temporal: Transversal. **Método:** ▪ Análisis e Inductivo.

			k. Plan de acción l. Financiamiento m. Modelo de gobernanza n. Enfoque de seguridad o. Rol del Ministerio de Defensa p. Operacionales militares q. Uso de la fuerza 3. Similitudes de las políticas de ciberdefensa 4. Diferencias de las políticas de ciberdefensa	

Problemas Específicos	**Objetivos Específicos**			**Diseño de investigación:** ▪ Análisis documental. **Población:** ▪ Registros bibliográficos y audiovisuales acerca de las unidades temáticas de estudio. ▪ Personas vinculadas con amplio conocimiento al tema de estudio. **Muestra:** ▪ Registros bibliográficos y audiovisuales entre 15 documentos normativos y 69 referencias bibliográficas con un total de 84 fuentes. ▪ Fueron 5 especialistas en el tema para ser entrevistados (menos el especialista de Brasil)
PE1: ¿Qué políticas de ciberdefensa tienen Argentina, Brasil, Chile, Colombia, Ecuador y Perú? PE2: ¿Qué componentes se pueden identificar de la estructura de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? PE3: ¿Cuáles son las similitudes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? PE4: ¿Cuáles son las diferencias de las políticas de ciberdefensa	OE1: Identificar las políticas de ciberdefensa que tienen Argentina, Brasil, Chile, Colombia, Ecuador y Perú. OE2: Especificar los componentes de la estructura de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú. OE3: Determinar las similitudes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.			

de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?	OE4: Determinar las diferencias de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú.			**Técnica de recolección de datos:** ▪ Análisis documental. ▪ Entrevistas. **Instrumentos de recolección de datos:** ▪ Fichas de Registro Bibliográfico. ▪ Fichas de resumen. ▪ Fichas de análisis. ▪ Guías de entrevista. **Técnica de procesamiento de información:** ▪ Análisis de contenido, y análisis del discurso.

Anexo B: Lista de acrónimos y abreviaturas

BID	Banco Interamericano de Desarrollo
CEDIP	Centro de Estudios de Derecho e Investigaciones Parlamentarias
COCID	Comando Operacional de Ciberdefensa
CCFFAA	Comando Conjunto de las Fuerzas Armadas
CONPES	Consejo Nacional de Política Económica y Social
DIEMCFFAA	División de Estado Mayor Conjunto de las Fuerzas Armadas
ENCS	Estrategia Nacional de Ciberseguridad
FFAA	Fuerzas Armadas
IBM	International Business Machines
IC	Infraestructura Crítica
ICI	Infraestructura Crítica de la Información
ISO	International Organization for Standardization
JID	Junta Interamericana de Defensa
OEA	Organización de Estados Americanos
PYMES	Pequeñas y Medianas Empresas
TIC	Tecnologías de la Información y las Comunicaciones

Anexo C: Guía de entrevista

Tomado de Hernández – Sampieri, Metodología de la Investigación, las rutas cuantitativa y mixta, 2018.

<table>
<tr><td colspan="2">Escuela Superior de Guerra Naval</td></tr>
<tr><td colspan="2">Tesis para optar por el grado académico de Maestro en Estrategia Marítima</td></tr>
<tr><td colspan="2">Guía de entrevista sobre “Análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú”</td></tr>
<tr><td>Fecha:</td><td>Hora:</td></tr>
<tr><td colspan="2">Lugar (ciudad o sitio específico):</td></tr>
<tr><td>Entrevistadora:</td><td>C. de C. Donna Melody Silva Gurrionero</td></tr>
<tr><td>Entrevistado (nombre, edad, género, puesto, dirección, gerencia o departamento):</td><td></td></tr>
<tr><td colspan="2">Introducción:</td></tr>
<tr><td colspan="2">Las tecnologías de información y comunicación han hecho accesible una gran cantidad de conocimientos de forma digital a nivel global. A pesar de esto, los Estados protegen cierta información clave para su propio interés. Los secretos estatales y los datos personales confidenciales se recopilan y almacenan, los cuales pueden ser utilizados para obtener ventajas económicas y políticas que contribuyan al desarrollo nacional. No obstante, la seguridad de esta información no es infalible y los conflictos por el acceso a la información siguen presentes, especialmente en el ámbito digital. Esto representa un riesgo de ataque cibernético a la información del estado y su secreto militar, el cual debe ser abordado de manera eficiente, existiendo para ello políticas para la prevención, abordaje y recuperación de la información, no obstante, puede tener deficiencias, que se pueden analizar y mejorar desde una comparación de los lineamientos de otros países que colindan con Perú, como Argentina, Brasil, Chile, Colombia y Ecuador.</td></tr>
<tr><td colspan="2">Características de la Entrevista</td></tr>
<tr><td colspan="2">• La entrevista se hará con personas expertas en el tema que tienen más de 3 años en el ámbito de la ciberseguridad en el contexto militar.
• Tendrá preguntas orientadas al conocimiento sobre las políticas de ciberdefensa y sus características, moldeando las mismas, de acuerdo con el país de donde proviene el especialista.</td></tr>
</table>

• La información adquirida será de carácter no reservado con la finalidad de poder ser utilizada en la investigación, sin violar los niveles de clasificación de información. • La entrevista tendrá un máximo de duración de 20 minutos.
Preguntas:
1. ¿Qué políticas de ciberdefensa tienen Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Señale el más adecuado y por qué, de acuerdo con su país y experiencia. 2. ¿Qué componentes se pueden identificar de la estructura de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Señale cuáles son de acuerdo con su país. 3. ¿Cuáles son las similitudes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Destaque las más importantes, en comparación con su país de procedencia. 4. ¿Cuáles son las diferencias de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Destaque las más significativas, en comparación con su país de procedencia. 5. ¿Cuáles son las similitudes y diferencias de las políticas de ciberdefensa en los países de Argentina, Brasil, Chile, Colombia, Ecuador y Perú?
Observaciones:
Se hará constancia al entrevistado que se le nombrará dentro de la investigación y se compromete para futuras participaciones.
Validación utilizando la V de Aiken a cargo de:
• No aplicable, dado que las preguntas son los mismos problemas, tanto específicos como general, del trabajo de investigación.
Entrevistados
1. ……. 2. ……. 3. …….

