Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Letras y Ciencias Humanas
Escuela Profesional de Bibliotecología y Ciencias de la Información

Ciberseguridad gubernamental: Una revisión sistemática de la literatura científica

TESIS

Para optar el Título Profesional de Licenciada en Bibliotecología y Ciencias de la Información

AUTOR

Críste l Antuanett NAVARRETE PÉREZ

ASESOR

Martín Alonso ESTRADA CUZCANO

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Navarrete, C. (2025). *Ciberseguridad gubernamental: Una revisión sistemática de la literatura científica*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Letras y Ciencias Humanas, Escuela Profesional de Bibliotecología y Ciencias de la Información]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Crístel Antuanett Navarrete Pérez
Tipo de documento de identidad	DNI
Número de documento de identidad	75131360
URL de ORCID	https://orcid.org/0000-0001-5220-9584
Datos de asesor	
Nombres y apellidos	Martín Alonzo Estrada Cuzcano
Tipo de documento de identidad	DNI
Número de documento de identidad	08435943
URL de ORCID	https://orcid.org/0000-0001-5039-1108
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Elizabeth Huisa Veria
Tipo de documento	DNI
Número de documento de identidad	09779795
Miembro del jurado 1	
Nombres y apellidos	Rosalía Quiroz Papa de García
Tipo de documento	DNI
Número de documento de identidad	08479121
Miembro del jurado 2	
Nombres y apellidos	Augusto Cortez Vásquez
Tipo de documento	DNI
Número de documento de identidad	08634618
Datos de investigación	

Línea de investigación	E.3.l.3. Sociedad de la información y tecnologías de la comunicación
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Latitud: -12.05590 Longitud: -77.08450
Año o rango de años en que se realizó la investigación	Marzo 2023 - septiembre 2025
URL de disciplinas OCDE	Bibliotecología https://purl.org/pe-repo/ocde/ford#5.08.03 Ciencias de la Información https://purl.org/pe-repo/ocde/ford#5.08.02

ACTA DE SUSTENTACIÓN DEL TESIS

A los veintitrés días del mes de octubre del dos mil veinticinco, a las dieciséis horas, en acto público se reúne el Jurado de sustentación integrado por los siguientes profesores del Departamento Académico de Bibliotecología y Ciencias de la Información de la Facultad de Letras y Ciencias Humanas y del Departamento Académico de Ciencias de la Computación de la Facultad de Ingeniería de Sistemas de la Universidad Nacional Mayor de San Marcos:

Elizabeth Huisa Veria	Presidente
Martín Alonso Estrada Cuzcano	Asesor
Rosalía Quiroz Papa de García	Informante
Augusto Cortez Vásquez	Informante (Experto interno, Facultad de Ingeniería de Sistemas)

Con el fin de recibir la sustentación de la tesis**: CIBERSEGURIDAD GUBERNAMENTAL: UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA CIENTÍFICA,** presentada por la bachiller **CRÍSTEL ANTUANETT NAVARRETE PÉREZ.**

Concluida la sustentación, el jurado procedió a la calificación con el siguiente resultado:

Aprobado con mención honrosa

Números (17) Letras (Diecisiete)

Luego del proceso de sustentación y la calificación correspondiente, se le comunicó al graduando el resultado obtenido y el Jurado recomienda a la Facultad que se le otorgue el título profesional de **Licenciada** en Bibliotecología y Ciencias de la Información.

Siendo las diecisiete horas, se concluyó el acto por lo cual, los miembros del jurado dan fe de lo actuado firmando la presente Acta.

Dra. Elizabeth Huisa Veria
Presidente (Principal)

Dr. Martín Alonso Estrada Cuzcano
Asesor (Principal)

Dra. Rosalía Quiroz Papa de García
Informante (Principal)

Mg. Augusto Cortez Vásquez
Informante (Principal)

UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

Anexo 1
CERTIFICADO DE SIMILITUD

Yo, Martín Alonso Estrada Cuzcano en mi condición de asesor acreditado con la Resolución Directoral N°013-2024-D-FLCH/UNMSM, de la tesis, cuyo título es **CIBERSEGURIDAD GUBERNAMENTAL: UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA CIENTÍFICA**, presentado por la bachiller **CRÍSTEL ANTUANETT NAVARRETE PÉREZ** para optar el título profesional de licenciada en Bibliotecología y Ciencias de la Información, CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 10% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título profesional de licenciado en Bibliotecología y Ciencias de la Información.

Lima, 9 de octubre del 2025



DNI: 08435943
Dr. Martin Alonso Estrada Cuzcano

* Según corresponda: bachiller, magíster, doctor; título profesional o título de segunda especialidad
La vigencia del presente certificado corresponde a un período de noventa (90) días desde la fecha de su emisión; siempre que no haya observaciones en el texto durante el proceso de revisión por el jurado informante o surja alguna contingencia.

Dedicado a mi familia, por educarme y acompañarme, a mis amistades por alentarme, y a Bruce, Miguel y Margaret por desvelarse conmigo.

En memoria de Leonor, Verónica y en especial a mi tía Gloria Navarrete

ÍNDICE DE CONTENIDO

RESUMEN 8

INTRODUCCIÓN 10

CAPÍTULO I 11

PROBLEMA DE INVESTIGACIÓN 11

1.1. Descripción del problema de investigación 11

1.2. Definición del problema 13

1.2.1. Problema general 13

1.2.2. Problemas específicos 13

1.3. Objetivos 13

1.3.1. Objetivo general 13

1.3.2. Objetivos específicos 14

1.4. Justificación e importancia de la investigación 14

1.5. Hallazgos y limitaciones de la investigación 15

CAPÍTULO II 16

REVISIÓN DE LA LITERATURA 16

2.1. Antecedentes del estudio 16

2.1.1. Internacionales 16

2.1.2. Nacionales 16

2.2. Bases teóricas 19

2.2.1. Ciberespacio 19

2.2.2. Gobierno 20

2.2.3. Seguridad ciudadana 21

2.2.4. Información pública y privada 23
2.3. Definición de categorías de análisis 24
2.3.1. Ciberseguridad 25
2.3.2. Delitos informáticos 26
2.3.3. Políticas nacionales 28
CAPÍTULO III 29
FUNDAMENTOS TEÓRICOS 29
3.1. Fundamentación teórica 29
3.2. Sistemas y categorías de análisis 30
CAPÍTULO IV 34
METODOLOGÍA 34
4.1. Enfoque de la investigación 34
4.2. Tipo de investigación 34
4.3. Diseño de investigación 34
4.4. Estrategias y técnicas de investigación 35
4.5. Búsqueda y recuperación de información 35
4.6. Criterios de selección de la información 36
CAPÍTULO V 38
RESULTADOS 38
5.1. Características generales de los resultados 38
5.2. Análisis teórico conceptual de la ciberseguridad gubernamental 42
5.2.1 Conceptos sobre ciberseguridad y seguridad de la información. 43
5.2.2 Implicancias de la guerra de la información y la ciberdelincuencia. 47
5.2.3 Componentes de una política nacional de ciberseguridad 54

CAPÍTULO VI 65
DISCUSIÓN 65
CONCLUSIONES 70
RECOMENDACIONES 72
REFERENCIAS BIBLIOGRÁFICAS 74
ANEXOS 84

ÍNDICE DE TABLAS

Tabla 1 Primera categoría de análisis 31

Tabla 2 Segunda categoría y de análisis 32

Tabla 3 Tercera categoría de análisis 33

Tabla 4 Cuadro de clasificación 35

Tabla 5 Términos de búsqueda 36

ÍNDICE DE FIGURAS

Figura 1 El triángulo del gobierno.....20

Figura 2 División de las categorías de análisis.....25

Figura 3 Tipos de documentos 38

Figura 4 Bases de datos 39

Figura 5 Idioma 40

Figura 6 Países de origen de la literatura utilizada.....41

Figura 7 Año de publicaciones.....42

RESUMEN

Las tecnologías de la información y comunicación están ligadas a las actividades diarias de las personas y es necesario protegerlas. La ciberseguridad es un tema recurrentemente estudiado en años recientes desde diversas perspectivas y en diversos tipos de instituciones. El presente trabajo analiza las características y el impacto de la ciberseguridad gubernamental a partir de la revisión de la literatura científica. La metodología empleada es de tipo cualitativa y utiliza como diseño metodológico la revisión sistemática; se obtuvieron 63 documentos relevantes recuperados de diversas bases de datos bibliográficos. El análisis exhaustivo de los registros bibliográficos permitió identificar que la ciberseguridad gubernamental se divide en 3 categorías: la ciberseguridad como concepto, los delitos informáticos y políticas nacionales en ciberseguridad. desglosando cada una en subcategorías se identificaron los temas de seguridad de la información, guerra de la información, ciberterrorismo y seguridad nacional. El trabajo también arrojó que la temática de la ciberseguridad gubernamental es un tema bastante serio en los países con un nivel socioeconómico alto, como Estados Unidos, Rusia o China y que a su vez es importante concientizar a la población sobre los riesgos de internet y como proteger los datos personales. Se recomienda realizar un estudio particular sobre Perú y qué acciones se han realizado para implementar y mejorar la ciberseguridad en las instituciones del estado.

PALABRAS CLAVE: ciberseguridad, ciberseguridad gubernamental, seguridad de la información, guerra de la información, delitos informáticos, políticas nacionales.

LÍNEA DE INVESTIGACIÓN: E. 3. l. 3. Sociedad de la información y tecnologías de la comunicación.

ABSTRACT

Information and communication technologies are linked to people's daily activities and need to be protected. Cybersecurity is a topic that has been recurrently studied in recent years from different perspectives and in different types of institutions. This paper analyzes the characteristics and impact of governmental cybersecurity based on a review of the scientific literature. The methodology employed is qualitative and uses systematic review as a methodological design; 63 relevant documents retrieved from various bibliographic databases were obtained. The exhaustive analysis of the bibliographic records made it possible to identify that government cybersecurity is divided into 3 categories: cybersecurity as a concept, computer crimes and national cybersecurity policies. The study also showed that government cybersecurity is a very serious issue in countries with a high socioeconomic level, such as the United States, Russia or China, and that it is important to raise awareness among the population about the risks of the Internet and how to protect personal data. It is recommended to conduct a particular study on Peru and what actions have been taken to implement and improve cybersecurity in state institutions.

KEY WORDS: cybersecurity, government cybersecurity, information security, information warfare, cybercrime, national policies.

RESEARCH LINE: E. 3. l. 3. Information society and communication technologies.

INTRODUCCIÓN

En el contexto actual, la ciberseguridad adquiere una importancia estratégica para los Estados que orientan sus políticas nacionales hacia la implementación de gobiernos digitales y dependen de las tecnologías de la información como componente estructural de la gestión pública. Esta transformación digital conlleva la necesidad imperativa de proteger la información confidencial tanto de empresas como de ciudadanos que forman parte del ecosistema estatal.

La finalidad del presente estudio es constituirse como un medio informativo para la toma de decisiones en materia de seguridad digital, facilitando un desenvolvimiento eficaz de los gobiernos que redunde en beneficios directos para la ciudadanía.

El objetivo de esta investigación consiste en analizar las experiencias documentadas sobre ciberseguridad gubernamental a nivel internacional durante el período 2010-2023, determinando sus características principales, examinando los conceptos fundamentales de ciberseguridad, comprendiendo las implicancias de la ciberdelincuencia y la guerra de la información, e identificando los componentes esenciales de una política nacional de ciberseguridad.

La metodología empleada adopta un enfoque cualitativo de tipo descriptivo, utilizando la revisión sistemática y el análisis documental de 63 documentos identificados en bases de datos especializadas como Scopus, Web of Science y Google Scholar.

Los resultados obtenidos evidencian que la ciberseguridad gubernamental constituye un tema de importancia crítica para países con mayor dependencia de las tecnologías de la información. Asimismo, se constata que la concientización ciudadana sobre los beneficios y riesgos del entorno digital contribuye significativamente a una implementación más efectiva de las políticas de ciberseguridad gubernamental.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1.Descripción del problema de investigación

Desde finales del siglo pasado se identifica a la guerra de información como una nueva modalidad de enfrentamiento que no deriva necesariamente en pérdidas humanas o materiales, sino que utiliza la información como arma esencial para alcanzar objetivos políticos y/o militares (Tovar, 2011).

En el contexto actual, la producción científica sobre la guerra de información o information warfare se incrementa considerablemente. En este escenario, la información se concibe como el poder que posee un país para reforzar su capacidad política, económica y militar. Así, la guerra de información constituye un tipo de conflicto entre naciones o sociedades en el que se atacan o incapacitan los sistemas y redes de información, buscando impactar los conocimientos y creencias de las personas para imponer la voluntad del adversario (Jordán, s/f: p.3; Szafranski, 1995: p.8).

Previo a la consolidación de este término, ya existían problemas relacionados con la seguridad de los sistemas de información debido a sus vulnerabilidades inherentes. Warner (2012) documenta las vulnerabilidades identificadas en los sistemas de información desde sus inicios, las cuales propiciaron que los gobiernos implementaran políticas de seguridad específicas. Durante las décadas de 1960 y 1970, el crecimiento exponencial de usuarios en la red generó que la información quedara expuesta y vulnerable, dado que constituía un espacio accesible para la mayoría de las personas. Consecuentemente, las primeras compañías informáticas comenzaron a comercializar software especializado para la protección de datos.

En la década de 1980, el gobierno de los Estados Unidos tomó conciencia, a través de un artículo del teniente coronel Roger Schell de las Fuerzas Aéreas, de la existencia de diversos métodos para acceder a información gubernamental —especialmente militar— desde largas distancias. Como señala Warner (2012), "los datos que podían ser robados, además, eran datos que podían ser manipulados para hacer que los sistemas actúen de forma confusa e incluso

peligrosa" (p. 786). Un ejemplo paradigmático de esta vulnerabilidad ocurrió en el Comando de Defensa Aérea de América del Norte, cuando alguien introdujo datos falsos en el sistema de alerta de misiles, haciendo creer que Moscú había lanzado 2200 misiles dirigidos al país, generando una falsa alarma de consecuencias potencialmente catastróficas.

Rona (1976) observó que el flujo de información —cada vez más interconectado y digitalizado— requerido por los sistemas de armamento avanzados se tornaba más frágil conforme aumentaba su complejidad. Esta observación fundamenta la noción contemporánea de guerra de información, donde la información desempeña un papel central al otorgar ventajas estratégicas sobre el oponente.

La magnitud del problema fue claramente articulada por el National Research Council:

> Estamos en riesgo. Estados Unidos depende cada vez más de los ordenadores. Controlan el suministro de energía, las comunicaciones, la aviación y los servicios financieros. […]. Aunque confiamos en ellos, son vulnerables a los efectos de un mal diseño y un control de calidad insuficiente, a los accidentes y, lo que es más alarmante, a los ataques deliberados. El ladrón moderno puede robar más con un ordenador que con una pistola. El terrorista del mañana puede hacer más daño con un teclado que con una bomba. (National Research Council & System Security Study Committee, 1990, p. 7)

La importancia de la ciberseguridad radica fundamentalmente en la protección de sistemas gubernamentales, privados y personales en el entorno digital. En el ámbito gubernamental, esta importancia se amplifica considerablemente, ya que el Estado custodia no solo información ciudadana, sino también datos relacionados con servicios esenciales y seguridad nacional. La comprometida vulnerabilidad de esta información podría poner en riesgo todo el sistema nacional, derivando potencialmente en una crisis de alcance nacional.

En consecuencia, la ciberseguridad gubernamental se constituye como el mecanismo fundamental para garantizar la defensa y protección de la información ciudadana, los servicios públicos esenciales y la seguridad nacional en la era digital.

1.2.Definición del problema

En la actualidad, la ciberseguridad se ha consolidado como un tópico de investigación recurrente, impulsado por los significativos avances tecnológicos desarrollados en las últimas décadas. Si bien la ciberseguridad abarca múltiples disciplinas, la presente investigación se enfoca específicamente en los aspectos relacionados con el ámbito gubernamental.

Los conflictos recientes entre Rusia y Ucrania, así como los desafíos derivados de la pandemia de COVID-19, han contribuido al incremento constante de la literatura especializada sobre ciberseguridad y seguridad de la información (Veale & Brown, 2020). Estos eventos han evidenciado la vulnerabilidad de los sistemas digitales gubernamentales y la necesidad crítica de fortalecer las capacidades de ciberseguridad a nivel estatal.

1.2.1. Problema general

- ¿Cuáles son las experiencias documentadas sobre la ciberseguridad en los gobiernos a nivel internacional, 2010-2023?

1.2.2. Problemas específicos

a) ¿Cuáles son las características de la producción científica sobre la ciberseguridad gubernamental?
b) ¿Qué conceptos sobre ciberseguridad y seguridad de la información existen?
c) ¿Cuáles son las implicancias de la guerra de la información y la ciberdelincuencia?
d) ¿Qué componentes debe tener una política nacional de ciberseguridad o seguridad de la información?

1.3.Objetivos

1.3.1. Objetivo general

- Analizar las experiencias documentadas sobre la ciberseguridad en los gobiernos a nivel internacional, 2010-2023.

1.3.2. Objetivos específicos

a) Determinar las características de la literatura existente sobre la ciberseguridad gubernamental.
b) Analizar los conceptos sobre ciberseguridad y seguridad de la información.
c) Conocer las implicancias de la guerra de la información y la ciberdelincuencia.
d) Identificar los componentes que como mínimo debe tener una política nacional de ciberseguridad o seguridad de la información.

1.4.Justificación e importancia de la investigación

La ciberseguridad implica tanto la protección de los datos personales de las organizaciones y sus usuarios como la salvaguarda de su infraestructura virtual. En el contexto gubernamental, esta protección se extiende a la información confidencial de empresas y ciudadanos, así como a la infraestructura digital estatal, lo cual fundamenta la importancia crítica de su implementación por parte de los gobiernos.

La finalidad de esta investigación responde a la necesidad de abordar un tema escasamente tratado en el Perú, pero de reconocida importancia a nivel internacional. Este estudio aspira a constituirse como un medio informativo para la toma de decisiones en materia de seguridad digital, facilitando un desenvolvimiento gubernamental eficaz que beneficie directamente a la ciudadanía.

El objetivo principal de la ciberseguridad consiste en proteger la información en el ciberespacio, lo cual implica comprender sus características fundamentales, beneficios —como la protección de datos personales—, vulnerabilidades —manifestadas en la ciberdelincuencia— y las implicancias de implementar sistemas de ciberseguridad en los gobiernos nacionales.

Resulta fundamental analizar las experiencias de ciberseguridad en países con mayor trayectoria en su implementación, particularmente aquellas naciones desarrolladas que poseen niveles socioeconómicos elevados y que, en algunos casos, mantienen tensiones internacionales con sus pares. Igualmente, es necesario examinar las experiencias de países que incursionan

recientemente en la ciberseguridad, identificando las políticas implementadas y las dificultades enfrentadas en este proceso.

Finalmente, se busca establecer criterios que determinen tanto la importancia como los riesgos asociados a la ausencia de políticas de ciberseguridad o de entidades especializadas en salvaguardar la seguridad digital. Estas políticas deben impactar positivamente en la sociedad, generando confianza ciudadana en la tecnología y promoviendo un entorno digital más seguro y resiliente.

1.5.Hallazgos y limitaciones de la investigación

El presente trabajo de investigación proporcionará información sistematizada acerca de la literatura existente sobre ciberseguridad gubernamental. En cuanto a los límites establecidos, se recolectaron documentos correspondientes a los años 2010 a 2023. A pesar de la amplitud de este período, los resultados obtenidos fueron satisfactorios, dado que las referencias sobre ciberseguridad son extensas, lo que requirió la implementación de estrategias específicas para seleccionar exclusivamente aspectos relacionados con la ciberseguridad en el ámbito gubernamental.

Los tipos documentales que conforman la muestra incluyen artículos científicos, libros especializados, memorias de conferencias y documentos de políticas nacionales, proporcionando así una perspectiva integral y multidimensional del tema de investigación.

