**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**

# "Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú"


**Presentado por:**

**Mayor EP. Franck Edgar Chivilches Seguil**

**https://orcid.org/0000-0002-5197-0029**

**Asesor metodológico:**

**Doctor. Arturo Guillermo Arriarán Schaffer**

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

**Asesor técnico:**

**Maestro. Luis Andrés Meza Medina**

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


**La Punta, 2023**

# Acta de sustentación

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

**ACTA DE SUSTENTACIÓN DE TESIS Nº 014**

**PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN ESTRATEGIA MARÍTIMA**

La Punta, 18 DIC 2023

En cumplimiento de lo establecido en la Resolución Directoral Nº 044-2023-MGP/DIRESUVAL de fecha 12 de diciembre del 2023, se reúne el Jurado, integrado por:

1. Doctor Carl Johan BLYDAL (Presidente)
2. Magíster C. de N. (r) Eduardo ZARAUZ Chávez (Miembro)
3. Magíster C. de N. (r) Eduardo PÉREZ Román (Miembro)

Para evaluar la sustentación del trabajo de investigación tipo tesis titulado: **"Estrategia para enfrentar la ciberdelincuencia que afecta la seguridad nacional en Perú"**, presentado por el Mayor EP. Franck Edgar CHIVILCHES Seguil.

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
Magíster. Capitán de Navío (r)
Eduardo ZARAUZ Chávez
DNI. 43127684

Integrante
Magíster. Capitán de Navío (r)
Eduardo PÉREZ Román
DNI. 43345640

# Declaración jurada de originalidad

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

**DECLARACIÓN JURADA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN TIPO TESIS**

La Punta, 29 de abril del 2024

Yo, Bachiller, Tte Crl EP, Franck Edgar Chivilches Seguil, identificado con DNI: 10678395, del programa de Maestría en Estrategia Marítima, declaro bajo juramento, que el presente trabajo de investigación tipo tesis titulado **"Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en 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,

(Firma)

Bachiller, Tte Crl EP, Franck Edgar Chivilches Seguil
DNI: 10678395

# Informe de similitud

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

## Informe de Similitud del Trabajo de Investigación

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.

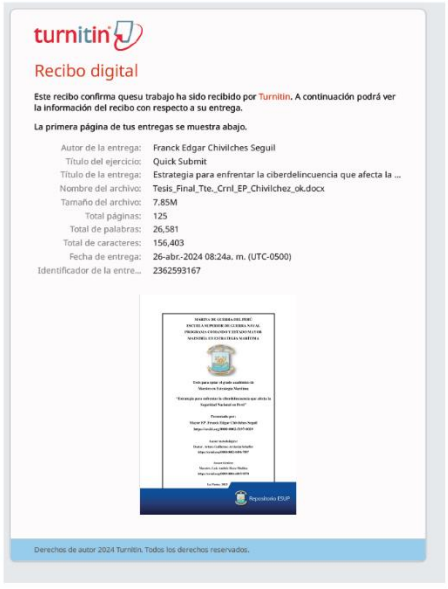
DECLARO:
Que la Tesis titulada **"Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú"**, presentada por el **Mayor EP, Bachiller, Franck Edgar CHIVILCHES Seguil**, para el otorgamiento del grado académico de **Maestro en Estrategia Marítima**, ha sido revisada con 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 **16%.**

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, 26 de abril de 2024

Doctor 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: | Franck Edgar Chivilches Seguil |
| Título del ejercicio: | Quick Submit |
| Título de la entrega: | Estrategia para enfrentar la ciberdelincuencia que afecta la ... |
| Nombre del archivo: | Tesis_Final_Tte._Crnl_EP_Chivilchez_ok.docx |
| Tamaño del archivo: | 7.85M |
| Total páginas: | 125 |
| Total de palabras: | 26,581 |
| Total de caracteres: | 156,403 |
| Fecha de entrega: | 26-abr.-2024 08:24a. m. (UTC-0500) |
| Identificador de la entre... | 2362593167 |



Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú

INFORME DE ORIGINALIDAD

| 16% | 15% | 3% | 6% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

# DEDICATORIA

*Dedico con profundo agradecimiento este trabajo a mi querida esposa, soporte emocional en mi vida, cuyo amor incondicional y apoyo constante han sido mi motivación en las horas nocturnas de esta investigación. A mis queridas hijas, quienes son mi inspiración constante, su inocencia y ternura son el soporte moral de esta travesía académica. Y a mi amada familia, mi eterna fortaleza, cuyo respaldo inquebrantable ha sido el soporte de este reto. En cada página, en cada desafío y en cada logro, sus gestos de ánimo, consejos y valores han sido la inspiración que ha dado vida a estas palabras. Con profundo amor y agradecimiento, les dedico este trabajo.*

*A los héroes anónimos de la pacificación, cuyos nombres permanecen en silencio, a menudo en la sombra se sacrifican incansablemente por construir un mundo mejor. Ustedes son el recordatorio que el espíritu humano prevalece ante los desafíos. Mi más profundo respeto, admiración y agradecimiento siempre.*

*A mi madre, que ahora brilla en el cielo como una estrella luminosa, te dedico este trabajo, con amor y gratitud. Aunque ya no estés físicamente conmigo, tu espíritu y tus enseñanzas me han guiado a lo largo de este camino académico. Este trabajo es un tributo a tu amor y a tu memoria.*

## AGRADECIMIENTO

*A nuestra Marina de Guerra del Perú y al Ejército peruano, por darme el privilegio de forjarme como oficial de Estado Mayor y perfeccionarme profesionalmente en la estrategia marítima, sirviendo con honor la misión que la patria me encomiende.*

*Mi más sincero agradecimiento a mis asesores, Capitán de Navío (r), doctor, Arturo Guillermo Arriarán Schaffer y al Capitán de Corbeta, Magister, Luis Andrés Meza Medina, por su acertada exploración de conocimiento para materializar esta tesis.*

# ÍNDICE

Página

# LISTADO DE TABLAS

Pág.

# LISTADO DE FIGURAS

pág.

## Resumen

La investigación se denomina “Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú”, en la cual se planteó como objetivo formular la estrategia que debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú. La metodología empleada consistió en un enfoque cualitativo, de tipo según su finalidad es básica, según su carácter es descriptiva y según su alcance es transversal y también presentó un diseño de análisis documental.

Como muestra se consideró el material bibliográfico relacionado a las unidades temáticas a la que se tenga acceso, personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional. Se empleó como técnicas el análisis documental y las entrevistas, y como instrumentos se emplearon las fichas bibliográficas, fichas de análisis y guía de entrevista semiestructurada, la cual fue validada a través de V de Aiken, obteniendo una puntuación de 0.8.

Los resultados dieron a conocer que la ciberdelincuencia en Perú afecta la Seguridad Nacional mediante ataques a instituciones clave y vulnerabilidades en sistemas de salud, generando impactos en la seguridad ciudadana.  además, es crucial contar con personal altamente capacitado en ciberseguridad, utilizar recursos tecnológicos avanzados, y mejorar la infraestructura y acuerdos internacionales para combatir la ciberdelincuencia, asimismo se señaló la urgencia de una Estrategia Nacional de Ciberseguridad, una Ley de Ciberseguridad, y la mejora de la infraestructura y recursos humanos especializados. Por último, se resalta la importancia de incentivar la capacitación del personal, evaluar la relación entre remuneración y capacitación, y desarrollar una Estrategia de Ciberseguridad nacional con colaboración interinstitucional.


**Palabras clave:** Ciberdelincuencia, estrategia, Fuerzas Armadas, Seguridad Nacional.

## Abstract

The research is called "Strategy to confront cybercrime affecting National Security in Peru", in which the objective was to formulate the strategy to be developed to confront cybercrime affecting National Security in Peru. The methodology used consisted of a qualitative approach, of the basic type according to its purpose, descriptive according to its nature and cross-sectional according to its scope, and also presented a documentary analysis design.

As a sample, the bibliographic material related to the thematic units to which access is available, personnel in charge of dealing with cybercrime affecting National Security, was considered as a sample. Documentary analysis and interviews were used as techniques, and bibliographic cards, analysis cards and a semi-structured interview guide were used as instruments, which was validated through Aiken's V, obtaining a score of 0.8.

The results showed that the Cybercrime in Peru affects national security through attacks on key institutions and vulnerabilities in health systems, generating impacts on citizen security. In addition, it is crucial to have highly trained personnel in cybersecurity, use advanced technological resources, and improve infrastructure and international agreements to combat cybercrime, as well as the urgency of a National Cybersecurity Strategy, a Cybersecurity Law, and the improvement of infrastructure and specialized human resources. Finally, staff training will be encouraged, the relationship between remuneration and training will be evaluated, and a National Cybersecurity Strategy will be developed with inter-institutional collaboration.


**Keywords:** Cybercrime, strategy, Armed Forces, National Security.

# Introducción

La ciberdelincuencia es un fenómeno que ha experimentado un crecimiento significativo en las últimas décadas, planteando desafíos cada vez más complejos para la seguridad nacional de los países. En este contexto, la presente investigación se propone abordar la problemática de la ciberdelincuencia y su impacto en la seguridad nacional en el contexto de Perú.

El Capítulo I se centra en el planteamiento del problema, abordando la situación problemática que enfrenta el país en relación con la ciberdelincuencia, la formulación del problema que incluye tanto el problema general como los problemas específicos a investigar, los objetivos de la investigación y su justificación, así como las limitaciones y la viabilidad del estudio.

El Capítulo II se centra en el marco teórico que respalda la investigación, por lo que se presentan antecedentes internacionales y nacionales relacionados con la Seguridad Nacional y la ciberdelincuencia, destacando casos relevantes y tendencias globales en este campo. Se explorarán las bases teóricas, incluyendo conceptos clave como la Seguridad Nacional y la ciberdelincuencia. Además, se examinará la base normativa que rige estas cuestiones en el contexto peruano, así como las definiciones conceptuales necesarias para comprender el marco de la investigación.

En el Capítulo III se aborda la metodología de la investigación de manera detallada, por lo que se describe el diseño metodológico, incluyendo el enfoque de investigación y el tipo de investigación utilizado. Se explicarán los métodos empleados y se detalla el diseño de la muestra y la población de estudio. Además, se formularon las hipótesis generales y específicas que sirven como guía para el análisis de datos, también se describieron las técnicas e instrumentos de recolección de datos utilizados y se abordaron los procedimientos para el procesamiento de la información. Asimismo, se discutieron los aspectos éticos relacionados con la investigación, asegurando la integridad y la confidencialidad de los datos recopilados.

El Capítulo IV se efectuó al análisis y discusión de los resultados de la investigación., empleando herramientas como el análisis PESTEL para evaluar la situación de la Seguridad Nacional y la ciberdelincuencia en Perú desde múltiples perspectivas, incluyendo la dimensión política, económica, legal y tecnológica. Además, se llevó a cabo una revisión

bibliográfica exhaustiva que se centró en la Seguridad Nacional de Perú, la ciberdelincuencia en el país y las estrategias existentes para enfrentarla, por lo que para obtener una comprensión más profunda se analizaron las entrevistas realizadas a expertos en el campo, abordando cuestiones clave relacionadas con la ciberdelincuencia y la Seguridad Nacional.

Finalmente, en el Capítulo V, se presentaron las conclusiones y recomendaciones basadas en los hallazgos de la investigación, donde las conclusiones resumieron los resultados clave y las recomendaciones ofrecieron un conjunto de acciones prácticas que pueden ayudar a mejorar la seguridad cibernética y la protección de la Seguridad Nacional en el país.

# CAPÍTULO I
# PLANTEAMIENTO DEL PROBLEMA

## 1.1. Situación problemática

Dado que las generaciones ahora se clasifican de acuerdo con la existencia del internet, ha habido una revolución tecnológica importante como consecuencia de ello; pues hoy en día, la sociedad se gestiona virtualmente, desde las tareas más básicas hasta las más complicadas y cruciales para un país o nación, como el ámbito industrial, social, político y de seguridad. Así también, se ha hecho evidente la necesidad de que las herramientas tecnológicas se incorporen al día a día de la sociedad como resultado del avance tecnológico. Por lo que el gobierno debe intervenir y proteger la información que brinda cada usuario del ciberespacio, garantizando su respectiva protección en la información, ya que los avances tecnológicos aumentan el cuidado con el que se maneja (Saiz et al., 2018).

El uso generalizado de herramientas digitales, el enfoque en los derechos humanos con respecto a cuestiones directamente concernientes con las telecomunicaciones, el potencial de usos maliciosos del ciberespacio, el reciente acrecentamiento en la innovación y la interdependencia en torno a los avances tecnológicos; son todos factores que requieren el estudio de la seguridad cibernética. Específicamente, la tecnología ha obligado a varios campos a converger en objetivos comunes, incluidos el acceso digital, defensa, seguridad, diplomacia, justicia penal, resiliencia y conectividad en el interior y en el exterior, la economía y el comercio, y tecnologías emergentes. Como resultado, los gobiernos han comenzado a implementar y adoptar legislación nacional en materia de seguridad cibernética, particularmente en aquellos estados cuyo desarrollo no contó con un marco regulatorio o que carecían de un marco actualizado (Ávila, 2022).

Debido a este uso, es pertinente aumentar la seguridad del ciberespacio, ya que el espionaje ha acompañado a la sociedad desde sus inicios, cuando se enviaban espías para monitorear los movimientos de la población vecina con un propósito específico. En el mundo digital actual, el espionaje no pasa desapercibido, con términos como ciberseguridad y ciberdefensa refiriéndose a la práctica de defender servicios electrónicos, redes y datos que existen en este medio electrónico.

En este sentido, es posible imaginar las enormes implicaciones de que la información electrónica existente, las redes sociales, las reuniones privadas de trabajo o estudio, o los archivos laborales provoquen ataques, daños o pérdidas; los efectos de fallas en bases de

datos, edificios inteligentes o sistemas de inventario de una empresa; las consecuencias de que la integridad de una persona se vea comprometida por manipulación o robo de información (Amato et al., 2018).

Las principales ciberamenazas en América Latina, según la Organización de los Estados Americanos (OEA, 2018) son ataques basados en programa maligno destinados a robar datos confidenciales o secretos. Los métodos más comunes son el *spear phishing* (correo electrónico diseñado específicamente para infectar una computadora personal) y el abrevadero (piratería de sitios web legítimos para propagar código malicioso a través de ellos). Asimismo, desde 2015, el número de troyanos destinados al fraude bancario se ha incrementado significativamente; se estima que el 92% de las instituciones financieras han sido atacadas y el 37% del total han tenido éxito (Organización de las Naciones Unidas, 2020). Además, Aguilar (2021) señala que las actividades relacionadas con el cibercrimen son más frecuentes (77,9%), a comparación de las relacionadas con instituciones gubernamentales o públicas, como el ciberespionaje o el hacktivismo.

Del mismo modo, los gobiernos y las organizaciones de seguridad reconocen que hoy en día existe un mayor riesgo de vulnerabilidad de la seguridad, incluidos los delitos cibernéticos, el terrorismo y otras amenazas cibernéticas que han causado daños sociales y pérdidas económicas (Izaguirre & León, 2018). Como consecuencia, el gobierno y varias organizaciones internacionales han fortalecido sus capacidades técnicas en ciberdefensa y seguridad de la información (implementando sistemas y protocolos de seguridad más sofisticados). Las nuevas leyes, las actualizaciones de las leyes existentes y los estándares de calidad técnica deben desarrollarse simultáneamente. La preocupación por este tipo de eventos (ciber catástrofes) ha llevado a los gobiernos a dedicar más recursos para garantizar la seguridad de Internet. Los avances de China y Rusia en el desarrollo de una Internet segura son ejemplos de esto.

El Sistema de Defensa Nacional del Perú tiene como fin declarar la garantía de la Seguridad Nacional; como resultado, el sistema incorpora varios principios, normas, prácticas, procedimientos, instrumentos y componentes a nivel estatal. A pesar de esto, parece haber poca preocupación por parte de las autoridades para formular tal sistema, quizás debido a la débil articulación de las reglas, el desconocimiento de las reglas o la animadversión contra las Fuerzas Armadas. Para cumplir con su deber constitucional, las Fuerzas Armadas deben modernizarse y equiparse para ello. Pero hacerlo requiere recursos

financieros que puedan apoyar a esas fuerzas. A pesar de esto, ha sido claro por más de 15 años que las FFAA deben ser asignadas con más fondos (Gonzales, 2022).

Bajo el contexto de lo anterior, Perú fue calificado en el puesto 95 por la Unión Internacional de Telecomunicaciones (UIT, 2018), y a nivel latinoamericano, se ubicó en el puesto 12, superando a países como Nicaragua, Guatemala, Venezuela, Ecuador, Panamá, entre otros. Leiva (2015) señala que los Estados miembros de la Organización de Estados Americanos (OEA) han emprendido tareas conjuntas para fortalecer la ciberseguridad desde 2004. Del mismo modo, el Plan Integral Interamericano de Ciberseguridad ha mostrado considerables desigualdades regionales desde su implementación, ya que algunas naciones tienen una capacidad mínima para reaccionar ante ciberataques, mientras que otras se encuentran en niveles intermedios con diferentes capacidades de respuesta. Perú se encuentra entre los países que tienen una capacidad de respuesta de moderada a débil en este aspecto.

Siendo así que diversas instituciones y organismos del Estado peruano, como las FFAA, utilizan datos e información digital a través de las redes de internet, las cuales han sido blanco de ataques cibernéticos diseñados para robar o destruir datos sensibles. Además, cuando se trata de proteger la información digital almacenada en los diversos sistemas del gobierno peruano, especialmente del Ejército del Perú, la ciberseguridad se utiliza de forma limitada, la seguridad se maneja principalmente mediante el uso de software antivirus y firewall adquirido, ninguno de los cuales es infalible (Villarrubia, 2021).

Específicamente, las entidades públicas en Perú tienden a enfocarse solo en las responsabilidades centrales que les corresponde cumplir según el sector o nivel de gobierno al que pertenecen, descuidando brindar su valioso aporte en temas transversales como la Seguridad Nacional y el Desarrollo. Cuando se trata de agencias gubernamentales responsables de garantizar la seguridad de las redes gubernamentales, el Centro Nacional de Seguridad Digital (CNSD) reporta directamente al presidente del Consejo de Ministros (PCM). La Policía Nacional del Perú (PNP) cuenta con una unidad especial dedicada a combatir el ciberdelito denominada División de Investigación de Delitos de Alta Tecnología (DIVINDAT). Las Fuerzas Armadas (FFAA) cuentan con ciber comandos responsables de la ciberdefensa, supervisados por el Comando Operacional de Ciberdefensa (COCID) del Comando Conjunto de las Fuerzas Armadas (CCFFAA).

Sin embargo, las autoridades competentes del Estado peruano no están de acuerdo en una sola estrategia o doctrina. Hasta ahora, la seguridad y la defensa cibernéticas se han desarrollado por separado en áreas por organizaciones separadas sin una fuerte interoperabilidad. Así también, no se ha establecido el rol del Ministerio de Relaciones Exteriores (MRE) y la organización carece de una estrategia de política externa que guíe la consolidación y mejora continuas de las capacidades de ciberseguridad, ciberdefensa y amenazas híbridas en la era de la Cuarta Revolución Industrial. El gobierno peruano también carece de la infraestructura física y digital necesaria para brindar una capacidad de ciberdefensa efectiva, así como del personal capacitado para mantener equipos de ciberdefensa de manera indefinida (Rossi, 2021).

Por otro lado, se sabe que el Ejército del Perú se adhiere a varias normas de privacidad de datos, incluidas las que se mencionan a continuación: En primer lugar, se encuentra la Directiva Única para el Funcionamiento del Sistema de Telemática y Estadística del Ejército (DUFSITELE) que aborda la regulación del uso de tecnología para la operación y transmisión de información, pero no aborda la temática de la protección de dicha información; luego, se cuenta con la Directiva de Seguridad de la Información del Ejército Peruano, que se basa en la Directiva N° 001-2021-PCM/SGD, “Directiva que establece los Lineamientos para la Conversión Integral de Procedimientos Administrativos a Plataformas o Servicios Digitales”, sin embargo, no se cumplen en su totalidad los lineamientos de seguridad de información para la ciberdefensa en el Ejército por parte de su personal de TI. Esto ha puesto al descubierto una serie de fallas en el Sistema de Defensa Nacional (SIDENA), entre ellas, la insuficiente coordinación e integración entre las distintas partes del sistema, la insuficiente iniciativa de los Organismos de Seguridad y Defensa Nacional para el cumplimiento efectivo de sus funciones, y una falta general de comprensión entre el público en general de la importancia de la seguridad y su papel en el desarrollo social (Zavaleta, 2020).

La Ley 30999, publicada el 26 de agosto de 2019, reestructura el entorno de la Estrategia Integrada de Ciberdefensa; sin embargo, las variables culturales y de aplicación de la norma plantean problemas que deben ser atendidos. Así, cada entidad gubernamental tiene su propio conjunto de protocolos de seguridad para las redes y datos alojados en los centros de datos. Los numerosos planes y políticas nacionales de ciberseguridad tienen todo el mismo objetivo general, que es proteger la integridad física y moral del Estado para que no se vea comprometida por peligros originados en el ciberespacio. Sin embargo, siguen

existiendo discrepancias entre las perspectivas de los Estados y los objetivos que se persiguen en el proceso de puesta en práctica de la política pública de ciberseguridad.

Por lo expuesto, ante las deficiencias que se evidencian en el Estado peruano para enfrentar adecuadamente la diversidad de ciberataques producidos por los ciber delincuentes, es necesaria la generación de estrategias que aborden esta problemática de forma integral y eficiente.

## 1.2. Formulación del problema

### 1.2.1. *Problema general*

¿Qué estrategia debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?

### 1.2.2. *Problemas específicos*

**PE1:** ¿Qué entes desarrollan ciberdelincuencia que podrían afectar la Seguridad Nacional en Perú?

**PE2:** ¿Cuáles son los aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos con los que se cuentan para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?

**PE3:** ¿Cuáles son las necesidades en aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?

**PE4:** ¿Cuáles son las acciones que podrían cubrir las necesidades presentadas para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?

## 1.3. Objetivos de la investigación

### 1.3.1. *Objetivo general*

Formular la estrategia que debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.

### 1.3.2. *Objetivos específicos*

**OE1.** Identificar los entes que desarrollan la ciberdelincuencia que podrían afectar la Seguridad Nacional en Perú.

**OE2.** Identificar los aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos con los que se cuentan para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.

**OE3.** Identificar las necesidades en aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.

**OE4:** Determinar las acciones que podrían cubrir las necesidades presentadas para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.

## 1.4. Justificación de la investigación

La necesidad e importancia de salvaguardar los datos estratégicos y críticos del Estado, así como los datos publicados por los peruanos en línea, sientan las bases del presente proyecto de investigación. A pesar de las muchas oportunidades que brinda Internet, también conlleva riesgos potenciales debido a la exposición de información confidencial y privada.

La justificación práctica de la investigación se sustenta en el aporte significativo para mejorar el estado actual de la protección de datos digitales en los centros de procesamiento de información asociados a la Seguridad Nacional. De igual manera, el estudio ayudó a potenciar y proponer una mejor estrategia para reducir el tema de los ciberataques en forma de robo o manipulación de información digital, que afecta no solo al Ejército, sino también a la Marina de Guerra y Fuerza Aérea, y cualquier otra entidad e institución gubernamental relacionada a la Seguridad Nacional. La investigación puede ayudar al Estado peruano en su conjunto y en particular a sus diversas instituciones públicas, entre ellas la Presidencia del Consejo de Ministros (PCM), el Comando Conjunto, la Policía Nacional, el Ministerio del Interior, las FFAA, el Ministerio de Defensa y la Secretaría de Gobierno Digital (SGDI). Los hallazgos de este estudio podrían ayudar al personal de las instituciones públicas antes mencionadas a tomar decisiones más informadas al iluminar enfoques novedosos para implementar un procedimiento de ciberseguridad.