Anexo D: Fichas de entrevista completadas

Categoría de análisis: Políticas de ciberdefensa de los Estados	
PREGUNTA 1: ¿Qué políticas de ciberdefensa tienen Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Señale el más adecuado y por qué, de acuerdo con su país y experiencia.	
NOMBRE	**RESPUESTA**
Capitán de Fragata Anselmo Omar Herrera (E-A)	Contamos con la política de ciberdefensa del año 2022, la cual da origen a la directiva de las políticas de ciberdefensa nacional, a partir de ello se obtiene la política de ciberdefensa y con esto se hace el planeamiento estratégico de las fuerzas armadas, lo que nosotros le llamamos el ciclo de planeamiento de defensa nacional. Estas políticas de ciberdefensa las saca el Ministerio de defensa a través de la sub-secretaria de ciberdefensa que es el órgano que conduce a la ciberdefensa quien deriva las directivas de acuerdo con las políticas nacionales al comando conjunto de ciberdefensa que es la parte operativa. Por otro lado, nosotros apuntamos a la ciberdefensa como parte militar y a la parte nacional la llamamos ciberseguridad.
Capitán de Fragata Roberto Siña Lazo (E-Ch)	Con el fin de comprender la Política de Ciberdefensa de Chile, es preciso señalar que nuestro país destaca por lograr complementar la protección de los Derechos Humanos y la Infraestructura Crítica de la Información en una Política Nacional de Ciberseguridad, que posteriormente durante el presente año, se ha materializado y fortalecido gracias la publicación de la Ley Marco de Ciberseguridad. Lo anterior, en comparación con nuestros pares en Latinoamérica, podría ser una práctica interesante, dado que las políticas y normativas de ciberdefensa de los países en comento, se basan principalmente en la protección de infraestructura y cooperación internacional, dejando de lado la protección de los derechos humanos.
Capitán de Fragata Francisco José Jaraba Hadechiny (E-Co)	La política de ciberdefensa en Colombia dio inicio desde el 2011, y fue establecida a través de los documentos CONPES (Consejo Nacional de Política Económica y Social) de Colombia, estos documentos que corresponden a órdenes gubernamentales son fundamentales para la formulación de políticas estratégicas en diversas áreas relacionada con el ámbito de la ciberdefensa y la ciberseguridad, estos son: El CONPES 3701, publicado en 2011, se enfoca en la ciberseguridad, estableciendo directrices para fortalecer la infraestructura tecnológica y proteger la información crítica del país contra amenazas cibernéticas. El CONPES 3854, publicado en 2015, trata sobre seguridad digital, buscando implementar políticas que garanticen la seguridad de las transacciones

	electrónicas y la integridad de los sistemas digitales en el país. Finalmente, el CONPES 3995, emitido en 2020, aborda también la seguridad digital, destacando la importancia de la protección de datos, la privacidad y la creación de un entorno digital seguro para ciudadanos y empresas, promoviendo el uso seguro y confiable de las tecnologías de la información y comunicación. Estos documentos reflejan el compromiso de Colombia con la protección de su infraestructura digital y la seguridad de sus ciudadanos en el entorno digital.
Capitán de Corbeta Vivanco Toala Danny (E-E)	Las políticas de ciberdefensa enmarcadas a través del Ministerio de Defensa Nacional del Ecuador son: La gobernanza, fundamentación estratégica y una guía que determina un plan de desarrollo de las capacidades requeridas para la defensa y protección de las infraestructuras digitales críticas, servicios esenciales del estado y la infraestructura digital crítica de la defensa; así como un modelo de gestión para la ciberdefensa. Estableciendo de esta manera la fundamentación político-estratégica para el desarrollo de la ciberdefensa en el sector Defensa. La Política de Ciberdefensa la cual instituye la base esencial para la creación de la estructura requerida en apoyo al desarrollo de las capacidades con el fin de apoyar la defensa y protección de la infraestructura crítica digital, servicios esenciales del estado y la infraestructura crítica digital de defensa. Es importante mencionar, que en adición a desarrollar las capacidades se establece un programa de ciberseguridad que hace cumplir los requerimientos establecidos por el EGSI v2.0 mediante políticas establecidas a través del Ministerio de Defensa.
Coronel FAP Luigui Aurelio Rivas Guevara (E-P)	Perú cuenta con una Ley y Reglamento de Ciberdefensa. Se vienen haciendo esfuerzos. Desde una perspectiva general y considerando la información sobre dicho dominio a la fecha, Chile y Colombia parecen destacarse entre todos estos países, por su enfoque integral y estructurado en ciberseguridad. La creación de la Agencia Nacional de Ciberseguridad de Chile y el fortalecimiento del ColCERT de Colombia, muestran un compromiso serio de esos gobiernos en la protección cibernética a nivel nacional. Además, Chile y Colombia han participado activamente en ejercicios internacionales y han fortalecido la colaboración público-privada, lo cual es crucial para enfrentar las amenazas cibernéticas modernas. Finalmente, la adecuación de una política de ciberdefensa puede variar según los recursos, las amenazas específicas que enfrenta cada país y la efectividad de la implementación de las medidas

	propuestas. Es fundamental revisar la situación actualizada y las métricas específicas de cada país para una evaluación y respuesta más precisa.

Categoría de análisis: Componentes de las políticas de los Estados	
PREGUNTA 2: ¿Qué componentes se pueden identificar de la estructura de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Señale cuáles son de acuerdo con su país.	
NOMBRE	**RESPUESTA**
Capitán de Fragata Anselmo Omar Herrera (E-A)	Las política de ciberdefensa en sí está enfocado a la protección de las infraestructuras críticas de información de nuestro país, la cual debemos de proteger y a su vez contamos con otras tareas que podemos realizar, en este sentido tenemos una postura defensiva, ya que nos basamos en nuestra política de defensa nacional, que nos permite también realizar el monitoreo las redes de las 3 fuerzas armadas a través del comando conjunto de ciberdefensa teniendo el propósito de proteger las infraestructuras críticas. Lo que sí nos falta es definir específicamente la política de ciberdefensa en cuanto a nivel de Estado.
Capitán de Fragata Roberto Siña Lazo (E-Ch)	Características, tales como el fortalecimiento de la cooperación internacional, el desarrollo de la protección infraestructuras críticas y la capacitación y educación, son una constante en las normativas en materias de ciberseguridad de los países en comento. A modo de complemento, Chile destaca por la constante integración que busca implementar, ejemplo de ello, son la creación de Equipos de Respuesta ante Incidentes Informáticos, la Colaboración Internacional que siempre busca con sus pares y los diversos programas educativos en materia de ciberseguridad que invita a generar colaboración pública/privada. De acuerdo con la experiencia personal e internacional, se estima que la Protección de Infraestructura Crítica es una de las características más cruciales.
Capitán de Fragata Francisco José Jaraba Hadechiny (E-Co)	Los documentos CONPES 3701, 3854 y 3995 de Colombia establecen diversas políticas y estrategias en el ámbito de la ciberseguridad y la seguridad digital, y también crean o formalizan características y entidades clave para su implementación. Algunos de los componentes son:

	-Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT): Proporciona asistencia técnica en caso de incidentes cibernéticos y coordina la respuesta a emergencias cibernéticas a nivel nacional. -Consejo Nacional de Seguridad Informática (CNSI): Formula políticas y estrategias en materia de ciberseguridad, asegurando la protección de la infraestructura crítica del país. -Marco de Seguridad de la Información: Desarrolla estándares y procedimientos para la protección de la información en las entidades del Estado y en el sector privado.
Capitán de Corbeta Vivanco Toala Danny (E-E)	La armonización de las políticas estatales y estrategias sectoriales de seguridad digital y defensa se han convertido en una de las características más importantes a considerar en la seguridad nacional. Las experiencias de varios países, que ya han sido testigos de las nuevas formas de guerra híbrida, demuestran que los niveles de seguridad y defensa nacional en el ciberespacio deben mantenerse, a pesar de las condiciones de crisis económica mundial y la disminución significativa de los gastos de las fuerzas armadas.
Coronel FAP Luigui Aurelio Rivas Guevara (E-P)	-La implementación de una Estrategia Nacional de Ciberdefensa: Establecer una estrategia clara y coherente que guíe las acciones y prioridades en materia de ciberdefensa a nivel nacional. -Un dominio principal, es la protección de Infraestructuras Críticas: Identificar y proteger las infraestructuras críticas que son vitales para el funcionamiento del país, como sistemas de energía, telecomunicaciones, agua, etc. -Gestión de Incidentes: Establecer protocolos y mecanismos de respuesta ante incidentes cibernéticos, incluyendo la creación de centros de respuesta y coordinación. -Legislación y Normativas: Desarrollar leyes y regulaciones que promuevan la seguridad cibernética, protejan datos personales y faciliten la cooperación entre entidades públicas y privadas. -Educación y Concienciación: Promover la conciencia sobre ciberseguridad a todos los niveles de la sociedad, desde el ciudadano común hasta los profesionales y tomadores de decisiones. -Colaboración o cooperación Internacional: Participar en iniciativas y colaboraciones internacionales para compartir información, mejores prácticas y enfrentar amenazas cibernéticas transnacionales.

	-Investigación y Desarrollo: Invertir en investigación y desarrollo en tecnologías y metodologías avanzadas para fortalecer la ciberdefensa. Cada país puede enfatizar algunos de estas características más que otros, dependiendo de sus necesidades específicas, recursos disponibles y amenazas particulares. Es importante destacar que la efectividad de una política o estrategia de ciberseguridad o ciberdefensa no solo depende de la inclusión de estos componentes, sino también de la implementación efectiva y el monitoreo continuo para adaptarse a un entorno cibernético en constante evolución.

Categoría de análisis: Similitudes de las políticas de ciberdefensa de los Estados	
PREGUNTA 3: ¿Cuáles son las similitudes de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Destaque las más importantes, en comparación con su país de procedencia.	
NOMBRE	**RESPUESTA**
Capitán de Fragata Anselmo Omar Herrera (E-A)	Nosotros hacemos únicamente la parte de ciberdefensa y estamos enfocados a la parte militar, a diferencia de los países de Sudamérica que también ven la ciberseguridad, ciberdefensa y tienen una mayor colaboración hacia al Estado Nacional en el sentido que participan en las distintas tareas de protección de las infraestructuras críticas.
Capitán de Fragata Roberto Siña Lazo (E-Ch)	De acuerdo con un análisis de las políticas de ciberdefensa de cada país, se concluye que en general todos abordan tres puntos u objetivos importantes. El primero de ellos, tiene relación con la protección de infraestructuras críticas. El segundo aborda la cooperación internacional para hacer frente a las amenazas cibernéticas, y el tercero corresponde a la integración de la política de ciberdefensa dentro un marco más amplio y robusto normativamente.
Capitán de Fragata Francisco José Jaraba Hadechiny (E-Co)	En las políticas públicas de diversos países, existen varias similitudes destacables. Sin embargo, es común la presencia de un Centro Nacional de Respuesta Cibernética. Este centro se encarga de orientar a los sectores más regulados, los cuales generalmente incluyen aquellos que involucran infraestructura crítica, como energía, agua, telecomunicaciones y servicios financieros, debido a su impacto crucial en la seguridad nacional y el bienestar de la población.
Capitán de Corbeta	No las conozco.

Vivanco Toala Danny (E-E)	
Coronel FAP Luigui Aurelio Rivas Guevara (E-P)	En líneas generales las políticas y estrategias de ciberseguridad y ciberdefensa tienen en común un objetivo, es contribuir en el fortalecimiento de la resiliencia cibernética de los países, asegurando de por medio, el bienestar del ciudadano a fin de que estos se sientan libres y confiados en hacer uso de los servicios digitales nacionales sin tener la preocupación de no ser afectados por actores maliciosos en el ciberespacio. Estas similitudes reflejan un enfoque compartido; el cual es adaptarse a un entorno digital cada vez más complejo y amenazante. Es importante mencionar, qué, cada país puede tener variaciones específicas en la implementación y priorización de estas políticas según sus contextos nacionales y desafíos particulares en ciberseguridad.