CAPÍTULO II

REVISIÓN DE LA LITERATURA

2.1.Antecedentes del estudio

2.1.1. Internacionales

En el ámbito internacional se encontraron dos trabajos que plantean estrategias de ciberseguridad nacional en Ecuador y Argentina. El primero es la tesis de Chiza & Izurieta (2020) *Estrategia nacional de ciberseguridad*, en donde reflexionan sobre los grandes avances tecnológicos que se han hecho a lo largo de los años y de los grandes peligros que conlleva el uso de estas tecnologías en la seguridad de la información, por tal motivo realizan una análisis de la situación actual de ciberseguridad en Ecuador y, teniendo en cuenta las limitaciones del país, plantean la creación de una directriz de estado que permita articular y coordinar los esfuerzos de diferentes organismos nacionales, juntamente con el apoyo de organismo internacionales. El segundo trabajo es la tesis doctoral de Albarracín (2019) *Inteligencia nacional y estrategia de ciberseguridad nacional*, en donde expone que el ambiente cibernético es una herramienta para la seguridad y defensa nacional, y al ser Argentina uno de los países de la región que cuentan con mayor actividad cibernética criminal, es necesaria la creación de una estrategia de ciberseguridad nacional

2.1.2. Nacionales

A nivel nacional existen diversas investigaciones sobre ciberseguridad, sin embargo, la gran mayoría se centran en el ámbito empresarial y otras abordan el tema desde una perspectiva más técnica o especializada. Sobre la ciberseguridad gubernamental o nacional, se encontraron trabajos que se circunscriben a aspectos generales encontrados en la literatura científica y en otros describen experiencias y casos reales de ciberseguridad nacional y proponen estrategias alternativas. A continuación, se presentan los trabajos más relevantes.

La tesis más reciente es de Bermúdez (2024) *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones*; expone la importancia de la aplicación de

estándares de ciberseguridad en las organizaciones, tomando en cuenta estándares internacionales, normas peruanas y experiencias personales. La metodología empleada fue de enfoque cualitativo empleando el método de investigación documental. Como resultado del trabajo se concluyó que la aplicación de estándares es crucial para el fortalecimiento de la confidencialidad, integridad y disponibilidad de la información.

Recientemente Vílchez (2022) en su tesis *Ciberseguridad y robo de información: Una revisión sistemática de la literatura*, tuvo como objetivo encontrar autores, países, revistas y repositorios que sirvieron como referencia para investigaciones sobre ciberseguridad enfocada al robo de información. Vílchez recopiló la información de tres bases de datos, ProQuest, ScienceDirect y CORE, para luego seleccionar la información y clasificar cada artículo según los objetivos de la investigación, autor, país, revista o repositorio. En los resultados señala que el autor más relevante es Brij Gupta y que el repositorio y país que producen más artículos sobre ciberseguridad vinculado al robo de información es arXiv.org y Estados Unidos respectivamente.

Castillo et al. (2021) abordan en su artículo *Estado del arte sobre la identificación amenazas no intencionales de ciberseguridad de parte de personal interno en instituciones públicas*, que la modernización de los estados ha llevado a presentar diversos servicios digitales de gobierno electrónico, sin embargo, también los llevó a considerar las amenazas que se podrían presentar para los activos de información de los servicios. Varios estudios afirman que muchas de las amenazas provienen del mismo personal de las instituciones públicas, pero estas no son intencionadas, por lo que el trabajo presenta un estado del arte de marcos, modelos y otras propuestas que identifican este tipo de amenazas. Entre los resultados se encontró que los modelos mitigan estas amenazas a través de estándares o buenas prácticas aplicadas a la institución, sin embargo, en los modelos no se encuentran estudios sobre amenazas no intencionales por parte del personal, por lo tanto, no hay un análisis de riesgos.

Taipe (2020) en *La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018*, analiza la importancia de la auditoría de seguridad informática tiene implicancia en la ciberseguridad en el sector público, con el objetivo de generar aportes que contribuyan a la solución de problemáticas que se presentan en el sector. Se

utilizaron dos cuestionarios, uno sobre auditoría en seguridad informática y otro sobre ciberseguridad en el sector público, aplicados a funcionarios del sector. Como resultado se obtuvo que los encuestados exponen que las auditorias sobre seguridad de la información sí tienen una implicancia directa en la ciberseguridad del sector público.

Alvines (2020) en su trabajo de investigación *Modelo de ciberseguridad para el sector de salud pública: 2018 -2020: una revisión de la literatura científica*, afirma que el sector de salud es uno de los 5 sectores que se encuentran expuestos a mayores riesgos de seguridad informática. Por tal motivo se realizó una revisión sistemática de la literatura con el objetivo de analizar modelos de ciberseguridad aplicado al sector de salud pública. Se recopilaron 50 artículo extraídos de bases de datos como IEEEXLORE, Scopus, WOS y Science Direct. El resultado obtenido determinó que las características de un marco de ciberseguridad aplicado al sector de salud pública serían: dimensión (pequeño a mediano), adaptable, componible y reusable.

Chilcon (2019) en su tesis *El Cibercrimen en el Perú y su incidencia en la Seguridad Nacional*, tuvo como objetivo determinar en qué medida el cibercrimen en el Perú afecta la seguridad nacional. La metodología usada es de enfoque cuantitativo, descriptivo explicativo y de diseño no experimental y aplica una muestra de 231 funcionarios de instituciones como la Policía Nacional del Perú, Ministerio Publico, y del Poder Judicial. Como conclusión se llegó a determinar que el cibercrimen sí afecta significativamente a la seguridad nacional del país y como recomendaciones se plantean algunas estrategias para combatir el mismo.

Villar (2019) expone en su trabajo de investigación *Las implicancias de los ciberataques del S. XXI en América Latina*, cuáles son las establecen la magnitud de los ciberataques para la comunidad internacional. Los ciberataques no solo son una amenaza momentánea para las empresas y naciones, sino que también tienen implicancias en el curso político y económico de un país, además de afectar psicológicamente a la población. El trabajo pretende brindar a la población, empresas y estados un medio de fuente de información que genere un impacto en la ciberseguridad de la región.

2.2.Bases teóricas

2.2.1. Ciberespacio

El internet es una herramienta que ha cobrado relevancia en la vida diaria de las personas y ha evolucionado de tal manera que ha creado un nuevo espacio virtual de interacción que se conoce como ciberespacio; un espacio virtual que ha mejorado increíblemente la comunicación a nivel internacional y en donde no solo se desarrollan asuntos de entretenimiento, sino también de carácter económico político y social con libertad para la producción de diversos contenidos en la red (buenos y malos). Es así como el ciberespacio se conoce como la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos (Perafán et al, 2021).

El término ciberespacio lo acuñó William Gibson en su novela Neuromancer de 1984, y acogido por la informática debido al parecido de lo que sucede en la obra con el mundo actual y el internet. Santana y Báez (2022) definen la palabra ciberespacio a partir de su origen etimológico dividiendo la palabra en dos:

- Ciber, que viene de cibernética, palabra de origen griego que se asignaba al arte de manejar un navío; más adelante Norbert Wiener y Arturo Rosenblueth la usaron para definir la posibilidad de autorregulación y control de cualquier sistema, y pasa a ser entendido, el concepto de cibernética, como el estudio de las estructuras de los sistemas reguladores.
- Espacio, bajo la postura de Gottfried Leibniz, hace referencia a la posibilidad de relaciones de cercanía y adyacencia entre una colección determinada de entidades.

Es así como los autores proponen definir al ciberespacio como “un espacio artificial y ficcional emergente en el que tienen lugar relaciones sociales entre personas, organizaciones y máquinas, y que no tiene existencia independiente del conjunto de equipos y programas informáticos que le posibilitan”.

El ciberespacio como nuevo escenario del conflicto es algo de los gobiernos han visto posible, ya que constituye un dominio global formado por las tecnologías de la información y

la comunicación (TIC) y otros sistemas electrónicos, en el que se desarrollan actividades vitales para la sociedad; hace dos siglos la guerra era considerada como un acto de fuerza para obligar al enemigo al cumplimiento de otra voluntad y la fuerza (física) es el medio. Hoy en día ese concepto ha cambiado, ya que la fuerza no solo se mide con el potencial militar, sino también con el económico, tecnológico, industrial, enérgico y, por supuesto, cibernético (Argumosa, 2022, pp. 68-69).

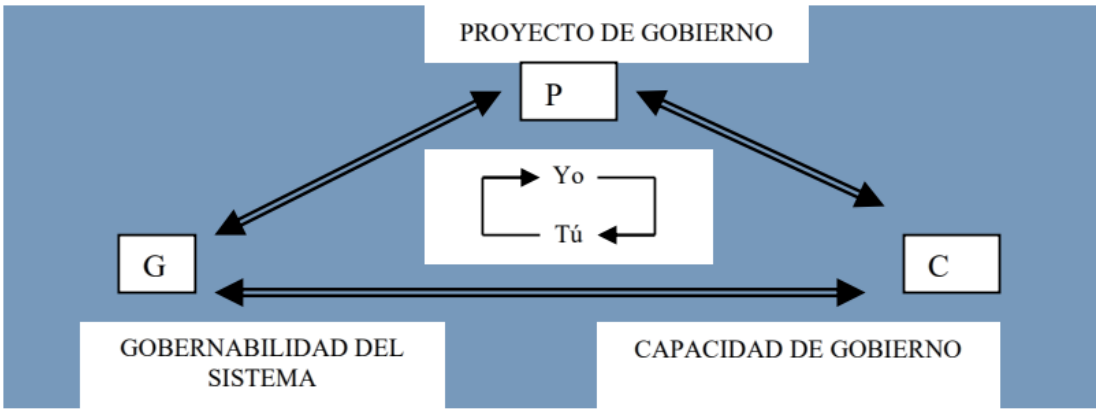
2.2.2. Gobierno

Se entiende por gobierno a un conjunto de organismos y personas que dirigen un territorio y las funciones que desempeñan (Pascual, 2010, p. 34). Para Matus (1987) el gobierno o gobernar no es una tarea fácil, ya que implica la aplicación de tres variables:

- Proyecto de gobierno: acciones que los actores se propone a realizar para alcanzar sus objetivos.
- Capacidad de gobierno: técnicas, métodos, destrezas, habilidades y experiencias de los actores para alcanzar sus objetivos.
- Gobernabilidad del sistema: variables que pueden o no controlar los actores en el proceso de gobierno. Mientras más variables de peso controle, tendrá más libertad de acción.

Figura 1

El Triángulo del Gobierno



Nota. Adaptado de *Política, planificación y gobierno* (p. 34), por C. Matus, 1987, Fundación Altadir.

Estas tres variables, por diferentes que perezcan, se relacionan entre sí y dan como resultado el triángulo de gobierno, un modelo muy simple pero potente para entender el proceso de gobierno.

2.2.2.1.Gobierno Digital

El gobierno digital se define como un mecanismo de política pública que permite a los ciudadanos el acceso rápido a la información y servicios que requieran, brindando transparencia y la confianza que el estado debe entablar con su pueblo para tener una buena relación y promover la participación ciudadana. Esto viene de la mano con la modernización del estado y la gobernanza digital, ya que es necesario agilizar los procesos a través de internet, herramienta que involucra a la ciudadanía y beneficia a todos (Vargas, 2021, pp. 3-4).

Los autores Toro-García et al. Mencionan que el gobierno digital incrementa el bienestar de los ciudadanos, haciendo que los servicios estatales operen de manera eficiente y transparente. Para crear esto se deben considerar dos aspectos: la capacidad del estado para involucrar a sus ciudadanos y empresas; y los facilitadores organizacionales con los que se apoya el gobierno (estrategia, gobernanza y organización, liderazgo, talento y cultura, y tecnología); se entiende entonces que el gobierno digital no solo se debe guiar por lo tecnológico, sino también en lo novedoso de los productos y servicios que se brindan.

> Un gobierno abierto es una técnica de administración pública, la cual es vista como el cambio estructural del Gobierno, integrando diversos factores como la tecnología, los ciudadanos, las empresas, que en conjunto son de gran importancia para de mejorar la calidad de vida de los ciudadanos con ayuda del gobierno digital. (Toro-García et al., 2020, p. 98)

2.2.3. Seguridad ciudadana

Según la real academia española, el termino seguridad implica varios conceptos, entre los que destaca, para la presente investigación, la seguridad ciudadana, definida como “situación

de tranquilidad pública y de libre ejercicio de los derechos individuales, cuya protección efectiva se encomienda a las fuerzas de orden público" (Real Academia Española, 2024).

En los años 80 el concepto de seguridad ciudadana se relacionaba más con el control de la criminalidad a través de las políticas de seguridad pública; es a finales del siglo XX que adquiere un nuevo enfoque, en el que incorpora a la ciudadanía como actor fundamental en la reducción del delito y la violencia. Este nuevo concepto se vincula directamente con el de "seguridad humana", término usado por el Programa de Naciones Unidas para el Desarrollo, que engloba las acciones de seguridad alimentaria, sanitaria, ambiental, etc. Es así como la seguridad ciudadana se entiende como la protección de un núcleo básico de derechos humanos, haciéndola una condición necesaria para el desarrollo humano (Dammert et al., 2017, p. 7).

La seguridad ciudadana también está ligada a las experiencias y la percepción de las personas con las conductas delictivas y la actuación de las autoridades frente a estas acciones. Caro et al. (2020, p. 10) identificaron que la seguridad ciudadana alberga cuatro dimensiones: victimización, miedo al delito, confianza en el sistema penal y demanda de castigo. Estas dimensiones se relacionan entre sí, ya que la desconfianza en el sistema penal o la demanda de castigo puede ser consecuencia de haber sido víctima o tener miedo al delito.

Un concepto claro es el del Instituto Nacional de Estadística e Informática (2018, p. 129):

> La inseguridad ciudadana es un fenómeno social complejo, multidimensional y multicausal, el cual se ha manifestado de la mano con el crecimiento económico, generando mayor movimiento comercial, más inversiones y por ende también nuevas formas de delincuencia. Es tarea del gobierno en conjunto con la ciudadanía, alcanzar las bases de una sociedad con altos niveles de seguridad ya que solo en un clima de paz se generan las condiciones sociales, económicas y políticas necesarias para el desarrollo y la prosperidad del país, por el contrario, la inseguridad o percepción de ésta, generan ansiedad y afectan la productividad.

Gonzales y Barbarán (2021, pp. 11-12) comentan que la seguridad ciudadana está ligada a la confianza que los mismos ciudadanos tienen con su gobierno, la falta de interés por parte

de las autoridades o el desconocimiento de los problemas sociales que aquejan a la población, añadiéndole la mala administración, afecta negativamente la participación ciudadana en las políticas gubernamentales que planteen los gobiernos sobre seguridad.

2.2.4. Información pública y privada

El acceso a la información pública y la privacidad de los datos son derechos fundamentales expresados en el artículo 2 de la constitución política del Perú y explayados en sus respectivas leyes. Según la Ley de Transparencia y Acceso a la Información Pública toda información que posea el Estado se presume pública, salvo las siguientes excepciones (Ley 27806, 2002, Artículo 15):

- Información que afecte la intimidad personal y/o familiar de otras personas.
- Información que involucre temas de inteligencia y/o seguridad nacional.
- Información clasificada en el ámbito militar.
- Información de negociaciones internacionales.
- Información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil.
- Investigaciones en curso de la Administración Pública que se hayan iniciado hace menos de 6 meses sin que se haya dictado una resolución final.
- Información de asesores jurídicos o abogados que puedan revelar la estrategia de la Entidad Pública ante un proceso administrativo o judicial.
- Información señalada por la Constitución o por una Ley aprobada por el Congreso de la República

Igualmente, según la Ley de Protección de Datos Personales, se consideran datos personales a "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados" (Ley 29733, 2011, Artículo 2).

En términos cotidianos podemos decir que lo público son aquellos datos e información concerniente a la sociedad en su conjunto y por lo tanto de interés general. Lo privado,

> es una idea extensa y genérica que cubre aquello que es parte de un individuo, y este no desea que llegue a ser del conocimiento general de la sociedad. (ICHITAIP, 2018, p. 5)

Astudillo (2020) explica que la transparencia de la información es clave para el ejercicio democrático, genera visibilidad y combate la corrupción; sin embargo, parte del buen desarrollo de una sociedad democrática también es mantener la reserva y el secreto, incluidos el derecho a la privacidad de las personas ya que es esencial para el pleno desarrollo de la personalidad de los ciudadanos.

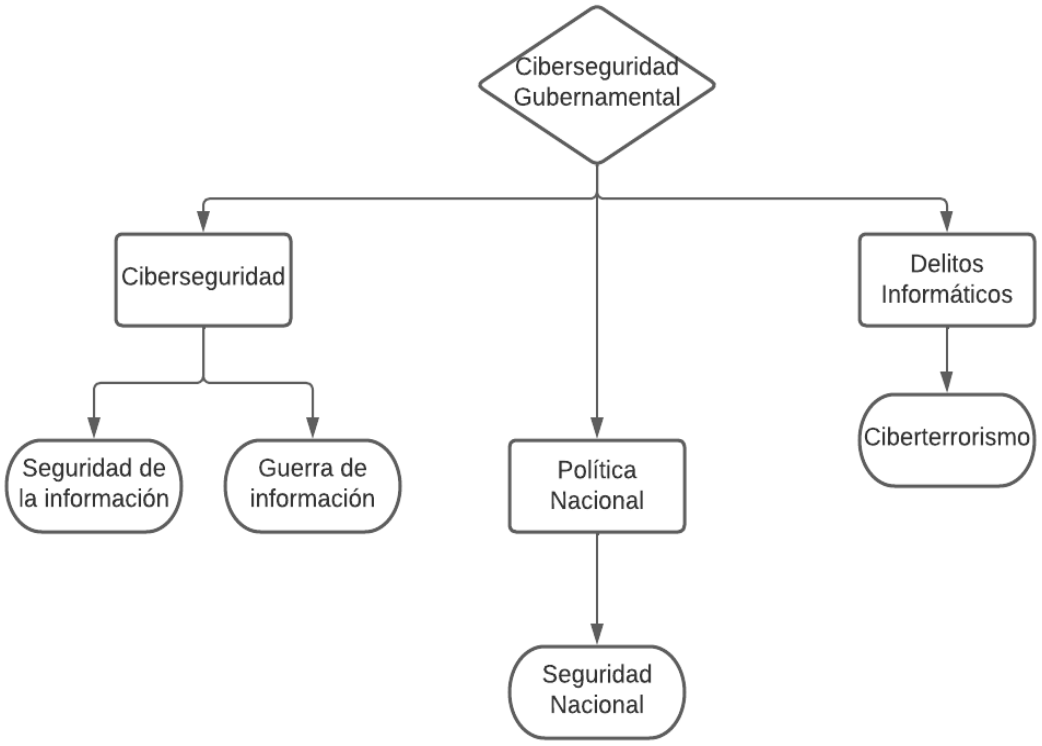
2.3.Definición de categorías de análisis

El trabajo de investigación es de tipo cualitativo por lo que se realiza una revisión de la literatura, para que la información seleccionada se estructure y analice de mejor forma; debe organizarse según por las categorías de análisis respectivas. Según Cisterna (2005), las categorías de análisis son tópicos que se obtienen a partir de la información recogida y que a su vez se pueden dividir en subcategorías para definir más aspectos específicos. Estás categorías y subcategorías pueden ser concebidas antes o después de la investigación, siempre desde la perspectiva del autor.

Se plantearon tres categorías y cuatro subcategorías de análisis para el presente trabajo:

Figura 2

División de las Categorías de Análisis



Nota: La figura 2 muestra las categorías y subcategorías utilizadas en la presente investigación.