En cuanto a la justificación teórica, este estudio reforzó la comprensión teórica de la seguridad de la información digital. Del mismo modo, tiene que ver con la adquisición y ampliación del conocimiento en áreas como la ciberdefensa y la gobernanza digital; esto brindó la oportunidad a los futuros investigadores comprender el estado de la seguridad de la información en Perú y cómo la transformación digital juega un papel en este desafío y campo complicado debido a su rápido ritmo de cambio y la falta de recursos humanos con las habilidades necesarias. Los hallazgos del estudio podrían proporcionar hipótesis, sugerencias y recomendaciones para futuras investigaciones.

## 1.5. Limitaciones de la investigación

El presente trabajo de investigación se perciben e identifican limitaciones referidas a la escasa información nacional sobre ciberdefensa, limitado acceso a información clasificada de otras FFAA en el contexto regional, restricciones sobre información de fuentes cerradas a razón de las políticas y medidas de seguridad; sin embargo no influyen en forma significativa al proceso de investigación, aspecto que se subsanaron accediendo a información de fuentes abiertas de libros, leyes, manuales, artículos, repositorios y portales especializados en el internet. Por otro lado, no se tiene limitaciones respecto al uso de recursos, disponibilidad de tiempo, entusiasmo y voluntad para desarrollar el presente trabajo de investigación.

# CAPÍTULO II
# MARCO TEÓRICO

## 2.1. Antecedentes de la investigación

### 2.1.1. *Antecedentes Internacionales*

Como un primer antecedente a esta investigación se encuentra el estudio realizado por González (2022), el cual se denominó "*Diligencias de investigación tecnológicas para la lucha contra la ciberdelincuencia*". En el estudio mencionado, el autor sostiene que los ataques cibernéticos afectan el funcionamiento de las infraestructuras críticas, y se han reconocido como amenazas que perjudican la seguridad tanto a nivel nacional como internacional. En este sentido, la tecnología desempeña un papel fundamental para hacer frente a estas amenazas y garantizar un uso seguro del ciberespacio. No obstante, las autoridades competentes desempeñan un papel estratégico en la aplicación de acciones legales en casos de ciberdelitos graves, como parte de las medidas de respuesta. A nivel local, regional y nacional, se debe garantizar un internet seguro, la Seguridad Nacional y los derechos de los ciudadanos que podrían convertirse en víctimas de ataques cibernéticos.

Nizovtsev et al. (2022) realizó un estudio sobre "*From self-affirmation to national security threat: Analyzing the Ukraine's foreign experience in countering cyberattacks*". Los autores sostienen que la finalidad de los ciberataques ya no se limita simplemente a obtener beneficios materiales ilegales directos. El objetivo de un ciberataque es desacreditar a empresas concretas o a países enteros (sus gobiernos) revelando su supuesta incompetencia y debilidad. Los objetos de los ciberataques pueden ser empresas de infraestructuras críticas, cuyo cierre sería crítico a escala nacional. El peligro de las modernas ciberguerras de grupos criminales de hackers supone una amenaza no sólo para las pequeñas, medianas y grandes empresas, sino también para la Seguridad Nacional de los distintos Estados o incluso para la seguridad de la comunidad internacional en su conjunto. Es importante destacar que la ciberdelincuencia no conoce fronteras y solo puede ser combatida mediante la colaboración entre las fuerzas del orden y los servicios de inteligencia de todos los países desarrollados.

Rincón et al. (2022) realizó un estudio sobre "*Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos?*". Según los autores, un obstáculo importante a la hora de abordar la ciberdelincuencia reside en las características inherentes al delito, que implica la utilización de herramientas tecnológicas en constante evolución.

Además, los posibles beneficios económicos que pueden obtener los ciberdelincuentes dependen de la frecuencia de sus ataques. La pandemia del COVID-19 ha puesto de relieve la importancia de las tecnologías de la información en un mundo globalizado, haciendo hincapié en la función esencial de los entornos ciberseguros que permiten a los usuarios disponer de servicios financieros sin temor a ciberataques. Los autores destacaron el aumento de informes sobre actividades fraudulentas y asaltos destinados a engañar a las personas para que divulguen su información personal a cambio de obtener ayuda o concesiones en medio de la recesión económica desencadenada por la pandemia.

Payá et al. (2017) realizó un estudio sobre "*El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito*". El autor sostuvo que la capacitación y formación del personal involucrado en la lucha contra la ciberdelincuencia es una tarea esencial que involucra a entidades gubernamentales, organizaciones empresariales e instituciones académicas. Sin embargo, cualquier programa destinado a enseñar a los participantes las técnicas y procedimientos necesarios para abordar eficazmente la ciberdelincuencia está destinado a volverse obsoleto en períodos cada vez más cortos. Esto se debe, en primer lugar, a la naturaleza cambiante de la amenaza, que se vuelve cada vez más sofisticada, compleja y extensa, lo que lleva a la continua aparición de nuevas técnicas y procedimientos para evadir las medidas de seguridad de los sistemas informáticos.

### 2.1.2. *Antecedentes nacionales*

Se encuentra el estudio de Quevedo (2023), al que denominó *"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"*. En su estudió resaltó que la defensa y seguridad cibernéticas, se han convertido en piedras angulares para preservar la estabilidad y el funcionamiento de una nación, por lo que se consideran temas cruciales en los estudios estratégicos. Sin embargo, Perú no ha logrado un mayor crecimiento en este aspecto, pese a la necesidad de su implementación y eficiencia. Consecuentemente en la actualidad, el país no invierte lo necesario en la promoción de medidas de ciberseguridad y ciberdefensa. Además, refirió que, a pesar de la baja frecuencia de batallas cibernéticas a gran escala a nivel de Latinoamérica, la Seguridad Nacional puede verse comprometida si no puede mantenerse al día con las demandas actuales. Finalmente concluyó que, para lograr estrategias efectivas de ciberdefensa y ciberseguridad, es

fundamental contar con un sistema que permita la cooperación e integración del sector público, privado y militar, a fin de cumplir con los objetivos de mantener una nación segura.

Asimismo, la investigación de Ormachea (2020) titulada *"Estrategias integradas de ciberseguridad para el fortalecimiento de la Seguridad Nacional"*, se expone que, debido a la creciente integración de la tecnología en la rutina diaria de los seres humanos, y en lo importante de su uso para el funcionamiento eficaz de sectores organizacionales, gubernamentales, entidades de defensa y para la sociedad en general; se generan mayores peligros que pueden afectar negativamente a las entidades ya descritas, si surge la presencia de posibles atacantes potenciales. Además, existen pruebas veraces de que determinadas naciones poseen competencias de inteligencia y militares para ejecutar ciberataques que ponen en peligro la seguridad del país. Por último, el análisis indicó que los factores predominantes en la formulación de políticas nacionales de ciberseguridad exhibidas por el país siguen siendo la promoción de la concienciación y la mejora de las capacidades cibernéticas militares. Frente a ello, es importante precisar que, si bien el Estado es el responsable principal del liderazgo, garantizar la ciberseguridad requiere de una obligación y responsabilidad sociales, que exige la colaboración entre los sectores privados y públicos. Sin embargo, en Perú todavía no se ha logrado esta coordinación. Por lo tanto, el desarrollo de estrategias de Ciberseguridad en la Nación es una necesidad urgente.

Por su parte, Taipe (2020) ejecutó un estudio denominado "*Sistema de Seguridad Cibernética Nacional frente a los ciberataques como amenaza a la Seguridad Nacional"*, en el cual, buscó analizar las variables ya descritas y brindar aportes e ideas que pudieran ayudar a afrontar los retos que se plantean. El estudio, resaltó la necesidad de mejorar las oportunidades formativas, educativas y de desarrollo profesional de los especialistas en ciberseguridad. También, consideró que es crucial promover la concienciación sobre la ciberseguridad en todas las etapas formativas a nivel profesional y académico de los ciudadanos. Asimismo, señaló que, si bien el establecimiento de una línea de seguridad base en sus determinadas instituciones es una obligación necesaria para la nación; no obstante, es imperativo que reconozcan que los esfuerzos individuales hacia la protección pueden no ser suficientes. Por lo tanto, para salvaguardar el ecosistema digital del Estado, es imperativo que el sistema en cuestión trabaje de manera colaborativa con sus contrapartes.

Finalmente, Astudillo (2019), efectuó un estudio titulado *"Diseño e implementación de una estrategia de Seguridad Nacional y el nivel de efectividad de la respuesta del Estado Peruano ante las amenazas a la Seguridad Nacional".* Donde tuvo por finalidad evaluar el impacto de una estrategia de Seguridad Nacional en la mejora de respuesta por parte del Estado a las amenazas de seguridad. Para ello, se examinaron las perspectivas y puntos de vista de expertos en seguridad, desarrollo y defensa nacional, en particular de aquellos con formación militar, sobre el diseño y la implementación de la citada estrategia. Los hallazgos determinaron que las estrategias de Seguridad Nacional tienen una importancia significativa y producen resultados favorables en la mejora de la eficacia de las contramedidas del gobierno peruano contra los riesgos de Seguridad Nacional.

## 2.2. Bases teóricas

Las nociones interrelacionadas de Seguridad y Defensa muestran una asociación que se refuerza mutuamente, según la cual la seguridad engendra un estado de confianza y una percepción de estar desprovisto de peligros. El concepto de seguridad se asocia a un estado de confianza y a la percepción de estar desprovisto de peligros, amenazas y riesgos. Por otro lado, la defensa se refiere a las diversas estrategias, ya sean militares o no militares, que protegen a los individuos de los peligros, amenazas y riesgos antes mencionados (Valencia-Arias et al., 2020).

Según Vargas (2008), los defensores de la seguridad pretenden garantizar la libertad individual mediante esfuerzos colectivos, mientras que los mecanismos de defensa se ponen en marcha para proteger y preservar a la comunidad respondiendo a las amenazas potenciales, infundiendo así una sensación de seguridad entre la población. Los conceptos mencionados están entrelazados y son intrínsecos al sustento y el avance de la sociedad, sobre todo cuando las naciones establecen su marco social y político en función de su capacidad para reaccionar y salvaguardarse frente a peligros potenciales. Esto quiere decir que todas las naciones deben estar equipadas para salvaguardar a sus ciudadanos de posibles amenazas, peligros y riesgos.

### 2.2.1. *Seguridad Nacional*

La Seguridad Nacional es el establecimiento de un marco global que comprenda factores políticos, económicos, militares, sociales y culturales es imperativo para garantizar la consecución de la soberanía, la independencia y el avance de los intereses nacionales. Este

marco debe reforzar los elementos constitutivos del proyecto nacional al tiempo que mitiga cualquier deficiencia o incongruencia que pudiera crear vulnerabilidades ante fuerzas externas (Ortega, 2018).

La política de Seguridad Nacional de Perú pretende incorporar y sincronizar eficazmente los esfuerzos de las diversas partes implicadas en las distintas facetas, con el fin de hacer frente a los intereses y amenazas más significativos. Algunas naciones carecen de un manuscrito de política de Seguridad Nacional global e integrado, y en su lugar dependen de las políticas de defensa o de los libros blancos. Este es el caso de Perú, donde dichos documentos se centran exclusivamente en cuestiones de defensa nacional. Algunos Estados se abstienen de divulgar los documentos que sustentan sus políticas o carecen de políticas de seguridad o defensa completas por escrito.

Cabe resaltar que la estabilidad y prosperidad de Perú dependen en gran medida de la seguridad y fiabilidad del ciberespacio. Esto se debe al impacto sustancial de los sistemas de información y telecomunicaciones en la economía y los servicios públicos. Sin embargo, estos atributos pueden verse socavados por factores técnicos, fenómenos naturales u hostilidades intencionadas. La creciente dependencia de la sociedad de las Tecnologías de la Información y la Comunicación (TIC) ha llevado a una mayor importancia de garantizar la protección y disponibilidad de estos recursos cruciales como una cuestión de importancia nacional (Taipe, 2017).

La ocurrencia de eventos que provoquen la perturbación de infraestructuras esenciales y servicios de tecnologías de la información y la comunicación (TIC) puede tener consecuencias adversas sustanciales en el funcionamiento tanto de la economía como de la sociedad. El establecimiento de un ciberespacio seguro se ha revelado como un reto primordial del siglo actual. En consecuencia, la seguridad informática ha ganado reconocimiento como preocupación nacional a nivel estratégico, con implicaciones para todos los estratos de la sociedad

#### 2.2.1.1.La seguridad cibernética.

La seguridad cibernética se refiere a las medidas adoptadas para prevenir o mitigar los efectos negativos de las interrupciones, fallos o uso inadecuado de las tecnologías de la información y la comunicación (TIC). Además, abarca las medidas adoptadas para rectificar cualquier daño que ya se haya producido. Rollano (2012) expone que las posibles

consecuencias negativas del uso de las TIC pueden abarcar una serie de cuestiones, entre las que se incluyen la fiabilidad comprometida, la accesibilidad restringida y la violación de la confidencialidad y/o integridad de los datos alojados en los sistemas de TIC (Amandeep et al., 2018).

La responsabilidad de mejorar la resiliencia digital no puede atribuirse únicamente al gobierno, dado que la infraestructura de las TIC y el conocimiento asociado residen predominantemente en dominios privados, nacionales e internacionales. La ciberseguridad es un esfuerzo colectivo de agencias gubernamentales, empresas, organizaciones e individuos, tanto a nivel nacional como mundial, como afirman Vargas et al. (2017), las líneas de demarcación entre seguridad exterior e interior son cada vez más indistintas, y la delegación de responsabilidades entre distintas entidades y ministerios ya no es un planteamiento satisfactorio para abordar los nuevos problemas de seguridad que surgen en el ámbito del ciberespacio.

La mitigación de estos ataques es un esfuerzo multifacético, debido al impacto de varios factores. Un aspecto destacado es la susceptibilidad de numerosos objetivos a los ataques, que son competencia de empresas privadas, lo que hace necesaria la aplicación de medidas por parte de estas entidades para salvaguardar sus sistemas. Esto sugiere que la asunción de costes puede ser recibida con reticencia y puede dar lugar a riesgos sustanciales. La falta de concienciación en materia de seguridad en determinados segmentos de la población plantea un reto a la hora de aplicar y sincronizar medidas eficaces, como señala Leiva (2015).

El ámbito de la ciberseguridad se considera un aspecto crucial de la Seguridad Nacional, que requiere la formulación de una estrategia global por parte de los gobiernos. Esta estrategia debe incorporar la participación tanto del sector público como del privado, al tiempo que debe estar en consonancia con la preservación de los derechos y libertades individuales. Además, es imperativo que esta estrategia esté sincronizada con otras medidas destinadas a identificar diversas amenazas, así como a establecer sistemas de respuesta y recuperación ante contingencias. Por otra parte, fomentar la colaboración internacional es imperativo para lograr tratados internacionales y cooperación, como se demostró tras el brote de Petya.

Álvarez (2018) afirma la necesidad de ejecutar Estrategias Nacionales de Ciberseguridad (ENC) a escala mundial. Estos esfuerzos tienen como objetivo encapsular la perspectiva del órgano de gobierno de una nación para abordar la cuestión de la administración de la ciberseguridad a escala mundial. Los objetivos de estas estrategias no se limitan únicamente a salvaguardar la seguridad de los ciudadanos y las infraestructuras vitales de la nación, sino que también abarcan la creación de un entorno que promueva la colaboración entre los sectores público y privado, así como la colaboración internacional. El razonamiento anterior subraya el carácter indispensable de la ciberseguridad como componente crucial de los ámbitos social y económico.

La proliferación de herramientas ofensivas ha conducido a una reducción del nivel de conocimientos necesarios para que un atacante ejecute con éxito un ataque contra los sistemas de información, la calidad, cantidad y accesibilidad de dichas herramientas han aumentado con el tiempo. En la actualidad, existe una considerable facilidad para acceder a herramientas de hacking ético en Internet que se basan en conocimientos informáticos y de seguridad para escudriñar las redes e identificar posibles vulnerabilidades, que posteriormente pueden denunciarse sin causar ningún daño (Leiva, 2015).

Además, existen herramientas informáticas forenses y de seguridad informática, entre otras, que se emplean con fines nefastos. Las circunstancias mencionadas presentan un nuevo conjunto de peligros que obligan al gobierno peruano a diseñar tácticas y políticas, y a reconocer la ciberseguridad como un peligro que exige atención para mejorar la seguridad general del país. El desarrollo de una estrategia nacional de ciberseguridad se considera un aspecto crucial de la Seguridad y Defensa de una nación, ya que mejora la resistencia de sus infraestructuras y servicios de información. En los niveles superiores de la toma de decisiones del Estado, se formula una estrategia nacional que esboza un conjunto de objetivos y prioridades que deben cumplirse en un plazo determinado. Según Taipe (2017), este marco ofrece un enfoque estratégico para los esfuerzos de ciberseguridad de un país.

#### *2.2.1.2.* Áreas de seguridad cibernética.

Los dominios subsiguientes de la ciberseguridad exigen una priorización en términos de inversión y un mayor enfoque de liderazgo:

La primera área es la eficiencia de la inversión, que alude a la mejora de las competencias internas con el fin de promover inversiones prudentes en ciberseguridad y maximizar la asignación de recursos financieros y materiales. Llevar a cabo un análisis de las inversiones realizadas por la organización con respecto a la evaluación comparativa, la alineación con los objetivos de la organización y las tendencias imperantes en materia de ciberseguridad. La gestión de activos puede presentar dificultades para las entidades gubernamentales, aunque representa un elemento esencial de cualquier iniciativa de seguridad.

La segunda área es el contexto estratégico de amenazas, que motiva a los demás a investigar amenazas concretas a la ciberseguridad, como la realización de una evaluación de riesgos geopolíticos, y para reconocer iniciativas y tecnologías relacionadas con la ciberseguridad que estén implantando organizaciones comparables. La aplicación de estas medidas garantiza que el programa de seguridad de un organismo esté en consonancia con sus objetivos estratégicos generales.

La tercera área es la resistencia cibernética, donde se lleva a cabo la evaluación de la capacidad de la organización para alcanzar la excelencia operativa a pesar de la presencia de adversarios cibernéticos perturbadores, y se utiliza la aplicación de metodologías de "diseño para la resiliencia" con el fin de mitigar los efectos de un posible ataque. El establecimiento de un sólido plan de respuesta, la provisión de vías eficientes de escalada de incidentes cibernéticos y la promoción de la participación integral de las partes interesadas en todas las funciones de la agencia son componentes cruciales de la preparación de la respuesta cibernética. Evaluar la aptitud de colaboración de los miembros del equipo de pruebas en el contexto de escenarios de gestión de crisis.

La cuarta área es la exposición de la agencia, donde se evalúa los escenarios de incidentes de ciberseguridad se lleva a cabo para conocer aquellos que tienen el potencial de afectar significativamente a la organización. Determinar los elementos cruciales, los momentos cruciales y los obstáculos que intervienen en la formulación de enfoques correctivos y transformadores.

Por último, el área de gobernanza, que se centra en promover la responsabilidad para cultivar una cultura orientada a la ciberseguridad, medir y divulgar el rendimiento de la ciberseguridad, idear incentivos de ciberseguridad atractivos para el personal y establecer una jerarquía de ciberseguridad bien definida. Es imperativo que los líderes redefinan la

noción de éxito de la ciberseguridad más allá de la mera consecución de los objetivos de cumplimiento. Alcanzar un grado adecuado de visibilidad e influencia reviste una importancia capital para detectar y abordar con prontitud posibles violaciones de la seguridad.

### 2.2.2. *Ciberdelincuencia.*

INTERPOL (2021) ha identificado una serie de actividades ilícitas que actualmente están experimentando un crecimiento significativo. Estas actividades implican principalmente ataques cibernéticos contra gobiernos, entidades, empresas y particulares, que resultan en violaciones de sus derechos e integridad. Según UNIR (2020), existe un conjunto de acciones o actividades que se llevan a cabo mediante el uso de medios tecnológicos y se cometen de forma ilícita. Estos ataques se dirigen específicamente contra individuos, empresas y gobiernos. Deptris (2021) concluye que la ciberdelincuencia se refiere a actividades ilícitas que implican operaciones técnicas y electrónicas que ponen en peligro la seguridad de los sistemas informáticos, lo que supone una amenaza para la seguridad interna de una empresa o el bienestar económico de un individuo.

#### *2.2.2.1.* **Entes que desarrollan ciberdelincuencia.**

Se puede caracterizar como tal a un grupo de individuos que poseen un motivo u objetivo común dentro de un entorno compartido. La entidad social surge de la mediación de normas y culturas entre individuos. Las entidades sociales pueden observarse tanto a nivel macroeconómico como microeconómico, abarcando desde naciones hasta grupos de individuos.

##### *2.2.2.1.1. Hackers.*

Un hacker es un individuo responsable del acceso remoto no autorizado a través de redes de comunicación, que pueden incluir Internet, entre otras posibilidades. Esta afirmación denota que el alcance del término se extiende a las personas que participan en el proceso de detección y rectificación de errores y disfunciones dentro de un sistema (Pandasecurity, 2019).

Cabe resaltar que los hackers tienen su propia categoría, la cual se divide en:

En primer lugar, se mencionan a los hackers de sombrero negro son personas que acceden sin autorización a sistemas informáticos con la intención de causar daños o cometer actividades ilegales. Es posible que los actores maliciosos desplieguen programa maligno con la intención de causar daños a documentos digitales, requisar sistemas informáticos o robar datos confidenciales como contraseñas, información de tarjetas de crédito o datos de identificación personal. Los motivos de sus ataques suelen ser venganzas personales, beneficios económicos, represalias o el mero deseo de infundir miedo. En ocasiones, los individuos pueden estar motivados por la ideología, lo que los lleva a atacar entidades o individuos con los que no comparten creencias similares. Normalmente, estos hackers inician sus actividades como "script kiddies", es decir, personas sin experiencia que aprovechan el software de hacking disponible en el mercado para explotar vulnerabilidades específicas del sistema. Según Red (2022), ciertos individuos reciben formación de hackers expertos con el objetivo de generar rápidas ganancias económicas.

Los grupos de sombrero negro colaboran frecuentemente con organizaciones delictivas, dedicándose a actividades comerciales. Las bandas reciben herramientas de hacking o kits de programa maligno, que van acompañados de garantías y servicio de atención al cliente. Con frecuencia, se dedican a la creación de instrumentos de phishing o de control de acceso remoto. La mayoría de estos individuos obtienen sus oportunidades de empleo a través de la utilización de la dark web. La mayoría de los individuos que se dedican a actividades de hacking muestran preferencia por la creación y venta de software malévolo. Sin embargo, existe un subconjunto de hackers que optan por alquilar dichas herramientas con el fin de ejecutar sus ataques. Según Mateos (2013), el trabajo solitario es el más frecuente entre los anarquistas debido a su naturaleza individualista. Sin embargo, hay casos en los que algunos anarquistas optan por afiliarse a grupos criminales, ya que les ofrece la oportunidad de obtener beneficios económicos rápidos y sin esfuerzo.

En segundo lugar, se mencionan a los hackers de sombrero gris ocupan una posición intermedia entre los hackers de sombrero blanco y los de sombrero negro. Estas categorías de piratas informáticos generalmente buscan vulnerabilidades del sistema sin el permiso explícito o la conciencia del propietario. Cuando descubren una vulnerabilidad, suelen notificarlo al propietario del sistema o del software en cuestión y pueden solicitar una cantidad simbólica para subsanarla. Algunos hackers de sombrero gris creen que la intrusión no autorizada en los sistemas y redes de las empresas puede ser beneficiosa para las mismas, a pesar de que estas entidades no suelen permitir el acceso no autorizado a sus sistemas. Los

hackers de sombrero gris ocasionalmente exceden los límites de la legalidad o las normas éticas, sin embargo, a diferencia de los hackers de sombrero negro, sus intenciones no son maliciosas. Algunas personas tienen la creencia de que Internet es un entorno inseguro para realizar negocios, y su razonamiento se ve respaldado por una serie de incidentes de piratería informática. Según Mateos (2013), los hackers no suelen infligir daños a los sistemas que violan, y pueden hacerlo por curiosidad o para evaluar su destreza como piratas informáticos.

#### *2.2.2.1.2. Crackers.*

Del mismo modo, los crackers se consideran individuos que participan en el acto de piratear u obtener acceso no autorizado a sistemas informáticos. La motivación de las acciones de los crackers puede atribuirse a una multitud de factores, incluyendo la búsqueda de beneficios económicos, la articulación de la oposición o la manifestación de inclinaciones insurgentes (Pandasecurity, 2019).