Categoría de análisis: Diferencias de las políticas de ciberdefensa de los Estados	
PREGUNTA 4: ¿Cuáles son las diferencias de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Destaque las más significativas, en comparación con su país de procedencia.	
NOMBRE	**RESPUESTA**
Capitán de Fragata Anselmo Omar Herrera (E-A)	En cuanto a las diferencias podemos ver que nosotros solo vemos ciberdefensa como parte militar, por ejemplo en el caso del Perú el comando de ciberdefensa de la armada participó en los juego olímpicos panamericanos, que actúan en la parte civil, en el caso nuestro si lo tenemos bien diferenciado , puesto que solo vemos la parte militar, por el tema de una política nacional, y la actuación de los militares es solamente para defensa ante un ataque externo producido por un Estado agresor, en cambio para la parte de ciberseguridad se encarga la fuerza de seguridad que son la fuerza policial.
Capitán de Fragata Roberto Siña Lazo (E-Ch)	De acuerdo con la información que se maneja, las principales diferencias se presentan en los niveles de responsabilidad en relación con la ciberseguridad que tiene cada Estado. Por ejemplo, Brasil tiene un Comando específico dedicado a la seguridad cibernética, en cambio, los demás países traspasan esta responsabilidad a diversas agencias. Por otra parte, el enfoque dado a la protección de los derechos humanos, Chile es enfático y pionero en legislar lo anterior en el ciberespacio, no así los demás señalados, de acuerdo con la información que se maneja. Si pudiéramos definir la diferencia más

	importante, se estima que la principal diferencia de la Política de Ciberdefensa de Chile en comparación con otros países de la región radica en su enfoque integral y multidimensional, una estructura organizativa clara y una fuerte coordinación interinstitucional, así como un énfasis en la actualización normativa y la cooperación internacional. Otros países, de acuerdo con sus necesidades, intereses y prioridades, tienden a tener un enfoque más militarizado y enfrentan desafíos en la coordinación y en la integración de diversos actores y sectores.
Capitán de Fragata Francisco José Jaraba Hadechiny (E-Co)	Las políticas de ciberdefensa en América Latina difieren notablemente entre los países, reflejando variaciones en la prioridad dada a la seguridad cibernética y el desarrollo de sus infraestructuras tecnológicas. Argentina, por ejemplo, ha aprobado su Segunda Estrategia Nacional de Ciberseguridad, que contempla la creación de una Unidad de Gestión y Cooperación de Ciberseguridad para modernizar y fortalecer las políticas ante los nuevos desafíos tecnológicos. Brasil ha estado implementando leyes específicas contra los ciberdelitos, centradas en el hacking y el acceso no autorizado a sistemas informáticos, especialmente los de funcionarios públicos. Chile fue uno de los primeros países en adoptar una legislación sobre cibercrimen y recientemente promulgó una Ley de Ciberseguridad e Infraestructura Crítica que obliga a las organizaciones a mejorar sus protocolos y respuestas a incidentes. Aunque queda mucho por desarrollar e implementar, Colombia destaca como el primer país latinoamericano en adoptar una estrategia nacional integral de ciberdefensa, que incluye la formación de unidades policiales especializadas en ciberdelitos, un comando cibernético para la defensa de las fuerzas armadas y un centro nacional de respuesta a incidentes. Ecuador y Perú están en proceso de desarrollar y fortalecer sus marcos legales y estratégicos para combatir el cibercrimen, con Perú habiendo aprobado recientemente una ley que penaliza una amplia gama de delitos cibernéticos
Capitán de Corbeta Vivanco Toala Danny (E-E)	No las conozco.
Coronel FAP Luigui Aurelio Rivas Guevara	Las políticas de ciberdefensa varían significativamente entre los países debido a diferencias en recursos, amenazas percibidas y enfoques estratégicos. Se podría considerar algunas diferencias y enfoques destacados y relevantes:

(E-P)	Recursos y Capacidades: Países como Brasil y Argentina, debido a su tamaño y desarrollo económico, pueden tener más recursos dedicados a la ciberdefensa en comparación con países más pequeños como Ecuador y Perú. Esto podría reflejarse en la sofisticación de sus políticas y la infraestructura de seguridad cibernética. Regulación y Marco Legal: Algunos países podrían tener marcos legales más desarrollados para regular aspectos clave de la ciberseguridad, como la protección de datos personales, la respuesta a incidentes y la cooperación público-privada. Estos aspectos son críticos para la efectividad de las políticas de ciberdefensa. Coordinación Interinstitucional: La eficacia de las políticas de ciberdefensa a menudo depende de la coordinación entre diferentes agencias gubernamentales y sectores privados. Países con una mejor coordinación tienden a responder de manera más eficaz a las amenazas cibernéticas. Enfoque en Sectores Críticos: Algunos países pueden tener políticas específicas centradas en proteger sectores críticos como energía, finanzas y salud, mientras que otros podrían tener un enfoque más amplio que abarque una gama más diversa de sectores. Educación y Concientización: Las campañas de educación y concientización pública sobre seguridad ciberseguridad y ciberdefensa pueden variar significativamente entre países, afectando la preparación y la respuesta ante amenazas cibernéticas.

Categoría de análisis: Similitudes y diferencias a destacar de las políticas de ciberdefensa de los Estados	
PREGUNTA 5: ¿Cuáles son las similitudes y diferencias de las políticas de ciberdefensa en los países de Argentina, Brasil, Chile, Colombia, Ecuador y Perú? Destaque de qué Estados y cuáles son las más importantes.	
NOMBRE	**RESPUESTA**
Capitán de Fragata Anselmo Omar Herrera (E-A)	Cambiar la parte de la política que solo menciona que un ataque proveniente de un Estado agresor y pasarlo a otra figura como grupos, ya que estos también pueden estar financiados por un Estado y establecer una relación más directa con una fuerza de seguridad para actuar muchas veces en el ámbito interno o tener una relación de manera que nosotros pasemos la información y puedan actuar ellos. Mejorar esa relación fuerza de seguridad con fuerza de defensa