2.3.1. Ciberseguridad

La ciberseguridad se concibe como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, acciones formativas, metodologías de gestión de riesgos y tecnologías que tienen como finalidad proteger el entorno cibernético y los activos que lo integran —dispositivos, infraestructuras, aplicaciones, servicios e información— garantizando su disponibilidad, integridad, autenticidad y confidencialidad frente a amenazas o riesgos relevantes (Unión Internacional de Telecomunicaciones [UIT], 2016).

En línea con esta perspectiva, la Organización de las Naciones Unidas (ONU) la define como el conjunto de estrategias, políticas, prácticas y medidas orientadas a identificar

vulnerabilidades, prevenir su explotación, mitigar daños y proteger a las personas, bienes e información en el ciberespacio (ONU, 2023).

Desde el ámbito académico, Velae & Brown (2020) amplían esta definición al señalar que "la ciberseguridad abarca el amplio abanico de cuestiones técnicas, organizativas y de gobernanza que deben tomar en consideración para proteger los sistemas de información en red contra las amenazas accidentales y deliberadas" (p.2). Complementariamente, Cortés (2015) enfoca la ciberseguridad desde una perspectiva estatal, definiéndola como "la capacidad del Estado para minimizar el nivel de riesgo cibernético al que están expuestos los ciudadanos, en áreas como transacciones financieras, protección a la información y propiedad intelectual" (p. 7).

En síntesis, estas definiciones convergen en caracterizar la ciberseguridad como el marco estratégico y técnico aplicado para salvaguardar los sistemas informáticos, redes, datos y servicios digitales frente a accesos no autorizados, ataques, fallos o destrucción, asegurando su funcionamiento seguro, resiliente y confiable.

2.3.2. Delitos informáticos

Los delitos informáticos son comportamientos ilícitos realizados a través de redes informáticas que ponen en peligro la integridad, fiabilidad y autenticidad de la información y sistemas de información almacenados en la red.

Estos delitos constituyen conductas ilícitas que ocasionan daños a personas e instituciones mediante la intrusión no autorizada en redes y sistemas de información, afectando recursos de comunicación al amenazar, paralizar, distorsionar o destruir datos mediante ataques como piratería informática, virus, interrupción de servicios, robo de información o manipulación de sitios web (Park, 2016). Su característica distintiva radica en que estas acciones tienen como propósito vulnerar los dispositivos y sistemas de seguridad y solo pueden ejecutarse a través de la tecnología, convirtiendo a las tecnologías de la información y comunicación (TIC) en el objetivo, el medio o el entorno de su ejecución (Villavicencio, 2014).

Desde una perspectiva institucional, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) define el delito cibernético como una modalidad de delincuencia transnacional que utiliza las tecnologías digitales y el ciberespacio para cometer fraudes, robo de identidad, difusión de contenidos ilegales, ataques a sistemas informáticos y otros actos ilícitos, caracterizándose por el anonimato de los autores, su rápida expansión y su vínculo con la delincuencia organizada (UNODC, 2013).

En el contexto actual, los delitos informáticos se manifiestan mediante múltiples modalidades, entre las que destacan el ransomware, que consiste en la extorsión mediante el secuestro de información; los fraudes electrónicos como el phishing; el uso de programas maliciosos para el robo de credenciales (infostealers); y los accesos no autorizados a sistemas con fines de espionaje o lucro económico. Esta problemática se ve agravada por la incorporación de tecnologías emergentes, como la inteligencia artificial, que facilita la creación de deepfakes, estafas más sofisticadas y campañas de desinformación a gran escala. Consecuentemente, el impacto del cibercrimen se proyecta como una amenaza global en constante crecimiento, vinculada a la delincuencia organizada y con consecuencias económicas de gran magnitud, lo que evidencia la necesidad de marcos regulatorios sólidos y políticas nacionales que fortalezcan la resiliencia digital de los Estados (Group-IB, 2025; World Economic Forum, 2025).

En síntesis, los delitos informáticos representan una amenaza creciente que, mediante el uso de tecnologías digitales y el ciberespacio, vulneran la integridad, disponibilidad y confidencialidad de la información, ocasionando daños tanto a personas como a instituciones. Estas conductas delictivas operan de forma anónima y transnacional, manifestándose en modalidades como el ransomware, el phishing, el robo de credenciales y los accesos no autorizados. Su sofisticación e impacto se ven potenciados por tecnologías emergentes como la inteligencia artificial, mientras que su vinculación con la delincuencia organizada y sus consecuencias económicas globales subrayan la urgencia de desarrollar marcos regulatorios sólidos y políticas nacionales que fortalezcan la resiliencia digital de los Estados.

2.3.3. Políticas nacionales

Una política nacional se concibe como un conjunto articulado de decisiones y acciones impulsadas por el Estado que establecen objetivos prioritarios, lineamientos y estándares para orientar la gestión pública y privada en torno a problemas de interés nacional. Estas políticas, de carácter obligatorio, trascienden los periodos de gobierno y garantizan la coherencia con los objetivos estratégicos de desarrollo del país (CEPLAN, 2018).

En el caso peruano, la Política Nacional de Ciberseguridad tiene como propósito fundamental garantizar la protección de la infraestructura de información, los datos estatales y las tecnologías asociadas frente a amenazas internas o externas, accidentales o deliberadas, asegurando así la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Adicionalmente, busca garantizar la implementación de la normativa y propuestas legislativas en materia de ciberseguridad, asignando los recursos y presupuestos necesarios para su cumplimiento. Por último, establece la necesidad de mantener la política permanentemente actualizada, fomentando la participación del sector público, privado, la sociedad civil y la academia, a fin de preservar su vigencia y eficacia (Presidencia del Consejo de Ministros, 2017).

En conclusión, las políticas nacionales representan decisiones estratégicas del Estado orientadas a resolver problemas prioritarios mediante objetivos, lineamientos y estándares que guían tanto las actividades públicas como privadas. Su eficacia depende no solo de la implementación normativa y la adecuada asignación de recursos, sino también de la actualización constante y la participación conjunta de diversos sectores, consolidando así un esfuerzo integral para salvaguardar la seguridad digital nacional.

CAPÍTULO III

FUNDAMENTOS TEÓRICOS

3.1.Fundamentación teórica

La presente investigación parte del reconocimiento de la ciberseguridad como un asunto de interés público que compete especialmente a los gobiernos, quienes deben orientar esfuerzos hacia la protección de la información estatal y ciudadana. En este contexto, realizar una revisión de la literatura sobre ciberseguridad gubernamental resulta fundamental para la toma de decisiones con criterios claros acerca de la importancia de este tema, analizando tanto los autores más reconocidos como los países que mayor producción científica generan en materia de ciberseguridad gubernamental.

La búsqueda de antecedentes permitió identificar investigaciones que resaltan la importancia de la ciberseguridad gubernamental o nacional, así como otros estudios que incorporan metodologías similares a la del presente trabajo. Se encontraron ocho tesis y un artículo, en su mayoría de origen nacional, que abordan temas como la creación de estrategias de ciberseguridad nacional, robo de información, amenazas en ciberseguridad, ciber-defensa y ciber-ataques.

A partir del análisis bibliográfico, se definieron las categorías y subcategorías de análisis basadas en los temas más recurrentes en la literatura especializada. El contenido se organizó en tres ejes principales:

Primero, ciberseguridad como tema central del estudio, cuyas subcategorías comprenden seguridad de la información y guerra de información. Segundo, delitos informáticos, considerado uno de los factores primordiales para el desarrollo de políticas de ciberseguridad, incluyendo aspectos específicos del ciber-terrorismo. Finalmente, la categoría de políticas nacionales, de particular relevancia desde la perspectiva gubernamental, que incluye la subcategoría de seguridad nacional.

La metodología empleada comprende un enfoque cualitativo de tipo descriptivo, utilizando como diseño metodológico la revisión sistemática. La información se obtuvo de bases de datos especializadas como Scopus y Web of Science, complementadas con el buscador Google Scholar. El contenido de la investigación se sistematizó en una tabla que incluye ítems como título, autor, fecha y tema principal, facilitando su recuperación posterior.

Durante el proceso de búsqueda se identificó una considerable cantidad de documentos en Close Access. Se estableció como criterio temporal la producción científica años 2010 a 2023, sin exclusión por idioma de publicación. El resultado final obtenido fue de 63 documentos que conforman la muestra del análisis.

3.2.Sistemas y categorías de análisis

La categoría de ciberseguridad se estructuró en dos subcategorías fundamentales: seguridad de la información y guerra de la información. Esta selección responde a la necesidad de comprender tanto la importancia como el contexto en el que se desarrolla la ciberseguridad, particularmente en lo que respecta a la protección de la información de ciudadanos y gobiernos.

La seguridad de la información abarca los mecanismos y estrategias destinados a salvaguardar los datos tanto del sector público como privado. Por su parte, la guerra de la información puede entenderse como una nueva modalidad de conflicto entre países, donde los actores estatales y no estatales utilizan medios digitales para generar información o desinformación con fines estratégicos.

Para cada subcategoría se incluyen los autores más representativos del campo, quienes abordan aspectos y conceptos fundamentales que contribuyen a la comprensión integral de estos temas.

Tabla 1

Primera Categoría de Análisis

Categoría de análisis	Subcategoría de análisis	Autores
Ciberseguridad	Seguridad de la información	Slayton (2021), de Bruijn & Janssen (2017), Dasgupta, Akhtar & Sen (2022), Veale & Brown (2020), Bresniker, Gavrilovska, Holt, Milojicic & Tran (2019), Silva (2013), Cárdenas-Solano, Martínez-Ardila, & Becerra-Ardila (2016), Onumo, Cullen, & Ullah-Awan (2017), Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando & Saltos-Gómez (2018)
	Guerra de la información	Whyte (2020), Buchyn & Kurus, (2018), Ivanov (2013), Topor & Tabachnik (2021), Aftergood (2017), Giles (2016), Lin (2020), Newmeyer, Cubeiro, & Sánchez (2015), Blank, (2010), De Álvaro (2023), Asbaş & Erdem Tuzlukaya (2023), Dipert (2010).

Nota: La Tabla 1 muestra la primera categoría de análisis con sus subcategorías y los autores más relevantes en el tema.

Para la segunda categoría, delitos informáticos, se definió una subcategoría específica: el ciber-terrorismo, concebido como una nueva modalidad de terrorismo que engloba actividades como el robo de información y el sabotaje de sistemas a gran escala, afectando principalmente la economía de empresas y gobiernos.

Esta subcategoría incluye los autores más relevantes del área, quienes documentan casos concretos y ejemplos representativos de ciber-terrorismo en diversos países, proporcionando un marco empírico para comprender las manifestaciones y el impacto de esta amenaza emergente.

Tabla 2

Segunda Categoría y de Análisis

Categoría de análisis	Subcategoría de análisis	Autores
Delitos informáticos	Ciber-terrorismo	Marsili (2019), Gross, Canetti & Vashdi (2017), Park (2016), Vila, (2019), Acurio (2016), Bresniker, Gavrilovska, Holt, Milojicic & Tran, (2019), Chigada & Madzinga, (2021), Coppolino, D'Antonio, Mazzeo, Romano & Sgaglione (2018), Villavicencio (2014), Jara Fuentealba & Jorquera Cruz (2021), Martin & Rice (2011), Snider, Shandler, Zandani & Canetti (2021), Guerrero (2018).

Nota: La Tabla 2 muestra la segunda categoría de análisis con sus subcategorías y los autores más relevantes en el tema.

Finalmente, la categoría de políticas nacionales comprende las bases y lineamientos que orientan las acciones gubernamentales en determinados periodos, aplicando métodos, procesos e instrumentos específicos para establecer marcos de seguridad y fortalecer las capacidades estatales mediante el aprovechamiento de las tecnologías de la información.

La subcategoría seguridad nacional incluye autores que establecen una vinculación directa entre la ciberseguridad y la seguridad nacional, explorando las intersecciones y dependencias entre ambos campos para el desarrollo de políticas públicas integrales.

Tabla 3

Tercera Categoría de Análisis

Categoría de análisis	Subcategoría de análisis	Autores
Políticas Nacionales	Seguridad nacional	Kryshtanovych, Ortynskyi, Zakharyash, Maziy & Krasivskyy (2021), Cai (2015), Dennis, Jones, Kildare & Barclay (2014), van Vuuren, Grobler, Leenen & Phahlamohlaka (2014), Arreola (2018), Akimenko & Giles (2020), Andreasson (2011), Borghello & Temperini (2013), Galán & Galán (2016), Charlet & King (2020), Coles-Kemp, Ashenden & O'Hara (2018), Comité Interministerial sobre Ciberseguridad (2017), Anderson (2014), Dupont (2019), Leiva (2015), European commission (2013), Jun (2016), Manley (2015), Maréchal (2017), Miroslaw (2021), Napetvaridze & Chochia (2019), Norris, Mateczun, Joshi & Finin (2018), Preis & Susskind (2022), van Steen, Norris, Atha & Joinson (2020), International Telecommunications Union (2012), Izaguirre & León (2018), Fojón & Sanz (2010), Cortés (2015), Doneda & Almeida (2015), Munkøe & Mölder (2022).

Nota: La Tabla 3 muestra la segunda categoría de análisis con sus subcategorías y los autores más relevantes en el tema.

CAPÍTULO IV

METODOLOGÍA

4.1.Enfoque de la investigación

La presente investigación adopta un enfoque cualitativo que, según Hernández, Fernández & Baptista (2014), busca conocer las perspectivas e interpretaciones de los participantes respecto a determinado fenómeno, mediante la recolección y análisis de datos diversos (verbales, audiovisuales, textuales, entre otros). Una característica distintiva de este enfoque es su naturaleza no lineal y flexible, que permite que las preguntas, objetivos e incluso el problema de investigación puedan evolucionar durante el transcurso del estudio, siempre sustentándose en la revisión constante de la literatura especializada.

4.2.Tipo de investigación

El tipo de investigación corresponde al nivel descriptivo, el cual tiene como propósito recolectar información sobre un fenómeno, situación, contexto o suceso específico para describir las propiedades y características más relevantes de dicho fenómeno tal como se presenta en la realidad, sin intervención del investigador (Hernández et al., 2014). En el marco de este trabajo, se busca describir las características fundamentales de la ciberseguridad gubernamental a través del análisis exhaustivo de la literatura especializada.

4.3.Diseño de investigación

El diseño metodológico seleccionado es la revisión sistemática (Systematic review), definida por Kitchenham (2004) como un medio para identificar, evaluar e interpretar toda la investigación científica relevante para una pregunta de investigación particular, área temática o fenómeno de interés. Este diseño implica la revisión comprehensiva de la literatura científica disponible sobre un tema específico dentro de un rango temporal determinado, estableciendo criterios rigurosos para la selección de información —como el campo de conocimiento, área temática específica, tipos de documento, entre otros— con el objetivo de sistematizar el

conocimiento existente y generar nuevas reflexiones que contribuyan al avance del campo disciplinar.

4.4.Estrategias y técnicas de investigación

La técnica de investigación empleada fue el análisis documental, que permite realizar una descripción y análisis sistemáticos basados en el contenido de las referencias bibliográficas seleccionadas. Como instrumento de recolección de datos, se utilizó una matriz desarrollada en Excel que incorpora categorías específicas para describir las características más relevantes de cada documento identificado, facilitando así la sistematización y posterior análisis de la información.

Tabla 4

Cuadro de Clasificación

Referencias Bibliográficas	Año	Autor	Idioma	País	Tipo	Base de datos	Acceso	Tema primario	Keywords	Termino de búsqueda	Doi	Enlace

Nota: El cuadro representa la clasificación de los documentos encontrados y las características más resaltantes de cada uno.

4.5.Búsqueda y recuperación de información

Para la búsqueda y recuperación de información se recurrió a las bases de datos más reconocidas en el ámbito de humanidades y ciencias sociales, específicamente Scopus y Web of Science. Dado que más de la mitad de la literatura identificada en estas bases se encuentra en idioma inglés, se complementó la búsqueda utilizando Google Scholar con el propósito de recuperar literatura especializada en español y ampliar así la diversidad lingüística de la muestra.

Se utilizaron los siguientes términos para la búsqueda:

Tabla 5

Términos de búsqueda

Término Español	**Término Inglés**
información AND guerra	*information AND warfare*
ciberataques	*cyberattacks*
ciberataques AND estado	*cyberattack AND state*
ciberseguridad nacional	*nacional cybersegurity*
ciberguerra	*cyberwar*
delitos informáticos	*cybercrime*
ciberseguridad gubernamental	*government cybersecurity*
guerra de información AND ciberseguridad	*information war and cybersecurity*
seguridad de la información	*information security*

Nota: La tabla muestra la lista de términos de búsqueda, tanto en español como en inglés.

Se obtuvo una muestra total de 63 documentos (Anexo 1), distribuidos de la siguiente manera: 44 en idioma inglés, 18 en español y uno en ruso. En cuanto al tipo documental, predominan los artículos científicos con un 71%, mientras que el 29% restante se distribuye entre conferencias, libros, notas y otros tipos de publicaciones académicas.

Como se mencionó anteriormente, el acceso a los documentos constituyó una limitante significativa del estudio; no obstante, fue posible acceder a algunos textos de acceso restringido, complementándose la muestra con documentos de acceso abierto (Open Access).

4.6.Criterios de selección de la información

Debido a lo extenso que puede llegar a ser este tema, se utilizaron los siguientes criterios de búsqueda para una recuperación más exacta del tema tratado.

Criterios de Búsqueda:

- Recuperar documentos solo de bases de datos o repositorios confiables.
- Documentos que no sobrepasen el periodo de años establecidos.

- Documentos relacionados con las categorías y subcategorías de análisis.
- Solo se toman como referencia documentos que estén dentro del campo de las Humanidades y Ciencias Sociales.