#### *2.2.2.1.3. Piratas.*

Según Mateos (2013) los piratas informáticos se dedican a la reproducción y difusión no autorizada de diversas formas de contenido, como software, música, juegos y otros materiales, violando así las leyes de propiedad intelectual y los derechos de los propietarios de los contenidos.

#### *2.2.2.1.4. Organizaciones delictivas.*

Existen varias definiciones de organizaciones delictivas, que dependen del autor y del campo de estudio. Sin embargo, estas definiciones suelen compartir las características comunes de implicar a múltiples individuos, dedicarse a múltiples actividades ilícitas y mostrar longevidad. Las variaciones entre el contrabando y otros delitos relacionados dependen de varios factores, entre otros: el número de casos del delito, si el acto se considera un delito o simplemente ilícito (dependiendo de la jurisdicción, el contrabando puede considerarse solo una infracción), la presencia de una pena mínima para el delito (como en el caso del robo o la suplantación de identidad, que pueden no cumplir los criterios necesarios), la duración del tiempo necesario para que se establezca una organización y la aparición de violencia durante la comisión del delito (Dupuy, 2019).

Algunas organizaciones emplean herramientas digitales para la comisión de sus actividades ilícitas. El factor distintivo entre las diversas actividades delictivas es el método empleado y no la categoría del delito, como la ciberdelincuencia. La justificación de esta diferenciación reside en el hecho de que la utilización de tecnologías digitales crea una disparidad crucial para estas entidades, ya que permite una reducción sustancial del riesgo (Ferrazzuolo, 2019).

### 2.2.3. *Estrategia para enfrentar la ciberdelincuencia*

La noción de estrategia se utiliza ampliamente en varias disciplinas, incluyendo un plan o una serie de actividades planificadas ejecutadas para abordar eficazmente un problema y obtener resultados óptimos. La estrategia es el proceso de deliberar y formular opciones, así como de idear planes de acción, para afrontar eficazmente una situación dada y alcanzar los objetivos previstos (Naranjo, 2018). Una estrategia puede conceptualizarse como un enfoque sistemático o una serie de actividades deliberadas que se ponen en práctica para abordar eficazmente un problema o reto con el objetivo de obtener resultados óptimos. La orientación de este enfoque es alcanzar eficazmente un objetivo predeterminado mediante la adhesión a un conjunto prescrito de acciones. El uso de la noción de estrategia se observa en varios ámbitos, como el militar, el empresarial, el educativo y el político, entre otros (Maldonado-Mera et al., 2017).

La estrategia militar es una disciplina estrechamente vinculada a la política y abarca diversos elementos, como la recopilación de información, la evaluación y la planificación. También implica la utilización de instrumentos de conflicto, lo que supone identificar tanto las oportunidades como las amenazas dentro del entorno militar. Además, la estrategia militar abarca el establecimiento de objetivos y metas a largo plazo, la asignación de recursos y la ejecución de acciones encaminadas a alcanzar los objetivos predeterminados. Según Segura (2021), en esencia, la estrategia militar es todo el proceso de formulación y supervisión de las operaciones bélicas, junto con el despliegue estratégico y la disposición de las tropas armadas. La estrategia militar abarca las dimensiones políticas de la guerra, el discernimiento de los factores ventajosos y desventajosos dentro del contexto militar, el establecimiento de objetivos y fines duraderos, la distribución de recursos y la ejecución de medidas para alcanzar los objetivos establecidos.

La formulación de una estrategia para enfrentar la ciberdelincuencia implica la delineación de medidas esenciales para el establecimiento de una sólida gobernanza de los datos dentro de la organización y la adopción de sólidas prácticas de ciber higiene personal, con el objetivo último de reducir las ramificaciones financieras de la ciberdelincuencia. Este enfoque debe proporcionar ayuda en la lucha contra el terrorismo y la prevención del blanqueo de capitales, al tiempo que restringe los canales de financiación de los grupos delictivos organizados. Por consiguiente, es imperativo que funcione en conjunción con un enfoque de ciberseguridad para garantizar el funcionamiento ininterrumpido de los servicios esenciales, como se prescribe en la Guía de Estrategia Nacional contra la Ciberdelincuencia (INTERPOL, 2021).

#### *2.2.3.1.* Capacidad del personal especializado.

La capacidad se refiere a la capacidad de ejecutar una tarea de acuerdo con criterios establecidos, utilizando una variedad de métodos y recursos, que pueden agotarse con el tiempo y/o gastarse con el uso. (Ministerio de Defensa, 2018).

El dominio de las herramientas de análisis forense es esencial, ya que sirven para dilucidar los factores causales y recopilar información pertinente relativa a un incidente. Los analistas forenses deben poseer una serie de recursos, incluidas herramientas de software y hardware, así como un conjunto bien definido de procedimientos, metodologías y mejores prácticas para la adquisición de pruebas digitales (Rada, 2022).

Para llevar a cabo un análisis forense digital eficaz, los investigadores informáticos forenses deben poseer los conocimientos y habilidades necesarios para cada fase del análisis forense en diversas fuentes de datos (Rada, 2022).

También es imperativo que los individuos posean una ciber inteligencia. definida por RSA (2012) como la comprensión de los adversarios cibernéticos y sus tácticas, así como la comprensión de la postura de seguridad de una organización en relación con sus adversarios en el ámbito digital y sus tácticas. Las organizaciones obtienen inteligencia procesable a partir de esta información. Una definición que se encuentra con frecuencia, pero que se considera demasiado restrictiva, se refiere al examen de las capacidades, motivaciones e iniciativas de un enemigo en el ámbito del ciberespacio. La definición del término en cuestión, proporcionada por INSA (2015), es más precisa y global. Se refiere a los productos y procesos implicados en el ciclo de inteligencia, que se utilizan para examinar las

capacidades, intenciones y actividades de los adversarios y competidores potenciales en el ciberespacio, sin limitarse a los aspectos técnicos.

Además, se necesita de las técnicas de ethical hacking, donde es posible salvaguardar la privacidad digital de los usuarios y mitigar de forma proactiva los posibles ciberataques. La cuestión de los riesgos cibernéticos se perfila cada vez más como un importante ámbito de preocupación para diversas organizaciones. En resumen, los ethical hacking realizan un análisis de seguridad es el más profundo, ya que pretende realizar una evaluación exhaustiva de la seguridad de los sistemas de información, con el objetivo de identificar posibles vulnerabilidades que puedan suponer una amenaza para una organización (Gaona et al., 2019).

#### *2.2.3.2.*Recursos materiales y tecnológicos.

Por recurso se entiende cualquier forma de medio que facilite el cumplimiento de un requisito o la consecución de un objetivo deseado. En cambio, la tecnología se refiere a los principios y metodologías que facilitan la aplicación pragmática de los conocimientos científicos (Diaz, 2018).

##### *2.2.3.2.1. Recursos materiales.*

Los recursos materiales se refieren a las entidades utilizadas con el fin de procesar o transformar, o las que se someten a procesamiento o transformación, dentro del proceso de producción de una mercancía o amenidad.

##### *2.2.3.2.2. Recursos tecnológicos.*

Los recursos tecnológicos se refieren a los componentes que surgen de los avances científicos y técnicos, que permiten o simplifican una tarea concreta, especialmente en el ámbito de la productividad (Diaz, 2018).

Dentro de los recursos tecnológicos se encuentran las herramientas de análisis informático donde se encuentran las herramientas:

Herramientas de disco y captura de datos que los analistas forenses utilizan herramientas de tratamiento de imágenes para extraer imágenes de discos duros con fines de investigación, así como para proteger, reparar y mejorar el rendimiento del disco duro investigado. Estas herramientas también ayudan a optimizar el espacio en disco, recuperar

información eliminada y capturar datos en diversos formatos como imágenes, vídeos, documentos, PDF y textos que existen en el sistema informático.

Herramientas de análisis de registro que facilitan la obtención de datos exhaustivos relativos a los registros producidos en sistemas informáticos equipados con el sistema operativo Windows, así como las instancias de instalación de programas. Los registros pueden abarcar una serie de datos, entre los que se incluyen la configuración del usuario del sistema, la ruta de acceso a los archivos y los permisos de acceso, los archivos o carpetas, los archivos ejecutados, la configuración del sistema, la dirección IP de la red y las aplicaciones instaladas y en ejecución.

Herramientas de análisis de correcto electrónico, donde cabe destacar que los ciberataques dirigidos a organizaciones, gobiernos y particulares, incluidos, entre otros, los engaños digitales, las estafas, el robo de datos, el phishing, la propagación de códigos maliciosos, los insultos o las amenazas, se ejecutan habitualmente mediante la transmisión de correos electrónicos con el objetivo de llegar a víctimas concretas. Los analistas forenses necesitan herramientas especializadas para localizar pruebas creíbles relativas a datos de correo electrónico modificados o borrados, con el fin de recuperar la información inicial, que incluye, entre otros datos, la fecha de creación, la fecha de transmisión, el remitente original y las cabeceras.

Herramientas de forense de red, que se utilizan para detectar e investigar actividades de red potencialmente maliciosas, identificar casos de programa maligno, conexiones de red anómalas y discernir patrones de ataque.

Herramientas de adquisición y análisis de memoria, donde esta tecnología facilita la recuperación y el examen exhaustivo de los datos almacenados en un dispositivo móvil, al tiempo que garantiza la salvaguarda de la integridad del dispositivo durante el proceso de análisis. Este proceso facilita la recuperación de datos o comandos almacenados en la memoria de acceso aleatorio (RAM) con el fin de realizar un análisis destinado a identificar posibles pruebas.

Herramientas de recuperación de contraseñas que permite acceder a diversas plataformas digitales como correos electrónicos, sistemas informáticos, aplicaciones, documentos y sitios web que requieren la autenticación de contraseñas. Este proceso facilita

la extracción de información relevante que puede servir como prueba digital para fines de investigación.

Herramientas de análisis de programa maligno, se utilizan para identificar el componente específico de un sistema o red que se ha visto comprometido y para autenticar la forma en que se produjo la violación de la seguridad dentro del sistema.

## 2.3. Base normativa

El marco jurídico legal hace referencia al conjunto de leyes, normas, decretos, reglamentos y otros instrumentos de gobierno obligatorios o indicativos que se aplican en un país, estado o institución determinados (Tenorio, 2021).

## 2.4. Definiciones conceptuales

**Capacidad:** Es el resultado de una combinación de factores que permiten la aplicación de procedimientos operativos, con el fin de alcanzar un resultado militar deseado a nivel estratégico, operativo o táctico. Esto ocurre durante la ejecución de operaciones y acciones militares, que se emprenden para hacer frente a amenazas, retos o preocupaciones en el cumplimiento de funciones estratégicas (Ministerio de Defensa, 2017).

**Ciberataque:** Es un acto de intrusión en una red informática con la intención de cometer actividades delictivas. El criminal se esfuerza por conseguir una entrada no permitida a los datos, o por modificar u obstruir el funcionamiento de los servicios (Camps, 2016).

**Ciberdefensa:** Capacidad militar para responder y contrarrestar las amenazas o agresiones que se produzcan en el ámbito del ciberespacio, especialmente cuando supongan un riesgo para la seguridad nacional (Ley N° 30999).

**Ciberdelincuencia:** Refiere a cualquier acción intencionada de una persona, donde ilegalmente manipule, añada, borre, degrade, modifique, suprima o haga inaccesibles datos informáticos será condenada a una pena de tres a seis años de cárcel y a una multa de 80 a 120 días (Ley N°30096).

**Ciberseguridad:** Es la capacidad tecnológica para mantener el funcionamiento óptimo de redes, activos y sistemas, así como para protegerlos frente a posibles amenazas y vulnerabilidades en el ámbito digital (Decreto de Urgencia N.° 007-2020).

**Cracker:** Son personas que se dedican a la piratería informática o al acceso no autorizado a sistemas informáticos. El ímpetu detrás de las acciones de los crackers puede atribuirse a una plétora de factores, como la búsqueda de beneficios económicos, la expresión de disidencia o la manifestación de tendencias rebeldes (Pandasecurity, 2019).

**Ente:** Se puede caracterizar como tal a un grupo de individuos que poseen un motivo u objetivo común dentro de un entorno compartido

**Estrategia:** Implica la delineación de medidas esenciales para el establecimiento de una sólida gobernanza de los datos dentro de la organización y la adopción de sólidas prácticas de ciber higiene personal, con el objetivo último de reducir las ramificaciones financieras de la ciberdelincuencia.

**Ethical hacking:** Realizan un análisis de seguridad es el más profundo, ya que pretende realizar una evaluación exhaustiva de la seguridad de los sistemas de información, con el objetivo de identificar posibles vulnerabilidades que puedan suponer una amenaza para una organización (Gaona et al., 2019).

**Hacker:** Es un individuo responsable de acceso remoto ilícito a través de redes de comunicación, incluyendo, pero no limitado a Internet. También engloba a los individuos que se dedican a la identificación y resolución de errores y disfunciones del sistema (Pandasecurity, 2019).

**Marco jurídico-legal:** Hace referencia al conjunto de leyes, normas, decretos, reglamentos y otros instrumentos de gobierno obligatorios o indicativos que se aplican en un país, estado o institución determinados (Tenorio, 2021).

**Organización delictiva:** Implican acciones de múltiples individuos, dedicarse a múltiples actividades ilícitas.

**Piratas informáticos:** Según Mateos (2013) los piratas informáticos se dedican a la reproducción y difusión no autorizada de diversas formas de contenido, como software, música, juegos y otros materiales, violando así las leyes de propiedad intelectual y los derechos de los propietarios de los contenidos.

**Recurso material:** Se refieren a las entidades utilizadas con el fin de procesar o transformar, o las que se someten a procesamiento o transformación, dentro del proceso de producción de una mercancía o amenidad (Diaz, 2018).

**Recurso tecnológico:** Se refieren a los componentes que surgen de los avances científicos y técnicos, que permiten o simplifican una tarea concreta, especialmente en el ámbito de la productividad (Diaz, 2018).

**Seguridad Nacional:** Es un marco global que engloba un conjunto de principios, normas, procedimientos, técnicas, instrumentos y elementos del Estado interconectados. Su objetivo primordial es garantizar la salvaguarda de la seguridad de una nación mediante la formulación, planificación, dirección, preparación, ejecución y supervisión de acciones en todos los ámbitos de la defensa nacional (Sistema de Defensa Nacional, 2015).

# CAPÍTULO III
# METODOLOGÍA

## 3.1. Diseño Metodológico

### *3.1.1. Enfoque de investigación*

El enfoque es cualitativo, dado que se centra en comprender y analizar el significado y los atributos de un acontecimiento o problema social a través de la lente de sus integrantes. A diferencia de los métodos cuantitativos, que utilizan medidas numéricas, la investigación cualitativa emplea la recopilación y el examen de datos descriptivos, como entrevistas, observaciones y documentos, para comprender las experiencias intrincadas y subjetivas de los individuos.

### *3.1.2. Tipo de investigación*

Según su finalidad es básica, porque se realiza con el objetivo de mejorar los conocimientos teóricos y la comprensión de una materia específica, sin una aplicación inmediata en entornos prácticos. En este contexto, este estudio se alinea con la investigación básica al perseguir la mejora y ampliación del conocimiento teórico en la temática de ciberdelincuencia, y su impacto en la seguridad nacional del país, con la finalidad de contribuir al cuerpo de teoría en este campo.

Según su carácter es descriptiva, ya que se da prioridad a la explicación y comprensión de los atributos y componentes que constituyen un determinado problema o circunstancia. El objetivo es presentar una descripción precisa y exhaustiva de los datos y sucesos observados, sin dilucidar ni evaluar necesariamente las conexiones causales entre ellos.

Según su alcance temporal es transversal, ya que se llevó a cabo mediante un diseño transversal, en el que se recopilaron los datos de varios participantes o partes interesadas al mismo tiempo, ya sea en un único momento o en un breve espacio de tiempo.

### *3.1.3. Método*

El método es de análisis porque el proceso puede implicar la utilización de técnicas de codificación para organizar los datos, el establecimiento de categorías temáticas y la identificación de interrelaciones entre ellas.

### *3.1.4. Diseño*

El proceso de análisis documental implica el escrutinio y la evaluación de material escrito, incluidas publicaciones científicas, informes, libros y otros documentos pertinentes. El objetivo es extraer la información pertinente y ordenarla de forma estructurada. La utilización de esta forma de análisis es frecuente en diversos ámbitos de investigación, como la erudición académica, la administración de la información y la clasificación documental.

## 3.2. Población y muestra

### 3.2.1. *Población de estudio*

Material bibliográfico relacionado a las unidades temáticas a la que se tenga acceso, expertos y personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional de Perú, perteneciente a las diferentes instituciones gubernamentales que se dedican a brindar la Seguridad Nacional (Dirección Nacional de Inteligencia, FFAA, Policía Nacional del Perú, entre otros).

### 3.2.2. *Muestra*

Todo material bibliográfico relacionado a las unidades temáticas a la que se tenga acceso y sea pertinente para la investigación, y al personal encargado de enfrentar la ciberdelincuencia que altera la Seguridad Nacional de Perú, siendo expertos en la temática. Siendo así que, se entrevistaron a las siguientes personas: Gral. Brig. EP Emanuel Pajuelo Barba (E. P. B.), como comandante en el Comando Operacional de Ciberdefensa del Comando Conjunto; Tte. Crl. EP David Rumiche Burga (D. R. B.), como comandante la Unidad Conjunta de Ciberdefensa; Cap. EP Víctor Irrazabal Gómez (V.I.G.) como Oficial de Planeamiento del Comando de Ciberdefensa del Comando Conjunto; capitán de corbeta MGP Luis Meza Medina (L.M.M.), como jefe de la sección de Operaciones (M-3) en la Comandancia de Ciberdefensa de la MGP, Cap. PNP Diaz Rifasto Walter (D.R.W.), como jefe del DIVINDAT; y Cap. PNP Guido Mullini Cutipa (G.M.C.), como jefe de la Sección de inteligencia de la DINI.

## 3.3. Temas, categorías de análisis o unidades temáticas

Seguridad Nacional

Ciberdelincuencia

- Entes que desarrollan ciberdelincuencia en contra de Perú
- Hackers
- Crackers
- Piratas informáticos
- Organizaciones delictivas

Estrategia para enfrentar la ciberdelincuencia

- Marco jurídico – legal
- Capacidad del personal especializado
- Recursos materiales y tecnológicos

## 3.4. Formulación de hipótesis

La estrategia que debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú, es una integral en donde implica la labor de las diferentes instituciones del Estado y que considera:

- Identificar los entes que desarrollan la ciberdelincuencia, a fin de combatirlos o neutralizarlos.
- La necesidad de un marco legal
- La capacidad que presenta el personal especializado para enfrentarla
- Los recursos materiales y tecnológicos que pueden emplearse

## 3.5. Técnicas e instrumentos de recolección de datos

### 3.5.1. *Técnicas*

La técnica fue el análisis documental, pues se aplicó un proceso sistemático que implica examinar y evaluar documentos, como artículos científicos, informes, libros y otros materiales escritos, con el objetivo de extraer información relevante y organizarla de manera estructurada, y se utiliza en diferentes campos de estudio, como la investigación académica, la gestión de información y la catalogación bibliotecaria.

Otra de las técnicas fue la entrevista, que normalmente implica un intercambio estructurado o semiestructurado de preguntas y respuestas entre el entrevistador y el

entrevistado (ver anexo 2). El objetivo principal de esta interacción es recabar información pertinente sobre un tema concreto, y en esta ocasión consistió en preguntas acerca de aspectos que vulneran la Seguridad Nacional de Perú.

### 3.5.2. *Instrumentos*

Los instrumentos fueron la ficha bibliográfica porque consistió en un registro o tarjeta que contiene información básica sobre un documento, como el título, el autor, el año de publicación, la editorial y otros datos relevantes, se utilizan para organizar y localizar fácilmente la información de los documentos en una biblioteca o base de dato. También se empleó la ficha de análisis que incluye un resumen o síntesis del contenido del documento, así como también comentarios o notas del analista que destaquen aspectos relevantes o interesantes. Esta ficha proporcionó una visión más detallada y crítica del documento, lo que facilita la revisión y el uso posterior de la información.

Por último, se utilizó una guía de entrevista, la cual ofreció al entrevistador un marco y una orientación que permitió la adaptabilidad necesaria para acomodar las respuestas y observaciones del entrevistado. Es por ello por lo que se realizó la validación de expertos de la entrevista semiestructurada empleada en el presente estudio, con la V de Aiken, las preguntas estaban muy relacionadas con los problemas tanto general como específicos de la presente tesis, es así como cinco especialistas en el área señalaron que se cumple con los criterios de claridad, coherencia y relevancia. Del mismo modo se obtuvo una puntuación de 0.8, lo cual evidencia que el instrumento es válido (ver anexo 5).

## 3.6. Técnicas para el procesamiento de la información

En el proceso de procesamiento de información se emplearon las técnicas de análisis de contenido y el método PESTEL. Inicialmente, se realizó la recopilación exhaustiva de informaciones relevantes, seguida de una fase de clasificación y organización de la información recopilada, y posteriormente se aplicó el análisis de contenido para examinar detalladamente el significado y la relevancia de los datos, identificando patrones y tendencias de los hallazgos y las respuestas de las entrevistas.

También se utilizó la técnica de PESTEL, pues ayudó a comprender los factores contextuales de la realidad de la Seguridad Nacional y la ciberdelincuencia, con el objetivo de explorar los diversos factores como las dimensiones: Política, Económica, Social,

Tecnológica, Ecológica y Legal. Sin embargo, para el presente estudio solo se consideraron la dimensión política, puesto que se revisaron los acuerdos internacionales y nacionales, las leyes implicadas, y las políticas relacionadas a la temática que pueden ayudar a mejorar la Seguridad Nacional; también se evaluó la dimensión económica, puesto que la estrategia que se propuso puede provocar impacto en el área; también se incluye la dimensión de la tecnología, pues dentro de la estrategia se mencionó los recursos materiales y tecnológicos que aportan el sustento de la estrategia; y por último, se consideró la estrategia legal, ya que están implicadas las normas, leyes y resoluciones que ayudan a enfrentar la ciberdelincuencia. Por otro lado, no se considera relevante el evaluar la dimensión ecológica, ni la social.

### 3.7. Aspectos éticos

Los documentos pertinentes utilizados para la selección de información en la investigación se citaron y referenciaron adecuadamente. Del mismo modo, cualquier información adicional fue objeto de escrutinio y se acompañó de un análisis personal para garantizar la originalidad y evitar el plagio.

# CAPÍTULO IV
# RESULTADOS DE LA INVESTIGACIÓN

Perú pertenece al Convenio de Budapest, el cual es un tratado internacional destinado a abordar y eliminar la ciberdelincuencia. Los principales delitos informáticos se pueden clasificar en varios grupos, entre ellos los delitos contra la intimidad, los delitos relacionados con el contenido, la piratería, el sabotaje y las violaciones de la propiedad intelectual. Es importante reconocer que existe una correlación entre la ciberdelincuencia y la delincuencia informática, y no es posible prescindir de un concepto sin tener en cuenta el otro (Núñez y Carhuancho, 2020).

## 4.1. Entes que desarrollan ciberdelincuencia en contra de Perú

Los actos de ciberdelincuencia se realizan mediante los medios digitales, especialmente medios sociales, u otras plataformas con las cuales tienen llegada a los ciudadanos, normalmente la delincuencia tiene como medios la estafa y la extorsión del ciudadano mediante el ciberespacio para lograr sus fines, y este tipo de ciberdelincuencia es la que más afecta la Seguridad Nacional desde el punto de vista de inseguridad ciudadana. Como anteriormente se mencionó, un caso bastante conocido de un ciberataque que pudo haber tenido mayor impacto a la Seguridad Nacional de Perú, es el del ciberataque del grupo de ransomware “Conti” realizado contra la DIGIMIN, llegando a robar documentos clasificados de Inteligencia de la Policía, este caso pasó relativamente desapercibido, posiblemente porque en el escenario nacional hubo otras noticias que tuvieron mayor importancia, pero esta afectación a la confidencialidad de la DIGIMIN, pudo haber tenido mayor impacto directo en la Seguridad Nacional.