	para producir un efecto más importante a los agresores, porque muchas veces son grupos que pueden estar atacando internamente infraestructura crítica nacional. Además, del caso nuestro lo que puedo rescatar es la parte de control y monitoreo que se está unificando a través del Estado Mayor conjunto de ciberdefensa y las fuerzas armadas en el sentido de monitoreo de todas redes de las Fuerzas Armadas y sobre todo las redes de comando y control, eso es lo que propone la política de ciberdefensa y apuntamos a tener un solo sistema de monitoreo de toda la fuerza, para unificar esfuerzos.
Capitán de Fragata Roberto Siña Lazo (E-Ch)	Sin contar con muchos antecedentes de su política, se estima que sería recomendable generar una respuesta coordinada a las amenazas del ciberespacio mediante la integración de la ciberdefensa en la Política Nacional de Ciberseguridad, similar a lo realizado en Chile. Es fundamental establecer una estructura organizativa clara, liderada por un ente coordinador, que coordine los esfuerzos entre diversas agencias gubernamentales y el sector privado. Esto permitirá una respuesta más rápida y efectiva ante incidentes cibernéticos. Además, es importante seguir fomentando la cooperación internacional para fortalecer la capacidad de respuesta de Perú a las amenazas cibernéticas globales. Participar activamente en foros internacionales, establecer acuerdos bilaterales y multilaterales, y colaborar con organizaciones internacionales puede mejorar significativamente la ciberdefensa peruana. Otro aspecto crucial es definir un lenguaje común y estandarizado en lo que respecta a las definiciones y terminologías relacionadas con la ciberdefensa y la ciberseguridad, no solo a nivel nacional, sino también regional. Esto facilitará la comunicación y la colaboración entre países, permitiendo una respuesta más unificada y coherente a las amenazas cibernéticas. Cada país tiene sus particularidades y realidades, por lo que es necesario adaptar estas recomendaciones a las necesidades específicas de Perú. Sin embargo, la adopción de buenas prácticas, como las observadas en la política chilena, puede proporcionar una base sólida para el desarrollo de una política de ciberdefensa robusta y eficaz en Perú. Para efectuar un análisis comparativo de las políticas de ciberdefensa de Chile y Perú, es esencial destacar los resultados más importantes que emergen de dicha comparación. La experiencia de Chile destaca la importancia de que los países de la región adopten una política integral que coordine la ciberdefensa

	y la ciberseguridad. Chile ha implementado una estructura organizativa clara y eficiente, liderada por el Ministerio de Defensa Nacional, que asegura una estrecha colaboración entre diversas agencias gubernamentales y el sector privado. Este enfoque integral permite una respuesta más rápida y efectiva ante las amenazas cibernéticas, algo que Perú puede considerar al desarrollar y fortalecer su propia política de ciberdefensa. Chile participa activamente en foros y acuerdos internacionales, lo que le permite estar al tanto de las mejores prácticas y estándares globales en ciberseguridad. Perú, de esta forma, puede fortalecer su capacidad de respuesta a las amenazas cibernéticas globales mediante la colaboración con otros países y organizaciones internacionales, promoviendo así un entorno más seguro y confiable. Finalmente, tanto Chile como Perú reconocen la importancia de proteger las infraestructuras críticas. La protección de estos sistemas y servicios esenciales es una prioridad común, ya que cualquier interrupción podría tener consecuencias devastadoras para la seguridad nacional y la estabilidad económica.
Capitán de Fragata Francisco José Jaraba Hadechiny (E-Co)	Más que dar recomendaciones específicas, los casos de éxito en Colombia destacan el desarrollo de capacidades por roles misionales. Cada fuerza militar o entidad del estado debe desarrollar sus capacidades de acuerdo con su rol específico y establecer un plan de comunicación adecuado sobre incidentes y lecciones aprendidas. De esta manera, su capacidad de ciberdefensa tendrá un direccionamiento y un crecimiento enfocado en sus necesidades particulares. El análisis comparativo de las políticas de ciberdefensa de Argentina, Brasil, Chile, Colombia, Ecuador y Perú revela varias similitudes y diferencias importantes en sus enfoques hacia la ciberseguridad y la ciberdefensa. A continuación, se destacan algunos de los resultados más importantes: El Enfoque en la Protección de Infraestructuras Críticas: Argentina, Brasil, Chile, Colombia y Perú: Todos estos países han reconocido la importancia de proteger sus infraestructuras críticas (como energía, telecomunicaciones y finanzas) contra ciberataques. Han implementado políticas y estrategias específicas para garantizar la seguridad de estas infraestructuras. La creación de Entidades y Organismos Especializados: Brasil, Chile y Colombia: Estos países han establecido organismos especializados en ciberdefensa, como el Comando de Defensa Cibernética en Brasil, el Equipo de Respuesta ante Emergencias Informáticas (CSIRT) en

	Chile, y el Grupo de Respuesta a Emergencias Cibernéticas (COLCERT) en Colombia.
Capitán de Corbeta Vivanco Toala Danny (E-E)	No las conozco.
Coronel FAP Luigui Aurelio Rivas Guevara (E-P)	Bueno a la fecha no contamos con una Política específica de Ciberdefensa, pero la pregunta es interesante porque Perú podría beneficiarse de estudiar las mejores prácticas y experiencias de países como Argentina, Brasil, Chile, Colombia y Ecuador para fortalecer su política. Esto incluye aspectos como la mejora del marco legal, la promoción de la colaboración público-privada, la implementación de programas de educación y concienciación, la protección de sectores críticos y la mejora de las capacidades de respuesta a incidentes. **Fortalecimiento del Marco Legal y Regulatorio:** Brasil y Chile han desarrollado marcos legales robustos para la protección de datos personales y la ciberseguridad, como la Ley General de Protección de Datos (LGPD) en Brasil y la Ley de Protección de la Vida Privada en Chile. Perú podría considerar fortalecer su legislación para alinearla con estándares internacionales y mejorar la protección de datos sensibles. **Coordinación Interinstitucional y Colaboración Público-Privada:** Colombia ha establecido una Agencia Nacional de Ciberseguridad y cuenta con un Comité Consultivo de Ciberseguridad que promueve la colaboración entre sectores público y privado. Perú podría mejorar su coordinación estableciendo mecanismos similares para facilitar una respuesta más coordinada y eficaz a las amenazas cibernéticas. **Capacitación y Concienciación:** Ecuador ha implementado programas de concienciación y capacitación en ciberseguridad dirigidos a diversos sectores de la sociedad. Perú podría mejorar sus políticas mediante la implementación de campañas educativas más amplias y accesibles que aumenten la concienciación sobre prácticas seguras en línea y la importancia de la ciberseguridad. **Protección de Sectores Críticos:** Argentina ha adoptado medidas específicas para proteger sectores críticos como energía, transporte y salud. Perú podría considerar desarrollar políticas