CAPÍTULO V

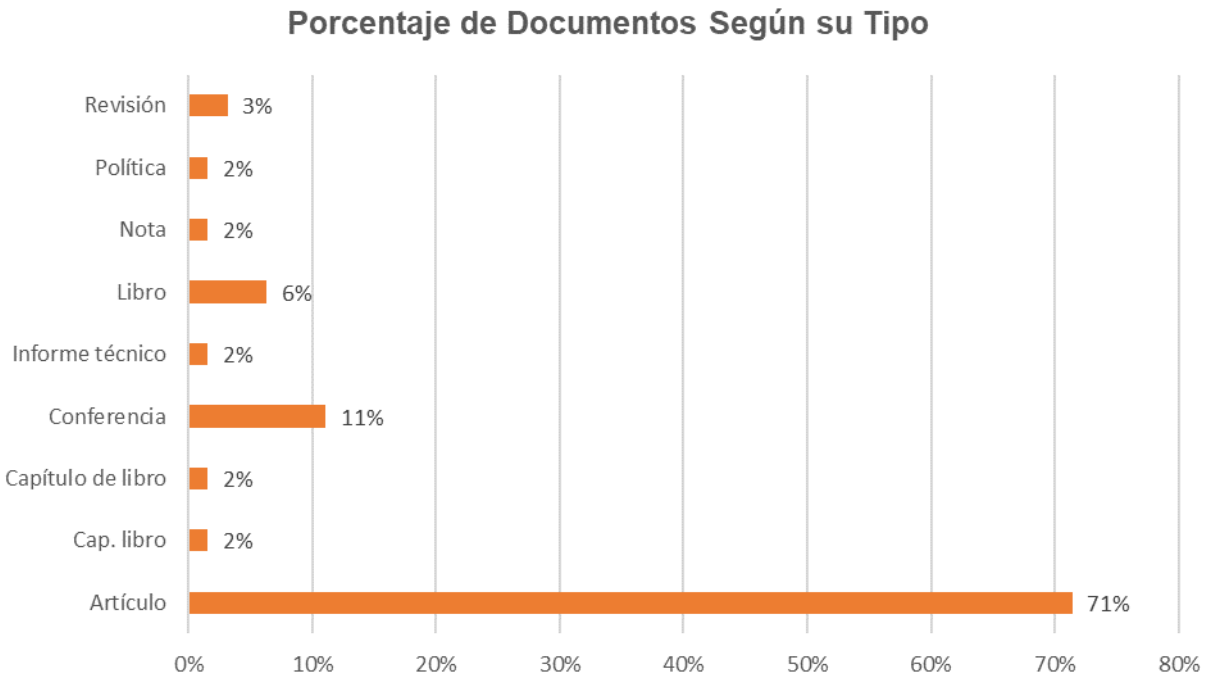
RESULTADOS

5.1.Características generales de los resultados

En este capítulo se presentan las características generales obtenidas en base a la literatura encontrada sobre ciberseguridad gubernamental. A continuación, los principales hallazgos:

Figura 3

Tipos de Documentos

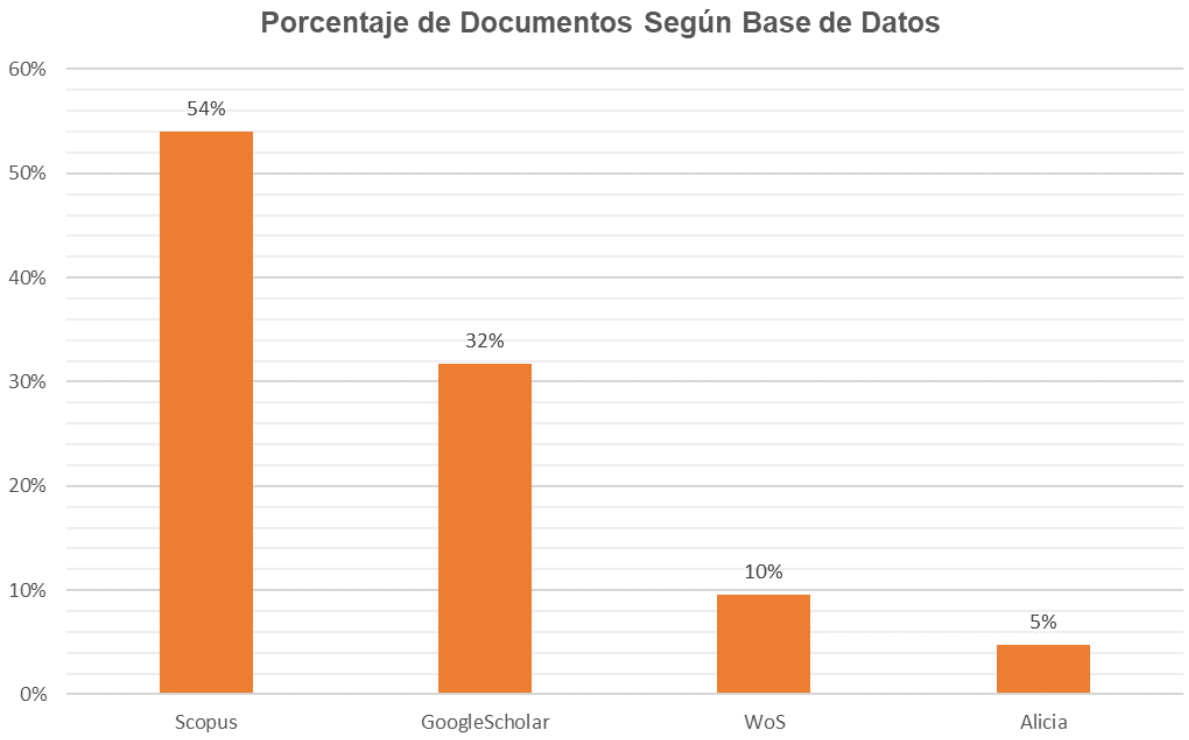


Nota: La Figura 3 representa los tipos documentales rescatados de la literatura encontrada.

De la literatura encontrada, se evidenció que el 71% de los documentos son artículos, debido a que es el tipo documental más usado para investigación; seguido por mucha diferencia de conferencias con un 11% y libros con un 6%.

Figura 4

Bases de Datos

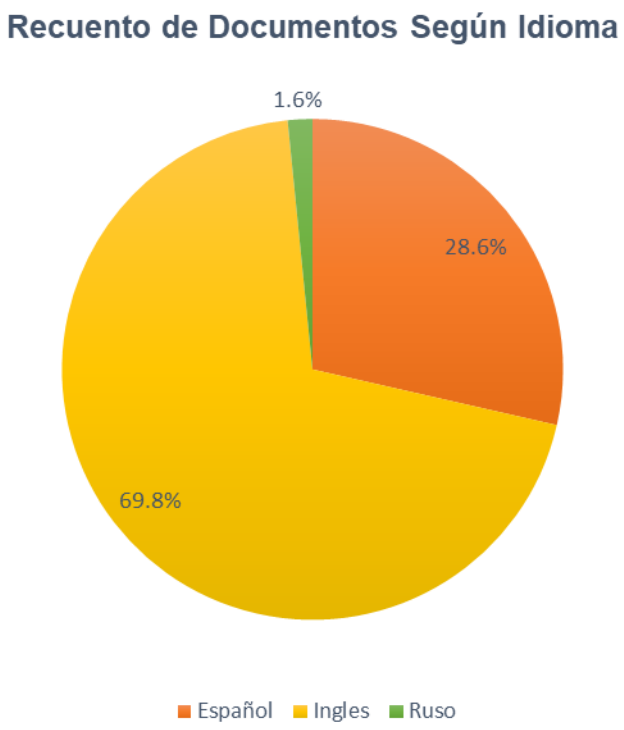


Nota: La Figura 4 muestra en porcentaje de documentos encontrados en cada base de datos.

Según los resultados, Scopus fue la base de datos más usada con un 54%, gracias a la amplitud de documentos que abarca y a la calidad de los mismos; viene seguido el buscador Google Scholar con un 32%.

Figura 5

Idioma

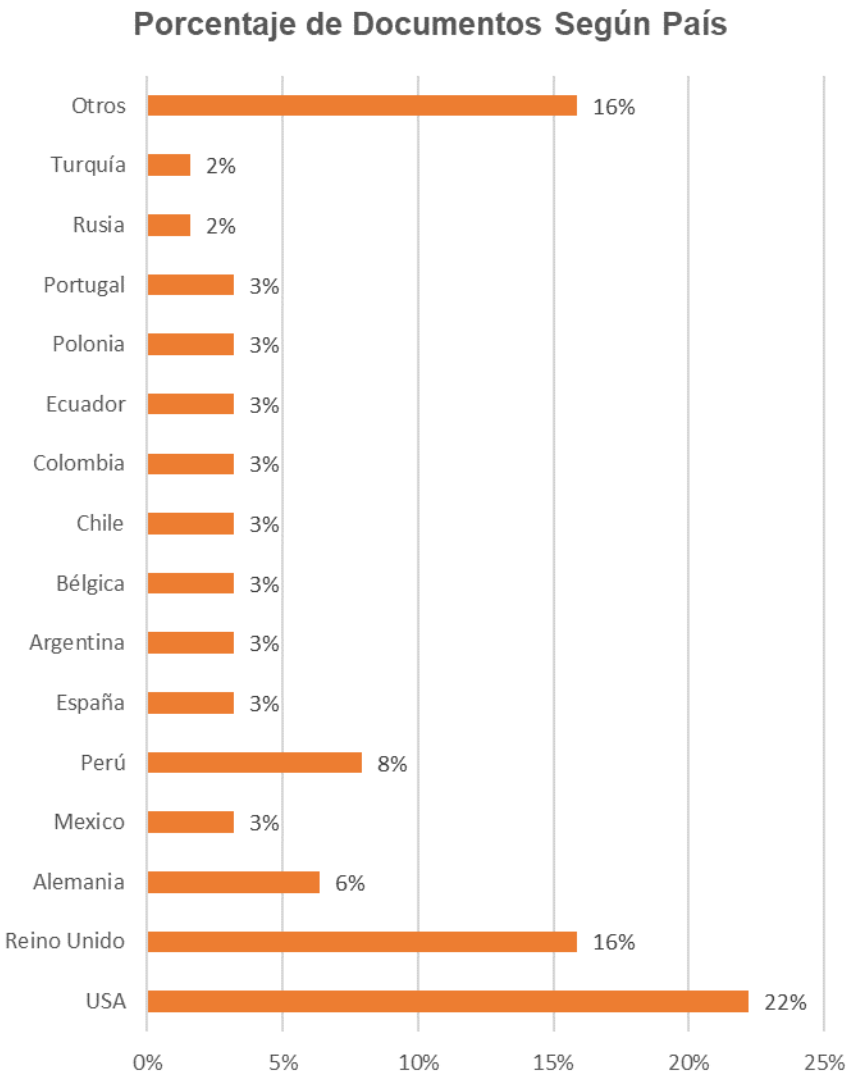


Nota: La Figura 5 muestra el porcentaje de documentos según su idioma.

Como se observa en la Figura 5, el idioma predominante es el inglés con un 69.8%, seguido por el español con 28.6%, más un documento en ruso que corresponde a el 1.6% del total.

Figura 6

Países de Origen de la Literatura Utilizada

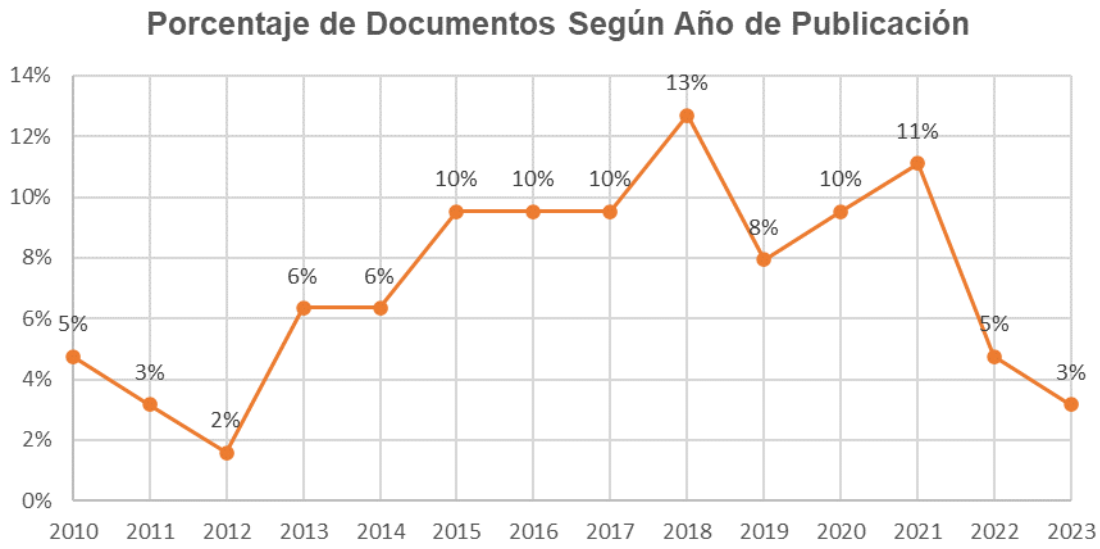


Nota: La Figura 6 muestra el porcentaje de documentos encontrados según su país de origen.

El país de donde provienen una gran cantidad de documentos es Estados Unidos con 22%, seguido de Reino Unido con 16%, el resto de la literatura se divide entre otros países del mundo cono se observa en la Figura 6.

Figura 7

Año de Publicaciones



Nota: La Figura 7 representa el porcentaje de los documentos según su año de publicación y el flujo de un año a otro.

El flujo de los años en los que se publicaron los documentos nos muestra que hubo un incremento significativo entre los años 2010 y 2021, con pequeñas disminuciones en los años 2012 y 2019. La gráfica también muestra un descenso en el 2023, sin embargo, esto se debe a que el presente trabajo se realizó en ese año y muchas publicaciones no están disponibles aún.

5.2.Análisis teórico conceptual de la ciberseguridad gubernamental

Las categorías que figuran en la presente investigación son producto de la búsqueda y recolección de la información, de acuerdo con ello se plantearon los objetivos, los cuales se tratarán uno por uno en los resultados de acuerdo con lo que se expone en los documentos encontrados.

5.2.1 Conceptos sobre ciberseguridad y seguridad de la información.

Los términos seguridad de la información y seguridad informática son diferentes, pero de igual forma están ligados entre sí. Figueroa-Suárez et al. (2018) define a la seguridad informática como la distinción táctica y operacional de la seguridad, atendiendo solo a la protección de medios informáticos o digitales, mientras que la seguridad de la información como la línea estratégica de la seguridad, es independiente a cualquier medio en el que esté, pero a su vez se apoya en la seguridad informática para cumplir sus objetivos, por lo que la seguridad de la información sería "la encargada de regular y establecer las pautas a seguir para la protección de la información." (Figueroa-Suárez, 2018, p. 152)

La *International Telecomunication Unión* (ITU) define a la ciberseguridad como:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardias de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, garantías y tecnologías que pueden usarse para proteger el entorno cibernético, la organización y los activos de los usuarios. (…) La ciberseguridad se esfuerza por garantizar el logro y el mantenimiento de las propiedades de seguridad de la organización y los activos del usuario contra los riesgos de seguridad relevantes en el entorno cibernético. La ciberseguridad juega un papel importante en el desarrollo continuo de la tecnología de la información, así como de los servicios de Internet. Mejorar la ciberseguridad y proteger las infraestructuras de información críticas son esenciales para la seguridad y el bienestar económico de cada nación.

A pesar de la definición de la ITU, Newmeyer, et al. (2015) afirman que no existe un consenso internacional en lo que constituye la definición de la Ciberseguridad. Las definiciones que imponen en los lineamientos de política de gobierno dependen de la percepción que tengan sobre la naturaleza de la amenaza del ciberespacio. Por lo tanto, la Ciberseguridad es "el conjunto de prácticas políticas, de entrenamiento y tecnología, diseñada para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño" (p. 79). van Vuuren, et al. (2014), también señala que la ciberseguridad es un concepto bastante vago e indefinido al no haber un consenso sobre

su definición. Además, señalan también que el ámbito cibernético tiende a ser volátil y a cambiar con rapidez, lo que crea un entorno competitivo en el que los actores tienden a no compartir información. Los autores demandan que se llegue a un acuerdo internacional sobre la definición de ciberseguridad, así como sobre la definición de normas de ciberseguridad.

Otros autores proponen su propia definición sobre ciberseguridad como Bresniker, et al. (2019) que señala que "La ciberseguridad se centra principalmente en la creación de herramientas que puedan proporcionar evaluaciones detalladas de las actividades en una red" (p. 47), mientras Vila (2019) determina que es un procedimiento que busca resguardar las infraestructuras críticas, sistemas de información y comunicaciones contra diversas amenazas, a través de medidas preventivas, de detección y de respuesta. El propósito fundamental de la seguridad informática consiste en evitar que terceros hagan uso no autorizado de estos recursos. Este enfoque de seguridad se guía por tres objetivos clave: garantizar la disponibilidad, confidencialidad e integridad de los sistemas y la información.

Jara Fuentealba & Jorquera Cruz (2021) deducen que la ciberseguridad puede conceptualizarse como el conjunto de medidas implementadas para salvaguardar la información presente en el ciberespacio o en un sistema informático conectado a él, y la infraestructura que sostiene dicha información. En otras palabras, se trata de la seguridad orientada a proteger y asegurar las interacciones entre seres humanos, entre computadoras y entre seres humanos y computadoras, centrándose en la protección de la información y los medios de comunicación utilizados para transmitirla.

E Silva (2013) menciona que, aunque la ciberseguridad abarca aspectos de la seguridad de las Tecnologías de la Información y Comunicación (TIC) tanto en el entorno como fuera de línea, la seguridad en internet es una faceta de la agenda de la ciberseguridad. Con frecuencia incorporada como un objetivo en las estrategias a nivel nacional, la seguridad en internet se refiere a la promoción de una cultura de concienciación, responsabilidad y preparación tanto a nivel individual como organizacional, con el propósito de hacer frente a las amenazas presentes en el entorno digital.

La Seguridad, incluida la Ciberseguridad, no se rige por fronteras perfectamente definidas; por el contrario, su configuración involucra la intersección, superposición, integración y, en ocasiones, la mutua erosión de conceptos, métodos, procedimientos, herramientas y regulaciones. Este proceso da lugar a una realidad diversa y multidisciplinaria (Galán & Galán, 2016).

Cárdenas-Solano et al. (2016) afirman que "la seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores a concentrarse en políticas, procedimientos y controles basados en las personas" (p. 932).

Otras definiciones enlazan la ciberseguridad con la gobernanza: "La ciberseguridad abarca el amplio abanico de aspectos técnicos, organizativos y de gobernanza que deben tenerse en cuenta para proteger los sistemas de información en red contra las amenazas accidentales y deliberadas" (Veale & Brown, 2020, p. 1). Slayton (2021) también emparenta la gobernanza con la seguridad de la información, afirma que esta, en teoría, pretende gobernar la incertidumbre mediante la gestión de riesgos, sin embargo, también corre riesgo de crear un régimen de inseguridad debido a la interdependencia de las tecnologías de la información, lo que le da mayor vulnerabilidad.

El concepto de seguridad de la información es mucho más importante para los académicos, ya que al estudiar este concepto también acarrea otros temas de más importancia como la seguridad de internet, violaciones de privacidad y la defensa de la democracia contra la guerra de la información (Veale & Brown, 2020). Por eso en muchos estados se militarizó este concepto, porque la sociedad depende cada vez más de la tecnología, introduciéndola en la vida cotidiana, lo que conocemos como internet de las cosas, por lo que cada vez hay nuevas formas de vulnerar la seguridad de las personas y la de los países.

Gracias a la presencia de todo tipo de dispositivos informáticos, hoy se producen muchos datos, públicos y clasificados, creados por personas naturales u organizaciones que procesan, almacenan y comercializan los datos mediante redes cibernéticas. Asegurar estos datos se ha convertido en algo primordial para todos, por lo que hoy en día se usa el Aprendizaje Automático (*Machine Learning*) para asegurar el ciberespacio, mejorando la solides de las

redes, así como el mantenimiento íntegro de los datos (Dasgupta et al., 2022). Bresniker et al. (2019) afirman también que una ciberseguridad adecuada requiere automatización, la cual, a su vez, requiere un medio para capturar el comportamiento de los analistas de ciberseguridad. (…) Como resultado, una mayor adopción de IA y ML en ciberseguridad reducirá la efectividad y el impacto de los ataques.

En cuanto a algunos problemas que han identificado los autores están de De Bruijn & Janssen (2017), quienes señalan que "el interés por las cuestiones de ciberseguridad suele centrarse en los incidentes y en cómo tratarlos a posteriori, mientras que la preocupación por la prevención y las inversiones en una mejor ciberseguridad han quedado rezagadas" (p. 2). Así mismo Onumo, Cullen, Ullah-Awan (2017) señalan que, en tiempos recientes, el ciberespacio ha experimentado una transformación significativa, convirtiéndose en una infraestructura global de tecnologías de la información y la comunicación que facilita las interacciones complejas entre redes de información y dispositivos electrónicos. Las naciones han aprovechado este entorno en constante evolución para promover sus intereses políticos y socioeconómicos, convirtiendo al ciberespacio en una de las infraestructuras críticas nacionales que requiere una protección estratégica.

Extrapolando las ideas de los autores ya mencionados, se puede entender que la seguridad de la información implica el uso de diversas herramientas, tecnológicas y humanas, para la correcta protección de información y datos de organizaciones e individuos contra amenazas o riesgos. Esta protección se debe basar en tres propósitos principales:

1. Confidencialidad: Asegurar que la información solo esté disponible para personas autorizadas y prohibir el acceso a cualquier otra.
2. Integridad: Garantizar que la información sea precisa y confiable, sin alteraciones o manipulaciones.
3. Disponibilidad: Garantizar la accesibilidad de la información cuando se necesite.

Cabe resaltar que no existe una sola definición de seguridad de la información o ciberseguridad, por lo que cada entidad y país la define según su propia perspectiva, esto deviene en una serie de consecuencias algo negativas para otros ámbitos, como en la guerra de

información. No hay una definición exacta, por lo tanto, no hay reglas de juego; o a la hora de diseñar políticas de ciberseguridad, cada país la define según sus propios intereses y por lo tanto hay una gran desigualdad en la protección de datos de cada nación.