Estos ciberataques se dirigieron a organismos de seguridad, inteligencia y justicia. Entre las principales víctimas estuvieron: DIGIMIN, Ministerio de Justicia y Derechos Humanos, la Fiscalía de la Nación, el Comando Conjunto de las Fuerzas Armadas, entre otros. En estos casos el vector de ataque fueron las vulnerabilidades en los sistemas de correo electrónico (Ver Tabla 1).

Los ciberataques de desinformación o FakeNews se extendieron mediante medios sociales, en el contexto de protestas sociales de origen social o político. Esta modalidad fue potenciada por el uso de inteligencia artificial para la creación de imágenes y mensajes falsos, en lo denominado DeepFake.

No hay registro o investigación que se haya realizado al respecto sobre situaciones que haya afectado la Seguridad Nacional en Perú; sin embargo, instituciones públicas y/o privadas han sido víctimas de la ciberdelincuencia, por ejemplo algunas entidades bancarias se les ha vulnerado su sistema de seguridad con el objetivo de obtener información de sus clientes; uno de los últimos casos que hemos tenido es el caso denominado “Zorrito run run”, en donde se vulneró a RENIEC, en esta oportunidad los ciberdelincuentes accedieron a datos de más de 30 millones de peruanos, lo que hicieron fue crear un link, y cualquier persona podía ingresar a ello mediante una retribución económica y se podía obtener cualquier ficha de RENIEC.

Un grupo de ciberdelincuentes atacaron el aeropuerto de Corpac, precisamente la torre de control, por lo que todo el sistema de aeronaves se vio afectado. Asimismo, en el 2022 se presentó un ataque a la dirección de inteligencia del Ministerio del Interior donde sustrajeron información de uso reservado, también atacaron la base de datos del EP y del Comando Conjunto. Asimismo el ente que realizó el ataque al EP fue un grupo de ciberdelincuentes que manifestó ser un equipo de informática que buscaban reivindicar su protesta en contra de las armas de la contaminación, siendo así que buscaron una vulnerabilidad del sistema del software Microsoft Change que usaba el EP para sus sistemas de envío e intercambio de información, y lograron penetrar la base de datos y sustraer correos electrónicos de uso de intercambio de información común por parte del personal militar (Ver Tabla 1).

Considerando los últimos 4 años, desde el contexto de la pandemia y la aceleración de la transformación digital del Estado, el país sufrió ciberataques que atentaron contra la intimidad de las informaciones personales, filtración de información reservada, y campañas de desinformación, principalmente. Todas estas modalidades de ataques afectaron la Seguridad Nacional en diferentes grados, efectos o consecuencias. Las principales vulnerabilidades de datos personales se dieron en los contextos de pandemia y protestas sociales. En el primer caso, ciberdelincuentes aprovecharon las vulnerabilidades de los sistemas de salud y de identificación para el robo de los bonos dirigidos a la población. En el segundo caso, los ciberdelincuentes publicaron información personal (direcciones, medios de comunicación, familiares, etc.) de autoridades políticas, fuerzas del orden (PNP y militares) y dirigentes sociales (periodistas, políticos, etc.), con el objetivo de dirigir la protesta a estos objetivos. Esta segunda modalidad fue posible por las bases de datos que se trafican en la Darkweb y vulnerabilidades de los sistemas informáticos estatales (Ver tabla 2).

**Tabla 1**

*Resumen de entrevista acerca de los entes que desarrollan ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| E. P. B. | - No conoce los nombres de los entes, sin embargo, narra las acciones que cometieron, como:<br>o Ciberdelincuentes que atacaron la torre de control del aeropuerto Corpac, afectando el sistema de aeronaves.<br>o En el 2022 se experimentó un ataque a la dirección de inteligencia del Ministerio Interior, donde sustrajeron información reservada.<br>o Un grupo de ciberdelincuentes que buscaban reivindicar la propuesta en contra de las armas de la contaminación, atacaron la base de datos del EP y del Comando Conjunto, impidiendo el intercambio de información entre ambas organizaciones. |
| D. R. B. | - Desconoce los nombres de los entes, pero narra las acciones que cometieron, como:<br>o Varios grupos no reportados que solo buscaban evidenciar las vulnerabilidades de los sistemas, siendo así que el grupo que estuvo realizando ello en Perú y Chile, fueron unos jóvenes de Wilson durante los años 2000. |
| V. I. G. | - Destaca un ciberataque al grupo "Conti" contra la DIGIMIN, que comprometió documentos clasificados de inteligencia policial, subrayando la importancia de la ciberseguridad para la seguridad nacional, a pesar de la limitada atención pública. |
| L. M. M. | - Manifiesta que se presentaron dos incidentes causados por los actores de amenaza Guacamaya que es un grupo Hacktivista y Conti, que es un grupo cibercriminal. |
| D. R. W. | - No conoce los nombres de los entes, sin embargo, narra las acciones que cometieron, como:<br>o El caso del “Zorrito run run”, en donde se vulneró a RENIEC, pues ciberdelincuentes accedieron a datos de más de 30 millones de peruanos, creando un enlace, y cualquier persona podía ingresar a ello mediante por una supuesta retribución económica y se podía obtener cualquier ficha de RENIEC. |

| | |
|---|---|
| G. M. C. | - Desconoce los nombres de los entes, pero narra las acciones que cometieron, como:<br>o Bastantes ciberataques que atentaron contra la privacidad de los datos personales, filtración de información reservada, y campañas de desinformación, principalmente. |

**Tabla 2**

*Resumen sobre los entes que desarrollan ciberdelincuencia*

| Entes | Resumen |
|---|---|
| Grupo "Conti" | Realizó un ciberataque contra la DIGIMIN, robando documentos clasificados de Inteligencia de la Policía. |
| Grupos de ciberdelincuentes anónimos | - Atacaron organismos de seguridad, inteligencia y justicia.<br>- Utilizaron inteligencia artificial para crear imágenes y mensajes falsos, en lo denominado DeepFake.<br>- Atacaron el aeropuerto de Corpac.<br>- Publicaron información personal en la Darkweb durante protestas sociales.<br>- Se aprovecharon las vulnerabilidades de los sistemas de salud y de identificación durante la pandemia.<br>- Realizaron el ataque al EP mediante la vulnerabilidad del sistema Microsoft Change.<br>- Atacaron la dirección de inteligencia del Ministerio del Interior, la base de datos del EP y del Comando Conjunto. |

## 4.2. Aspectos para enfrentar la ciberdelincuencia

### 4.2.1. *Aspectos jurídico-legales*

Actualmente, Perú cuenta con las siguientes leyes relacionadas a la Ciberseguridad Nacional:

En primer lugar, se menciona la Ley de Delitos Informáticos Nº 30096, que tiene el objetivo primordial de disuadir y sancionar las actividades ilícitas que comprometen la integridad de las redes informáticas, los datos y otros bienes jurídicamente protegidos de relevancia penal. Estos delitos se llevan a cabo mediante la utilización de las tecnologías de

la información y la comunicación, y el fin último es garantizar una respuesta contundente a la lacra de la ciberdelincuencia. En cierta medida, aborda el vacío normativo que existía anteriormente con respecto a las formas prevalentes de ciberataques, como el acceso no autorizado a sistemas informáticos (Ver tabla 3).

Esta norma luego fue perfeccionada en el 2014 con la Ley 30999 o Ley de Ciberdefensa, que menciona que las normas que regulan la protección de los sistemas cibernéticos en el Estado Peruano. Se refiere a la supervisión de las actividades militares realizadas por las entidades adscritas al Ministerio de Defensa. El término "ciberdefensa" se define como una capacidad militar que involucra la contención y respuesta a amenazas en el ciberespacio. Esta responsabilidad se delega en las FFAA, a las que se encomienda la ejecución de las medidas de ciberdefensa. Esta legislación entró oficialmente en vigor el nueve de agosto de dos mil diecinueve (Ver tabla 3).

Por otro lado, se encuentra la Ley de Protección de Datos Personales Nº 29733, que busca garantizar la salvaguarda del derecho fundamental a la salvaguarda de la información personal, estipulado en el Artículo 2, párrafo 6 de la Constitución Política del Perú. Ello a través de un adecuado tratamiento de dichos datos, respetando simultáneamente los demás derechos fundamentales consagrados en la Constitución (Ver tabla 3).

Asimismo, Huancco (2018) destaca que la Constitución Política del Perú, específicamente en el artículo 44, en relación con el artículo 163, estipula las responsabilidades fundamentales del Estado, entre las que se encuentran velar por la seguridad y bienestar de la población, salvaguardar los derechos humanos, proteger la seguridad y soberanía de la nación, entre otras obligaciones. Además, se afirma que la disponibilidad de contenidos y material gráfico en línea puede tener efectos perjudiciales, en particular para los menores, que pueden verse expuestos a contenidos sexuales explícitos, violencia y contenidos relacionados con las drogas. Además, la sociedad en su conjunto es susceptible de sufrir diversos riesgos, como el acceso no autorizado y el robo de información personal, entre otras posibles consecuencias.

Sin embargo, en 2011 se aprobó un Plan Estratégico de Desarrollo Nacional, conocido como Plan Bicentenario. Este plan pretendía potenciar tanto el ciberespacio como el sector comercial, con especial énfasis en este último. Estaba previsto que se extendiera hasta 2021. Por lo tanto, es imperativo fomentar una dedicación social, que abarque tanto a la población como a los organismos gubernamentales, corporativos y militares, con el fin de mitigar

eficazmente las consecuencias de las amenazas cibernéticas, minimizar las vulnerabilidades y mantener la integridad de la seguridad nacional.

Es importante reconocer que el caso peruano destaca por su particularidad, caracterizada por un extenso cuerpo normativo en materia de ciberseguridad que se distribuye en diversos instrumentos legales. En el año 2019, se promulgó con éxito la legislación conocida como Ley de Ciberdefensa, mientras que la Ley de Ciberseguridad se encontraba pendiente de promulgación en ese momento. Ambas piezas legislativas ofrecen contribuciones innovadoras para mejorar el índice de ciberseguridad. Sin embargo, es importante señalar que actualmente solo se encuentra vigente la Ley de Ciberdefensa (Huamán, 2020).

Según León et al. (2022), es imperativo diferenciar entre los dos instrumentos en cuestión. La Ley de Ciberdefensa tiene por finalidad regular las operaciones militares en el ámbito de la ciberdefensa, mientras que la Ley de Ciberseguridad se enfoca en implementar medidas cautelares para combatir las amenazas cibernéticas. Tanto el instrumento existente como el que está en proceso de formulación pretenden alinearse con los indicadores de la UIT. Este alineamiento busca proteger al Estado y a la sociedad peruana de las amenazas cibernéticas y de las consecuencias negativas del rezago tecnológico derivado del rápido avance de las fuerzas productivas digitales.

No obstante, la legislación por sí misma es insuficiente en materia de protección de la estructura económica y el bienestar social; en tanto, la celeridad de los desarrollos de tecnologías de información y la comunicación (TIC) tiende a la obsolescencia normativa, aun antes del alcance de los efectos de novísimas legislaciones. Ello no deriva en el indefectible rezago normativo, solo induce a la adecuación permanente en materia reglamentaria que responda a las buenas prácticas en ciberseguridad y ciberdefensa.

Además, los entrevistados expusieron que la normatividad que garantiza la Seguridad Nacional son las herramientas que tiene el Estado para combatir las ciberdelincuencia, es decir, existen dos sistemas que se dividen dos partes de la ley, una parte que ve toda la ciberdelincuencia qué está cargo de la policía y la prevención a cargo de la presencia del Consejo de Ministros a través de la Secretaría del Gobierno Digital y la parte militar que se ha emitido por la Ley 30 999, la cual se emplea para dar o garantizar la Seguridad Nacional frente a amenazas que no siempre se dan por ciberdelincuentes, sino por un grupo de hackers que se denominan activistas que buscan tener un beneficio económico a través del ciberespacio.

Todo está gobernado por la Secretaría de Gobierno y Transformación Digital, siendo así que la seguridad está directamente relacionada a la seguridad de la infraestructura del equipamiento y la seguridad digital está más relacionada con la seguridad de la información. Además, se tienen normas con respecto al ámbito de seguridad, con respecto a la implementación y aplicación de todas las normativas internacionales de seguridad e información.

En resumen, Perú se adhiere a convenio de Budapest sobre ciberseguridad y ayuda judicial en el 2019, se presenta la Ley de delitos informáticos N° 30096 y su actualización luego de adherirse al convenio de Budapest Ley N° 30171, del mismo modo la Ley 27309 que incorpora los delitos informáticos al Código Penal, la Ley de Ciberdefensa N° 30999, el Decreto Supremo 050-2018-PCM, donde aprueban la definición de seguridad digital en el ámbito nacional, y la Resolución Ministerial 004-2016-PCM, donde se aprueban el uso obligatorio de la norma técnica peruana "ISO NTP/IEC 27001:2014, que habla sobre la tecnología de la información. técnicas de seguridad. Asimismo, se encuentra la Ley N° 27269 de Firmas y Certificados Digitales, la Ley N° 27291 que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica, La Ley N° 28493 que regula el uso del Correo Electrónico comercial no solicitado (Ver tabla 4).

**Tabla 3**

*Resumen de entrevista acerca del aspecto jurídico-legal para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| E. P. B. | - Indica que la Ley 30 999 reestructura el entorno de la Estrategia Integrada de Ciberdefensa. |
| V. I. G. | - Manifiesta que la Ley de Delitos Informáticos es la normativa clave para penalizar la ciberdelincuencia en Perú, definiendo las acciones consideradas como delitos en el ciberespacio.<br>- Expone normativas relacionadas con políticas de transformación digital y ciberdefensa, como el DL-1412 y la Ley N° 30999. |
| L. M. M. | - Expone las siguientes Leyes y normativas: Ley de delitos informáticos N° 30096, el Convenio de Budapest, la Ley N° 30171, Ley 27309 que incorpora los delitos informáticos al Código Penal, la Ley de Ciberdefensa N° 30999, el Decreto Supremo 050-2018-PCM, Resolución Ministerial 004-2016-PCM y la Norma Técnica Peruana "ISO NTP/IEC 27001:2014. |
| D. R. W. | - Comenta que se tiene la Ley 30096 de delitos informáticos, que tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal. |
| G. M. C. | Expone la Ley de delitos informáticos (Ley Nº 30096, con su modificatoria y el Código Penal) y la Ley Nº 30618 de 2017 que modifica el Decreto Legislativo 1141, el cual define la Seguridad Digital como la “situación de confianza en el entorno digital”. |

**Tabla 4**

*Resumen del aspecto jurídico-legal para enfrentar la ciberdelincuencia*

| Elemento | Resumen |
|---|---|
| Leyes | - Ley de Delitos Informáticos Nº 30096<br>- Ley de Ciberdefensa Nº 30999<br>- Ley de Protección de Datos Personales Nº 29733<br>- Ley de Ciberseguridad (pendiente de promulgación en ese momento)<br>- Ley de Ciberdefensa y Ley de Ciberseguridad (contribuciones innovadoras para mejorar el índice de ciberseguridad)<br>- Ley N° 30171 (actualización de la Ley de Delitos Informáticos después de adherirse al Convenio de Budapest)<br>- Ley N° 27309 (incorpora los delitos informáticos al Código Penal)<br>- Ley N° 27269 (de Firmas y Certificados Digitales)<br>- Ley N° 27291 (modifica el código civil permitiendo la utilización de medios electrónicos)<br>- Ley N° 28493 (regula el uso del Correo Electrónico comercial no solicitado - SPAM)<br>- Ley N° 30618 de 2017 (modifica el Decreto Legislativo 1141, define la Seguridad Digital como la "situación de confianza en el entorno digital") |
| Decreto Legislativo | DL-1412 (normativas relacionadas con políticas de transformación digital y ciberdefensa) |
| Decreto Supremo | Decreto Supremo 050-2018-PCM (define la seguridad digital en el ámbito nacional) |
| Resolución ministerial | Resolución Ministerial 004-2016-PCM (aprueba el uso obligatorio de la norma técnica peruana "ISO NTP/IEC 27001:2014") |
| Otros | - Plan Estratégico de Desarrollo Nacional (Plan Bicentenario)<br>- Convenio de Budapest sobre ciberseguridad y ayuda judicial |

### 4.2.2. *Capacidades que presenta el personal especializado*

En el contexto actual, donde la ciberdelincuencia representa una amenaza creciente para la Seguridad Nacional en Perú, es imperativo contar con profesionales altamente capacitados y versátiles. Como subraya Díaz (2022), la resolución efectiva de esta problemática demanda una diversidad de habilidades que abarquen no solo la comprensión profunda de sistemas informáticos, redes y ciberamenazas, sino también destrezas analíticas avanzadas.

Los especialistas en ciberseguridad no solo deben ser expertos en la identificación y respuesta a estrategias de piratas informáticos, sino que también deben destacar en el análisis de datos. Esta capacidad se convierte en un componente vital para la identificación proactiva de riesgos potenciales, así como para el reconocimiento de patrones que puedan indicar actividades dañinas. En este sentido, la habilidad de interpretar grandes conjuntos de datos se erige como una herramienta esencial en la lucha contra la ciberdelincuencia.

El conocimiento detallado de las amenazas y metodologías más recientes, como el programa maligno, ransomware y phishing, constituye otra pieza fundamental en el arsenal de los profesionales de la ciberseguridad. Este entendimiento actualizado es crucial para anticipar y contrarrestar las tácticas cambiantes de los ciberdelincuentes, así como para desarrollar estrategias efectivas de prevención.

Además, el dominio de la ciencia forense digital es esencial para llevar a cabo investigaciones efectivas en el ámbito digital. Esta capacidad permite rastrear y analizar evidencia digital de manera forense, siendo fundamental para la identificación de perpetradores y la recopilación de pruebas admisibles en procesos legales. Por otro lado, la habilidad para construir y evaluar aplicaciones y sistemas seguros se convierte en un componente crucial para mitigar vulnerabilidades desde las fases tempranas del desarrollo de software.

En el ámbito de las Fuerzas Armadas (FFAA) y la Dirección Nacional de Inteligencia (DINI), la preparación del personal se vuelve aún más relevante. Aunque, hasta el momento, los ciberataques no han impactado totalmente, la creciente interconexión de sistemas impone la necesidad de contar con capacidades para prevenir, tratar y responder a ciberamenazas que podrían afectar la Seguridad Nacional.

La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) dentro de la Policía Nacional requiere un personal altamente calificado. La necesidad de haber seguido cursos especializados, con énfasis en el curso de investigación de delitos informáticos, destaca la importancia de la formación específica. La experiencia laboral acumulada, con la mayoría de los efectivos contando con más de 5 años en la unidad, añade un nivel adicional de especialización. La combinación de la experiencia práctica y la formación formal en informática fortalece la capacidad de respuesta frente a amenazas digitales (Ver tabla 5).

En cuanto a los especialistas en ciberdelincuencia, se espera que posean un extenso conocimiento técnico. Esto incluye habilidades en análisis forense informático, ingeniería inversa de programa maligno, hacking ético, cibercriminalística, y ciberinteligencia. Además, se valora un profundo conocimiento de redes, software, encriptación y arquitectura informática, junto con experiencia internacional en la prevención, tratamiento y respuesta a incidentes de seguridad cibernética de alcance nacional (Ver tabla 5).

Por último, el compromiso de las FFAA con los estándares internacionales, como la ISO 27001-2, refleja un enfoque proactivo hacia la seguridad cibernética. La iniciativa de establecer un convenio con Estados Unidos en noviembre de 2023 para brindar cursos de actualización demuestra el compromiso continuo con la mejora y la adaptación constante frente a los cambios tecnológicos. Este enfoque progresivo garantiza que el personal esté equipado con las habilidades más recientes y relevantes para enfrentar las amenazas digitales en evolución constante (Ver tabla 5 y 6).

**Tabla 5**

*Resumen de entrevista acerca de las capacidades del personal especializado para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| E. P. B. | - Menciona que el personal está capacitado de acuerdo con las normas y estándares internacionales en Perú la ISO 27001-2. |
| L. M. M. | - Considera que el personal debería estar mejor capacitado y que deben existir mejores programas de capacitación y retención del talento humano.<br>- Expone que las capacidades y conocimientos básicos son el análisis forense informático, incluido la Ingeniería inversa de programa maligno, el hacking ético, conocer sobre ciber criminalística y ciber inteligencia. |
| D. R. W. | - El personal sigue diferentes cursos de investigación, de los cuales el más importante, es el de delitos informáticos,<br>- Se debe contar con experiencia laboral, ya que en su mayoría de los efectivos cuentan con más de 5 años en dicha unidad. |
| G. M. C. | - Considera que el personal de las FFAA y la DINI cuenta con capacidades para prevenir, tratar y responder a ciberataques que representen amenazas contra la Seguridad Nacional. |

**Tabla 6**

*Resumen de las capacidades del personal especializado para enfrentar la ciberdelincuencia*

| Elementos | Resumen de respuesta |
|---|---|
| Capacidades | - Dominio de la ciencia forense digital, incluyendo la capacidad de construir y evaluar aplicaciones y sistemas seguros para mitigar vulnerabilidades en el desarrollo y pruebas de software.<br>- Capacidades para prevenir, tratar y responder a ciberataques.<br>- Capacidad para la prevención, tratamiento y respuesta a incidentes de seguridad cibernética de alcance nacional. |
| Habilidades | - Habilidad en el análisis de datos |
| Conocimientos | - Conocimiento exhaustivo de sistemas informáticos, redes, protocolos, programación y ciberamenazas.<br>- Conocimientos sobre amenazas y metodologías cibernéticas, sobre todo programa maligno, ransomware, phishing, entre otros.<br>- Conocimientos técnicos avanzados sobre análisis forense informático, ingeniería inversa de programa maligno, hacking ético, cibercriminalística, y ciberinteligencia.<br>- Conocimiento de redes, software, encriptación y arquitectura informática. |

### 4.2.3. *Recursos materiales y tecnológicos*

Para hacer frente a la ciberdelincuencia que representa una amenaza para la Seguridad Nacional en Perú, es necesario el uso de una serie de recursos materiales y técnicos. Estos recursos juegan un papel crucial en la prevención, detección, respuesta y mitigación de los ciberataques, por ello, la Organización de los Estados Americanos (OEA, 2014) brinda los siguientes recursos tecnológicos.

Las herramientas de ciberseguridad incluyen una serie de componentes de software y hardware especializados, como cortafuegos, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, así como soluciones antivirus y antimalware. Del mismo modo, los sistemas de supervisión y análisis de la seguridad proporcionan una vigilancia continua de la infraestructura de tecnología de la información con el fin de identificar

cualquier comportamiento atípico o malintencionado. Esto puede incluir herramientas de análisis de registros y sistemas de gestión de eventos de seguridad, a menudo denominados SIEM. Asimismo, el uso de la tecnología de cifrado es crucial para salvaguardar la confidencialidad de los datos sensibles. Esto incluye la aplicación de protocolos de cifrado tanto para la comunicación como para el almacenamiento de datos.

Los sistemas de autenticación y control de acceso desempeñan un papel crucial en la salvaguarda de los sistemas y datos sensibles, garantizando que sólo se conceda acceso a las personas con la debida autorización. Por otro lado, las tecnologías de exploración de vulnerabilidades que se utilizan para realizar exploraciones sistemáticas de los sistemas informáticos con el fin de identificar y evaluar las vulnerabilidades conocidas que pueden ser susceptibles de explotación por parte de agentes maliciosos en el ámbito de la ciberdelincuencia. Esto permite a las empresas abordar o rectificar estas vulnerabilidades antes de su explotación.

Las instituciones poseen centros de datos que incluyen dispositivos informáticos que almacenan información y se comparte por diferentes órganos del Comando Conjunto. Además, se tienen equipos de seguridad perimetral para protegerse de un ataque informático, por ejemplo, un Firewall qué va a limitar el ingreso de personas no autorizadas a las bases de datos y puede filtrar las direcciones IP, usuario y contraseñas a través del “Firewall”, también se tiene un “Waflt” que se comparte a través de aplicación que ha sido desarrollada por las FFAA. Siendo así que existen equipos de detección y prevención, por ejemplo, se tiene a un equipo de seguridad perimetral que evita que los correos falsos ingresen, por ende, lo identifica y bloquea el ingreso (Ver tabla 7).