	sectoriales específicas que identifiquen y protejan sus infraestructuras críticas ante posibles ciberataques. **Resiliencia y Respuesta a Incidentes:** Chile ha avanzado en la creación de capacidades de respuesta a incidentes cibernéticos a través de la formación de equipos especializados y la implementación de planes de acción específicos. Perú podría fortalecer sus capacidades en este ámbito mediante la inversión en formación especializada y el establecimiento de protocolos claros para la gestión de incidentes cibernéticos. En resumen, es fundamental que Perú adapte estas lecciones según sus propias necesidades y realidades específicas para lograr un desarrollo efectivo y sostenible en materia de ciberseguridad y ciberdefensa Bueno haciendo una comparación, considero que el común denominador de las políticas de ciberdefensa es establecer primeramente una resiliencia cibernética que le permita a los países mencionados en poder prevenir, detectar y recuperarse de forma rápida y articulada, minimizando los efectos o los impactos de un ataque cibernético efectivo. Asimismo, es poder establecer la cooperación internacional entre los Estados para que los delitos cibernéticos no sean impunes y de alguna manera se puedan atribuir; sé que es difícil en este entorno, pero al menos generar una disuasión orientado a minimizar o reducir el accionar delictivo en el ciberespacio.

Anexo E: Ficha bibliográfica

Datos bibliográficos
Autores: **Año:** **Título:** **Nombre de la revista:** **Volumen:** **Número:** **Paginas:** **Editorial:** **Link:** **Web:**

Anexo F: Ficha de análisis de las políticas de ciberdefensa de los Estados

Estado	Ley, documento normativo o estratégico	Componentes de la estructura según subtítulos
Argentina		
Brasil		
Chile		
Colombia		
Ecuador		
Perú		

Anexo G: Ficha resumen del contenido de los componentes de las políticas de ciberdefensa de los Estados

Ficha de resumen del contenido de los componentes de las políticas de ciberdefensa de los Estados

ESTADOS	OBJETIVO PRINCIPAL	OBJETIVOS ESPECÍFICOS ESTRATÉGICOS	PRINCIPIOS	CAPACIDADES	ACTIVOS CRÍTICOS	ORGANISMO EJECUTORES
ARGENTINA	Establecimiento de directrices y líneas de acciones de los organismos para la gestión y protección de datos con los cuales trabaja, considerando preservar la confidencialidad, integridad y disponibilidad de dicha información, además de cumplir con las normativas aplicables, gestionar los riesgos y mejorar continuamente para incrementar su efectividad.	• Concientización, capacitación y educación. • Desarrollo de un marco normativo. • Fortalecimiento de capacidades de prevención, detección y respuesta. • Protección y recuperación de los sistemas de información. • Fomento de la industria de la ciberseguridad. • Cooperación internacional. • Protección de las infraestructuras críticas nacionales. • Fortalecimiento del sistema institucional.	• Principio de confidencialidad. • Principio de integridad. • Principio de disponibilidad. • Principio de cumplimiento normativo. • Principio de Paz y seguridad. • Principio de Derechos Humanos. • Principio de Desarrollo de capacidades. • Principio de Cooperación Internacional. • Principio de Soberanía Nacional. • Principio de Cultura de ciberseguridad. • Principio de Desarrollo socioeconómico.	• Capacidad de prevención. • Capacidad de detección. • Capacidad de respuesta. • Capacidad de protección. • Capacidad de recuperación.	Definir e identificar las Infraestructuras Críticas Nacionales de Información, como las de operación y comunicación, cooperando con entidades públicas y privadas e invirtiendo en las mismas para este propósito. Para la clasificación se tienen en cuenta la confidencialidad, integridad y disponibilidad de los datos, así como las funciones que soporta el activo y la normativa aplicable.	Comité de Ciberseguridad. Comando conjunto de Ciberdefensa.
BRASIL	• Asegurar el uso del ciberespacio, impidiendo o dificultando, dentro de su ámbito, acciones contrarias a los intereses del país y de la sociedad.	• Promover el desarrollo de productos, servicios y tecnologías de carácter nacional destinados a ciberseguridad;	• Principio de Protección de derechos fundamentales. • Principio de Prevención de incidentes cibernéticos.	• Capacidad de posicionamiento y respuesta de la nación. • Capacidad de resiliencia.	Son las Infraestructuras Críticas que protegen y poseen los activos de información que afectan directamente	• Comando de Ciberdefensa • Comité Nacional de Ciberseguridad

ESTADOS	OBJETIVO PRINCIPAL	OBJETIVOS ESPECÍFICOS ESTRATÉGICOS	PRINCIPIOS	CAPACIDADES	ACTIVOS CRÍTICOS	ORGANISMO EJECUTORES
	• Hacer que Brasil sea más próspero y confiable en el entorno digital, incrementando la resiliencia brasileña ante las amenazas cibernéticas; y fortalecer el desempeño brasileño en materia de ciberseguridad en el escenario internacional.	• Asegurar a confidencialidad, integridad, autenticidad y disponibilidad de soluciones y datos utilizados para el procesamiento, almacenamiento y transmisión electrónica o digital de información. • Fortalecer el rendimiento diligente en el ciberespacio, especialmente de niños, adolescentes y ancianos. • Contribuir a la lucha cibercrimen y otras acciones maliciosas en el ciberespacio. • Fomentar la adopción de protección cibernética y medidas de gestión de riesgos para prevenir, prevenir y mitigar, mitigar y neutralizar vulnerabilidades, incidentes y ataques cibernética, y sus impactos. • Aumentar la resiliencia de organizaciones públicas y privadas a incidentes y ataques cibernéticos. • Desarrollar la educación y la formación técnico-profesional en ciberseguridad en la sociedad. • Promover actividades investigación científica, desarrollo tecnológico e	• Principio de Resiliencia de las entidades públicas y privadas. • Principio de Educación y desarrollo tecnológico en ciberseguridad. • Principio de gobernanza. • Principio de Política Nacional. • Principio de capacidad de respuesta nacional. • Principio de compromiso de alta administración. • Principio de marco legal. • Principio de articulación y alianzas. • Principio de soberanía nacional. • Principio de cooperación. • Principio de integración. • Principio de resiliencia.		la misión del Estado y la seguridad de la sociedad.	