5.2.2 Implicancias de la guerra de la información y la ciberdelincuencia.

5.2.2.1 Guerra de información

A medida que las nuevas tecnologías y la revolución de la información transforman nuestra sociedad, surgen nuevos espacios de conflicto. Entre estos un nuevo termino llamado guerra de información, que según Ivanov (2013), es un enfrentamiento o acción militar que daña los sistemas de información y recursos con el fin de obtener superioridad en información. También está el hecho de que estos actos no solo causan daños físicos, sino psicológicos, causando un gran impacto en la mente de las personas.

Con los cambios actuales en las estrategias militares, los campos de batalla se han diversificado considerablemente, más allá de las divisiones convencionales terrestres, aéreas y marítimas. Una de estas áreas emergentes es el ciberespacio, donde todas las acciones se aprovechan de ventajas como la accesibilidad, el bajo costo, el anonimato y la independencia de la distancia, dando lugar a lo que se conoce como guerra cibernética: una forma de asimetría de ataque. En esta guerra, los estados u organizaciones utilizan ataques cibernéticos para infligir daño en los sistemas de información, redes e infraestructuras informáticas de otros, dentro del contexto de conflictos. A pesar de su naturaleza única, la lógica subyacente detrás de estos ataques es similar a otros tipos de guerra, lo que hace que la guerra cibernética sea tanto una dimensión de los conflictos reales como un campo de batalla independiente (Asbaş & Erdem Tuzlukaya, 2023).

Esto supone una amenaza para la funcionalidad de las democracias porque no todas las naciones tienen los suficientes recursos para salvaguardar sus sistemas de información. En muchos casos esta guerra consiste en vulnerar los sistemas de información de alguna nación, bloquear algunas actividades y así crear caos en la sociedad, o sustraer información importante y pedir una recompensa por ella.

Un ejemplo de este tipo de conflicto es lo que sucede con Rusia y Ucrania, en donde el espacio cibernético ucraniano es sumamente vulnerable a los ataques informáticos de Rusia. A pesar de la existencia en Ucrania de una base de datos de mecanismos legislativos para la seguridad de la información y para contrarrestar la guerra de la información de Rusia contra Ucrania, no está debidamente formada. Algo importante del porqué es sumamente difícil vulnerar los sistemas de información rusos es que restringe la posible influencia informativa occidental e indeseable sobre su población, a través de diversas leyes que restringen el uso de información en su población, cosa que en muchas naciones no se hace, ya que va en contra de su naturaleza democrática (Buchyn & Kurus, 2018; Topor & Tabachnik, 2021).

Ivanov (2013) señala que el desarrollo de internet es lo que condujo al surgimiento de guerras de información en el ciberespacio, también la describe como "un complejo de influencias informativas y psicológicas destinadas principalmente a crear la opinión pública deseada, así como patrones de comportamiento individuales y grupales" (p. 276). Igualmente, Buchyn & Kurus (2018) describen la guerra de información como un impacto informativo negativo sobre el enemigo cuyo adversario puede ser un individuo o un grupo de personas y actúa de forma espontánea o planificada; así mismo exponen el hecho de que este tipo de guerra no es considerado por muchos académicos como un conflicto armado debido a que no asume pérdidas de vidas humanas o derramamiento de sangre.

Según De Álvaro (2023), la guerra de la información daña seriamente a la población porque ataca infraestructuras básicas y frena el funcionamiento de ciudades enteras, es así como esta es "una guerra que no se ajusta a los principios clásicos de un conflicto y que escapa a cualquier regulación, una guerra en la que pueden participar actores de todo tipo y, a primera vista, salir indemnes" (p. 4). Park (2016) explica que una guerra cibernética implica la realización de una guerra física, electrónica, económica, mental y humana para dañar la seguridad del país y de su pueblo, mientras Blank (2010) menciona que, la guerra de información no debe ser definida exclusivamente como ataques mediante tecnologías informáticas dirigidos a objetivos militares o redes de información del adversario. Las bombas lógicas, los virus, etc. no agotan el repertorio de la guerra informática. Los escritores soviéticos y rusos tuvieron razón al señalar que las nuevas armas que están siendo desplegadas incorporan

un componente tanto de información como de ataque. En este sentido, la guerra de información comprende ataques contra las redes de información y contra el componente informativo de los sistemas de armas.

Otros autores destacan la importancia de una mejora en los sistemas de ciberseguridad, tal como Whyte (2020) quien refleja la relación entre los ciber atacantes beligerantes y los sistemas de información sobre los que operan, entendiendo que un mayor análisis sobre estos sistemas y atacantes podría disminuir o prevenir los ataques, sin embargo, existe una mayor preocupación sobre la relación entre las acciones digitales conflictivas y las implicaciones para la seguridad nacional debido al alcance que tienen que tienen los ciudadanos sobre las tecnologías digitales en evolución. En esa misma línea, Lin (2020) por su parte define la guerra de información como el uso deliberado de información para confundir, engañar y afectar las elecciones y decisiones del adversario, sin embargo, considera que una mejora en la ciberseguridad no impediría que un adversario inicie una guerra de información.

Newmeyer, et al. (2015) sostienen que los ciberataques y las prácticas de seguridad deficientes posibilitan que terceros capturan a los ordenadores y se utilicen para realizar actividades como el envío de correos no deseados (spam), la propagación de virus o la participación en ataques de denegación de servicio. (...) La dificultad en la atribución presenta limitaciones a aquellos encargados de planificar políticas y llevar a cabo acciones en respuesta. A diferencia de los ataques militares históricos, la naturaleza de un ciberataque no deja rastros evidentes que indiquen el lugar de origen, como sucede con la estela de un cohete. Finalmente, algunos autores mencionan las prácticas de ciberguerra y ciberdefensa de los tres países que tienen un poder político bastante alto:

Topor & Tabachnik (2021) afirman que la guerra cibernética de la información es un arma de doble filo en Estados Unidos. Por un lado, los estados pueden emplearla para influir en la mentalidad de las sociedades y generar opinión publica de los líderes políticos extranjeros. Por otro lado, los Estados también son susceptibles a la influencia extranjera a través de la guerra de la información.

Aftergood S. (2017) menciona que las fuerzas de la "Internet libre" abogan por el libre flujo de información sin restricciones por fronteras nacionales o barreras culturales. En contraste, el bando de la "ciber soberanía", liderado por Rusia y China, aboga por un mayor control gubernamental sobre Internet y la información. En el caso de China, para mantener su operación de censura masiva, el “Gran Cortafuegos” emplea a más personas que las que sirven en las fuerzas armadas del mismo país.

Finalmente, Giles (2016) apunta que, para Rusia, el término "confrontación informativa" o "guerra informativa" es un concepto amplio e inclusivo que engloba una variedad de actividades. Esto incluye actividades hostiles que emplean la información como herramienta, como objetivo o como campo de operaciones.

La llamada guerra de la información se puede entender también como una guerra cibernética, ya que todo sucede en el ámbito digital usando las tecnologías de información y comunicación. Los objetivos de esta guerra es como la de cualquier otra, políticos militares, ideológicos, etc.; con la diferencia de que el arma es la información y el campo de batalla el ciberespacio.

Como se mencionó anteriormente, la guerra de la información no tiene reglas, por lo que no hay una entidad internacional que vele por la ciberseguridad en el espacio digital, y aunque lo hubiera, según Dipert (2010), la regulación de la guerra cibernética a través de tratados internacionales es problemática y se predice la posibilidad de períodos prolongados de guerra cibernética de bajo nivel, similar a una Guerra Fría Cibernética; mientras, se busca un equilibrio en la teoría de juegos y que cada país posee sus propias reglas de juego y diferentes formas de atacar: usando la desinformación, utilizando información falsa, influyendo en la opinión pública, realizando el espionaje y ataques cibernéticos a sistemas de entidades públicas o privadas, y saboteando la información a los procesos y servicios que brindan.

5.2.2.2 Ciberterrorismo

El ciberterrorismo o ciberguerra no puede ser considerado un conflicto convencional como la guerra en sí, a pesar de que el componente de violencia está presente en ambos, la

guerra tiene un espacio temporal y físico en el que se desarrolla y se pone un fin, cosa que en el ciberespacio no se puede definir porque es virtual e ilimitado (Marsili, 2019); También hay una diferencia entre un ciberdelito convencional y el ciberterrorismo y la distinción parte de las motivaciones que son económicas más que ideológica: en consecuencia, se considera un delito cibernético.

Acurio (2016), llama al cibercrimen "delincuencia informática" y la define como "todo acto o conducta ilícita que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes, que tenga como finalidad causar lesiones o poner en peligro un bien jurídico cualquiera" (p. 14); mientras que Vila (2019), toma como referencia lo estipulado por el Ministerio de Defensa de España y define el ciberterrorismo como "un ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico" (p. 24).

Entre las definiciones más populares de ciberterrorismo está Park (2016) quien señala que un ciberdelito se refiere a una conducta delictiva que causa daño al país y a las personas al invadir una red de información y comunicación sin autorización para acceder a ella. Este tipo de delito amenaza, perturba, paraliza o destruye recursos de información y comunicación mediante ataques de piratería informática. Por otro lado, un ataque terrorista cibernético se caracteriza por la comisión de al menos dos delitos cibernéticos; puede incluir acciones como robo, distorsión y propagación de información relacionada con la infraestructura nacional y social, afectando áreas cruciales para la seguridad nacional, como asuntos exteriores, defensa nacional, unificación, administración, vida social y seguridad de las personas. Estos delitos, como infringir la información, mal uso de los derechos, operar sitios web ilegales, corromper y eliminar la información, ocurren simultáneamente a través de una red de información y comunicación.

Gross et al. (2017) menciona las diferencias que hay entre ciberterrorismo, guerra cibernética y ciberdelito; se concluye que el ciberterrorismo se distingue del terrorismo convencional por el uso de tecnología informática maliciosa en lugar de fuerza cinética. Aunque emplea métodos digitales, comparte similitudes con el terrorismo tradicional al buscar promover

objetivos políticos, religiosos o ideológicos mediante la provocación de daño físico o psicológico a civiles. En contraste, la guerra cibernética utiliza *malware* y virus con el propósito de desactivar objetivos militares, mientras que el delito cibernético busca obtener ganancias financieras o dañar a otros por motivos personales (como venganza o intimidación), sin estar necesariamente relacionado con conflictos políticos.

El ciberterrorismo a pesar de no ser letal como el terrorismo convencional, afecta a la población de diversas maneras, incrementando la ansiedad, la inseguridad personal y la percepción de amenaza, esta última conlleva a que algunas personas estén a favor de algunas políticas gubernamentales firmes que podrían afectar negativamente el discurso de una sociedad democrática abierta. Chigada & Madzinga (2021) afirman que durante la época de pandemia hubo un gran incremento en las ciber amenazas y los ataques ya que estas se potencian aprovechando el miedo y la incertidumbre provocados por la inestable situación social y económica provocada por la pandemia de COVID-19.

Similar al impacto del terrorismo convencional, el ciberterrorismo tiende a generar un endurecimiento de las actitudes políticas. En este contexto, las personas pueden mostrar disposición a sacrificar las libertades civiles y la privacidad en aras de la seguridad. Además, es probable que respalden medidas como la vigilancia gubernamental, una mayor regulación de Internet y respuestas militares contundentes como respuesta a los ciberataques. Este cambio de actitud refleja la percepción de amenaza y la búsqueda de medidas de seguridad más estrictas en un esfuerzo por hacer frente a las amenazas cibernéticas. (Gross et al., 2017).

Gross et al. en su estudio concluyó que la percepción de la amenaza y no un ataque real, es más inquietante para los individuos afectados. Entonces no es necesaria la exposición a sucesos reales para desencadenar la ansiedad, sino la mera percepción de la amenaza. Por eso las autoridades deben reconocer que no pueden reducir o eliminar el temor al ciberterrorismo, por lo que una solución sería comunicar eficazmente los riesgos del ciberterrorismo y educar a su población sobre ciberseguridad.

En ese sentido Villavicencio (2014) también aclara que no puede constituirse como un delito informático solo por usar la tecnología informática como medio, sino el hecho de ingresar

sin autorización a sistemas de datos o sabotearlos, ya que estos delitos no serían posibles sin la informática.

El ciberterrorismo también acarrea pérdidas económicas, Martin & Rice (2011) mencionan que la literatura especializada en la disciplina del delito cibernético se enfoca en cómo estas actividades delictivas afectan a individuos y organizaciones, así como en las medidas que podrían implementarse (como educativas, legales y policiales) para ayudar a las partes afectadas. Este enfoque cobra especial relevancia; por ejemplo, en el contexto australiano, donde algunas estimaciones indican que individuos y organizaciones pueden perder hasta 650 millones de dólares australianos cada año debido a eventos de delitos cibernéticos.

Por último, De Álvaro (2023) sostiene un problema importante en ciberespacio que da paso a los delitos informáticos y es que, en el contexto de la intangibilidad mencionada, surge uno de los mayores desafíos del ciberespacio: la falta de control. No existe una autoridad mundial que supervise lo que sucede en este dominio y vigile las actividades ilícitas que puedan desarrollarse. Como resultado, ha surgido un movimiento de ataques y amenazas a la seguridad de las personas a través de diversos delitos cibernéticos. Estos delitos cibernéticos se refieren a acciones antijurídicas que se realizan a través de Internet. Aunque existe el Convenio de Budapest, que crea un marco legal común para combatir el ciberdelito, muchos países se niegan a serlo por no ser beneficioso para sus intereses, ya que debe haber cooperación e intercambio de información constante entre los miembros (Guerrero, 2018). Se demuestra que, aunque hubiera un organismo internacional que tenga control sobre el ciberespacio, pocos serían los países que accedan a ser parte de ese control.

La delgada línea que diferencia el cibercrimen con el ciberterrorismo es la motivación u objetivos del mismo; el cibercrimen se comete por lo general para obtener ganancias económicas por el espionaje o la venta de información importante mientras el ciberterrorismo se lleva a cabo por razones ideológicas (políticas, religiosas, sociales, etc.), causando miedo y caos entre la población para que así origine un desequilibrio en la sociedad.

Algunos de los problemas que causa el ciberterrorismo es la atribución, que en el momento es complicado diferenciar si un ciberataque es o no causado por terrorismo, por lo que

en muchos casos nunca se logra saber las motivaciones, salvo que los mismos responsables deseen salir a la luz y se atribuyan sus propios actos. Otro problema es lo que provoca en la seguridad nacional y se puede desestabilizar un país entero con el hackeo a una base de datos o a algún servicio del estado por lo que también tiene un gran impacto económico y social.

5.2.3 Componentes de una política nacional de ciberseguridad

La sociedad de la información que tanto ha ayudado a resolver un sinfín de tareas cotidianas de una manera práctica y veloz, así como genera oportunidades, también genera riesgos y amenazas, lo que es directamente proporcional al grado de dependencia digital de la sociedad. Los conflictos actuales hacen cada vez más uso del ciberespacio como campo de batalla, por lo que los estados deben adecuarse a las ciber amenazas actuales a través de normativas, organizaciones, estrategias, etc.; Vila (2019) sostiene que no puede existir seguridad en los sistemas nacionales si no existe una política de ciberseguridad, que tampoco podría existir si no existe una cultura de seguridad y defensa en la sociedad; por lo que propone los siguiente:

- Incrementar la formación de recursos humanos altamente especializados para trabajar en el campo de las TIC.
- Incrementar la formación de los niños y jóvenes en su paso por el Sistema Educativo Nacional (SEN) en el dominio de las habilidades y destrezas informáticas.
- Actualizar y completar la legislación vigente.
- Continuar desarrollando la infraestructura nacional de comunicaciones e informática.
- Potenciar los mecanismos de ciberseguridad de los sistemas nacionales y de respuesta ante incidentes informáticos.

Promover una cultura de ciberseguridad, desde individuos hasta organizaciones, contribuye a construir una sociedad de la información segura, sin embargo, actualmente muchos de los esfuerzos solo se centran en la concienciación, pero no es suficiente. Por lo que Dennis et al. (2014) proponen un marco nacional de ciberseguridad, una guía que pueda utilizarse como plataforma para que los gobiernos y las empresas ayuden en su infraestructura de información crítica. Dentro del ámbito del ciberdelito y la ciberseguridad, un sistema nacional de ciberseguridad resulta útil para proporcionar orientación tanto al gobierno como a los

ciudadanos sobre cómo protegerse contra el ciberdelito y cómo responder en caso de cualquier incidente. El gobierno puede identificar consideraciones clave para desarrollar un marco proactivo de ciberseguridad y comprender los requisitos necesarios para planificar y responder a incidentes cibernéticos a nivel nacional. Se pueden desarrollar e implementar medidas técnicas apropiadas, junto con acciones legislativas, para proteger la infraestructura crítica del país. Esto, a su vez, contribuirá a mejorar la resiliencia de la ciberseguridad mediante la implementación de medidas adecuadas.

La International Telecommunications Union (2012), expone que la formulación e implementación de un marco y una estrategia nacionales para la ciberseguridad requieren un enfoque integral. Las estrategias de ciberseguridad, como el desarrollo de sistemas técnicos de protección o la educación de los usuarios para evitar que se conviertan en víctimas de delitos cibernéticos, pueden contribuir significativamente a reducir el riesgo de cibercrimen. El desarrollo y apoyo de estas estrategias de ciberseguridad son elementos vitales en la lucha contra el cibercrimen.

Diversos autores dan su opinión sobre la implementación de estrategias nacionales de ciberseguridad, como Arreola (2018) quien dice que implementar un sistema de ciberseguridad nacional eficiente trae consigo desafíos técnicos, educativos, culturales, políticos, legislativos y humanos que deben ser atendidos con presteza. Propone también que la solución a los desafíos de la ciberseguridad no es solamente de carácter tecnológico, se trata también de la concientización, educación y capacitación. Por lo que los problemas de la ciberseguridad dependen de tres elementos principales: la tecnología, los procesos y las personas, debido a que el individuo es quién cierra el círculo de las fortalezas y vulnerabilidades; el usuario se considera no sólo la primera línea de defensa, sino también el mayor riesgo a la ciberseguridad.

Andreasson (2011) menciona que la ciberseguridad es uno de los mayores retos a los que se han enfrentado nunca los gobiernos, en parte porque nunca ha habido un reto igual. El gobierno se ha organizado en torno a la geografía física durante siglos, pero la amenaza cibernética no tiene fronteras y desafía a los sectores de seguridad nacional e interior del gobierno para lograr una arquitectura de cooperación sin fisuras. Hasta ahora, tanto el sector público como el privado se han limitado a afrontar los retos a medida que iban surgiendo.

Aunque algunos de ellos han sido embarazosos, se han solucionado, normalmente en un plazo de tiempo aceptable. En otras palabras, hasta ahora el sistema de ciberseguridad ha sido en gran medida capaz de hacer frente a la amenaza.

Según Borghello & Temperini (2013), desde el punto de vista legal, se ha observado que más allá de la necesidad lógica de dotar a los sistemas informáticos con medidas de seguridad, existen obligaciones legales vigentes de adoptar una Política de Seguridad adecuada a la institución que se trate, incluso estableciéndose la obligación de definir una persona encargada de la Seguridad de la Información de dicho organismo. Igualmente, Galán & Galán (2016) afirman que la ciberseguridad ya no es una opción y que gracias a la dependencia de las sociedades occidentales de sus sistemas de información (públicos y privados) es de tal magnitud que no puede abordarse ningún proyecto de interés nacional que no contemple la seguridad de los sistemas de información, la información tratada y los servicios prestados, como requisitos tan importantes como la propia prestación de aquellos servicios.