Todo personal especializado en combatir la ciberdelincuencia debería contar con recursos materiales y tecnológicos de última generación, estandarizados y verificados por un ente responsable (que no tenemos en Perú) tales como computadoras, servidores, laptops, kits, herramientas, software, equipamiento de comunicaciones (switches, routers, etc.) e infraestructura (Ver tabla 8).

La DIVINDAT cuenta con tres departamentos de investigación en delitos informáticos, asimismo, cuenta con un departamentos de patrullaje virtual que nos permite identificar, ubicar y/o capturar a los ciberdelincuentes a través de las redes sociales o el uso de las OSINT (conjunto de técnicas y herramientas que se utilizan para recopilar información pública, analizar datos y relacionarlos para convertirlos en conocimiento útil), también se

cuenta con el departamento de análisis forense en donde se remiten todos aquellos dispositivos electrónicos (celulares, laptops, computadoras, etc.) que estén involucrados en una investigación para su pericia correspondiente, a efectos de probar si ha sido afectado por algún virus, o también para recuperar información que haya sido borrado para su posterior visualización por el personal de investigación, ellos cuentan con una herramienta forense llamada CELLEBRITE; por otro lado se cuenta con el departamento de geolocalización quienes tiene conexión directa con los proveedores de servicios de telecomunicaciones que les proveen en tiempo real la ubicación de los números telefónicos que estén involucrados en una investigación la cual cumple con ciertos requisitos para acceder a ello.

**Tabla 7**

*Resumen de entrevista acerca de los recursos materiales y tecnológicos para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| E. P. B. | - Se tiene una base de datos en donde están los dispositivos informáticos que almacenan información y es compartida por diferentes órganos del Comando Conjunto. |
| D. R. B. | - Expone que la mayoría de las herramientas que se está disponiendo ahora para los ciberdelincuentes están publicadas en las redes, lo cual debilita el sistema de Seguridad. |
| V. I. G. | - Menciona que uno de los principales desafíos de la DIVINDAT es el vencimiento de licencias de software y equipos. |
| L. M. M. | - Actualmente se cuentan con computadoras, servidores, laptops, kits, herramientas, software, equipamiento de comunicaciones (switches, routers, etc.). |
| D. R. W. | - Menciona que muchos de los recursos forenses han sido donados por parte de la embajada americana, como por ejemplo el software CELLEBRITE. |

**Tabla 8**

*Resumen de los recursos materiales y tecnológicos para enfrentar la ciberdelincuencia*

| Elementos | Resumen |
|---|---|
| Herramientas de Ciberseguridad | - Cortafuegos.<br>- Sistemas de detección de intrusiones. |

| | |
|---|---|
| | - Sistemas de prevención de intrusiones.<br>- Soluciones antivirus y antimalware. |
| Sistemas de Supervisión y Análisis de Seguridad: | - Herramientas de análisis de registros.<br>- Sistemas de gestión de eventos de seguridad (SIEM). |
| Tecnología de Cifrado | - Aplicación de protocolos de cifrado para comunicación y almacenamiento de datos. |
| Tecnologías de Exploración de Vulnerabilidades | - Tecnologías que garantizan el acceso solo a personas autorizadas. |
| Centros de Datos | - Herramientas para explorar y evaluar vulnerabilidades en sistemas informáticos. |
| Equipos de Seguridad Perimetral | - Firewalls para limitar el acceso no autorizado.<br>- "Waflt" para compartir aplicaciones desarrolladas por las FFAA. |
| Equipos de Detección y Prevención | - Equipos de seguridad perimetral para evitar correos falsos y bloquear el acceso no autorizado. |
| Recursos materiales | - Computadoras, servidores, laptops, kits, herramientas, software, equipamiento de comunicaciones, etc. |

## 4.3. Necesidades de los aspectos para enfrentar la ciberdelincuencia

### 4.3.1. *Análisis PESTEL*

A continuación, se muestra el análisis PESTEL desarrollado para la investigación, donde se consideraron la dimensión política, puesto que se revisaron los acuerdos internacionales y nacionales, y políticas relacionadas a la temática. También se evaluó la dimensión económica, puesto que la estrategia que se propondrá puede provocar impacto en el área. Del mismo modo, la dimensión tecnológica, pues dentro de la estrategia se mencionó los recursos materiales y tecnológicos que aportan el sustento de la estrategia. Por último, se consideró la dimensión legal, ya que están implicadas las normas, leyes y resoluciones que ayudaron a enfrentar la ciberdelincuencia. No se considera el evaluar la dimensión ecológica, ni social (Ver figura 1).

La decisión de no incluir ambos aspectos se justifica tomando en cuenta que la ciberdelincuencia no presenta impactos directos sobre el medio ambiente o aspectos ecológicos. Dado que la investigación se enfoca en estrategias para enfrentar amenazas

cibernéticas, la inclusión de la dimensión ecológica en el análisis PESTEL podría resultar redundante y desviar la atención de los elementos cruciales relacionados con la seguridad nacional en el ciberespacio. Por otro lado, respecto a la dimensión social, es necesario señalar que, en el contexto del estudio, dicho aspecto supone al análisis de la percepción pública sobre la ciberdelincuencia y la disposición de la sociedad para colaborar en medidas de seguridad. En este sentido, considerando que las entrevistas han estado centradas en agentes estratégicos y expertos, incluyendo a autoridades militares, policiales y especialistas en ciberseguridad; si bien estas voces son cruciales para abordar la ciberdelincuencia desde una perspectiva técnica y estratégica, no necesariamente reflejan la percepción y disposición del público en general. Por tanto, debido a limitación en la obtención de datos representativos de la percepción general de la sociedad se optó por no incluir este aspecto en el análisis.

Este enfoque selectivo en las dimensiones políticas, económicas, legales y tecnológicas se justifica al considerar la naturaleza técnica y altamente especializada de la ciberdelincuencia y su impacto en la seguridad nacional. La exclusión de las dimensiones social y ecológica no disminuye la importancia de estos aspectos en otros contextos, pero refleja una elección deliberada para enfocarse en los elementos más críticos para la formulación de estrategias efectivas contra la ciberdelincuencia en el ámbito nacional.

#### *4.3.1.1.*Dimensión Política.

- La Ley 30999 de Ciberdefensa busca proteger la soberanía, intereses nacionales y sistemas informáticos.
- Se ha firmado el Convenio de Budapest para la cooperación internacional en materia de delitos informáticos.
- La política de ciberseguridad aún se encuentra en una fase de desarrollo, manteniendo aún vulnerables su ciberespacio y recurso, por lo que falta de una estrategia sólida y coherente ha llevado a un enfoque fragmentado en la respuesta a amenazas.
- Existe una falta de una coordinación efectiva entre las agencias gubernamentales y las entidades encargadas de la ciberseguridad puede debilitar la capacidad de respuesta a las amenazas cibernéticas.
- Se presenta una falta de concienciación y priorización política en relación con la ciberseguridad puede llevar a la asignación insuficiente de recursos y atención a este problema.

#### *4.3.1.2.*Dimensión Económica.

- La ciberdelincuencia tiene un impacto económico en sectores financieros y administrativos, pues suelen enfrentar pérdidas.
- Los delitos comunes son el fraude informático, estafa agravada, suplantación de identidad, entre otros.
- Los ciberataques pueden tener un alto costo económico para las empresas y el gobierno, incluyendo la pérdida de datos, la interrupción de operaciones y los gastos de recuperación.
- Existe una falta de inversión en ciberseguridad puede dejar a las organizaciones vulnerables a las amenazas cibernéticas debido a la falta de recursos y tecnologías adecuadas.
- La percepción de una deficiente ciberseguridad puede disuadir la inversión extranjera en Perú, afectando negativamente el desarrollo económico.

#### *4.3.1.3.*Dimensión Legal.

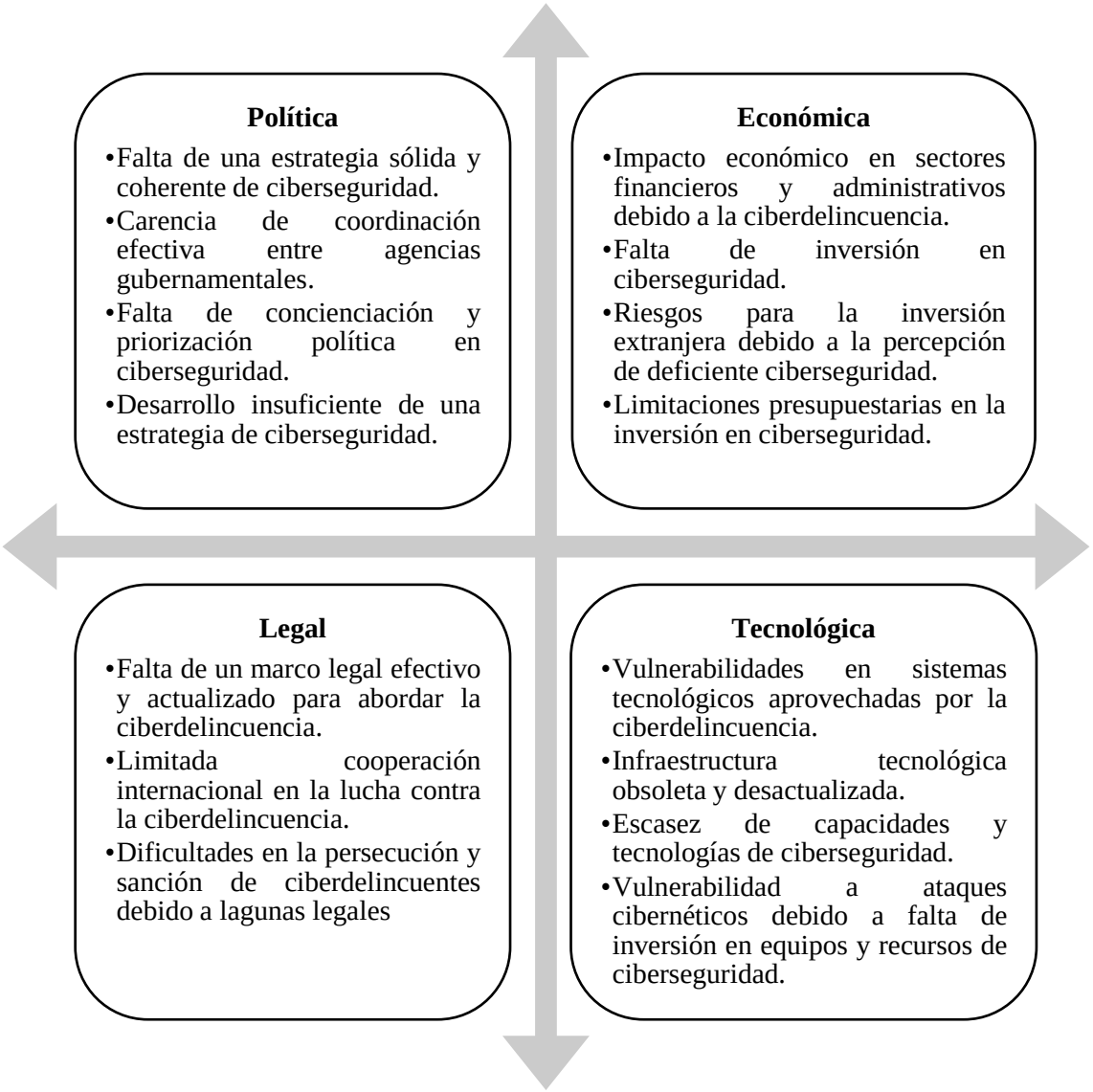
- La Ley 30999 establece medidas para proteger los sistemas informáticos del país y sancionar a los responsables de delitos informáticos.
- El Convenio de Budapest permite a jueces y fiscales realizar requerimientos de cooperación internacional en casos de ciberdelincuencia.
- Se presenta un marco legal insuficiente y desactualizado para abordar de efectivamente la ciberdelincuencia.
- Las leyes relacionadas con la ciberseguridad pueden carecer de claridad, actualización y capacidad para abordar las amenazas emergentes de la ciberdelincuencia.
- Existen lagunas en la legislación que pueden dificultar la persecución y sanción de los ciberdelincuentes, ya que las leyes pueden no estar actualizadas
- En algunos casos la cooperación internacional suele ser limitada en la lucha contra la ciberdelincuencia, lo que dificulta la extradición de delincuentes y la obtención de pruebas en casos transfronterizos.

#### *4.3.1.4.*Dimensión Tecnológica.

- La ciberdelincuencia se aprovecha de vulnerabilidades en los sistemas informáticos y tecnológicos.
- La pérdida de la capacidad de coordinación digital entre entidades públicas podría causar daños fatales.
- Se enfrentan desafíos en la mejora de infraestructura de ciberseguridad y la capacitación de expertos en ciberseguridad.
- Se presenta la falta de personal capacitado y tecnologías avanzadas en ciberseguridad puede hacer que Perú sea vulnerable a los ataques cibernéticos.
- La infraestructura desactualizada puede ser un objetivo fácil para los ciberdelincuentes, lo que aumenta el riesgo de ataques exitosos, por una falta de inversión.
- Es necesario tomar medidas de protección contra ataques cibernéticos en coordinación con sectores públicos y privados.

**Figura 1**

*Resumen de análisis PESTEL*




### 4.3.2. *Aspectos jurídico-legales*

Con relación a las necesidades jurídico-legales, se señala que cada que se descubre una nueva forma de ciberdelincuencia recién se implementa en alguna ley y que los encargados de promover las leyes suelen ser muy “técnicos”; por ejemplo, la policía que tiene a cargo la lógica que previene el delito suele conocer de las modalidades de delincuencia en el exterior, pero no presenta una rapidez para implementar una ley que combata eso. En resumen, se presenta un vacío en las leyes, lo que genera que las entidades que combaten ciberdelitos busquen constantemente alianzas para combatirlos (Ver tabla 9).

Además, se requiere que el personal se especialice en temas jurídicos-legales, que conozcan y dominen todo el marco normativo nacional e internacional con la experiencia y las relaciones internacionales necesarias para poder encaminar correctamente este enfrentamiento a la ciberdelincuencia, pues no es suficiente con firmar el convenio de Budapest; siendo así que se debe solicitar más apoyo internacional a las diversas organizaciones.

Por otro lado, se destaca la necesidad de incrementar las penas o medidas legales, por lo que se requiere implementar un "law enforcement", es decir el forzar a los ciberdelincuentes a cumplir la ley para hacer efectivo el marco normativo ya existente. Por ello se recalca a las entidades públicas y privadas, que puedan remitir la información inmediata a la PNP para que se realice las investigaciones ante el requerimiento por parte de este, ya que en la actualidad la información solicitada es recibida después de las 48 horas, tiempo que limita a las investigaciones (Ver tabla 9).

Sin embargo, si bien se ha puesto en marcha una Política Nacional de Ciberseguridad, se destaca la necesidad de una Estrategia Nacional de Ciberseguridad y la creación de un Comité Nacional de Ciberseguridad. Asimismo, quedan pendientes la formulación de la Ley de Ciberseguridad, la implementación de las capacidades descritas en la Ley de ciberdefensa y leyes que especifiquen las sanciones penales detalladamente a los ataques que afecten a la Seguridad Nacional (Ver tabla 10).

**Tabla 9**

*Resumen de entrevista acerca de las necesidades del aspecto jurídico-legal para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| D. R. B. | - Plantea la necesidad de separar el marco normativo de seguridad en las comunicaciones y la seguridad de datos, enfocándose en la importancia de entender la capa de datos en la transmisión digital.<br>- Expone la necesidad de establecer metadatos para proteger a las personas y facilitar la búsqueda de ciberdelincuentes para definir jurídicamente la información que circula en Internet como prueba o evidencia. |
| V. I. G. | - Considera que las normativas, penas o medidas legales existentes, no ayudan a implementar el "law enforcement", que serviría para obligar a los ciberdelincuentes a cumplir con el marco normativo existente.<br>- Recomienda una propuesta integral para fortalecer la División de Investigación de Delitos Informáticos, abordando la aplicación de la ley, disuasión mediante operaciones de información y destacada capacitación en ciberseguridad.<br>- Incluyendo incentivos económicos y diferimiento salarial para retener talento clave frente a ofertas del sector privado. |
| L. M. M. | - Considera que no hay una estrategia bien definida para combatir la ciberdelincuencia, con un personal mejor preparado en temas jurídicos-legales que conozcan y dominen todo el marco normativo nacional e internacional. |
| D. R. W. | - Manifiesta que hace tiempo no existe un incremento en las penas para quienes cometen este tipo de delitos. |
| G. M. C. | - Manifiesta que no se especifica jurídicamente los delitos penales que, en el ámbito digital o informático, atentan contra la Seguridad Nacional como bien jurídico protegido. |

**Tabla 10**

*Resumen de las necesidades del aspecto jurídico-legal para enfrentar la ciberdelincuencia*

| Resumen |
| --- |
| - Necesidad de una mayor agilidad en la implementación de leyes para abordar nuevas formas de ciberdelincuencia.<br>- Necesidad de que el personal encargado de prevenir y combatir ciberdelitos se especialice en temas jurídico-legales, con conocimiento del marco normativo nacional e internacional, así como experiencia y relaciones internacionales.<br>- Necesidad de incrementar las penas o medidas legales y la implementación de un "law enforcement".<br>- Necesidad de una Estrategia Nacional de Ciberseguridad y la creación de un Comité Nacional de Ciberseguridad.<br>- Necesidad de separar el marco normativo de seguridad en las comunicaciones y la seguridad de datos, con un enfoque en comprender la capa de datos en la transmisión digital.<br>- Necesidad de establecer metadatos para proteger a las personas y facilitar la búsqueda de ciberdelincuentes, definiendo jurídicamente la información en Internet como prueba o evidencia.<br>- Necesidad de fortalecer la División de Investigación de Delitos Informáticos, incluyendo incentivos económicos y diferimiento salarial para retener talento clave frente a ofertas del sector privado.<br>- Necesidad de especificación jurídica de los delitos penales que atentan contra la Seguridad Nacional en el ámbito digital o informático, como bien jurídico protegido. |

### 4.3.3. *Capacidades que presenta el personal especializado*

El personal debería estar mejor capacitado en todos los niveles y especialidades requeridas en todo lo que a ciberdelincuencia respecta, al igual que deberían existir mejores programas de capacitación y retención del talento humano para que el personal esté capacitado en la parte estratégica (nivel político) y que pueda enrumbar hacia la implementación de una correcta Estrategia de Ciberseguridad y contra la Ciberdelincuencia.

Se resalta que la capacitación es lo que más falta por desarrollar, debido a que se habla que del 40% de 120 personas, posee una capacitación óptima, o un nivel de capacitación básica, por lo cual es imperativo para la DIVINDAT trabajar en la capacitación

de sus efectivos, asimismo, toda organización operativa, tiene una gran carga administrativa que la sostiene, y en el caso de la DIVINDAT, además de sólo realizar la parte técnica relacionada a sistemas, también se requieren trámites legales para hacer efectivo el trabajo operativo y esto consume bastante tiempo, por lo cual, además de capacitar personal, en un escenario en el cual se cometen mayor cantidad de delitos informáticos, sus capacidades administrativas también deberían crecer.

Sin embargo, la principal carencia es el recurso humano especializado en materia de ciberseguridad. si bien existe experiencia en materia de criptografía y análisis de señales con dispositivos especializados; las capacidades de gestión de arquitectura sistemas informáticas de alcance nacional y de respuesta ante ciberataques es muy baja. De otro modo, el uso de las tecnologías en los últimos años se ha incrementado, por ende se van actualizando, eso quiere decir que el ciberdelincuente también busca las formas de cometer sus delitos y también se actualiza; por lo que se requiere que el estado siga capacitando al personal de esta unidad especializada en el uso de las nuevas técnicas de información ya sea dentro del territorio nacional o en el extranjero, ya que va a permitir recibir experiencias de otros países en cuanto al tratamiento de dicho delito, permitiendo estar un paso adelante que el ciberdelincuente (Ver tabla 11 y 12).

**Tabla 11**

*Resumen de entrevista acerca de las necesidades de la capacidad del personal especializado para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| V. I. G. | - Resaltó que se debe fortalecer las capacidades administrativas de la organización para agilizar trámites legales y optimizar el trabajo operativo. |
| L. M. M. | - Considera que el personal debería estar mejor capacitado y que deben existir mejores programas de capacitación y retención del talento humano. |
| D. R. W. | - Se debe contar con experiencia laboral, ya que en su mayoría de los efectivos cuentan con más de 5 años en dicha unidad.<br>- Requiere que el estado siga capacitando al personal de esta unidad especializada en el uso de las nuevas técnicas de información ya sea dentro del territorio nacional o en el extranjero. |
| G. M. C. | - Considera que la principal carencia es el recurso humano especializado en materia de ciberseguridad. |

**Tabla 12**

*Resumen de las necesidades de la capacidad del personal especializado para enfrentar la ciberdelincuencia*

| Necesidad | Resumen |
|---|---|
| Mejora en la Capacitación Técnica | Necesidad crítica de mejorar la capacitación técnica del personal en todos los niveles y especialidades relacionadas con la ciberdelincuencia. |
| Desarrollo de Programas de Capacitación y Retención | Se requieren programas más efectivos de capacitación y retención del talento humano para asegurar que el personal esté actualizado y comprometido, especialmente en la parte estratégica a nivel político. |
| Fortalecimiento de Capacidades Administrativas | Se necesita fortalecer sus capacidades administrativas para agilizar trámites legales y optimizar el trabajo operativo. |
| Gestión de Arquitecturas de Sistemas y Respuesta a Ciberataques | Se necesita un enfoque en el desarrollo de habilidades para gestionar y responder de manera efectiva a las amenazas cibernéticas. |
| Carencia de Recurso Humano Especializado | Se presenta una falta de recursos humanos especializados en materia de ciberseguridad. |

### 4.3.4. *Recursos materiales y tecnológicos*

Por otro lado, dentro de las necesidades identificadas se expone que se requiere mucha tecnología para identificar el autor de un delito informático porque existen herramientas que permitan a los ciberdelincuentes camuflarse y generando una demora de más de medio año para poder ser identificado, por esta razón los delitos informáticos es un trabajo de largo tiempo. Hace falta una mejor infraestructura donde se pueda implementar todo el equipamiento que se vaya adquiriendo progresivamente y según lo planificado. Del mismo modo, hace falta una compra de dispositivos y actualización de licencias para cubrir las necesidades de las FFAA, y lo considera como aspectos básicos para el desarrollo de las actividades para enfrentar la ciberdelincuencia (Ver tabla 13).

El fortalecimiento del Equipo de Respuesta ante Incidentes de Seguridad Digital del Perú (PCERT), el establecimiento de otros Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT), la constitución de centros de datos nacionales que aseguren

la continuidad de los servicios estratégicos nacionales (principalmente los de seguridad y defensa), incremento de los nodos de conexión a las redes submarinas que permiten el acceso a Internet. Por eso se destaca la necesidad de acuerdos de cooperación con países potencia en ciberseguridad, ciberdefensa y ciber inteligencia, principalmente para desarrollar las capacidades del recurso humano mediante becas de estudio, intercambios y pasantías (Ver tabla 14).

Los softwares que tiene esta unidad especializada se actualicen cada año, así como las licencias; pero estas deben ser abordadas por el estado, ya que actualmente estas herramientas forenses han sido donadas por parte de la embajada americana, como por ejemplo el software CELLEBRITE.