ESTADOS	OBJETIVO PRINCIPAL	OBJETIVOS ESPECÍFICOS ESTRATÉGICOS	PRINCIPIOS	CAPACIDADES	ACTIVOS CRÍTICOS	ORGANISMO EJECUTORES
		innovación relacionado con la ciberseguridad. • Aumentar el rendimiento coordinado y el intercambio de información de ciberseguridad. • Desarrollar mecanismos de regulación, supervisión y control destinados a mejorar la seguridad resiliencia cibernética nacional. • Implementar estrategias de colaboración para desarrollar la cooperación internacional en seguridad cibernética. • Fortalecer las acciones de gobernanza cibernética. Establecer un modelo centralizado de gobernanza en el ámbito nacional. • Promover un ambiente participativo, colaborativo, confiable y seguro entre el sector público, privado y la sociedad. • Elevar el nivel de protección gubernamental. • Elevar el nivel de protección de las Infraestructuras Críticas Nacionales. • Mejorar el marco legal en materia de ciberseguridad.				

ESTADOS	OBJETIVO PRINCIPAL	OBJETIVOS ESPECÍFICOS ESTRATÉGICOS	PRINCIPIOS	CAPACIDADES	ACTIVOS CRÍTICOS	ORGANISMO EJECUTORES
		• Fomentar el diseño de soluciones de seguridad innovadoras cibernética. • Ampliar la cooperación internacional de Brasil en Seguridad cibernética. • Ampliar la alianza, en ciberseguridad, entre el sector público, el sector privado, la academia y la sociedad. • Elevar el nivel de madurez de la sociedad en ciberseguridad.				
CHILE	Contar con una infraestructura de la información robusta y resiliente en el sector de la Defensa Nacional, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una perspectiva de gestión de riesgos.	• Empleo de medio de ciberdefensa. • Cooperación internacional y promoción de transparencia y confianza entre Estados. • Desarrollo de capacidades.	• Principio de Equivalencia. • Principio de Respeto del derecho internacional público. • Principio de Promoción de la democracia y el respeto a los derechos humanos. • Principio de Protección de la población, de los intereses nacionales, y de la integridad territorial.	• Capacidad de uso de inteligencia artificial. • Capacidad de prevención. • Capacidad de respuesta.	Infraestructura considerada estratégica y vital para el país, como la red de transporte y la red de centros de salud, entre otras	Comando Conjunto de Ciberdefensa

ESTADOS	OBJETIVO PRINCIPAL	OBJETIVOS ESPECÍFICOS ESTRATÉGICOS	PRINCIPIOS	CAPACIDADES	ACTIVOS CRÍTICOS	ORGANISMO EJECUTORES
COLOMBIA	Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.	• Implementación de instancias apropiadas para ciberseguridad y ciberdefensa. • Capacitación especializada y ampliación de investigación. • Fortalecimiento legislativo y cooperación internacional.	• Principio de confianza. • Principio de coordinación. • Principio de colaboración entre partes interesadas. • Principio de cooperación. • Principio de gestión de riesgos. • Principio de gradualidad. • Principio de inclusión. • Principio de proporcionalidad. • Principio de salvaguarda de los derechos fundamentales. • Principio de uso eficiente de la infraestructura y recursos para la protección de activos críticos.	• Capacidad de prevención. • Capacidad de respuesta.	Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía	• ColCERT, • Comando Conjunto Cibernético • Centro Cibernético Policial

ESTADOS	OBJETIVO PRINCIPAL	OBJETIVOS ESPECÍFICOS ESTRATÉGICOS	PRINCIPIOS	CAPACIDADES	ACTIVOS CRÍTICOS	ORGANISMO EJECUTORES
ECUADOR	Reforzar las capacidades de ciberdefensa y desarrollar capacidades en Ciberinteligencia que permitan obtener información útil y oportuna de las amenazas presentes en ciberespacio para la toma de decisiones.	• Fortalecimiento de ciberdefensa para la protección de la infraestructura crítica del estado. • Incremento de las capacidades de defensa activa y respuesta para contrarrestar amenazas. • Articulación y coordinación de acciones conjuntas para el desarrollo de normativas y fortalecimiento interinstitucional. • Intensificar la cooperación internacional. • Fortalecer la cultura de ciberdefensa.	• Principio de liderazgo y responsabilidad compartida. • Principio de salvaguarda de los derechos fundamentales. • Principio de gestión de riesgos y resiliencia. • Principio de visión inclusiva y colaborativa.	• Capacidad de prevención. • Capacidad de defensa activa. • Gestión de riesgo. • Seguimiento y evaluación.	Parte de la infraestructura y los servicios críticos, que comprende sistemas de información y comunicación que son esenciales para el buen funcionamiento de la sociedad	Comando de Ciberdefensa
PERÚ	Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.		• Principio de legalidad. • Principio de necesidad militar. • Principio de proporcionalidad. • Principio de oportunidad.	• Capacidad de defensa. • Capacidad de explotación. • Capacidad de respuesta. • Capacidad de investigación digital.	Recursos, infraestructuras y sistemas esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales	Comando Operacional de Ciberdefensa

Ficha de resumen del contenido de los componentes de las políticas de ciberdefensa de los Estados

ESTADOS	COMPONENTES SISTÉMICOS SUBSIDIARIOS	ENFOQUE SISTÉMICO	ALCANCE Y ÁMBITO DE APLICACIÓN	INSTRUMENTOS	EJES TEMÁTICOS	PLAN DE ACCIÓN	FINANCIAMIENTO	MODELO DE GOBERNANZA	ENFOQUE DE SEGURIDAD	ROL DEL MINISTERIO DE DEFENSA	OPERACIONES MILITARES	USO DE LA FUERZA
ARGENTINA	Diseño de la defensa del ciberespacio desde un enfoque multidimensional.	Reúne un conjunto de Componentes contribuyentes al desarrollo de la capacidad, que son las bases del planteo tanto estratégico como operacional, como la evolución dinámica, mejora de talento humano con inversión tecnológica	Aplicado a todo el ámbito del organismo ejecutor y cualquiera con vínculo contractual o jerárquico. En donde participan entidades obligadas a las disposiciones contenidas en las normativas que conforman la Administración Pública.	Para el planeamiento estratégico militar	Eje de revisión y actualización para modificar la normativa y mejorar los objetivos estratégicos				Se incluye en sus componentes sistémicos subsidiarios, aspectos de seguridad en políticas, en tecnologías, entre otros	Detallada el rol del ministerio de defensa	Entiéndase como detección temprana, no sólo a la que se configura cuando el Ciberataque está en sus fases preparatorias de reconocimiento y distribución, sino también en sus fases de Comando y Control.	