Coppolino, et al. (2018) sostienen que las amenazas cibernéticas representan un riesgo en constante aumento y se han convertido en el desafío más significativo que enfrentan las organizaciones del sector público. Los informes indican que aproximadamente el 40% de los ataques de *malware* y, en general, de las ciber amenazas dirigidas a entidades gubernamentales se concentran en estas organizaciones, superando incluso a sectores tradicionalmente considerados como objetivos principales, como el financiero.

Es crucial que las administraciones públicas locales reconozcan los riesgos cibernéticos a los que están expuestas y tomen las medidas necesarias para resguardar sus infraestructuras contra posibles interrupciones cibernéticas. Además, deben garantizar la protección de la información de ciudadanos y empresas que gestionan. Preis & Susskind (2022) mencionan al respecto que la adopción de habilidades y herramientas varía en función del tamaño de las entidades gubernamentales involucradas, a pesar de que los ataques de *ransomware* de los últimos años dejan en claro que ningún gobierno local está exento. Aunque las investigaciones resaltan que la falta de financiamiento y la formación inadecuada son desafíos fundamentales, aún hay aspectos que no se conocen completamente. Desde la perspectiva práctica, se observa que algunos gobiernos estatales buscan respaldar a las entidades gubernamentales locales en sus

jurisdicciones, brindándoles información, recursos financieros y logísticos, y procurando equiparlas con herramientas para proteger al público. No obstante, estas acciones carecen de un estudio sistemático que evalúe su eficacia y razón de ser.

La implementación de medidas de ciberseguridad suficientes y oportunas por parte de los servicios públicos se considera una exigencia esencial para que la administración del estado funcione bien. En situaciones en las que los órganos administrativos encargados de los bancos de datos personales incumplen de alguna manera este estándar de ciberseguridad y, como consecuencia, la entidad sufre un ciberataque que afecta directamente al derecho a la autodeterminación informativa y la protección de datos personales, los usuarios del servicio, quienes son titulares de dichos datos, pueden responsabilizar al Estado por la falta de servicio del órgano correspondiente. En este contexto, se argumenta que ha ocurrido un funcionamiento deficiente o por debajo de los estándares del servicio, lo que habilita la imputación de responsabilidad bajo el concepto de falta de servicio (Jara Fuentealba & Jorquera Cruz, 2021).

Particularmente para Kryshtanovych, et al. (2021), la seguridad cibernética del sistema de administración pública, en el marco del desarrollo de las tecnologías financieras, constituye el fundamento de la seguridad nacional. Contribuye a la protección del Estado, la sociedad, el sistema de administración pública y la población del país en el ciberespacio mediante la implementación de mecanismos de tecnologías financieras diseñados para asegurar la ciberseguridad en la gestión pública.

También existe la posibilidad de una asociación público-privada entre el gobierno y el sector privado, para una mejor operación en el ciberespacio; sin embargo, para tener éxito, según Manley (2015), es fundamental contar con cuatro elementos esenciales: confianza mutua, una orientación clara respaldada por contratos u otros instrumentos legales, un enfoque ascendente en la estructura operativa, y la participación activa de la comunidad tanto dentro como alrededor de las entidades públicas y privadas involucradas.

Ante todo, Dupont (2019) resalta que a pesar de las considerables inversiones que gobiernos y organizaciones están realizando para mejorar la ciberseguridad, resulta preocupante la falta de esfuerzos más rigurosos desde el punto de vista científico para determinar qué

políticas y programas están contribuyendo de manera cuantificable a la seguridad de nuestro ecosistema digital. La Internet, sin fronteras y con múltiples capas, se ha consolidado como uno de los instrumentos más poderosos para el progreso mundial, operando sin supervisión ni regulación gubernamental. Aunque el sector privado continúa desempeñando un papel central en la construcción y gestión diaria de Internet, la creciente urgencia de establecer requisitos de transparencia, responsabilidad y seguridad es innegable (European Commission, 2013).

La implementación efectiva de la ciberseguridad es vital para que el Estado preserve su autoridad exclusiva, y una política digital segura por defecto refuerza aún más esta posición. (...) La soberanía en el ciberespacio es un tema complejo y controvertido, y la proyección de la soberanía se evidencia, al menos en parte, a través de las actividades estatales relacionadas con la ciberseguridad (Coles-Kemp et al., 2018). La principal de estas actividades busca mejorar el comportamiento de las personas en el ámbito de la ciberseguridad y desarrolla la actualización de las campañas de concientización para que se enfoquen en comportamientos y audiencias específicas (van Steen et al., 2020).

La disposición del público a aceptar políticas y regulaciones gubernamentales que restringen las libertades civiles personales y la privacidad es parte de un delicado equilibrio entre seguridad y privacidad. En cierta medida, se considera que la privacidad es un costo aceptable para mejorar la seguridad personal y social frente a nuevas amenazas. No obstante, la sociedad ha adquirido una sensibilidad creciente respecto a la importancia de la privacidad en línea y está plenamente consciente de los dilemas éticos, políticos, legales y de derechos relacionados con la vigilancia gubernamental de la actividad y las comunicaciones en línea. Doneda & Almeida (2015) argumentan que la noción de privacidad tiende a ser influenciada por factores específicos como la nacionalidad, la cultura y el contexto histórico, y los derechos asociados a la privacidad suelen abarcar estos aspectos culturales e históricos particulares. Por otro lado, la protección de datos adopta un enfoque más práctico, argumentando que se centra en salvaguardar a las personas al proteger algo que está externo a ellas: sus datos personales. Además, las normativas para regular los datos pueden ser más concretas y estar sujetas a una armonización global en comparación con los derechos de privacidad. Una conclusión fundamental es que la implementación de regulaciones de ciberseguridad debe tener en cuenta

la percepción pública de las ciber amenazas y la exposición de la población a los ciberataques (Snider, et al. 2021).

Las organizaciones, tanto públicas como privadas, pueden desarrollar políticas de ciberseguridad y establecer procedimientos para su cumplimiento, ofreciendo capacitación a sus empleados sobre las mejores prácticas en ciberseguridad y responsabilizando a los usuarios finales por cualquier acción que ponga en peligro la ciberseguridad (Norris et al., 2018).

Es importante destacar que, si bien la tecnología puede ser costosa, la adopción e implementación de políticas, así como la capacitación y la responsabilización de los usuarios finales, resultan considerablemente menos onerosas. Aunque la capacitación y la responsabilización de los usuarios finales no son gratuitas, su costo es significativamente inferior al de la tecnología (Norris et al., 2018).

La ciberseguridad es fundamental en la implementación de la gobernanza electrónica, ya que si los usuarios de los servicios electrónicos no tienen la certeza de que se asegura la ciberseguridad, la idea de establecerla estará destinada al fracaso desde el principio (Napetvaridze & Chochia, 2019).

A nivel internacional existen estudios sobre la ciberseguridad en determinados países como el de Karpiuk (2021), cuyos hallazgos en su estudio sobre la ciberseguridad en los gobiernos locales de Polonia señalan que mejorar el nivel de ciberseguridad en los municipios polacos demanda no solo una mayor asignación de recursos financieros, sino también la contratación de empleados más capacitados, la adquisición de mejores equipos y software. También es imprescindible aumentar la concienciación sobre los riesgos potenciales entre los funcionarios, desarrollar normas y procedimientos claros de ciberseguridad, y asegurar la aplicación rigurosa de la legislación en esta área.

Maréchal (2017), en su estudio sobre las políticas de internet en Rusia, encontró que este país no aborda la gobernanza de Internet, la ciberseguridad y la política de medios de comunicación como dominios separados. En cambio, desde la perspectiva de la política exterior rusa, todas las áreas abarcadas por estas disciplinas se integran en el concepto de "seguridad de

la información". La vigilancia nacional, la censura de contenidos y la reforma antiliberal de la gobernanza de Internet están vinculadas con las campañas de desinformación en el extranjero y se utilizan estratégicamente para objetivos geopolíticos.

Siguiendo esta misma línea, Akimenko & Giles (2020) concluyeron que, aunque los homólogos rusos pueden estar preparados para enfrentar desafíos cibernéticos "puros", las capacidades e intenciones adoptadas por Rusia indican la necesidad de estar preparados también para una guerra de la información. En este escenario, los desafíos cibernéticos se entrelazan de manera fluida con la desinformación, la subversión y los efectos de la guerra cinética y electrónica, con objetivos ambiciosos que pueden incluir incluso cambios de régimen. El problema de la propaganda y la desinformación, como parte de una campaña de información rusa más amplia, es al menos tan relevante como la noción tradicional (aunque a menudo equivocada) de un "ciber Pearl Harbor", que implica ciberataques paralizantes contra infraestructuras nacionales críticas.

La Unión Europea (UE) lanzó en 2020 su estrategia de ciberseguridad, sin embargo, Munkøe & Mölder (2022) manifiestan que a pesar de que la UE se percibe como una importante entidad reguladora, sigue siendo un actor relativamente pequeño en lo que respecta a las políticas de seguridad, ya que muchos de sus estados miembros prefieren manejar estos asuntos de manera individual o dentro del marco de la OTAN. La ciberseguridad implica una amplia gama de actividades, desde la cooperación judicial y operativa para hacer cumplir la ley hasta la defensa militar contra otros estados o grupos respaldados por estados. Para la UE, encontrar una distribución adecuada de responsabilidades y un método de operación que garantice la colaboración efectiva entre los numerosos actores de diferentes niveles resulta difícil, pero es esencial para asegurar una respuesta adecuada en Europa frente a las crecientes amenazas cibernéticas.

A nivel latinoamericano, Chile tiene una Política Nacional de Ciberseguridad; establece que el desafío radica en establecer una política que guíe la actuación del país en ciberseguridad, al mismo tiempo que se implementan y ejecutan las medidas necesarias para salvaguardar la seguridad de los usuarios en el ciberespacio. Esto implica considerar estrategias educativas centradas en el autocuidado y la prevención en el entorno digital, alineándose con el programa

de Gobierno de la presidenta Michelle Bachelet, que aboga por "desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos" (Ciberseguridad, C. I. S., 2017, p. 11).

En Perú, Anderson (2014) menciona que la falta de una legislación armonizada en el ámbito de la ciberseguridad, junto con el diseño inicial de internet como un canal accesible, sencillo y útil sin tener en cuenta su dimensión de seguridad, son factores que aumentan las posibilidades de que las amenazas cibernéticas se materialicen en el Perú.

Otras propuestas sobre la implementación de una política de ciberseguridad son:

España: Fojón & Sanz (2010, pp. 7-8) aplican los siguientes principios para una gestión española de ciberseguridad:

1. El gobierno de España debe identificar la seguridad de su ciberespacio como un objetivo estratégico de la Seguridad Nacional, puesto que la materialización de una amenaza sobre el ciberespacio puede afectar muy negativamente al desarrollo social, económico y cultural de nuestro país.
2. Se debe elaborar una Estrategia Nacional de Ciberseguridad de la que emane un marco normativo específico que regule el ciberespacio y su seguridad.
3. La dirección de la ciberseguridad debe realizarse de manera centralizada, es decir, el Estado debe crear un organismo con la misión de dirigir la ciberseguridad nacional, coordinando a las entidades públicas y privadas implicadas.
4. El gobierno debe fomentar y reforzar la cooperación internacional en materia de ciberseguridad. Las alianzas multinacionales y bilaterales en materia de ciberseguridad son indispensables. En el caso español, tenemos una oportunidad de liderazgo responsable con países iberoamericanos y se deberán alcanzar acuerdos con aquellos países que, aunque no se encuentren dentro de nuestro entorno geopolítico más próximo, son relevantes para controlar las amenazas sobre nuestro ciberespacio.
5. Las administraciones del Estado se deberán promover una cultura de la ciber responsabilidad, basada en la concienciación y formación continua en

ciberseguridad. Para ello, los planes de estudio de las enseñanzas primaria, secundaria y universitaria deberían incluir en sus currículos materias relacionadas con el uso responsable del ciberespacio.

6. El Estado debe promover e invertir en la investigación, el desarrollo y la innovación (I+D+i) del sector de la ciberseguridad, que proporcione soluciones TIC de primer nivel y empleo cualificado.

Los autores aseguran que el gobierno debe asumir el liderazgo y la dirección en materia de ciberseguridad nacional para concientizar a la ciudadanía sobre la protección del ciberespacio y lo importante que es para el funcionamiento de la sociedad.

China: En este país la protección de la ciberseguridad adopta un enfoque estatal dominante, para mantener la estabilidad social y política. Es por eso por lo que realizan esfuerzos para promover la cooperación en materia de ciberseguridad, por lo que no solo desempeña un papel positivo en el tema, sino que también propone crear diversas plataformas de comunicación para cuestiones cibernéticas. Cai (2015) afirma que la cooperación en materia de ciberseguridad es una tendencia internacional, y que para la seguridad común del ciberespacio mundial los países deben tener confianza mutua a través medios como:

- El respeto a la soberanía de Internet de los demás.
- Alcanzar un código de conducta unificado para el ciberespacio.
- Identificar las amenazas comunes a la ciberseguridad.
- Estableciendo un mecanismo de intercambio de información sobre amenazas a la red.
- Poner en marcha líneas directas y concluir acuerdos bilaterales o multilaterales

América Latina: Izaguirre & León (2018) concluyeron que la mayoría de los países en América Latina no existe una codificación general y sistemática sobre ciberseguridad. Sin embargo, los gobiernos hacen un esfuerzo no solo en mejorar infraestructura y centros de protección a través de universidades, empresas y leyes, sino también en capacitar a la población para concientizar sobre la problemática

Actualmente casi todos los países cuentan con una política de ciberseguridad nacional, y no solo una política sino una entidad encargada de tal política. Como el caso de Estado Unidos con su Estrategia Nacional de Ciberseguridad, cuyos objetivos a largo plazo son "sobre cómo las personas, el gobierno y las empresas pueden operar de manera segura en el mundo digital" (Widakuswara, 2023), además de contar con la Agencia de Seguridad Nacional (NSA) y el Departamento de Seguridad Nacional (DHS).

El Centro Nacional de Seguridad Cibernética (NCSC) de Reino Unido siendo la entidad de mayor autoridad en ciberseguridad, que vela por la Estrategia de Nacional de Ciberseguridad para "compartir conocimientos, abordando vulnerabilidades sistémicas y liderar cuestiones clave de ciberseguridad nacional" (Her Majesty's Government, 2016, p. 10). Además, actualmente cuentan con la "Ciber estrategia nacional 2022" que pretende formar una ciudadanía más informada y participativa en el ciberespacio y ciberseguridad con miras hacia el futuro (Her Majesty's Government, 2022).

China, ya mencionada antes, cuenta con la *Cyberspace Administration of China* (traducción oficial al inglés), entidad superior encargada de regular y censurar el internet en China, implementando nomas, autorizando licencias e incluso tiene la autoridad de impartir justicia en el ámbito del cibernético. Como se sabe, esta es la entidad que acarrea gran controversia por la políticas y castigos que imparte, ya que es bastante estricta con la seguridad de la información y la libertad de expresión en el país.

En Rusia existen diversas normas y leyes sobre ciberseguridad como la Ley Federal N ° 187-FZ sobre la seguridad de la infraestructura de información crítica de la Federación de Rusia, la Ley Federal N.º 152-FZ sobre datos personales, la Ley Federal No. 149-FZ sobre Información, Tecnologías de la Información y Protección de la Información (la Ley de Información), entre otras (Ciberseguridad, 2023). Y las entidades gubernamentales que regulan este aspecto también son muchas, como el Servicio Federal de Control Técnico y de Exportaciones (FSTEC), que vela por la seguridad de la información rusa, el Servicio Federal de Seguridad (FSB) y el Ministerio de defensa.

Todas estas políticas, leyes y entidades tienen un impacto en la población, positivo o negativo, como ejemplo está Rusia y China, cuyas políticas son tan seguras y estrictas que ni su propia población puede acceder a estas políticas o tener la libertad de usarla. También están Reino Unido y Estados Unidos protegen la seguridad de su información gubernamental y la de su población, pero están más preocupados por los ataques externos que puedan recibir y a su vez esa preocupación se la transmiten a su población generando temor y desconfianza.

Asegurar la seguridad del territorio nacional y preservar la ley y el orden son funciones fundamentales del Estado. Proteger el territorio nacional de ciberataques malintencionados es una de estas responsabilidades. Por lo tanto, resulta obligatorio que el Estado cuente con los medios apropiados para llevar a cabo esta misión (Jun, S., 2016). A nivel global, cada país aborda la ciberseguridad de manera única, influenciado por su entorno económico, político y cultural predominante. Para algunos, la ciberseguridad se percibe como un tema relacionado con la seguridad nacional y la defensa. Otros países consideran que tiene un impacto más significativo en el desarrollo económico o en la competitividad internacional. También hay quienes la ven como un elemento crucial para la educación, la interacción social y el bienestar de los ciudadanos. De manera sabia, muchos países están intentando integrar todas estas consideraciones en sus Estrategias Nacionales de Ciberseguridad (Leiva, 2015).

Es crucial comprender que políticas informadas y tecnológicamente avanzadas pueden permitir defensas más sólidas contra las amenazas digitales actuales y futuras. Los responsables políticos, deben reconocer que la ciberseguridad tiene mayor éxito cuando adopta un enfoque proactivo en lugar de reactivo, y cuando tiene en cuenta los rápidos cambios tecnológicos (Charlet & King, 2020).

CAPÍTULO VI

DISCUSIÓN

La discusión se estructurará según los objetivos específicos de la investigación para así responder al objetivo general que es analizar las experiencias documentadas sobre la ciberseguridad en los gobiernos a nivel internacional, 2010-2023.

Las categorías y subcategorías de análisis sirvieron de guía para la realización de este objetivo. Primero, los autores conceptualizan la ciberseguridad, dando una mirada al pasado para analizar su historia y origen, pero hablando más sobre su significado en la actualidad.

El término está ligado a los conflictos que existen o pueden existir entre países que dependan cada vez más de las tecnologías de la información para gestionar aspectos de su nación. Aquí los autores tienen en cuenta la llamada guerra de la información y las repercusiones de esta para la estabilidad democrática de cada país.

Por otra parte, se hace hincapié en los ciber delitos o más específicamente en el ciberterrorismo ya que este no puede ser tratado como un delito convencional, puesto que, si bien no afecta físicamente a los ciudadanos, sí puede llegar a generar pánico entre ellos, incrementando la inseguridad y desconfianza hacia los gobernantes de su país, una posible consecuencia de esto son manifestaciones y sublevaciones.

Otros autores han mostrado su preocupación por la ciberseguridad de ciertos países, por lo que proponen medidas para su implementación o mejora. Entre las recomendaciones que proponen están fomentar la especialización en el área y las destrezas informáticas de los jóvenes, y concienciar a la población sobre la ciberseguridad, su implicancia en la estabilidad del país y los riesgos de internet, y muchos recomiendan tener una legislación actualizada para que llegue a todas las instituciones del país y trabajar juntamente con el sector privado.

- **O.E.1. Determinar las características que señala la literatura existente sobre ciberseguridad gubernamental.**

Basándose en la Figura 3 se observa que el tipo documental más usado para la difusión de conocimiento en temas de ciberseguridad gubernamental son los artículos, seguido por mucha diferencia de las conferencias. Que sea un tema tratado en muchas conferencias implica que preocupa a la comunidad científica y política de todo el mundo.

El idioma que predomina en la literatura científica, como se puede ver en la Figura 5, es el inglés, nada sorpresivo ya que es la lengua preferida para la difusión del conocimiento científico, seguido del español y finalmente un documento en ruso. Sin embargo, hay muchos documentos en muchos otros idiomas, que no se consideraron para este estudio por su poca relevancia con el tema tratado en esta investigación.

Lo anterior se refleja más en la Figura 6, ya que representa el país de origen de estos documentos, teniendo a Estados Unidos como el principal exportador de la literatura científica de este tema, seguido por Reino Unido una gran variedad de países tanto de Asia, Europa y América Latina. Este hecho denota, como se dijo líneas atrás, que el tema de ciberseguridad les concierne a todos, es algo independiente de las culturas o costumbres de los países, ya que, si el internet no tiene límites ni fronteras, la seguridad tampoco.