**Tabla 13**

*Resumen de entrevista acerca de las necesidades de los recursos materiales y tecnológicos para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| V. I. G. | - Destaca la necesidad de priorizar la eficiencia mediante la adquisición de dispositivos y actualización de licencias. |
| D. R. B. | - Sugiere una mayor coordinación entre entidades gubernamentales y empresas extranjeras<br>- Necesidad de regulación para mejorar la precisión en la recopilación de datos, reconociendo desafíos en velocidad de implementación, voluntad política y presupuesto. |
| L. M. M. | - Existe la necesidad de mejorar la infraestructura donde se pueda implementar todo el equipamiento que se vaya adquiriendo progresivamente y según lo planificado. |

**Tabla 14**

*Resumen de las necesidades de los recursos materiales y tecnológicos para enfrentar la ciberdelincuencia*

| Resumen |
| --- |
| - Se requiere tecnología avanzada para identificar a los autores de delitos informáticos.<br>- Necesidad de una infraestructura mejorada para implementar el equipamiento adquirido de manera progresiva y planificada.<br>- Se requiere la compra de dispositivos y la actualización de licencias para cubrir las necesidades de las FFAA.<br>- Fortalecimiento de Equipos Especializados:<br>o Fortalecimiento del Equipo de Respuesta ante Incidentes de Seguridad Digital del Perú.<br>o Establecimiento de otros Equipos de Respuesta ante Incidentes de Seguridad Informática.<br>o Constitución de centros de datos nacionales para garantizar la continuidad de servicios estratégicos.<br>- Necesidad de acuerdos de cooperación con países líderes en ciberseguridad, ciberdefensa y ciberinteligencia.<br>- Los softwares de la unidad especializada deben actualizarse anualmente, incluyendo las licencias.<br>- Falta de priorización de la eficiencia mediante la adquisición oportuna de dispositivos y la actualización de licencias.<br>- Falta de coordinación entre entidades gubernamentales y empresas extranjeras. |

## 4.4. Acciones que podrían cubrir las necesidades presentadas para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú

Existen varios factores a considerar que merecen un análisis en profundidad. Uno de ellos consiste en fortalecer la aplicación de la ley, es decir, la imposición efectiva de las normativas legales, que generalmente se logra a través de la captura y sanción de los delincuentes. Esto puede complementarse con operaciones de información destinadas a disuadir a quienes intenten cometer actos delictivos. Además, es importante destacar que las áreas relacionadas con la ciberseguridad ofrecen oportunidades laborales muy bien remuneradas por las empresas. A diferencia de otros tipos de organizaciones, en las cuales

la mejora de las capacidades suele lograrse mediante la adquisición de equipamiento, en este caso, la capacitación se presenta como la estrategia más efectiva para mejorar las capacidades de la DIVINDAT (Ver tabla 15).

Sin embargo, esta opción plantea un dilema para los miembros de la DIVINDAT, ya que podrían recibir ofertas laborales más atractivas en otros lugares. Por lo tanto, se deben explorar estrategias que incentiven al personal a capacitarse y permanecer en la unidad. Estas estrategias podrían incluir bonificaciones económicas basadas en la productividad, es decir, a mayor productividad, mayores recompensas, así como la posibilidad de diferir los salarios por capacitación. Para ilustrar este punto, se considera un escenario hipotético en el que el sueldo del personal de la policía se basa en su rango. Esto conduce a una incongruencia en cuanto a los niveles de capacitación requeridos, ya que los conocimientos técnicos necesarios para un desempeño eficaz en la DIVINDAT exigen un alto grado de preparación, el cual no se ve reflejado adecuadamente en la remuneración.

Además, si se toma en cuenta la diferencia salarial entre el personal de la DIVINDAT y aquel que trabaja en el sector privado con un nivel similar de capacitación, surgen dos posibles situaciones que podrían obstaculizar cualquier estrategia destinada a combatir la ciberdelincuencia. La primera es que el personal puede desmotivarse a capacitarse y trabajar en la DIVINDAT debido a la falta de reconocimiento institucional. La segunda es que, si se capacitan de manera excepcional, podrían encontrar más ventajosas las ofertas laborales en el sector privado, abandonando sus puestos en la DIVINDAT. Estos son factores que requieren una evaluación detallada en el desarrollo de una estrategia eficaz de lucha contra la ciberdelincuencia.

Lo que se requiere para que las investigaciones sobre ciberdelincuencia sean exitosas, es que se mantenga una relación coordinada entre el ministerio público y la DIVINDAT, por ende, es importante abordar públicamente el tema de la ciber inteligencia, para proporcionar conocimiento y desarrollar capacidades operativas, podría ser de mayor interés para la investigación.

Se requiere contar con una Estrategia de Ciberseguridad primero que contenga la situación actual de la ciberseguridad en el país. Luego determinar el responsable de la elaboración e implementación de la estrategia para combatir la ciberdelincuencia. Toda estrategia necesita de un presupuesto anual fijo para lograr objetivos, buscando fortalecer la Seguridad Nacional en Perú ante la ciberdelincuencia mediante medidas como la

capacitación del personal y la colaboración público-privada, con el objetivo de mejorar la resiliencia del país frente a las amenazas cibernéticas identificadas contando con una Estrategia de Ciberseguridad primero que contenga la situación actual de la ciberseguridad en el país.

Destaca la relevancia de marcos normativos y entidades especializadas para la construcción de una estructura sólida en seguridad cibernética. Se subraya la importancia del personal capacitado y la colaboración interinstitucional para monitorear el marco normativo destinado a proteger los activos críticos. Se plantea la idea de una coordinación más estrecha entre entidades gubernamentales y empresas privadas extranjeras, como Google y Facebook. Además, se reflexiona sobre la obtención de información a través de metadatos y la necesidad de analizar frecuencias y orígenes de accesos, destacando plataformas como WhatsApp, Instagram y Facebook. Se menciona la dependencia de servicios gratuitos que utilizan datos personales y se plantea la posibilidad de acceder a información de manera ética. Se aborda la falta de capacidad para bloquear acciones y se sugiere una mayor regulación y obtención de metadatos por parte de entidades gubernamentales para una recopilación más precisa de datos. Concluyendo, se destaca la importancia de un sistema integrado y se reconoce que, aunque se avanza en esa dirección, aún hay desafíos en términos de velocidad de implementación, voluntad política y presupuesto (Ver tabla 16).

**Tabla 15**

*Resumen de entrevista acerca de las acciones presentadas para enfrentar la ciberdelincuencia*

| Expertos | Resumen de respuesta |
|---|---|
| E. P. B. | - La formación de personal y la colaboración público-privada son algunas de las medidas que sugiere para reforzar la seguridad nacional de Perú frente a la ciberdelincuencia, con el objetivo último de aumentar la resistencia de la nación frente a las ciberamenazas identificadas. |
| D. R. B. | - Recomienda una mayor colaboración entre las organizaciones gubernamentales y las corporaciones internacionales, además de la necesidad de medidas reguladoras para mejorar la precisión de la recopilación de datos, al tiempo que reconoce los obstáculos relacionados con los recursos financieros, la determinación política y el tiempo de implementación. |
| V. I. G. | - Recomienda un plan global para mejorar la División de Investigación de Delitos Informáticos, que debería abarcar la aplicación de la ley, la disuasión mediante operaciones de inteligencia y una formación excepcional en ciberseguridad.<br>- Sugiere implementar el aplazamiento salarial y los incentivos financieros para retener al personal clave frente a las ofertas del sector privado", dice la propuesta. |
| L. M. M. | - Recomienda desarrollar una estrategia de ciberseguridad que abarque el estado actual de la ciberseguridad en la nación. |
| D. R. W. | - Sugiere determinar la responsabilidad de formular y ejecutar la estrategia de lucha contra la ciberdelincuencia.<br>- Recomienda que las investigaciones sobre ciberdelincuencia tengan éxito es necesaria una colaboración coordinada entre la DIVINDAT y el Ministerio Público. |
| G. M. C. | - Recomienda que la cuestión de la ciberinteligencia se aborde públicamente para generar capacidades operativas y difundir información podría suscitar más investigaciones. |

**Tabla 16**

*Resumen de acciones presentadas para enfrentar la ciberdelincuencia*

| Acción | Resumen |
|---|---|
| Fortalecer la aplicación de la ley | - Imposición efectiva de las normativas legales.<br>- Captura y sanción de los delincuentes. |
| Operaciones de información | - Realizar operaciones de información para disuadir a posibles delincuentes. |
| Capacitación en ciberseguridad | - Reconocer la importancia de la capacitación en ciberseguridad.<br>- Considerar la capacitación como la estrategia más efectiva para mejorar las capacidades de la DIVINDAT. |
| Incentivos para retener personal | - Explorar estrategias para incentivar al personal a capacitarse y permanecer en la unidad.<br>- Ofrecer bonificaciones económicas basadas en la productividad.<br>- Considerar la posibilidad de diferir los salarios por capacitación. |
| Coordinación entre entidades | - Mantener una relación coordinada entre el ministerio público y la DIVINDAT.<br>- Abordar públicamente el tema de la ciberinteligencia para proporcionar conocimiento y desarrollar capacidades operativas. |
| Desarrollo de una Estrategia de Ciberseguridad | - Contar con una estrategia de ciberseguridad que contenga la situación actual de la ciberseguridad en el país.<br>- Determinar el responsable de la elaboración e implementación de la estrategia. |
| Colaboración público-privada | - Buscar fortalecer la seguridad nacional mediante la colaboración público-privada. |
| Relevancia de marcos normativos | - Hay que destacar la importancia de marcos normativos y entidades especializadas para construir una estructura sólida en seguridad cibernética. |

| | |
|---|---|
| Colaboración internacional | - Recomendar una mayor colaboración entre organizaciones gubernamentales y corporaciones internacionales. |
| Regulación y obtención ética de datos | - Abordar la falta de capacidad para bloquear acciones y sugerir una mayor regulación y obtención ética de metadatos por parte de entidades gubernamentales. |
| Formación de personal y colaboración público-privada | - Recomendar la formación de personal y la colaboración público-privada para reforzar la seguridad nacional frente a la ciberdelincuencia. |
| Plan global para la División de Investigación de Delitos Informáticos | - Recomendar un plan global que abarque la aplicación de la ley, operaciones de inteligencia y formación excepcional en ciberseguridad para mejorar la División de Investigación de Delitos Informáticos. |
| Abordar públicamente la ciberinteligencia | - Sugerir abordar públicamente la ciberinteligencia para generar capacidades operativas y fomentar más investigaciones. |

## 4.5. Estrategia para enfrentar la ciberdelincuencia

Se va a presentar un lineamiento de Estrategia para fortalecer, en base a lo observado en el análisis de la realidad y situación actual, las necesidades en cada uno de los aspectos considerados, en donde se contemplan los siguientes puntos:

### 4.5.1. *Marco Jurídico- Legal*

- Crear una Ley específica en materia de ciberseguridad que:
    - Comprenda un inventario exhaustivo de los ciberdelitos, facilitando su tipificación, detección, disuasión, investigación y persecución.
    - Incluya la intención o tentativa de causar daño tecnológico, aunque el acto delictivo de violar el sistema tecnológico fracase debido a la eficacia de los controles diseñados para contener el ataque.
    - Defina, delimite y establezca los derechos, responsabilidades, obligaciones y facultades de los sectores público, privado y social en materia de ciberseguridad.
    - Homologue los siguientes términos: ciberseguridad, ciberdelincuencia organizada, ciberdelincuente, ciberespacio, cibergobierno, ciberpolicía,

ciberempresa, cibercompra, ciberproducto, ciberservicio, ciberusuario, cibertrabajador y ciberofensor.

- Elegir una autoridad competente para supervisar y llevar a cabo la Estrategia Nacional de Ciberseguridad.
- Adaptar las normas y reglamentos relacionados con los datos personales a los peligros del mundo digital.
- Asignar autoridades competentes y específicas que gobiernen, procuren justicia y juzguen el ámbito cibernético, incluidos los juicios a través de internet; utilizando las plataformas de TIC de comunicación disponibles, garantizando su disponibilidad, integridad y confidencialidad.
- Capacitar a los jueces que conocerán los casos relacionados con ciberseguridad, ciberdelincuencia, ciberdelitos y funcionamiento de las TIC para que los jueces tengan una perspectiva clara y a la vanguardia sobre los casos que les sean presentados por fiscales especializados.
- Incorporar un componente de colaboración internacional, ya que los delitos cibernéticos son internacionales.
- Elaborar un mapa de ruta específico que incluya autoridades involucradas, mecanismos de colaboración interinstitucional e indicadores de seguimiento.
- Establecer un cronograma de ejecución para las reformas legislativas.
- Promover acuerdos bilaterales y multilaterales con el fin de mejorar la colaboración global en la lucha contra la ciberdelincuencia.
- Establecer protocolos claros para la extradición y la prueba de casos transfronterizos de ciberdelincuentes.
- Participar activamente en iniciativas regionales e internacionales para compartir información y mejores prácticas.
- Fomentar la conciencia jurídica a través de la:
    - Creación de campañas para concienciar a jueces, fiscales y abogados sobre los desafíos y la gravedad de la ciberdelincuencia.
    - Planificación de programas de capacitación continua en ciberseguridad a los empleados del sistema legal.
    - Creación de métodos para que el sistema legal y las fuerzas del orden compartan información relevante sobre ciberdelitos.

### 4.5.2. *Capacidad del personal especializado*

- Hacer hincapié en las Administraciones Públicas, capacidades militares y de Defensa y otros sistemas de interés nacional, aumentar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas.
- Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas que permitan la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una defensa y protección más eficaz de las redes nacionales.
- Crear y mantener actualizados los procedimientos de prevención y detección, incluidos los procedimientos de respuesta a situaciones de crisis y los planes de contingencia específicos para incidentes de ciberseguridad de ámbito nacional, asegurándose de que se integren en el Sistema de Seguridad Nacional.
- Crear y llevar a cabo un programa de ejercicios de simulación de incidentes de ciberseguridad con el fin de evaluar y mejorar las medidas tomadas en este campo.
- Ampliar y mejorar continuamente las habilidades de defensa cibernética de las FFAA para garantizar la protección adecuada de sus redes y sistemas de información y telecomunicaciones, así como de otros sistemas que puedan afectar la Defensa Nacional. La creación del Mando Conjunto de Ciberdefensa será fortalecida y su colaboración con los diversos órganos capaces de reaccionar ante ataques cibernéticos en temas de interés común se incrementará.
- Potenciar las habilidades militares y de inteligencia para responder en el ciberespacio de manera oportuna, legítima y proporcionada ante amenazas o agresiones que puedan afectar la Defensa Nacional.

### 4.5.3. *Recursos materiales y tecnológicos*

- Mejorar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios, utilizando herramientas de colaboración entre el sector público y privado.
- Fomentar iniciativas de apoyo a la investigación, desarrollo e innovación en seguridad digital y ciberseguridad para pequeñas empresas, empresas, universidades y centros de investigación, a través de la facilitación del acceso a

programas de incentivos nacionales e internacionales y a través de programas innovadores de compra pública.

- Fomentar la innovación, la inversión, la internacionalización y la transferencia tecnológica en el sector industrial y de servicios de ciberseguridad, fomentando medidas de apoyo a las micropymes y pymes.
- Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, así como la seguridad desde el diseño, específicamente aquellas que apoyan las necesidades de interés nacional para fortalecer la autonomía digital, la propiedad intelectual e industrial.
- Promover las actividades de normalización y exigencia de requisitos de ciberseguridad en los productos y servicios de TIC, facilitar el acceso a productos y servicios que respondan a estos requisitos, fomentar la evaluación de la conformidad y la certificación, y apoyar la elaboración de catálogos.
- Promover la incorporación de perfiles profesionales de ciberseguridad en las relaciones laborales del sector público.
- Identificar, promover y conservar el talento en seguridad cibernética, con especial atención al ámbito de la investigación.
- Apoyar proyectos específicos de investigación, desarrollo e innovación en seguridad y defensa cibernéticas.
- Aumentar la inversión en herramientas de análisis forense y tecnologías avanzadas de ciberseguridad.
- Establecer acuerdos con empresas y organizaciones especializadas para la adquisición de tecnología de última generación.
- Garantizar que las herramientas utilizadas para investigar y prevenir ciberdelitos estén constantemente actualizadas.

# CAPÍTULO V
# CONCLUSIONES Y RECOMENDACIONES

## 5.1. Conclusiones

Las conclusiones a las que se llegaron en este estudio se presentan guardando relación con el análisis de los problemas, objetivos específicos y hallazgos, los cuales resolvieron la pregunta y cumplieron el objetivo general, confirmando de igual manera la hipótesis general postulada. No obstante, para un mejor entendimiento con los resultados analizados en el capítulo 4, se enuncian las conclusiones desde lo general a lo específico.

**Conclusión General.** Para abordar la ciberdelincuencia de manera efectiva, la estrategia propuesta enfatiza el fortalecimiento de la ciberseguridad mediante una serie de medidas integrales, entre estas, se destaca la creación de una legislación específica que contemple una amplia gama de ciberdelitos, acompañada por la designación de una autoridad responsable de supervisar su cumplimiento y la actualización de las normativas de datos personales para su adecuación al contexto digital, además, se sugiere una revisión exhaustiva de la legislación vigente para cerrar posibles brechas legales, en consecuencia, la estrategia también promueve una firme colaboración internacional mediante el establecimiento de acuerdos y protocolos para enfrentar desafíos transfronterizos.

**Conclusión específica 1.** La Ciberdelincuencia en Perú ha afectado la Seguridad Nacional a través de ataques a instituciones clave como el aeropuerto de Corpac, el Ministerio del Interior y las FFAA. Estos incidentes abarcan desde ransomware y filtraciones de información confidencial hasta campañas de desinformación. La pandemia resaltó la vulnerabilidad de los sistemas de salud, con ciberdelincuentes explotando la situación para sustraer bonos destinados a la población. Además, la seguridad e inteligencia del país se vieron comprometidas por la filtración de datos, con grupos como "Conti" y "Guacamaya" perpetrando estos ataques.

**Conclusión específica 2.** La realidad actual de los aspectos para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú es la siguiente:

- En cuanto a los aspectos jurídico-legales para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú, el país cuenta con varias leyes, entre ellas la Ley de Delitos Informáticos Nº 30096 y la Ley de Ciberdefensa Nº 30999, que regulan las actividades ilícitas relacionadas con la integridad de las redes

informáticas y establecen medidas de ciberdefensa a cargo de las FFAA, también está la Ley de Protección de Datos Personales Nº 29733, que busca salvaguardar la información personal.

- En cuanto a las capacidades del personal especializado, los profesionales de ciberseguridad deben poseer un conocimiento exhaustivo de sistemas informáticos, redes, protocolos y amenazas cibernéticas. Además, la habilidad de analizar datos y entender las últimas estrategias de ciberdelincuentes, como programa maligno, ransomware y phishing, es crucial. El personal de las FFAA se capacita según normas internacionales, y se ha iniciado un convenio con Estados Unidos para cursos de actualización en ciberseguridad.
- En cuanto a los recursos y materiales tecnológicos se emplean herramientas de ciberseguridad, sistemas de monitoreo, y centros de datos, donde la DIVINDAT es la encargada de combatir estos delitos, pues cuenta con departamentos especializados y herramientas como CELLEBRITE.

**Conclusión específica 3.** La realidad actual de las necesidades de los aspectos para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú es la siguiente:

- En cuanto a las necesidades jurídico-legales, se destaca la falta de celeridad en la implementación de leyes para abordar nuevas formas de ciberdelincuencia, generando un vacío legal que requiere alianzas constantes. Se aboga por incrementar las penas y medidas legales, así como la necesidad de políticas y estrategias más amplias, incluyendo la creación de un Comité Nacional de Ciberseguridad y la formulación de leyes específicas.
- En cuanto a las necesidades de las capacidades del personal, se subraya la importancia de implementar programas de formación y retención de talento humano, especialmente en aspectos estratégicos a nivel político, para garantizar la correcta ejecución de una estrategia integral contra la ciberdelincuencia. Además, se presenta una carencia en los recursos humanos especializados en ciberseguridad, particularmente en la gestión de sistemas a nivel nacional y la respuesta a ciberataques, evidenciando la baja capacidad en estas áreas.
- En cuanto a las necesidades de los recursos materiales y tecnológico, se rescata la urgencia de mejorar la infraestructura, adquirir progresivamente equipamiento de última generación, y mantener actualizados dispositivos y licencias; asimismo existentes demoras en las compras y actualizaciones continuas, el fortalecimiento

de entidades como PeCERT y CSIRT, la creación de centros de datos nacionales, y la búsqueda de acuerdos de cooperación internacional para el desarrollo del recurso humano y la obtención de software.

**Conclusión específica 4.** Se presentaron varias acciones estratégicas que destacan la importancia de fortalecer la aplicación de la ley, mediante la imposición efectiva de normativas legales y operaciones de información para disuadir a los delincuentes, reconociendo la necesidad de incentivar la capacitación del personal de la DIVINDAT, considerando bonificaciones económicas basadas en la productividad y la posibilidad de diferir salarios por formación. Adicionalmente, se sugiere una evaluación detallada de la relación entre la remuneración y el nivel de capacitación, así como estrategias para evitar desmotivación o la pérdida de talento. Además, se propone el desarrollo de una Estrategia de Ciberseguridad Nacional con un presupuesto anual fijo, responsables claros y consideración de la cooperación nacional e internacional. Por último, se reflexiona sobre la necesidad de una mayor regulación y obtención ética de metadatos, así como la importancia de un sistema integrado para abordar desafíos en velocidad de implementación, voluntad política y presupuesto.

## 5.2. Recomendaciones

Las recomendaciones se presentan en relación con cada una de las conclusiones previamente mencionadas.

**Recomendación general.** Se recomienda la implementación de algunas o todas las acciones expuestas en el punto 4.5., el cual es referente a la propuesta de la Estrategia para enfrentar la Ciberdelincuencia que afecta la Seguridad Nacional en Perú, por parte de las FFAA del Perú (CCFFAA – COCID), PNP (DIVINDAT), organizaciones privadas y públicas y a otras entidades.

**Recomendación específica 1.** Se recomienda a las FFAA del Perú, organizadas para las Acciones Militares por intermedio del Comando Operacional de Ciberdefensa (COCID), perteneciente al Conjunto de las Fuerzas Armadas, responsable del planeamiento operacional de la Ciberdefensa, así como también el Centro Nacional de Incidentes de Seguridad Informática (CENSI), Corporación Peruana de Aeropuertos y Aviación Comercial (CORPAC), Ministerio del Interior, Ministerio de Defensa y a otras entidades encargadas de enfrentar la ciberdelincuencia, establecer relaciones y fomentar un grupo de

trabajo que permita implementar medidas de seguridad más robustas y actualizadas en las instituciones clave. Además, establecer protocolos de respuesta ante incidentes de ciberseguridad y fortalecer la concienciación sobre la importancia de la seguridad cibernética en todos los niveles.

**Recomendación específica 2.** Se recomienda al Ministerio del Interior por intermedio del DIVINDAT (División de Investigación de Delitos de Alta Tecnología), Ministerio de Relaciones Exteriores, Ministerio de Economía y Finanzas, y otras instituciones relacionadas, dar una prioridad a la cooperación internacional a través de acuerdos bilaterales y multilaterales en la lucha contra el cibercrimen transnacional. También invertir en investigación y desarrollo en ciberseguridad, así como actualizar y fortalecer la legislación relacionada con la ciberdelincuencia, asegurando sanciones adecuadas.

**Recomendación específica 3.** Se sugiere a la Agencia Peruana de Cooperación Internacional (APCI) y otras empresas de ciberseguridad relacionadas, promover la formación de profesionales en ciberseguridad, integrar la ciberseguridad en la educación formal y establecer un programa nacional de concienciación pública sobre las amenazas cibernéticas.

**Recomendación específica 4.** Se recomienda a las FFAA del Perú (EP, MGP, FAP y CCFFAA), Ministerio de Transportes y Comunicaciones (MTC), Agencia de Compras de las Fuerzas Armadas (ACFFAA), y a otras entidades encargadas de preparar y equipar a la fuerza u órganos con responsabilidad de enfrentar la ciberdelincuencia, agilizar los procesos de adquisición de recursos materiales y tecnológicos para evitar demoras. Priorizar la mejora de la infraestructura y la obtención de equipos de última generación. Asimismo, se recomienda fortalecer las entidades como PeCERT y CSIRT para una respuesta más rápida y efectiva ante amenazas cibernéticas. Buscar activamente acuerdos de cooperación internacional para compartir conocimientos y recursos.

**Recomendación específica 5.** Se recomienda al Ministerio de Justicia, Agencia Nacional de Seguridad, y a otras entidades encargadas de enfrentar la ciberdelincuencia, reforzar la aplicación de la ley mediante la imposición efectiva de normativas legales y operaciones de información. Incentivar la capacitación del personal de la DIVINDAT con bonificaciones económicas basadas en la productividad y posibilidades de diferir salarios por formación. Evaluar y ajustar la relación entre la remuneración y el nivel de capacitación para evitar desmotivación. Desarrollar y financiar una Estrategia de Ciberseguridad Nacional

con enfoque en la cooperación nacional e internacional. Considerar una mayor regulación ética de metadatos y la implementación de un sistema integrado para abordar desafíos en velocidad de implementación, voluntad política y presupuesto.