ESTADOS	COMPONENTES SISTÉMICOS SUBSIDIARIOS	ENFOQUE SISTÉMICO	ALCANCE Y ÁMBITO DE APLICACIÓN	INSTRUMENTOS	EJES TEMÁTICOS	PLAN DE ACCIÓN	FINANCIAMIENTO	MODELO DE GOBERNANZA	ENFOQUE DE SEGURIDAD	ROL DEL MINISTERIO DE DEFENSA	OPERACIONES MILITARES	USO DE LA FUERZA
BRASIL		Diseño estratégico nacional sistémico	Alcanzar a un gran número de organizaciones, incluidas aquellas que representan infraestructuras críticas, que por prestar servicios esenciales a la sociedad tienen un alto nivel de criticidad, indica las entidades encargadas para la implementación y evolución del plan nacional de ciberdefensa	Documentos: Estrategia Nacional de Ciberseguridad y el Plan Nacional de Ciberseguridad.	1. Eje protección y seguridad: para formular acciones estratégicas de ciberseguridad nacional. 2. El eje transformador: para modificar las estrategias a nivel normativo, tecnología, vínculos etc.	Lo tiene en el Plan Nacional de Ciberseguridad		Establecer un modelo de gobernanza centralizada para el país, a través de la creación de un sistema nacional de ciberseguridad				
CHILE			Reúne un conjunto de Component	Instrumento de política		informar al CSIRT Nacional	Financiamiento del Ministerio					Sobre el cuerpo militar,

ESTADOS	COMPONENTES SISTÉMICOS SUBSIDIARIOS	ENFOQUE SISTÉMICO	ALCANCE Y ÁMBITO DE APLICACIÓN	INSTRUMENTOS	EJES TEMÁTICOS	PLAN DE ACCIÓN	FINANCIAMIENTO	MODELO DE GOBERNANZA	ENFOQUE DE SEGURIDAD	ROL DEL MINISTERIO DE DEFENSA	OPERACIONES MILITARES	USO DE LA FUERZA
			es contribuyentes al desarrollo de la capacidad, que son las bases del planteo tanto estratégico como operacional, como la evolución dinámica, mejora de talento humano con inversión tecnológica	pública normativo para la planificación y empleo de la Defensa Nacional		su plan de acción, tan pronto lo hubieren adoptado	del Interior y Seguridad Pública, pero no detalla cuánto					podrá hacer uso de la fuerza en legítima defensa en el ciberespacio.
COLOMBIA			Entidades obligadas a las disposiciones contenidas en las normativas que conforman la	Convenios resoluciones		Se especifican las acciones concretas a desarrollar como la capacitación en ciberseguridad y	Señala el costo de aquí a varios años.	Esquema de trabajo compuesto por un conjunto de políticas de	Enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética	Especifica su rol para dirigir, normar, supervisar y evaluar las disposiciones en ciberdefensa.	Especifica lo que hace el Comando Conjunto Cibernético de las Fuerzas Militares	

ESTADOS	COMPONENTES SISTÉMICOS SUBSIDIARIOS	ENFOQUE SISTÉMICO	ALCANCE Y ÁMBITO DE APLICACIÓN	INSTRUMENTOS	EJES TEMÁTICOS	PLAN DE ACCIÓN	FINANCIAMIENTO	MODELO DE GOBERNANZA	ENFOQUE DE SEGURIDAD	ROL DEL MINISTERIO DE DEFENSA	OPERACIONES MILITARES	USO DE LA FUERZA
			Administración Pública.			ciberdefensa, el fortalecimiento de la legislación y la cooperación internacional.		operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país.				

ESTADOS	COMPONENTES SISTÉMICOS SUBSIDIARIOS	ENFOQUE SISTÉMICO	ALCANCE Y ÁMBITO DE APLICACIÓN	INSTRUMENTOS	EJES TEMÁTICOS	PLAN DE ACCIÓN	FINANCIAMIENTO	MODELO DE GOBERNANZA	ENFOQUE DE SEGURIDAD	ROL DEL MINISTERIO DE DEFENSA	OPERACIONES MILITARES	USO DE LA FUERZA
ECUADOR			Facultad de ejecución de políticas públicas, operaciones de ciberseguridad, ciberdefensa, Ciberinteligencia dentro del territorio nacional y en el exterior con la colaboración internacional respectiva	Convenios resoluciones	Infraestructura digital, seguridad de la información y uso responsable de las TIC		Las fuentes de financiación podrían ser internas o de donantes internacionales	Con planificación multisectorial, involucra a diversos actores	Se describe diversos sub-enfoques adoptados, como de planificación estratégica, integral, sistémico, multisectorial y multidimensional, de desarrollo sostenible, derechos digitales, resiliencia, gobernanza y confianza digital, enfoques que guían las acciones sobre ciberseguridad y ciberdefensa.	Especifica su rol para dirigir, normar, supervisar y evaluar las disposiciones en ciberdefensa.	Destaca la capacidad n prevenir y contrarrestar las ciberamenazas, ciberataques, incidentes en el ciberespacio o actos hostiles que afecten a la soberanía e integridad territorial, el orden constitucional y los intereses nacionales	
PERÚ			Entidades obligadas a							Especifica su rol para	Menciona acciones	Se justifica el empleo

ESTADOS	COMPONENTES SISTÉMICOS SUBSIDIARIOS	ENFOQUE SISTÉMICO	ALCANCE Y ÁMBITO DE APLICACIÓN	INSTRUMENTOS	EJES TEMÁTICOS	PLAN DE ACCIÓN	FINANCIAMIENTO	MODELO DE GOBERNANZA	ENFOQUE DE SEGURIDAD	ROL DEL MINISTERIO DE DEFENSA	OPERACIONES MILITARES	USO DE LA FUERZA
			las disposiciones contenidas en las normativas que conforman la Administración Pública.							dirigir, normar, supervisar y evaluar las disposiciones en ciberdefensa.	estratégicas que se planifican y ejecutan en el ciberespacio con el objetivo de lograr resultados militares específicos para proteger la seguridad nacional.	de la fuerza, para tomar medidas que debiliten o anulen las habilidades y acciones del oponente en el ciberespacio, señalando las reglas de enfrentamiento.