- **O.E.2. Analizar los conceptos sobre ciberseguridad y seguridad de la información.**

Según la ITU (International Telecomunication Union) la ciberseguridad abarca un conjunto de herramientas, políticas y tecnologías destinadas a proteger el entrono cibernético y los activos de los usuarios; sin embargo, esta definición cambia según las amenazas en el ciberespacio y a quienes afecta. Autores como Bresniker et al., Vila y Jara & Joquera proponen otros enfoques para la ciberseguridad como la creación de herramientas para evaluar actividades en redes, la protección de las infraestructuras a través de medidas preventivas de detección y respuesta, y medidas para proteger la información y la infraestructura en el ciberespacio.

Las nuevas tecnologías como el internet de las cosas aumentan las formas de vulnerar las infraestructuras virtuales de las personas o de instituciones, por lo que el uso del aprendizaje automático es esencial para reducir la efectividad de los ciberataques. Esto va de la mano con

lo que mencionan De Brujim & Janssen, que la ciberseguridad debería centrarse más en la prevención que en la subsanación de los ataques cibernéticos.

Es evidente que al no haber una única definición de ciberseguridad o que esta varíe dependiendo de la situación, lleva a tener desigualdades en la protección de datos entre estados, lo que afecta directamente en la guerra de la información y la creación de políticas de ciberseguridad.

- **O.E.3. Conocer las implicancias de la guerra de la información y la ciberdelincuencia.**

Actualmente, y debido a los últimos sucesos que han ocurrido entre los países con un poder político elevado, el tema de ciberseguridad gubernamental tiende a inclinarse hacia los conflictos que existen entre estos países, hablando más específicamente de Rusia, Ucrania, Estados Unidos y ocasionalmente China, tratando el tema de la ciberguerra como un nuevo tipo de guerra; sin embargo, los motivos y las consecuencias de esta no son tan diferentes a las de una guerra convencional, muy aparte de la pérdida de vidas humanas, ya que al final se busca desestabilizar una nación e imponer la superioridad de otra.

Por otra parte, en los países en donde no hay muchos conflictos políticos externos, toman la ciberseguridad como una forma de concientizar a su propia población sobre los riesgos de internet y como protegerse ante una posible estafa o ataque cibernético. Se ha de evidenciar que debido a la poca motivación que tienen los estados para crear o mejor sus políticas de ciberseguridad, estos cuentan con un sistema algo débil y propenso a ataques.

En menor medida hay estudios que hablan sobre ataques particulares a sistemas tanto públicos como privados, señalando los errores y recomendando una mejora en sus sistemas de ciberseguridad. Sin embargo, casi toda la literatura estudiada para esta investigación concluye que siempre hay que realizar mejoras y actualizaciones en las políticas y sistemas de ciberseguridad.

- **O.E. 4. Identificar los componentes que como mínimo debe tener una política nacional de ciberseguridad o seguridad de la información**

Una política de seguridad de la información o ciberseguridad debe basarse en tres cuestiones: la seguridad del estado, la seguridad de los ciudadanos y el derecho a la privacidad, si bien los autores mencionan que es complicado manejar estos temas a la vez, ya que muchas veces son los mismo ciudadanos los que lanzan ciberataques al estado y este para protegerse debe vulnerar el derecho a la privacidad de las personas, la creación de una política de ciberseguridad bien escrita e implementada hará que se fortalezca la confianza entre el estado y sus ciudadanos.

1. En primer lugar, los objetivos y alcances de la política deben ser claros y precisos, así como definir cuáles son las responsabilidades, derechos y obligaciones de todos los involucrados, por lo que debe haber una entidad que vele por su cumplimiento.
2. Definir lo que es la ciberseguridad, sus beneficios tanto para el estado como para los ciudadanos, haciendo hincapié en la seguridad de la información personal.
3. Establecer un plan de gestión de riesgos cibernéticos, aquí se deben localizar, evaluar y monitorear las infraestructuras críticas, como son las redes de energía, salud, transporte, economía, etc. Y los sistemas de información, que son las plataformas digitales, bases de datos, etc.
4. Fomentar la colaboración entre el sector público, sector privado y la ciudadanía para implementar medidas de ciberseguridad.
5. Concientizar y capacitar a la población sobre los riesgos de internet, la ciberseguridad y la protección de sus datos personales.
6. Fomentar la cooperación internacional en temas de ciberseguridad, como acuerdos y tratados cuyo fin sea la lucha contra los ciberdelitos.
7. Promover la investigación científica y proyectos en ciberseguridad para recopilar información y crear conocimiento que se pueda utilizar para mejorar la política de ciberseguridad.
8. Por último, debe haber una evaluación y actualización constante de la políticas y normas de ciberseguridad.

En Perú existen proyectos de ley sobre Ciberseguridad (Del Castillo, 2019) que tiene por objetivo establecer el marco normativo en materia de seguridad digital del estado peruano,

también se propone la creación de una Plan de Acción Nacional en Ciberseguridad y un Comité Nacional de Ciberseguridad. Un año después se presentó el proyecto de ley que garantiza la ejecución de operaciones de ciberseguridad y seguridad digital a través de un centro nacional de ciberseguridad (Podemos Perú, 2020), que busca establecer medidas "que garanticen la seguridad, en el ciberespacio frente a las amenazas o los ataques que afecten la Seguridad Nacional, para la ejecución de operaciones de Ciberseguridad y Seguridad Digital, a través del Centro Nacional de Ciberseguridad del Perú-CENAC", con el paso del tiempo esto devino en la creación del Centro Nacional de Seguridad Digital (CNSD) que "gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital en el país, a fin de fortalecer la confianza digital." (Plataforma digital única del Estado Peruano, 2023), y la Estrategia Nacional de Seguridad y Confianza Digital, que como el nombre lo dice busca crear confianza en el entorno digital, a través de la protección de datos personales, la transparencia, la economía digital, la seguridad digital y la protección del consumidor en el entorno digital, de esta forma aumenta el desarrollo nacional y la reducción de las brechas sociales (Centro Nacional de Seguridad Digital, 2021).

CONCLUSIONES

1. La literatura científica sobre ciberseguridad gubernamental se caracteriza por una amplia difusión a través de artículos y conferencias, lo que refleja la preocupación global por este tema. La comunidad científica y política de todo el mundo participa activamente en la generación y difusión de conocimiento sobre ciberseguridad gubernamental, independientemente de las culturas o costumbres de los países. Esto se evidencia en la diversidad de idiomas y países de origen de los documentos analizados, con Estados Unidos y Reino Unido como líderes en la producción de literatura científica sobre este tema. La ciberseguridad gubernamental es un tema universal que trasciende las fronteras y requiere una colaboración global para abordar los desafíos y amenazas en este ámbito.
2. La ciberseguridad es un concepto dinámico y multifacético que abarca diversas herramientas, políticas y tecnologías para proteger el entorno cibernético y los activos de los usuarios. Sin embargo, la falta de una definición única y universal de ciberseguridad genera desigualdades en la protección de datos entre estados, lo que tiene implicaciones directas en la guerra de la información y la creación de políticas de ciberseguridad efectivas. Es fundamental adoptar un enfoque proactivo y preventivo, que incluya el uso de tecnologías como el aprendizaje automático, para reducir la efectividad de los ciberataques y proteger la infraestructura y la información en el ciberespacio.
3. La ciberseguridad gubernamental se ha convertido en un tema prioritario en la actualidad, especialmente en países con alto poder político, donde se utiliza como herramienta para desestabilizar e imponer superioridad sobre otros. Sin embargo, en países con menor conflicto político externo, la ciberseguridad se enfoca en concientizar a la población sobre los riesgos de internet y protegerse contra ataques cibernéticos. A pesar de la importancia del tema, muchos estados carecen de políticas y sistemas de ciberseguridad sólidos, lo que los hace vulnerables a ataques. La literatura sugiere que es fundamental realizar mejoras y actualizaciones constantes en las políticas y sistemas de ciberseguridad para proteger la seguridad nacional y la integridad de la información.
4. La creación de una política de ciberseguridad efectiva requiere considerar la seguridad del estado, la seguridad de los ciudadanos y el derecho a la privacidad. Para lograr esto,

es fundamental establecer objetivos claros, definir responsabilidades y derechos, y crear un plan de gestión de riesgos cibernéticos. La colaboración entre el sector público, privado y la ciudadanía es crucial para implementar medidas de ciberseguridad y concientizar sobre los riesgos de internet. En el caso de Perú, se han presentado proyectos de ley y se han creado instituciones como el Centro Nacional de Seguridad Digital y la Estrategia Nacional de Seguridad y Confianza Digital, que buscan fortalecer la confianza digital y proteger la seguridad nacional. Sin embargo, es importante destacar que la ciberseguridad es un tema en constante evolución, por lo que es fundamental realizar evaluaciones y actualizaciones constantes de las políticas y normas de ciberseguridad.

RECOMENDACIONES

1. Inversión en ciberseguridad:

   Es importante que los países que quieran implementar tecnologías de la información y comunicación en los gobiernos tengan muy en cuenta la seguridad de sus sistemas y muestren las ventajas de invertir en un buen sistema de ciberseguridad, como la protección de datos sensibles, prevención de ataques y la mejora de la confianza pública.

2. Actualización de las políticas de ciberseguridad:

   La tecnología cambia y evoluciona constantemente, por lo tanto, las políticas de ciberseguridad también deben cambiar y evolucionar con ellas. Los nuevos descubrimientos en cuanto las TICs, traen consigo nuevas formas de vulnerabilidad y es crucial para que las políticas estén actualizadas; esto se puede lograr creando un equipo de expertos en ciberseguridad que supervisen regularmente a las entidades públicas y participen en foros internacionales de ciberseguridad. A su vez se recomienda la capacitación y concientización de los empleados del sector público sobre las últimas amenazas y tecnologías de ciberseguridad.

3. Implementación de macro políticas de ciberseguridad:

   Se recomienda implementar macro políticas en ciberseguridad que abarquen todos los sectores del estado e instituciones ligadas a este, y dar a conocer a los ciudadanos los cambios que se implementan y establezcan cómo pueden contribuir a la seguridad del país. Se recomienda también la coordinación interinstitucional para garantizar la implementación de estas políticas o en el mejor de los casos, la creación de un comité interinstitucional de ciberseguridad.

4. Colaboración con instituciones privadas:

   Trabajar en conjunto con las instituciones privadas es de mucho valor, tanto para la implementación de políticas de ciberseguridad como para la concientización de la población. Se podrían crear modelos de colaboración como la participación en proyectos de investigación y desarrollo, así como realizar ejercicios de simulación de ataques cibernéticos; de esta forma se intercambia conocimiento, experiencias, se reducen costos y mejora la seguridad.

5. Implantación de un gobierno de ciberseguridad:

   La implantación de un gobierno digital por el estado peruano conlleva mucho tiempo, pero es crucial que primero se disminuya la brecha digital que todavía existe en el país y que todos los ciudadanos tengan acceso a las TIC, acompañado de una alfabetización digital acerca de los beneficios y riesgos. Para esto se recomienda establecer indicadores de éxito que midan el progreso de la implantación del gobierno digital, como la mejora de eficiencia y la transparencia, la reducción de costos y la mejora de la satisfacción ciudadana.

REFERENCIAS BIBLIOGRÁFICAS

Acurio Del Pino, S. (2016). *Delitos informáticos: generalidades*. http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Aftergood, S. (2017). Cybersecurity: The cold war online. *Nature, 547*(7661), 30-31. https://doi.org/10.1038/547030a

Akimenko, V. y Giles, K. (2020). Russia's cyber and information warfare. *Asia Policy, 15*(2), 67-75. https://doi.org/10.1353/asp.2020.0014

Anderson, O. (2014). Ciberseguridad Nacional. https://repositorio.esup.edu.pe/bitstream/20.500.12927/252/1/Anderson.pdf

Albarracín, A. (2019). *Inteligencia nacional y estrategia de ciberseguridad nacional* [Tesis Doctoral, Universidad Nacional de La Plata]. Repositorio Institucional de la UNLP. https://doi.org/10.35537/10915/87062

Alvines, M. (2020). *Modelo de ciberseguridad para el sector de salud pública: 2018 -2020: una revisión de la literatura científica* [Trabajo de investigación, Universidad Privada del Norte]. Repositorio de la Universidad Privada del Norte**.** https://hdl.handle.net/11537/26050

Andreasson, K. (2011). Cybersecurity: Public sector threats and responses. CRC Press.

Argumosa, J. (2022). Impacto del ciberespacio en las guerras del siglo XXI. *Ejército,* (972), 68-71. https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/e/revista_ejercito_972.pdf

Arreola, A. (2018). Ciberseguridad Nacional en México y sus desafíos. *Instituto de investigaciones estratégicas de la armada de México*, 17. https://cesnav.uninav.edu.mx/cesnav/ININVESTAM/docs/docs_analisis/da_48-18.pdf

Asbaş, C. y Erdem Tuzlukaya, Ş. (2023). Cyberwarfare: War Activities in Cyberspace. En Advances in Digital Crime, Forensics, and Cyber Terrorism (pp. 128-145). IGI Global. https://doi.org/10.4018/978-1-6684-6741-1.ch007

Astudillo Muñoz, J. (2020). El derecho a la vida privada de los funcionarios públicos frente al derecho de acceso a la información pública. Un estudio a la luz de la jurisprudencia del Consejo para la Transparencia en Chile. *Derecho global. Estudios sobre derecho y justicia, 5*(15), 89-112. https://doi.org/10.32870/dgedj.v5i15.277

Bermúdez, M. (2024). *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones* [Tesis de pregrado, Pontificia Universidad Católica del Perú] Repositorio de tesis PUCP. http://hdl.handle.net/20.500.12404/27284

Blank, S. (2010). Can information warfare be deterred? Defense Analysis, 17(2), 121-138. https://doi.org/10.1080/07430170120064212

Borghello, C. y Temperini, M. G. I. (2013). *Ciberseguridad nacional argentina: cracking de servidores de la administración pública*. XI Simposio Argentino de Informática y Derecho (SID) - JAIIO 42 (2013).

Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D. y Tran, T. (2019). Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. *Computer, 52*(12), 45-52. https://doi.org/10.1109/mc.2019.2942584

Buchyn, M. y Kurus, Y. (2018). Russian information war against Ukraine: peculiarities and mechanisms of countering. *Humanitarian vision, 4*(1), 55-62. https://doi.org/10.23939/shv2018.01.055

Cai, C. (2015). Cybersecurity in the Chinese context: Changing concepts, vital interests, and prospects for cooperation. *China Quarterly of International Strategic Studies, 1*(3), 471–496. https://doi.org/10.1142/s2377740015500189

Cárdenas-Solano, L.-J., Martínez-Ardila, H. y Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: revisión bibliográfica. *Profesional de la información, 25*(6). https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/epi.2016.nov.10/32176

Caro Cabrera, M. J., Pozo Cuevas, F., López Menchón, A., y Navarro Ardoy, L. (2020). *Encuestas de seguridad ciudadana* (Cuadernos Metodológicos, 61). Centro de Investigaciones Sociológicas. https://books.google.com.pe/books?hl=es&lr=&id=GVkVEAAAQBAJ&oi=fnd&pg=PA3&dq=seguridad+ciudadana&ots=IIYT9Mb5xe&sig=Kvjs4po8J2kkWHMsA_3U05qiNdQ&redir_esc=y#v=onepage&q=seguridad%20ciudadana&f=false

Castillo, A., Bruzza, M., y Tupia, M. (2021). Estado del arte sobre la identificación amenazas no intencionales de ciberseguridad de parte de personal interno en instituciones públicas. *Revista Ibérica de Sistemas e Tecnologias de Informação, E*41, 70-82. https://www.proquest.com/openview/4fc3316c510c3b225e5378667120e7e6/1?pq-origsite=gscholar&cbl=1006393

Centro Nacional de Planeamiento Estratégico – CEPLAN. (2018). *Reglamento que regula las Políticas Nacionales* (D.S. N.º 029-2018-PCM, modificado por D.S. N.º 038-2018-PCM). CEPLAN. https://www.ceplan.gob.pe/wp-content/uploads/2018/05/Reglamento-Politicas-Nacionales.pdf

Centro Nacional De Seguridad Digital [CNSD]. (2021). *Estrategia Nacional De Seguridad Y Confianza Digital*. https://bit.ly/48BWP9m

Charlet, K. y King, H. (2020). The future of cybersecurity policy. *IEEE security & privacy, 18*(1), 8-10. https://doi.org/10.1109/msec.2019.2953368

Chigada, J. y Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management, 23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Chilcon, M. (2019). *El Cibercrimen en el Perú y su incidencia en la Seguridad Nacional* [Tesis de doctorado, Centro de Altos Estudios Nacionales - Escuela de Posgrado]. Registro Nacional de Trabajos de Investigación. http://renati.sunedu.gob.pe/handle/sunedu/393223

Chiza, D. y Izurieta, H. (2020). *Estrategia nacional de ciberseguridad* [Tesis de maestría, Universidad de las Fuerzas Armadas ESPE]. Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE. http://repositorio.espe.edu.ec/handle/21000/23141

Ciberseguridad. (2023, 20 de setiembre). *Rusia*. https://ciberseguridad.com/normativa/rusia/

Ciberseguridad, C. I. S. (2017). *Política Nacional de Ciberseguridad*. Comité Interministerial sobre Ciberseguridad. http://biblioteca.digital.gob.cl/handle/123456789/738

Cisterna, F. (2005). Categorización y triangulación como proceso de validación del conocimiento en investigación cualitativa. *Theoria, 14*(1), 61-71. http://www.ubiobio.cl/theoria/v/v14/a6.pdf

Coles-Kemp, L., Ashenden, D. y O'Hara, K. (2018). Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. *Politics and governance, 6*(2), 41-48. https://doi.org/10.17645/pag.v6i2.1333

Cortés, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho Comunicaciones y Nuevas Tecnologías, 14*, 1-17. https://doi.org/10.15425/redecom.14.2015.06

Coppolino, L., D'Antonio, S., Mazzeo, G., Romano, L. y Sgaglione, L. (2018). *How to protect public administration from cybersecurity threats: The COMPACT project*. 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA).