**Recomendación específica 6.** Actualizar el marco normativo debido a que se cuenta con la norma internacional ISO 27001: 2022 y de esta forma mejorar significativamente la eficiencia y la eficacia y de la gestión de la seguridad de la información, lo que a su vez puede ayudar a mitigar los riesgos y proteger todos nuestros activos de información.

**Recomendación específica 7.** Se recomienda constituir un grupo de juristas que trabajen con los miembros especialistas en Ciberdefensa y lucha contra la Delincuencia de los sectores Interior, Defensa y PCM, para que puedan generar normativa funcional y coherente que permita regularizar el vacío legal existente que, ya que, al no tener un marco normativo actualizado o una propuesta de ley no estaríamos cumpliendo con el objetivo de formular correctamente una estrategia adecuada.

**Recomendación especifica 8.** Se recomienda implementar la ley de ciberseguridad cuyos responsables serian: La Presidencia del Consejo de Ministros, a través de la secretaria de gobierno digital (SEGDI), el Poder Judicial, la Dirección Nacional de Inteligencia (DINI), el MINDEF, el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), la Asociación de Gobiernos Regionales (AGR), la Sociedad Nacional de Industrias, la Cámara de Comercio de Lima (CCL), el Colegio de Abogados de Lima, la Confederación Nacional de Instituciones Empresariales Privadas (CONFIEP), la Asociación de Bancos del Perú, la Asociación para el fomento de la Infraestructura Nacional (AFIN) y la Red Científica Peruana (RCP).

**Recomendación específica 9.** Se recomienda a futuros investigadores interesados en la ciberdelincuencia que afecta la Seguridad Nacional en Perú o temas relacionados, que puedas continuar con el presente estudio, ampliando la información o implementando parte de la Estrategia propuesta, para que de esta manera se puedan potenciar la situación actual y cubrir las necesidades encontradas en los aspectos estudiados.

## REFERENCIAS BIBLIOGRÁFICAS


Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la Seguridad Nacional y Política Exterior. *Estudios Internacionales*, *53*(198), 169. https://doi.org/10.5354/0719-3769.2021.57067

Álvarez, D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista chilena de derecho y tecnología, 7(*1), 1-2.

Amandeep, S., Rajinder-Sandhu R., Sood, S., Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-ofthings environments. *Computers & Security*, *74*: 340-354. https://doi.org/10.1016/j.cose.2017.08.016

Amato, R., Pearson, R., Almagro-Garcia, J., Amaratunga, C., Lim, P., Suon, S., Sreng, S., Drury, E., Stalker, J., Miotto, O., Fairhurst, R. & Kwiatkowski, D. (2018). Origins of the current outbreak of multidrug-resistant malaria in southeast Asia: a retrospective genetic study. *The Lancet. Infectious Diseases*, *18*(3), 337–345. https://doi.org/10.1016/S1473-3099(18)30068-9

Astudillo, E. (2019). *El diseño e implementación de una estrategia de Seguridad Nacional y el nivel de efectividad de la respuesta del Estado Peruano ante las amenazas a la Seguridad Nacion*al. [Tesis Doctoral, Centro de Altos Estudios Nacionales -CAEN]. Repositorio CAEN. https://hdl.handle.net/20.500.13097/69

Ávila, V. (2022). Análisis sobre el establecimiento de una Agencia Nacional de Ciberseguridad con base en las Recomendaciones de la Estrategia Nacional de Ciberseguridad. *INFOTEC Centro De Investigación E Innovación En Tecnologías De La Información Y Comunicación*. Infotec Repositorio. https://infotec.repositorioinstitucional.mx/jspui/handle/1027/565

Camps, P. (2019). Ciber*defensa y ciberseguridad: Nuevas amenazas a la Seguridad Nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito*. Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). 6: 80-93. https://acortar.link/vi344T

Devia, E. (2017). *Delito informático: Estafa informática del artículo 248.2 del Código Penal*. [Tesis doctoral, Universidad de Sevilla]. Depósito de Investigación Universidad de Sevilla. https://idus.us.es/handle/11441/75625

Decreto de Urgencia N° 007-2020 (2020). *Decreto de urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento*. El Peruano. https://acortar.link/XohmxR

Diaz, R, (2022). Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe *Comisión Económica para América*. Comisión Económica para América Latina y el Caribe. Repositorio CEPAL. https://hdl.handle.net/11362/48065

Díaz, J. (2018). Ciencia y Tecnología en clave de Seguridad Nacional. *Revista de Estudios en Seguridad Internacional*, *4*(2), 253-275.

http://www.seguridadinternacional.es/resi/index.php/revista/article/view/108

Dupuy, D. (2019), *"Ciberdelitos. Desafíos para trabajar", en Era digital: delito y prevención*. Editorial Jusbaires.

Ferrazzuolo, V. (2019), *Era digital: delito y prevención*. Buenos Aires, Editorial Jusbaires.

Gaona, L., Trillos, J., & Bayona, A. (2019). *Ciberseguridad y ethical hacking: la importancia de proteger los datos del usuario. Encuentro internacional de educación en ingeniería*. pp.1-10. https://doi.org/10.26507/ponencia.248

González-Pulido, I. (2022). *Diligencias de investigación tecnológicas para la lucha contra la ciberdelincuencia. Especial referencia a la utilización del registro remoto para la investigación de ciberataques contra infraestructuras críticas y estratégicas* [Tesis doctoral, Universidad de Salamanca, España]. Repositorio Documental Gredos. http://hdl.handle.net/10366/149611

Gonzales, P. (2022). *Análisis de la participación de las fuerzas armadas para optimizar el cumplimiento de la política multisectorial de Seguridad y Defensa Nacional al 2030* [Tesis de maestría, Centro de Altos Estudios Nacionales-CAEN]. Repositorio CAEN. https://repositorio.caen.edu.pe/items/c27ef099-6078-4857-bac5-12703d4c0058

Huamán, M. (2020). *Los delitos informáticos en Perú y la suscripción del convenio de Budapest* [Tesis de licenciatura, Universidad Andina del Cusco-UAC]. Repositorio UAC. https://hdl.handle.net/20.500.12557/4116

Huancco, E. (2017). *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017* [Tesis de Licenciatura, Universidad Nacional de San Agustín-UNSA]. Repositorio UNSA. https://repositorio.unsa.edu.pe/handle/UNSA/6436

Intelligence and National Security Alliance (INSA, 2013) *Operational Levels of Cyber Intelligence.* INSA. https://acortar.link/2YAnco

INTERPOL. (2021). *La Ciberdelincuencia*. Madrid: Interpol.

Izaguirre, J. & León, F. (2018). Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal*, *3*(9), 180–189. https://doi.org/10.33890/INNOVA.V3.N9.2018.837

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

León, E., Tesillo, C., Escobar, Y., & Godoy, L. (2022). Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. *Innovación Y Software*, *3*(2), 109-120. https://doi.org/10.48168/innosoft.s9.a62

Ley Nº 30999 del 2005. Ley de Ciberdefensa. Libro Blanco de la Defensa Nacional del Perú. Ministerio de Defensa.

Ley Nº 30096 del 2013. Delitos Informáticos (22 de octubre del 2013). Diario Oficial El Peruano Nº 505484-2013.

Ley Nº 29733 del 2011. Protección de Datos Personales (03 de julio del 2011). Diario Oficial El Peruano Nº 445746- 2011. https://www.minjus.gob.pe/wpcontent/uploads/2013/04/LEY29733.pdf

Maldonado-Mera, B., Benavides, K., & Buenaño, J. (2017). Dimensional analysis of the strategy concept. *Revista Ciencia UNEMI, 10*(25), 25-35. https://doi.org/10.29076/issn.2528-7737vol10iss25.2017pp25-35p

Mateos, I. (2013). Ciberdelincuencia Desarrollo y persecución tecnológica. Universidad Politécnica de Madrid. https://oa.upm.es/22176/

Ministerio de Defensa. (2017). *Planeamiento estratégico del sector defensa en el campo militar/Directiva General (DG) N.° 05-2017-MINDEF-SG/VPD/DIGEPE/DIPPED*. https://www.mindef.gob.pe/informacion/documentos/RM%20927_2017.pdf

Naranjo, Y., Ávila, M., & Concepción, J. (2018). Las estrategias como herramienta en el desarrollo científico de Enfermería. *Revista Archivo Médico de Camagüey, 22*(4), 564-580. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1025-02552018000400564&lng=es&tlng=es.

Nizovtsev, Y., Lyseiuk, A., & Kelman, M. (2022). From self-affirmation to national security threat: Analyzing the Ukraine's foreign experience in countering cyberattacks. *Revista científica General José María Córdova, 20*(38), 355–370. https://doi.org/10.21830/19006586.905

Núñez, F., & Carhuancho, B. (2020). Ciberdelincuencia en tiempos de COVID-19: ¿La vulneración a derechos constitucionales? *Revista Lumen, 16*(1), 93-100. https://doi.org/10.33539/lumen.2020.v16n1.2287

Ormachea, F. (2020). *Estrategias integradas de ciberseguridad para el fortalecimiento de la Seguridad Nacional* [Tesis de Doctoral. Centro de Altos Estudios Nacionales-CAEN]. Repositorio CAEN. https://www.recide.caen.edu.pe/index.php/recide/article/view/36

Organización de los Estados Americanos (2020). *Reporte Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe.* Banco Interamericano de Desarrollo.

Organización de los Estados Americanos (2022). *Reporte sobre el desarrollo de la fuerza laboral y ciberseguridad en una era de escasez de talento y habilidades*. Organización de los Estados Americanos. *https://acortar.link/SJ438V*

Organización de los Estados Americanos (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe*. Symantec. https://acortar.link/QbetIT

Ortega, J. (2018). Seguridad y Defensa Nacional en México. *Estudios en Seguridad y Defensa, 13*(26), 141-152. https://doi.org/10.25062/1900-8325.225

Panda Security (2019) *Glosario de términos-Portal web Antivirus Panda*. https://www.pandasecurity.com/es/security-info/glossary/LetraC#

Panda Security (2017) *Peligros del Spyware* /Portal web de la plataforma Antivirus Panda. https://www.pandasecurity.com/spain/mediacenter /seguridad/peligros-spyware/.

Paredes, J. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010* [Tesis de maestría, Universidad Nacional Mayor de San Marcos-UNMSM]. Repositorio UNMSM. https://hdl.handle.net/20.500.12672/10314

Rada, K. (2022). *Herramientas de análisis forense digital orientadas a infraestructuras ti como medio de investigación en delitos informáticos* [Tesis de segunda especialidad]. Universidad Nacional Abierta y a Distancia. Repositorio UNED. https://repository.unad.edu.co/handle/10596/48990

Payá-Santos, C., Cremades-Guisado, Á., & Delgado-Morán, J. J. (2017). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. *Ventana indiscreta, 7*(1), 237–270. https://doi.org/10.5377/rpsp.v7i1.4312

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*, 55-76. https://doi.org/10.58211/recide.v4i1.99

Rincón-Arteaga, J., Quijano-Díaz, A., Castiblanco-Hernández, S., Urquijo-Vanegas, J., & Pregonero-León, Y. (2022). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista criminalidad, 64*(3), 95–116. https://doi.org/10.47741/17943108.368

Rollano, R (2012) *Ataques a la seguridad informática y telecomunicaciones en el contexto internacional*. Artículo publicado en La Razón/Gaceta Jurídica.

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-JPC"]. Repositorio JPC. https://repositorio.adp.edu.pe/handle/ADP/170

RSA (2012). Getting Ahead of Advanced Threats. The Security Division of EMC. https://www.rsashare.com/leadership/articles/gettingahead-of-advanced-threats.htm

Saiz, G., Saiz, G., Gómez, G., & Martínez, M. (2018). Tecnologías de la Información y las Comunicaciones: desafío que enfrenta la universidad de ciencias médicas. *EDUMECENTRO*, *10*(1), 168–182. https://revedumecentro.sld.cu/index.php/edumc/article/view/908

Sistema de Defensa Nacional (2015). Doctrina de Seguridad y Defensa Nacional. Secretaria de Seguridad y Defense materiales.

Segura, C. (2021). Innovación de la estrategia militar. *Revista Fuerza Aérea EU, 3(2).* 13-23. https://acortar.link/kfA4bS

Taipe, I. (2017). *La auditoría de seguridad informática y su relación en la ciberseguridad de la Fuerza Aérea del Perú año 2017* [Tesis doctoral]. Fuerza Aérea del Perú. http://repositorio.fap.mil.pe/handle/fap/49

Tenorio, J. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia* [Tesis de maestría, Academia Diplomática del Perú "Javier Pérez de Cuéllar-JPC"]. Repositorio Institucional JPC. https://repositorio.adp.edu.pe/handle/ADP/71

Tenorio, M. (2021). Aproximaciones a la seguridad y a la supremacía civil en el entorno constitucional de México y Colombia. *Prolegómenos*, *24*(48), 69–81. https://doi.org/10.18359/prole.5411

Unión Internacional de Telecomunicaciones (2018). *Global Cybersecurity Index (GCI).* Unión Internacional de Telecomunicaciones. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Valencia-Arias, A., Patiño-Toro, O., Arenas-Fernández, A., Garcés-Giraldo, L., Umba-López, A., & Benjumea-Arias, M. (2020). Tendencias investigativas en el estudio de la ciberdefensa: un análisis bibliométrico. *Revista Ibérica de Sistemas e tecnologías de Informaçã, 1(*29), 366-379. https://acortar.link/NWq5ia

Vargas, A. (2008) ¿Cómo entender la seguridad y la defensa? *Democracia, seguridad y defensa* (29), 2-4.

Vargas, R., Recalde, L. y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, *Revista Latinoamericana de Estudios de Seguridad*, (20).

https://doi.org/10.17141/urvio.20.2017.2571

Villarrubia, G. (2021). *Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la política de seguridad y defensa nacional en la región Lima* [Tesis de maestría, Centro de Altos Estudios Nacionales-CAEN]. Repositorio CAEN. https://repositorio.caen.edu.pe/server/api/core/bitstreams/cdccbd52-9e8f-4c82-80ff-3b5260d9b677/content

Zavaleta, H. (2020). Análisis y reflexiones de la Política de Seguridad y Defensa Nacional (2001-2018) en pos del fortalecimiento de la Seguridad Nacional. *Revista De Ciencia E Investigación En Defensa - CAEN*, *1*(4), 63–75. https://recide.caen.edu.pe/index.php/recide/article/view/45

# ANEXOS

## Anexo 1: Matriz de consistencia

### Título: Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú

| Problema | Objetivo | Hipótesis | Categorías de análisis o unidades temáticas | Metodología |
|---|---|---|---|---|
| **Problema General**<br>¿Qué estrategia debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?<br><br>**Problemas Específicos**<br>¿Qué entes desarrollan ciberdelincuencia que podrían afectar la Seguridad Nacional en Perú?<br><br>¿Cuáles son los aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos con los que se cuentan para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | **Objetivo General**<br>Formular la estrategia que debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.<br><br>**Objetivos Específicos**<br>Identificar los entes que desarrollan la ciberdelincuencia que podrían afectar la Seguridad Nacional en Perú.<br><br>Identificar los aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos con los que se cuentan para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú. | **Hipótesis General**<br>La estrategia que debe desarrollarse para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú, es una integral en donde implica la labor de las diferentes instituciones del Estado y que considera:<br>- Identificar los entes que desarrollan la ciberdelincuencia, a fin de combatirlos o neutralizarlos.<br>- La necesidad de un marco legal.<br>- La capacidad que presenta el personal especializado para enfrentarla.<br>- Los recursos materiales y tecnológicos que pueden emplearse. | Seguridad Nacional<br>Ciberdelincuencia<br>- Entes que desarrollan ciberdelincuencia en contra de Perú<br>- Hackers<br>- Crackers<br>- Piratas informáticos<br>- Organizaciones delictivas<br>Estrategia para enfrentar la ciberdelincuencia<br>- Marco jurídico – legal<br>- Capacidad del personal especializado<br>- Recursos materiales y tecnológicos | **Enfoque**<br>- Cualitativo<br><br>**Tipo**<br>- Según su finalidad: Básica<br>- Según su carácter: Descriptiva<br>- Según su alcance temporal: Transversal.<br><br>**Método**<br>- Análisis<br><br>**Diseño**<br>Análisis documental<br><br>**Población**<br>Material bibliográfico y audiovisual relacionado a las unidades temáticas a la que se tenga acceso.<br>Personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional de Perú, perteneciente a las diferentes instituciones gubernamentales que se dedican a brindar la Seguridad Nacional (Dirección Nacional de Inteligencia, FFAA, Policía Nacional del Perú, entre otros).<br><br>**Muestra**<br>Todo el material bibliográfico relacionado a las unidades temáticas a la que se tenga acceso.<br>Personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional de Perú, al cual sea viable entrevistar y |

| | | | | |
|---|---|---|---|---|
| ¿Cuáles son las necesidades en aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?<br><br>¿Cuáles son las acciones que podrían cubrir las necesidades presentadas para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | Identificar las necesidades en aspectos jurídico-legales, capacidades del personal especializado, y recursos materiales y tecnológicos para poder enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.<br><br>Determinar las acciones que podrían cubrir las necesidades presentadas para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú. | | | que pertenezca a alguna institución gubernamental que se dedique a brindar la Seguridad Nacional (Dirección Nacional de Inteligencia, FFAA, Policía Nacional del Perú, entre otros).<br><br>**Técnicas e instrumentos de recolección de información**<br><br>**Técnicas:** Análisis documental y entrevista.<br><br>**Instrumentos:** Ficha bibliográfica, ficha de análisis y guía de entrevista semiestructurada.<br><br>**Técnicas de procesamiento de la información:**<br>Análisis de contenido<br>PESTEL |

## Anexo 2. Instrumento para la toma de datos

## GUÍA DE ENTREVISTA

1. **Presentación del investigador**
2. **Presentación del objetivo de la investigación**
3. **Introducción a la entrevista**
4. **Datos sociodemográficos**
   - Nombre del entrevistado:
   - Grado profesional:
   - Área de formación académica:
   - Áreas de experiencia profesional:
   - Institución donde labora:
   - Tiempo de experiencia:
5. **Preguntas principales**
   - ¿Usted conoce actores, gentes o entes que en algún momento han desarrollado actos de ciberdelincuencia que afectaron la Seguridad Nacional en Perú? ¿Cuáles?
   - ¿Usted conoce aspectos jurídico-legales con los que se cuentan para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuales?
   - ¿Usted conoce las capacidades que presenta el personal especializado para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles?
   - ¿Usted conoce los recursos materiales y tecnológicos que se emplean para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles?
   - ¿Cuáles considera que son las necesidades en aspectos jurídico-legales para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?
   - ¿Cuáles considera que son las capacidades del personal que falta desarrollar para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?
   - ¿Cuáles considera que son los recursos materiales y tecnológicos que hacen falta para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?

6. **Preguntas para cierre de entrevista**

   - ¿Qué otros aspectos consideran necesarios tomar en cuenta para la investigación, con relación al desarrollo de una estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú?

## Anexo 3. Formato de V de Aiken

### 1. Datos generales:

| | |
|---|---|
| Nombre del juez: | |
| Grado profesional: | |
| Área de formación académica: | |
| Áreas de experiencia profesional: | |
| Institución donde labora: | |
| Tiempo de experiencia: | |

### 2. Propósito de la evaluación:

Validar el contenido del instrumento por juicio de expertos.

### 3. Presentación de instrucciones para el juez:

De acuerdo con los siguientes indicadores califique cada una de las preguntas según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br><br>La pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | La pregunta no es clara. |
| | 2. Bajo Nivel | La pregunta requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos de la pregunta. |
| | 4. Alto nivel | La pregunta es clara, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** | 1. Totalmente en desacuerdo (no | La pregunta no tiene relación lógica con la categoría. |

| | | |
|---|---|---|
| La pregunta tiene relación lógica con la categoría que está midiendo. | cumple con el criterio) | |
| | 2. Desacuerdo (bajo nivel de acuerdo) | La pregunta tiene una relación tangencial /lejana con la categoría. |
| | 3. Acuerdo (moderado nivel) | La pregunta tiene una relación moderada con la categoría que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | La pregunta se encuentra está relacionado con la categoría que está midiendo. |
| **RELEVANCIA**<br><br>La pregunta es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | La pregunta puede ser eliminado sin que se vea afectada la medición de la categoría. |
| | 2. Bajo Nivel | La pregunta tiene alguna relevancia, pero otra pregunta puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | La pregunta es relativamente importante. |
| | 4. Alto nivel | La pregunta es muy relevante y debe ser incluido. |

***Leer con detenimiento las preguntas y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente***

| |
|---|
| 1. No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

**4. Criterios de validación:**

Puntúe a continuación cada pregunta

| Pregunta | Claridad | Coherencia | Relevancia | Sugerencia |
|---|---|---|---|---|
| ¿Usted conoce actores, agentes o entes que en algún momento han desarrollado actos de ciberdelincuencia que afectaron la Seguridad Nacional en Perú? ¿Cuáles? | | | | |
| ¿Usted conoce aspectos jurídico-legales con los que se cuentan para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles? | | | | |
| ¿Usted conoce las capacidades que presenta el personal especializado para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles? | | | | |
| ¿Usted conoce los recursos materiales y tecnológicos que se emplean para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles? | | | | |
| ¿Cuáles considera que son las necesidades en aspectos jurídico-legales para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | | | | |

| | | | | |
|---|---|---|---|---|
| ¿Cuáles considera que son las capacidades del personal que falta desarrollar para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | | | | |
| ¿Cuáles considera que son los recursos materiales y tecnológicos que hacen falta para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | | | | |
| ¿Qué otros aspectos consideran necesarios tomar en cuenta para la investigación, con relación al desarrollo de una estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | | | | |

_____

Firma

DNI:

Fecha:

# Anexo 4. Validación de expertos

**Formato de V de Aiken**

1. **Datos generales:**

| | |
|---|---|
| Nombre del juez: | Guido Mulluni Cutipa |
| Grado profesional: | Magister |
| Área de formación académica: | Universidad Católica |
| Áreas de experiencia profesional: | Área T.I. |
| Institución donde labora: | Dirección Nacional de Inteligencia |
| Tiempo de experiencia: | 5 Años |

2. **Propósito de la evaluación:**

   Validar el contenido del instrumento por juicio de expertos.

3. **Presentación de instrucciones para el juez:**

   De acuerdo con los siguientes indicadores califique cada uno de las preguntas según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br><br>La pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | La pregunta no es clara. |
| | 2. Bajo Nivel | La pregunta requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos de la pregunta. |
| | 4. Alto nivel | La pregunta es clara, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** | 1. Totalmente en desacuerdo (no | La pregunta no tiene relación lógica con la categoría. |

| | | |
|---|---|---|
| La pregunta tiene relación lógica con la categoría que está midiendo. | cumple con el criterio) | |
| | 2. Desacuerdo (bajo nivel de acuerdo) | La pregunta tiene una relación tangencial /lejana con la categoría. |
| | 3. Acuerdo (moderado nivel) | La pregunta tiene una relación moderada con la categoría que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | La pregunta está relacionada con la categoría que está midiendo. |
| **RELEVANCIA**<br><br>La pregunta es esencial o importante, es decir debe ser incluida. | 1. No cumple con el criterio | La pregunta puede ser eliminada sin que se vea afectada la medición de la categoría. |
| | 2. Bajo Nivel | La pregunta tiene alguna relevancia, pero otra pregunta puede estar incluyendo lo que mide esta. |
| | 3. Moderado nivel | La pregunta es relativamente importante. |
| | 4. Alto nivel | La pregunta es muy relevante y debe ser incluida. |

***Leer con detenimiento las preguntas y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente***

| |
|---|
| 1 No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

**4. Criterios de validación:**

Puntúe a continuación cada pregunta

| Pregunta | Claridad | Coherencia | Relevancia | Sugerencia |
|---|---|---|---|---|
| ¿Tiene Ud. conocimiento de agentes o actores de amenaza que hayan participado en ciberdelincuencia con un potencial riesgo para la Seguridad Nacional? ¿Cuáles son y cómo los clasificaría? | **4** | **4** | **4** | |
| ¿Está Ud. familiarizado con el marco normativo nacional relacionado con la ciberdelincuencia y su conformidad con el marco normativo internacional? ¿Podría mencionar algunos ejemplos de ambos? | **4** | **4** | **4** | |
| ¿Conoce las capacidades con las que cuenta actualmente el personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Podría mencionar algunas? | **4** | **4** | **3** | **En general las capacidades son de índole reservadas. Por otro lado, esta pregunta puede estar siendo incluida en una que viene más adelante: ¿Qué capacidades/habilidades cree Ud. que el personal encargado necesita desarrollar …?** |
| ¿Puede mencionar los recursos materiales y tecnológicos utilizados actualmente para combatir la | **4** | **4** | **3** | **De la misma manera, los recursos en general son reservados. También puede** |

| | | | | |
|---|---|---|---|---|
| ciberdelincuencia que afecta la Seguridad Nacional en Perú? | | | | **estar siendo incluida en otra que viene más adelante: ¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios …?**<br>**Por otro lado, los recursos tecnológicos incluyen los materiales que pueden ser tangibles e intangibles (hardware y software). Podría quedar solo con recursos tecnológicos.** |
| ¿Cuáles cree Ud. que son las deficiencias en el marco normativo nacional para combatir la ciberdelincuencia que afecta la Seguridad Nacional?" | **4** | **4** | **4** | |
| ¿Qué capacidades/habilidades cree Ud. que el personal encargado necesita desarrollar para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | **3** | **4** | **4** | **Puede ser un poco más claro de la siguiente forma:**<br>**¿Qué capacidades/habilidades cree Ud. que el personal encargado de combatir la ciberdelincuencia que afecta la Seguridad Nacional necesita desarrollar?** |
| ¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios para combatir la ciberdelincuencia que | **4** | **4** | **4** | **Los recursos tecnológicos incluyen los materiales que pueden ser tangibles e** |

| | | | | |
|---|---|---|---|---|
| afecta la Seguridad Nacional en Perú y que actualmente no están disponibles? | | | | **intangibles (hardware y software). Podría quedar solo con recursos tecnológicos.** |
| ¿Qué otros aspectos creen Ud. que deban ser considerados al desarrollar una estrategia para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | **4** | **4** | **4** | |

**En general no se hace explicita el rol de la sociedad, empresa privada y la academia, en su participación en combatir la ciberdelincuencia que afecta la Seguridad Nacional. Si fuera posible se podría incluir en alguna pregunta.**

Firma

DNI: 40399624

Fecha: 1 – 10 - 23

**Formato de V de Aiken**

1. **Datos generales:**

| | |
|---|---|
| Nombre del juez: | Enrique B. Dobbertin Guerrero |
| Grado profesional: | Magister |
| Área de formación académica: | Escuela de Oficiales de la Fuerza Aérea del Perú |
| Áreas de experiencia profesional: | Calificación en Ciberdefensa |
| Institución donde labora: | Fuerza Aérea del Perú |
| Tiempo de experiencia: | 23 años |

2. **Propósito de la evaluación:**

Validar el contenido del instrumento por juicio de expertos.

3. **Presentación de instrucciones para el juez:**

De acuerdo con los siguientes indicadores califique cada uno de las preguntas según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br><br>La pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | La pregunta no es clara. |
| | 2. Bajo Nivel | La pregunta requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos de la pregunta. |
| | 4. Alto nivel | La pregunta es clara, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** | 1. Totalmente en desacuerdo (no | La pregunta no tiene relación lógica con la categoría. |

| | | |
|---|---|---|
| La pregunta tiene relación lógica con la categoría que está midiendo. | cumple con el criterio) | |
| | 2. Desacuerdo (bajo nivel de acuerdo) | La pregunta tiene una relación tangencial /lejana con la categoría. |
| | 3. Acuerdo (moderado nivel) | La pregunta tiene una relación moderada con la categoría que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | La pregunta está relacionada con la categoría que está midiendo. |
| **RELEVANCIA**<br><br>La pregunta es esencial o importante, es decir debe ser incluida. | 1. No cumple con el criterio | La pregunta puede ser eliminada sin que se vea afectada la medición de la categoría. |
| | 2. Bajo Nivel | La pregunta tiene alguna relevancia, pero otra pregunta puede estar incluyendo lo que mide esta. |
| | 3. Moderado nivel | La pregunta es relativamente importante. |
| | 4. Alto nivel | La pregunta es muy relevante y debe ser incluida. |

***Leer con detenimiento las preguntas y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente***

| |
|---|
| 1 No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

**4. Criterios de validación:**

Puntúe a continuación cada pregunta

| Pregunta | Claridad | Coherencia | Relevancia | Sugerencia |
|---|---|---|---|---|
| ¿Tiene Ud. conocimiento de agentes o actores de amenaza que hayan participado en ciberdelincuencia con un potencial riesgo para la Seguridad Nacional? ¿Cuáles son y como los clasificaría? | **4** | **4** | **4** | |
| ¿Está Ud. familiarizado con el marco normativo nacional relacionado con la ciberdelincuencia y su conformidad con el marco normativo internacional? ¿Podría mencionar algunos ejemplos de ambos? | **4** | **4** | **4** | |
| ¿Conoce las capacidades con las que cuenta actualmente el personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Podría mencionar algunas? | **4** | **4** | **4** | |
| ¿Puede mencionar los recursos materiales y tecnológicos utilizados actualmente para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | **4** | **4** | **4** | |

| | | | | |
|---|---|---|---|---|
| ¿Cuáles cree Ud. que son las deficiencias en el marco normativo nacional para combatir la ciberdelincuencia que afecta la Seguridad Nacional?" | **4** | **4** | **4** | |
| ¿Qué capacidades/habilidades cree Ud. que el personal encargado necesita desarrollar para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | **4** | **4** | **4** | |
| ¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú y que actualmente no están disponibles? | **4** | **4** | **4** | |
| ¿Qué otros aspectos creen Ud. que deban ser considerados al desarrollar una estrategia para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | **4** | **4** | **4** | |

Firma Digital Fuerza Aérea del Perú
Firmado digitalmente por DOBBERTIN GUERRERO Enrique Bernardino FAU 20144364059 hard
Motivo: Soy el autor del documento
Fecha: 26.09.2023 12:21:26 -05:00

Firma

DNI: 43718855

Fecha: 26/09/2023

**Formato de V de Aiken**

1. **Datos generales:**

| | |
|---|---|
| Nombre del juez: | DIAZ MANTILLA JORGE JUAN |
| Grado profesional: | BACHILLER EN CIENCIAS MATEMÁTICAS |
| Área de formación académica: | CONCYBERDEF |
| Áreas de experiencia profesional: | CONCYBERDEF |
| Institución donde labora: | CONCYBERDEF |
| Tiempo de experiencia: | 13 AÑOS |

2. **Propósito de la evaluación:**

Validar el contenido del instrumento por juicio de expertos.

3. **Presentación de instrucciones para el juez:**

De acuerdo con los siguientes indicadores califique cada uno de las preguntas según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br><br>La pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | La pregunta no es clara. |
| | 2. Bajo Nivel | La pregunta requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos de la pregunta. |
| | 4. Alto nivel | La pregunta es clara, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** | 1. Totalmente en desacuerdo (no | La pregunta no tiene relación lógica con la categoría. |

| | | |
|---|---|---|
| La pregunta tiene relación lógica con la categoría que está midiendo. | cumple con el criterio) | |
| | 2. Desacuerdo (bajo nivel de acuerdo) | La pregunta tiene una relación tangencial /lejana con la categoría. |
| | 3. Acuerdo (moderado nivel) | La pregunta tiene una relación moderada con la categoría que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | La pregunta está relacionada con la categoría que está midiendo. |
| **RELEVANCIA**<br><br>La pregunta es esencial o importante, es decir debe ser incluida. | 1. No cumple con el criterio | La pregunta puede ser eliminada sin que se vea afectada la medición de la categoría. |
| | 2. Bajo Nivel | La pregunta tiene alguna relevancia, pero otra pregunta puede estar incluyendo lo que mide esta. |
| | 3. Moderado nivel | La pregunta es relativamente importante. |
| | 4. Alto nivel | La pregunta es muy relevante y debe ser incluida. |

***Leer con detenimiento las preguntas y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente***

| |
|---|
| 1 No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

**4. Criterios de validación:**

Puntúe a continuación cada pregunta

| Pregunta | Claridad | Coherencia | Relevancia | Sugerencia |
|---|---|---|---|---|
| ¿Tiene Ud. conocimiento de agentes o actores de amenaza que hayan participado en ciberdelincuencia con un potencial riesgo para la Seguridad Nacional? ¿Cuáles son y como los clasificaría? | 4 | 4 | 4 | |
| ¿Está Ud. familiarizado con el marco normativo nacional relacionado con la ciberdelincuencia y su conformidad con el marco normativo internacional? ¿Podría mencionar algunos ejemplos de ambos? | 4 | 4 | 4 | |
| ¿Conoce las capacidades con las que cuenta actualmente el personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Podría mencionar algunas? | 4 | 4 | 4 | |
| ¿Puede mencionar los recursos materiales y tecnológicos utilizados actualmente para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | 4 | 4 | 4 | |

| | | | | |
|---|---|---|---|---|
| ¿Cuáles cree Ud. que son las deficiencias en el marco normativo nacional para combatir la ciberdelincuencia que afecta la Seguridad Nacional?" | 4 | 4 | 4 | |
| ¿Qué capacidades/habilidades cree Ud. que el personal encargado necesita desarrollar para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | 4 | 4 | 4 | |
| ¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú y que actualmente no están disponibles? | 4 | 4 | 4 | |
| ¿Qué otros aspectos cree Ud. que deban ser considerados al desarrollar una estrategia para combatir la ciberdelincuencia que afecta la Seguridad Nacional ? | 4 | 4 | 4 | |

Firma

DNI: 43669448

Fecha: 22 DE SETIEMBRE DEL 2023

**Formato de V de Aiken**

1. **Datos generales:**

| | |
|---|---|
| Nombre del juez: | Víctor Antonio Irrazabal Gómez |
| Grado profesional: | Magister |
| Área de formación académica: | Ingeniería de Telecomunicaciones |
| Áreas de experiencia profesional: | Telecomunicaciones, Investigación y Ciberdefensa |
| Institución donde labora: | Comando Operacional de Ciberdefensa |
| Tiempo de experiencia: | 04 Años |

2. **Propósito de la evaluación:**

Validar el contenido del instrumento por juicio de expertos.

3. **Presentación de instrucciones para el juez:**

De acuerdo con los siguientes indicadores califique cada uno de las preguntas según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br><br>La pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | La pregunta no es clara. |
| | 2. Bajo Nivel | La pregunta requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos de la pregunta. |
| | 4. Alto nivel | La pregunta es clara, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** | 1. Totalmente en desacuerdo (no | La pregunta no tiene relación lógica con la categoría. |

| | | |
|---|---|---|
| La pregunta tiene relación lógica con la categoría que está midiendo. | cumple con el criterio) | |
| | 2. Desacuerdo (bajo nivel de acuerdo) | La pregunta tiene una relación tangencial /lejana con la categoría. |
| | 3. Acuerdo (moderado nivel) | La pregunta tiene una relación moderada con la categoría que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | La pregunta está relacionada con la categoría que está midiendo. |
| **RELEVANCIA**<br><br>La pregunta es esencial o importante, es decir debe ser incluida. | 1. No cumple con el criterio | La pregunta puede ser eliminada sin que se vea afectada la medición de la categoría. |
| | 2. Bajo Nivel | La pregunta tiene alguna relevancia, pero otra pregunta puede estar incluyendo lo que mide esta. |
| | 3. Moderado nivel | La pregunta es relativamente importante. |
| | 4. Alto nivel | La pregunta es muy relevante y debe ser incluida. |

***Leer con detenimiento las preguntas y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente***

| |
|---|
| 1 No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

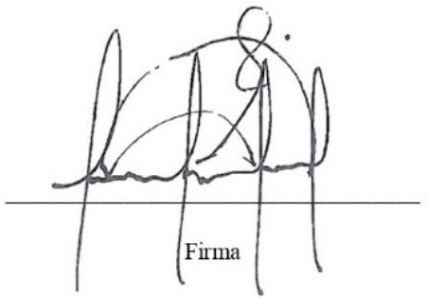
4. **Criterios de validación:**

Puntúe a continuación cada pregunta

| Pregunta | Claridad | Coherencia | Relevancia | Sugerencia |
|---|---|---|---|---|
| ¿Tiene Ud. conocimiento de agentes o actores de amenaza que hayan participado en ciberdelincuencia con un potencial riesgo para la Seguridad Nacional? ¿Cuáles son y como los clasificaría? | **3** | **3** | **4** | Se sugiere definir según referencia bibliográfica específica o definición en la investigación los términos "ciberdelincuencia" y el alcance de "seguridad nacional" de forma previa a las preguntas propias de la entrevista, dada la falta de consenso en el tema. Asimismo, se sugiere presentar la siguiente pregunta: ¿Qué ciberdelincuentes u organizaciones dedicadas a la ciberdelincuencia que en algún momento hayan afectado la Seguridad Nacional del Perú conoce Usted? Y de acuerdo a su apreciación, ¿Cómo afectaron a la Seguridad Nacional? |
| ¿Está Ud. familiarizado con el marco normativo nacional relacionado con la ciberdelincuencia y su conformidad con el marco normativo internacional? ¿Podría mencionar algunos ejemplos de ambos? | **2** | **4** | **4** | En la matriz de consistencia, se presentó como categoría de análisis o unidad temática el término "Marco jurídico-legal", por lo cual se sugiere emplear el mismo término para la pregunta; y, asimismo, definir de forma previa a la entrevista este término, especificando su alcance al entrevistado. Asimismo, se sugiere presentar la siguiente pregunta:<br>¿Conoce usted el marco jurídico-legal con el que se cuenta para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Qué normativa específica conoce? |
| ¿Conoce las capacidades con las que cuenta actualmente el personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Podría mencionar algunas? | **3** | **3** | **4** | El término "Personal especializado encargado de enfrentar la ciberdelincuencia" hace referencia directa al personal de la DIVINDAT en la PNP, este término puede mantenerse, pero requiere definir "Personal Especializado" en matriz de consistencia, de preferencia hacer referencia directa a DIVINDAT y además, requiere definir "capacidades" según referencia bibliográfica específica o definición en la investigación. |

| | | | | |
|---|---|---|---|---|
| ¿Puede mencionar los recursos materiales y tecnológicos utilizados actualmente para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | **3** | **3** | **4** | El término "recursos materiales y tecnológicos" es bastante abierto y requiere ser definido según referencia bibliográfica específica o definición en la investigación. Asimismo, la pregunta no detalla quién utiliza los "recursos materiales y tecnológicos", se sobreentiende que es la DIVINDAT, pero se recomienda mencionarlo por escrito. |
| ¿Cuáles cree Ud. que son las deficiencias en el marco normativo nacional para combatir la ciberdelincuencia que afecta la Seguridad Nacional?" | **2** | **4** | **4** | Al haberse definido en la matriz de consistencia el término "marco jurídico-legal", se sugiere modificar la pregunta de la siguiente manera:<br>¿Cuáles considera que son las necesidades en el marco jurídico-legal para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Considera Usted que este marco satisface todas las necesidades? ¿Qué necesidades en el marco jurídico-legal considera usted que no son satisfechas y afectan directamente el enfrentamiento contra la ciberdelincuencia? |
| ¿Qué capacidades/habilidades cree Ud. que el personal encargado necesita desarrollar para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | **4** | **4** | **4** | Al igual que la tercera pregunta, se recomienda definir los términos "capacidades" y "personal encargado" previo a la entrevista, así como el alcance de la "Seguridad Nacional" para mejor entendimiento del entrevistado. |
| ¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú y que actualmente no están disponibles? | **3** | **4** | **3** | Se recomienda definir los términos "recursos materiales y tecnológicos" y explicar al entrevistado, así como detallar qué personal u organización es la que dispone de dichos recursos materiales y tecnológicos, se sugiere modificar la pregunta de la siguiente manera:<br>¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú y que actualmente no están disponibles para el personal encargado de combatirla? |

| | | | | |
|---|---|---|---|---|
| ¿Qué otros aspectos cree Ud. que deban ser considerados al desarrollar una estrategia para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | **4** | **4** | **4** | |




DNI: 72805683

Fecha: 22 de Setiembre del 2023

**Formato de V de Aiken**

1. **Datos generales:**

| | |
|---|---|
| Nombre del juez: | José Aguirre Ruiz |
| Grado profesional: | Doctorando |
| Área de formación académica: | Ing. Sistemas/Telecomunicaciones/Ciberseguridad |
| Áreas de experiencia profesional: | Ing. Sistemas/Telecomunicaciones/Ciberseguridad |
| Institución donde labora: | Marina de Guerra del Perú / Privados |
| Tiempo de experiencia: | 20 años |

2. **Propósito de la evaluación:**

Validar el contenido del instrumento por juicio de expertos.

3. **Presentación de instrucciones para el juez:**

De acuerdo con los siguientes indicadores califique cada uno de las preguntas según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br><br>La pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | La pregunta no es clara. |
| | 2. Bajo Nivel | La pregunta requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos de la pregunta. |
| | 4. Alto nivel | La pregunta es clara, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** | 1. Totalmente en desacuerdo (no | La pregunta no tiene relación lógica con la categoría. |

| | | |
|---|---|---|
| La pregunta tiene relación lógica con la categoría que está midiendo. | cumple con el criterio) | |
| | 2. Desacuerdo (bajo nivel de acuerdo) | La pregunta tiene una relación tangencial /lejana con la categoría. |
| | 3. Acuerdo (moderado nivel) | La pregunta tiene una relación moderada con la categoría que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | La pregunta está relacionada con la categoría que está midiendo. |
| **RELEVANCIA**<br><br>La pregunta es esencial o importante, es decir debe ser incluida. | 1. No cumple con el criterio | La pregunta puede ser eliminada sin que se vea afectada la medición de la categoría. |
| | 2. Bajo Nivel | La pregunta tiene alguna relevancia, pero otra pregunta puede estar incluyendo lo que mide esta. |
| | 3. Moderado nivel | La pregunta es relativamente importante. |
| | 4. Alto nivel | La pregunta es muy relevante y debe ser incluida. |

***Leer con detenimiento las preguntas y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente***

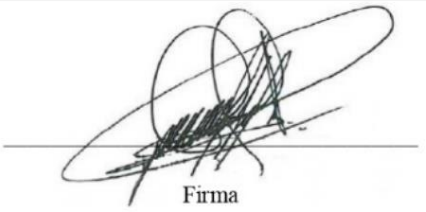
| |
|---|
| 1 No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

**4. Criterios de validación:**

Puntúe a continuación cada pregunta

| Pregunta | Claridad | Coherencia | Relevancia | Sugerencia |
|---|---|---|---|---|
| ¿Tiene Ud. conocimiento de agentes o actores de amenaza que hayan participado en ciberdelincuencia con un potencial riesgo para la Seguridad Nacional? ¿Cuáles son y como los clasificaría? | 4 | 3 | 4 | Esta pregunta debe, de no existir, previamente, un contexto que permita al entrevistado responder con la mayor conciencia posible sobre la tema presentado. |
| ¿Está Ud. familiarizado con el marco normativo nacional relacionado con la ciberdelincuencia y su conformidad con el marco normativo internacional? ¿Podría mencionar algunos ejemplos de ambos? | 4 | 4 | 4 | S/N. |
| ¿Conoce las capacidades con las que cuenta actualmente el personal encargado de enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Podría mencionar algunas? | 4 | 4 | 4 | S/N. |
| ¿Puede mencionar los recursos materiales y tecnológicos utilizados actualmente para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | 4 | 4 | 4 | S/N. |

| | | | | |
|---|---|---|---|---|
| ¿Cuáles cree Ud. que son las deficiencias en el marco normativo nacional para combatir la ciberdelincuencia que afecta la Seguridad Nacional?" | 4 | 4 | 4 | Se recomienda vincular también el marco normativo que pudiera regir la afectación en el entorno digital de la nación. |
| ¿Qué capacidades/habilidades cree Ud. que el personal encargado necesita desarrollar para combatir la ciberdelincuencia que afecta la Seguridad Nacional? | 4 | 4 | 4 | S/N. |
| ¿Qué recursos materiales y tecnológicos cree Ud. que son necesarios para combatir la ciberdelincuencia que afecta la Seguridad Nacional en Perú y que actualmente no están disponibles? | 4 | 4 | 4 | Para efectos de proteger los activos cibernéticos de Seguridad Nacional, se recomienda orientar la pregunta no únicamente a la ciberdelincuencia, dado que los recursos se orientan a defender el todo. |
| ¿Qué otros aspectos cree Ud. que deban ser considerados al desarrollar una estrategia para combatir la ciberdelincuencia que afecta la Seguridad Nacional ? | 4 | 4 | 4 | S/N. |



Firma

DNI: 43307735

Fecha: 27 de setiembre del 2023

## Anexo 5. Cálculo para la validación de expertos

| N° | Pregunta | Criterios | | | T | Criterios | | | T | Criterios | | | T | Criterios | | | T | Criterios | | | T | Total, de puntuación | Promedio |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | CL | CO | RE | | CL | CO | RE | | CL | CO | RE | | CL | CO | RE | | CL | CO | RE | | | |
| 1 | ¿Usted conoce actores, agentes o entes que en algún momento han desarrollado actos de ciberdelincuencia que afectaron la Seguridad Nacional en Perú? ¿Cuáles? | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 3.0 | 3.0 | 4.0 | **3.3** | 4.0 | 3.0 | 4.0 | 3.7 | 3.8 | 0.8 |
| 2 | ¿Usted conoce aspectos jurídico-legales con los que se cuentan para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles? | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 2.0 | 4.0 | 4.0 | **3.3** | 4.0 | 4.0 | 4.0 | 4.0 | 3.9 | 0.8 |
| 3 | ¿Usted conoce las capacidades que presenta el personal especializado para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles? | 4.0 | 4.0 | 3.0 | **3.7** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 3.0 | 3.0 | 4.0 | **3.3** | 4.0 | 4.0 | 4.0 | 4.0 | 3.8 | 0.8 |
| 4 | ¿Usted conoce los recursos materiales y tecnológicos que se emplean para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? ¿Cuáles? | 4.0 | 4.0 | 3.0 | **3.7** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 3.0 | 3.0 | 4.0 | **3.3** | 4.0 | 4.0 | 4.0 | 4.0 | 3.8 | 0.8 |
| 5 | ¿Cuáles considera que son las necesidades en aspectos jurídico-legales para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 2.0 | 4.0 | 4.0 | **3.3** | 4.0 | 4.0 | 4.0 | 4.0 | 3.9 | 0.8 |

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **6** | ¿Cuáles considera que son las capacidades del personal que falta desarrollar para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | 3.0 | 4.0 | 4.0 | **3.7** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | 4.0 | 3.9 | 0.8 |
| **7** | ¿Cuáles considera que son los recursos materiales y tecnológicos que hacen falta para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 3.0 | 4.0 | 3.0 | **3.3** | 4.0 | 4.0 | 4.0 | 4.0 | 3.9 | 0.8 |
| **8** | ¿Qué otros aspectos consideran necesarios tomar en cuenta para la investigación, con relación al desarrollo de una estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú? | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | **4.0** | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 0.8 |
| | **TOTAL** | **3.9** | **4.0** | **3.8** | **3.9** | **4.0** | **4.0** | **4.0** | **4.0** | **4.0** | **4.0** | **4.0** | **4.0** | **3.0** | **3.6** | **3.9** | **3.5** | **4.0** | **3.9** | **4.0** | **4.0** | **3.9** | **0.8** |

***Regla de decisión:***

- Si el promedio es mayor e igual a 0.8, el instrumento es válido.
- Si el promedio es menor a 0.8, el instrumento no es válido.

***Conclusión:***

- La puntuación final es de 0.8, concluyendo así que el instrumento es válido.