Dammert, L., Mujica, J., y Zevallos, N. (2017). *Seguridad ciudadana. Balance de Investigación en Políticas Públicas 2011-2016 y Agenda de Investigación 2017-2021*. Consorcio de investigación económica y social. https://cies.org.pe/investigacion/seguridad-ciudadana/

Dasgupta D., Akhtar Z. y Sen S. (2022). Machine learning in cybersecurity: a comprehensive survey. *Journal of Defense Modeling and Simulation, 19*(1), 57-106. 10.1177/1548512920951275

De Álvaro, M. (2023). El ciberespacio en tiempos de guerra: la IT Army ucraniana. Instituto Español de Estudios Estratégicos, 24(2023).

https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO24_2023_MARALV_Ciberespacio.pdf

De Bruijn, H. y Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Del Castillo, J. (mayo 17, 2019). Proyecto de ley 4352/2018-CR. Ley de Ciberseguridad. https://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0435220190517.pdf

Dennis A., Jones R., Kildare D. y Barclay C. (2014). Design science approach to developing and evaluating a national cybersecurity framework for Jamaica. *Electronic Journal of Information Systems in Developing Countries, 62*(1), 1–18. https://doi.org/10.1002/j.1681-4835.2014.tb00444.x

Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics, 9*(4), 384-410. https://doi.org/10.1080/15027570.2010.536404

Doneda, D. y Almeida, V. A. F. (2015). Privacy Governance in Cyberspace. *IEEE internet computing, 19*(3), 50-53. https://doi.org/10.1109/mic.2015.66

Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice, 42*(5), 500-515. https://doi.org/10.1080/0735648x.2019.1691855

E Silva, K. (2013). Europe's fragmented approach towards cyber security. *Internet Policy Review, 2*(4). https://doi.org/10.14763/2013.4.202

European commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Figueroa-Suárez, J.; Rodríguez-Andrade, R.; Bone-Obando, C. y Saltos-Gómez, J. (2018). La seguridad informática y la seguridad de la información. *Polo del conocimiento, 2*(12),45-155. http://dx.doi.org/10.23857/pc.v2i12.420

Fojón, J. y Sanz A. (2010). Ciberseguridad en España: una propuesta para su gestión. *Boletín Elcano*, (126), 8. http://biblioteca.ribei.org/id/eprint/1879/

Galán, C. M. y Galán, C. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad, 47*, 293-306. https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/18892/19110

Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College. https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf

Gonzales Rodríguez, F. y Barbarán Mozo, H. (2021). La seguridad ciudadana como política gubernamental en América Latina en el último quinquenio. *Ciencia Latina Revista Científica Multidisciplinar, 5*(1), 422-435. https://doi.org/10.37811/cl_rcm.v5i1.241

Gross M., Canetti D. y Vashdi D. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity, 3*(1), 49-58. https://doi.org/10.1093/cybsec/tyw018

Group-IB. (2025). *High-Tech Crime Trends Report 2025*. Group-IB. https://www.group-ib.com/landing/high-tech-crime-trends-2025/

Guerrero, C. (2018). De Budapest al Perú: análisis sobre el proceso de implementación del convenio de ciberdelincuencia. Impacto en el corto, mediano y largo plazo. https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf

Her Majesty's Government [HMG]. (2016). *National Cyber Security Strategy 2016-2021.* https://bit.ly/3PDw23R

Her Majesty's Government [HMG]. (2022). *National Cyber Strategy* 2022. https://bit.ly/3PX87gS

Hernández, R., Fernández, C. y Baptista, M. (2014). M*etodología de la Investigación*. México D.F: McGraw Hill Education.

International Telecomunication Union [ITU]. (2012). Understanding cybercrime: Phenomena, challenges and legal response. En Telecomunication Development Sector. https://bit.ly/47o6Wxo

Instituto Chihuahuense para la transparencia y acceso a la información pública [ICHITAIP]. (2018). *Datos personales: los límites entre lo público y lo privado*. https://www.ichitaip.org/infoweb/archivos/ensayos/datospersonales.pdf

Instituto Nacional de Estadística e Informática [INEI]. (2018). *Encuesta Nacional de Programas Presupuestales 2011-2017.* https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1855/

Ivanov, S. (2013). Information Warfare: Its Contents and Forms. *Izvestiya of Altai State University*, 276-279. https://www.researchgate.net/publication/274102120_Information_Warfare_Its_Contents_and_Forms

Izaguirre, J. y León, F. (2018). Análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal, 3*(9), 172-181. https://doi.org/10.33890/innova.v3.n9.2018.837

Jara Fuentealba, N. y Jorquera Cruz, A. (2021). La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. *Revista chilena de derecho y tecnología, 10*(1), 201. https://doi.org/10.5354/0719-2584.2021.58776

Jordan, J. (s/f) *La guerra de la información*. Centro de Estudios y Análisis de Seguridad. Universidad de Granada.

Jun, S.-I. (2016). National security or privacy: A second thought on the DNC hack. *AJIL Unbound, 110*, 352-357. https://doi.org/10.1017/aju.2017.4

Karpiuk, M. (2021). The local government's position in the polish cybersecurity system. Lex localis - *Journal of Local Self Government, 19*(3), 609-620. https://doi.org/10.4335/19.3.609-620(2021)

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele University, 33*(2004), 1-26. https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Kryshtanovych, M., Ortynskyi, V., Zakharyash, O., Maziy, N. y Krasivskyy, O. (2021). *The impact of threats on the cybersecurity system of public administration in the context of the development of financial technologies*. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT).

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

Ley 27806. (2002). *Ley de transparencia y acceso a la información pública.* Congreso de la República del Perú. https://cdn.www.gob.pe/uploads/document/file/105104/_27806_-_07-11-2012_12_42_43_-LEY-27806.pdf?v=1586905330

Ley 29733. (2011). *Ley de protección de datos personales*. Congreso de la República del Perú. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Lin, H. (2020). On the organization of the U.S. government for responding to adversarial information warfare and influence operations. En Routledge (Ed.), Information Warfare in the Age of Cyber Conflict (p. 20). Routledge. https://kb.osu.edu/bitstream/handle/1811/91791/ISJLP_V15N1-2_001.pdf;jsessionid=BB5FB2FD833D5FD83C7E2E85EF6C0625?sequence=1

Manley, M. y US Air Force, American Military University. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of strategic security, 8*(3Suppl), 85-98. https://doi.org/10.5038/1944-0472.8.3s.1478

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and communication, 5*(1), 29-41. https://doi.org/10.17645/mac.v5i1.808

Marsili, M. (2019). The war on cyberterrorism. *Democracy and Security, 15*(2), 172-199. https://doi.org/10.1080/17419166.2018.1496826

Martin, N. y Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security, 30*(8), 803-814. https://doi.org/10.1016/j.cose.2011.07.003

Matus, C. (1987). *Política, planificación y gobierno* (Vol. 2). Caracas: Fundación Altadir. https://claudiabernazza.ar/wp-content/uploads/2020/10/matus1.pdf

Munkøe, M. y Mölder, H. (2022). La ciberseguridad en la era de hipercompetitividad: ¿puede la Union Europea afrontar los nuevos retos? *Revista CIDOB d Afers Internacionals, 131*, 69-94. https://doi.org/10.24241/rcai.2022.131.2.69

National Research Council & System Security Study Committee. (1990). *Computers at risk: safe computing in the information age*. National Academies Press. https://doi.org/10.17226/1581

Napetvaridze, V. y Chochia, A. (2019). Cybersecurity in the making – policy and Law: A case study of Georgia. *International and Comparative Law Review, 19*(2), 155-180. https://doi.org/10.2478/iclr-2019-0019

Newmeyer, K., Cubeiro, E. y Sánchez, M. (2015). Ciberespacio, Ciberseguridad y Ciberguerra. Marina de Guerra del Perú. *Escuela Superior de Guerra Naval. 20*, p. 500. Escuela Superior de Guerra Naval. https://hdl.handle.net/

Norris, D. F., Mateczun, L., Joshi, A. y Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of Homeland Security and Emergency Management, 15*(3). https://doi.org/10.1515/jhsem-2017-0048

Onumo, A., Cullen, A. y Ullah-Awan, I. (2017). *An empirical study of cultural dimensions and cybersecurity development*. 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud). https://doi.org/10.1109/ficloud.2017.41

Organización de las Naciones Unidas. (2023). Basic facts about the global cybercrime treaty. Naciones Unidas. https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty

Park, D.-W. (2016). Analysis and comparison of regulations for national cybersecurity. *International journal of security and its applications, 10*(10), 207-214. https://doi.org/10.14257/ijsia.2016.10.10.19

Pascual Esteve, J. M., y Goldás I Pérez, X. (2010). *El buen gobierno 2.0: la gobernanza democrática territorial* (1a ed.). Tirant Lo Blanch.

Perafán Del Campo, E. A., Polo Alvis, S., Sánchez Acevedo, M. E., y Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi, 16*(1), 1-46. https://www.redalyc.org/journal/5602/560268690006/560268690006.pdf

Plataforma digital única del Estado Peruano. (2023, 20 de setiembre) Centro Nacional de Seguridad Digital (CNSD). https://www.gob.pe/cnsd

Podemos Perú (octubre 23, 2020). Proyecto de ley 6544/2020-CR. Proyecto de ley que garantiza la ejecución de operaciones de ciberseguridad y seguridad digita a través de un centro nacional de ciberseguridad. https://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL06544-20201023.pdf

Preis, B. y Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review (Thousand Oaks, Calif.), 58*(2), 614-629. https://doi.org/10.1177/1078087420973760

Presidencia del Consejo de ministros del Perú. (2017). *Política Nacional de Ciberseguridad*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/\$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf

Real Academia Española [RAE]. (1 de julio de 2024). *Seguridad.* https://dle.rae.es/seguridad

Rona, T. (1976). *Weapon Systems and Information War*. Washington d.c. https://bit.ly/3vBI5VR

Santana-Soriano, E., y Báez Vizcaíno, K. (2022). Ciberespacio y Cibermundo: delimitaciones conceptuales desde el materialismo sistémico. *Ciencia y Sociedad, 47*(1), 45–57. https://doi.org/10.22206/cys.2022.v47i1.pp45-57

Slayton, R. (2021). Governing uncertainty or uncertain governance? Information security and the challenge of cutting ties. *Science, Technology & Human Values, 46*(1), 81–111. https://doi.org/10.1177/0162243919901159

Snider, K. L. G., Shandler, R., Zandani, S. y Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyab019

Szafransky, R. (1995). Una Teoría de la Guerra de Información Para el 2020. *Air & Space Power Journal – español. – invierno. Alabama: US Air Force*. http://www.airpower.maxwell.af.mil/apjinternational/apjs/szafra.html

Taipe, D. (2020). *La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018* [Tesis de maestría, Universidad Nacional de Piura] Repositorio institucional UNP. http://repositorio.unp.edu.pe/handle/20.500.12676/2361

Topor, L. y Tabachnik, A. (2021). Russian Cyber Information Warfare International Distribution and Domestic Control. *Journal of Advanced Military Studies, 12*(1), 112–127. https://doi.org/10.21140/mcuj.20211201005

Toro-García, A. F., Gutiérrez-Vargas, C. C., y Correa-Ortiz, L. C. (2020). Estrategia de gobierno digital para la construcción de Estados más transparentes y proactivos. *Trilogía Ciencia Tecnología Sociedad, 12*(22), 71-102. https://doi.org/10.22430/21457778.1235

Tovar, H. (2011). Guerra de información ¿el arma es el mensaje? *UCV. Caracas*.

Unión Internacional de Telecomunicaciones. (2016). Cybersecurity. UIT. https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. United Nations. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

van Steen, T., Norris, E., Atha, K. y Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa019

van Vuuren, J. J., Grobler, M., Leenen, L. y Phahlamohlaka, J. (2014). *Proposed model for a cybersecurity centre of innovation for South Africa*. En IFIP Advances in Information and Communication Technology (pp. 293-306). Springer Berlin Heidelberg.

Vargas Bravo, C. (2021). El gobierno digital y su implementación en el estado. *Ciencia Latina Revista Científica Multidisciplinar, 5*(6). https://doi.org/10.37811/cl_rcm.v5i6.1356

Veale, M. y Brown, I. (2020). Cybersecurity. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1533

Vila, G. (2019). Los ciberataques como amenazas a las infraestructuras y recursos críticos de un Estado. *Revista Estrategia, 3*(6), 22-40. https://www.gub.uy/ministerio-defensa-nacional/sites/ministerio-defensa-nacional/files/2020-11/Revista_Estrategia_06_0.pdf#page=24

Vílchez, J. (2022). *Ciberseguridad y robo de información: Una revisión sistemática de la literatura* [Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo] Repositorio de tesis USAT. http://hdl.handle.net/20.500.12423/4937

Villar, M. (2019). *Las implicancias de los ciberataques del S. XXI en América Latina* [Trabajo de Investigación, Universidad San Ignacio de Loyola] Repositorio institucional USIL. https://repositorio.usil.edu.pe/handle/usil/9574

Villavicencio, F. (2014). Delitos Informáticos. IUS ET VERIT, 49, 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and National Security*. Pag. 781-799. https://doi.org/10.1080/02684527.2012.708530

Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa013

Widakuswara, P. (2023, 2 de marzo). *EE. UU. lanza agresiva estrategia nacional de ciberseguridad*. La Voz de América. https://bit.ly/3RE9Clu

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

ANEXOS

Anexo 1. Lista de documentos encontrados

#	Referencias Bibliográficas	Año	Autor	Idioma	País	Tipo
1	Delitos informáticos: generalidades	2016	Acurio Del Pino, S.	Español	Mexico	Libro
2	Cybersecurity: The cold war online	2017	Aftergood S.	Ingles	Reino Unido	Nota
3	Russia's cyber and information warfare	2020	Akimenko, V., & Giles, K.	Ingles	USA	Artículo
4	Ciberseguridad Nacional	2014	Anderson, O.	Español	Perú	Informe técnico
5	Cybersecurity: Public Sector Threats and Responses	2011	Andreasson K.J.	Ingles	USA	Libro
6	Ciberseguridad Nacional en México y sus desafíos	2018	Arreola, A.	Español	Mexico	Artículo
7	Cyberwarfare: War activities in cyberspace	2023	Asbaş, C., & Erdem Tuzlukaya, Ş.	Ingles	Turquia	Cap. libro
8	Can Information Warfare Be Deterred?	2010	Blank, S.	Ingles	Reino Unido	Artículo
9	Ciberseguridad nacional argentina: cracking de servidores de la administración pública	2013	Borghello, C., & Temperini, M. G. I.	Español	Argentina	Conferencia

10	Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity	2019	Bresniker, K. et al.	Ingles	USA	Artículo
11	Russia's information war against Ukraine: features and mechanisms of control	2018	Buchyn, M., & Kurus, Y.	Ingles	Ucrania	Revisión
12	Cybersecurity in the Chinese context: Changing concepts, vital interests, and prospects for cooperation	2015	Cai, C.	Ingles	Singapur	Artículo
13	Gestión de seguridad de la información: revisión bibliográfica	2016	Cárdenas-Solano, L.-J. et al.	Español	Colombia	Artículo
14	The Future of Cybersecurity Policy INTRODUCTION	2020	Charlet, K., & King, H.	Ingles	USA	Artículo
15	Cyberattacks and threats during COVID-19: A systematic literature review	2021	Chigada, J., & Madzinga, R.	Ingles	Sudafrica	Revisión
16	Política Nacional de Ciberseguridad	2017	Ciberseguridad, C. I. S.	Español	Chile	Política
17	Why should I? Cybersecurity, the security of the state and the insecurity of the citizen	2018	Coles-Kemp, L. et al.	Ingles	Portugal	Artículo

18	How to protect public administration from cybersecurity threats: The COMPACT project	2018	Coppolino, L. et al.	Ingles	Polonia	Conferencia
19	Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia	2015	Cortés, R.	Español	Colombia	Artículo
20	Machine learning in cybersecurity: a comprehensive survey	2022	Dasgupta D.,	Ingles	USA	Artículo
21	El ciberespacio en tiempos de guerra: la IT Army ucraniana	2023	De Álvaro, M.	Español	España	Artículo
22	Building Cybersecurity Awareness: The need for evidence-based framing strategies	2017	De Bruijn, H., & Janssen, M.	Ingles	Reino Unido	Artículo
23	Design science approach to developing and evaluating a national cybersecurity framework for Jamaica	2014	Dennis A. et al.	Ingles	China	Artículo
24	The ethics of cyberwarfare	2010	Dipert, R. R.	Ingles	USA	Artículo
25	Privacy Governance in Cyberspace	2015	Doneda, D., & Almeida, V. A. F.	Ingles	USA	Artículo

26	Enhancing the effectiveness of cybercrime prevention through policy monitoring	2019	Dupont, B	Ingles	Reino Unido	Artículo
27	Europe's fragmented approach towards cyber security	2013	E Silva K.	Ingles	Alemania	Artículo
28	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	2013	European commission	Ingles	Bélgica	Artículo
29	La seguridad informática y la seguridad de la información	2018	Figueroa-Suárez, J. et al.	Español	Ecuador	Artículo
30	Ciberseguridad en España: una propuesta para su gestión	2010	Fojón, J. & Sanz A.	Español	España	Artículo
31	La ciberseguridad pública como garantía del ejercicio de derechos	2016	Galán, C. M. & Galán, C.	Español	Perú	Artículo
32	Handbook of Russian information warfare	2016	Giles, K	Ingles	Italia	Libro
33	Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes	2017	Gross M. et al.	Ingles	Reino Unido	Artículo
34	De Budapest al Perú: análisis sobre el proceso de implementación del convenio de ciberdelincuencia. Impacto en el corto, mediano y largo plazo.	2018	Guerrero, C.	Español	Perú	Artículo

35	Understanding Cybercrime: Phenomena, Challenges and Legal Responses	2012	International Telecommunications Union	Ingles	Suiza	Libro
36	Information Warfare: Its Contents and Forms	2013	Ivanov, S.	Ruso	Rusia	Artículo
37	Análisis de los ciberataques realizados en América Latina	2018	Izaguirre, J. & León, F.	Español	Ecuador	Artículo
38	La responsabilidad de la Administración del Estado por incidentes de ciberseguridad	2021	Jara Fuentealba, N., & Jorquera Cruz, A.	Español	Chile	Artículo
39	National Security or Privacy: A Second Thought on the DNC Hack	2016	Jun S.-I.	Ingles	USA	Conferencia
40	The local government's position in the polish cybersecurity system	2021	Karpiuk, M.	Ingles	Eslovenia	Artículo
41	The Impact of Threats on the Cybersecurity System of Public Administration in the Context of the Development of Financial Technologies	2021	Kryshtanovych, M. et al.	Ingles	Alemania	Conferencia
42	Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque	2015	Leiva, E. A.	Español	Argentina	Artículo

	Top-Down desde una Visión Global a una Visión Local					
43	On the organization of the U.S. government for responding to adversarial information warfare and influence operations	2020	Lin, H.	Ingles	USA	Capítulo de libro
44	Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership	2015	Manley, M., & US Air Force, American Military University.	Ingles	USA	Artículo
45	Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy	2017	Maréchal N.	Ingles	Portugal	Artículo
46	The war on cyberterrorism	2019	Marsili M.	Ingles	Reino Unido	Artículo
47	Cybercrime: Understanding and addressing the concerns of stakeholders	2011	Martin, N., & Rice, J.	Ingles	Reino Unido	Artículo
48	Cybersecurity in the era of hypercompetitiveness: can the EU meet the new challenges?	2022	Munkøe, M., & Mölder, H.	Ingles	Belgica	Artículo

49	Cybersecurity in the Making-Policy and Law: A Case Study of Georgia	2019	Napetvaridze, V., & Chochia, A.	Ingles	Polonia	Artículo
50	Ciberespacio, Ciberseguridad y Ciberguerra.	2015	Newmeyer, K. et al.	Español	Perú	Conferencia
51	Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security	2018	Norris, D. F. et al.	Ingles	Alemania	Artículo
52	An empirical study of cultural dimensions and cybersecurity development	2017	Onumo, A., Cullen, A., & Ullah-Awan, I.	Ingles	Republica Checa	Conferencia
53	Analysis and comparison of regulations for national cybersecurity	2016	Park D.-W.	Ingles	Corea del Sur	Artículo
54	Municipal Cybersecurity: More Work Needs to be Done	2022	Preis, B., & Susskind, L.	Ingles	USA	Artículo
55	Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties	2021	Slayton, R.	Ingles	USA	Artículo
56	Cyberattacks, cyber threats, and attitudes toward cybersecurity policies	2021	Snider, K. L. G. et al.	Ingles	Reino Unido	Artículo

57	Russian Cyber Information Warfare International Distribution and Domestic Control	2021	Topor, L. & Tabachnik, A.	Ingles	USA	Artículo
58	What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?	2020	Van Steen, T. et al.	Ingles	Reino Unido	Artículo
59	Proposed Model for a Cybersecurity Centre of Innovation for South Africa	2014	van Vuuren, J. J. et al.	Ingles	USA	Conferencia
60	Cybersecurity	2020	Veale, M. & Brown, I.	Ingles	Alemania	Artículo
61	Los ciberataques como amenazas a las infraestructuras y recursos críticos de un Estado	2019	Vila, G.	Español	Uruguay	Artículo
62	Delitos informáticos	2014	Villavicencio, F.	Español	Perú	Artículo
63	Cyber conflict or democracy hacked? How cyber operations enhance information warfare	2020	Whyte, C.	Ingles	Reino Unido	Artículo